Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ
ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: АКТУАЛЬНІ ПИТАННЯ ТА ІННОВАЦІЇ

Матеріали Міжнародної науково-практичної конференції

(м. Дніпро, 4 листопада 2021 р.)

Дніпро
2021

УДК 33+004+4+35
Е40

Схвалено науково-методичною радою
Дніпропетровського державного університету
внутрішніх справ (протокол № 3 від 18.11.2021)

Е 40 **Економічна та інформаційна безпека: актуальні питання та інновації** : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 4 листоп. 2021 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2021. 400 с.

ISBN 978-617-8032-40-1

Збірник містить матеріали однойменної міжнародної науково-практичної конференції. У заході взяли участь науковці, викладачі та здобувачі вищих навчальних закладів та наукових установ України і зарубіжжя, а також фахівці-практики правоохоронних органів. Тематика публікацій охоплює актуальні питання економічної та інформаційної безпеки.

Матеріали конференції можуть бути використані в науково-дослідній роботі та навчальному процесі спеціалізованих ВНЗ, а також у законотворчості та правоохоронній діяльності.

ISBN 978-617-8032-40-1

Вітальне слово
ректора Дніпропетровського державного університету внутрішніх справ
ФОМЕНКА АНДРІЯ ЄВГЕНОВИЧА,
доктора юридичних наук, доцента,
заслуженого юриста України,
полковник поліції

Шановні учасники конференції! Радий Вас вітати від імені науково-педагогічного колективу Дніпропетровського державного університету внутрішніх справ та від себе особисто на Міжнародній науково-практичній конференції «Економічна та інформаційна безпека: актуальні питання та інновації». Статус заходу є міжнародним і це підтверджує актуальність питань, що нами розглядаються.

Сучасний вік – вік інформації не тільки відкриває можливості, а й ставить нові завдання, та потребує вирішення нових проблем. Тому необхідно адекватно реагувати на подібні виклики. Можна сміливо стверджувати, що економічна та інформаційна небезпеки становлять один з найбільш небезпечних видів загроз, і свідченням цього є постійне обговорення проблем економічної та інформаційної безпеки як науковою спільнотою, практиками, так і на офіційних зустрічах на найвищому політичному рівні.

Наш університет має певні досягнення в цьому напрямі. Останнім часом створено відповідну кафедру та факультет підготовки курсантів для підрозділів стратегічних розслідувань Національної поліції за спеціалізацією «фінансово-економічна безпека». Споруджено спеціалізований полігон для відпрацювання фабул з документування та розкриття злочинів в економічній сфері. Відкриті нові спеціальності для підготовки студентів у сфері менеджменту за спеціалізацією «економіко-фінансова безпека» й економіки за спеціалізацією «захист економіки».

Зважаючи на сучасні реалії, тема нашого обговорення є надзвичайно актуальною, глибокою і водночас складною.

Складність і глобальний характер завдань вимагають розробки ґрунтовного наукового супроводження і консолідації зусиль представників наукової спільноти.

Тож з огляду на зазначене мета сьогоднішнього наукового заходу – обговорити такі питання:

- використання інформаційних технологій в діяльності поліції;
- безпека в інформаційній та економічній сфері;

– сучасний стан, проблеми та перспективи розвитку фінансової та економічної безпеки підприємств, регіонів, суспільства.

Саме для отримання відповідей на ці проблемні питання та удосконалення практичних і теоретичних навичок проводиться цей захід.

Завдяки присутності на заході фахівців різних сфер науки і практики, а саме: економіки, менеджменту, інформаційних технологій, економічної та інформаційної безпеки, юриспруденції, бізнесу та правоохоронних органів ми маємо виняткову змогу перейняти позитивний досвід у зазначеній сфері, а також поділитися власним досвідом.

Переконаний, що наукова дискусія під час обговорення визначених питань матиме глибокий та плідний характер і сприятиме розвитку вітчизняної науки, подальшому підвищенню рівня протидії злочинності в економічній та інформаційній сферах.

Від імені оргкомітету конференції щиро дякую вам за те, що знайшли час взяти участь у конференції з цієї, безперечно актуальної на сьогодні, проблематики.

Вітальне слово
т.в.о. начальника Департаменту
інформаційно-аналітичної підтримки
Національної поліції України,
кандидата юридичних наук
ТИМЧЕНКА ЛЕОНІДА ЛЕОНІДОВИЧА

Дозвольте мені від імені колективу Департаменту інформаційно-аналітичної підтримки поліції України привітати вас з проведенням Міжнародної науково-практичної конференції «Економічна та інформаційна безпека: питання та інновації».

Варто зауважити, що розвиток публічних послуг дозволяє провідним країнам світу в цій сфері не лише підвищувати швидкість та якість обслуговування, але й суттєво економити бюджетні кошти та час держави на обслуговування громадян.

У 2020 році, порівняно з попереднім роком, міжнародна пропускна здатність Інтернету зросла на 35 %, приблизно з 450 до 600 Тбіт/с. З 2014 року зростання відбувалося майже тричі.

Кількість користувачів Інтернету у світі досягла майже 5 млрд осіб, що становить приблизно 63 % від загальної кількості світового населення. За 2020 рік в Україні кількість користувачів зросла з 19 до 26 млн, або з 45 % до 58 % населення. До 2023 року в уряд України має намір приєднати 95 % соціальної інфраструктури до Інтернету.

Говорячи про зростання даних, можна відмітити, що тільки ютуб

завантажується до 300 годин відео. Однак оцінки дозволяють припустити, що тільки 0,5 % усіх даних коли-небудь аналізуються та використовуються.

Стрімке поширення цифрових технологій робить «цифрові» навички людей одними з основних. Цифровізація та робота з даними зараз головні тренди на загальному ринку праці. Тобто вміння працювати з цифровими технологіями поступово стає необхідним для більшості спеціальностей. Для всебічної цифровізації ДІАП розбудовує середовище інформаційних технологій для користувачів баз даних, цифрових сервісів, телекомунікаційних послуг та радіозв'язку.

Сподіваюсь, що під час обговорень та наукових дискусій учасниками конференції буде розроблено нові методи та підходи створення якісного цифрового сервісу. Розроблені рекомендації сприятимуть розробленню законодавства та практики його застосування.

Вітальне слово т.в.о. начальника
Департаменту кримінального аналізу
Національної поліції України
ХУДЕНКА ДМИТРА МИКОЛАЙОВИЧА

Шановний голово організаційного комітету! Шановні члени організаційного комітету та учасники Міжнародної науково-практичної конференції! Щиро вітаємо всіх від імені колективу Департаменту кримінального аналізу Національної поліції України з нагоди відкриття цього заходу! Проведення конференції на міжнародному рівні та заявлені учасниками теми наукових розвідок наголошують на особливій актуальності досліджень питань економічної та інформаційної безпеки.

Вкрай важливою передумовою інновацій у згаданих сферах безпеки залишається наука. Не менш важливою для науки є практика. Ці два феномени взаємозалежні у своєму розвитку і потребують обміну думок між українськими науковими школами, фахівцями й представниками міжнародних організацій та наукових еліт іноземних країн.

Програма нашої конференції містить різноаспектний масив питань, зокрема пов'язаних із кримінальними аналізом. Для Департаменту кримінального аналізу, який також розробляє, впроваджує та застосовує нові методи та напрями здійснення кримінального аналізу, спрямовані на підвищення ефективності протидії злочинності, цей формат конференції є надзвичайно цікавим.

У сучасних умовах світового розвитку, коли, наприклад, економіка зазнала впливу пандемії, назріває чергова науково-технічна революція, обсяг

інформації зростає шаленими темпами, а фізичний світ шукає альтернатив у віртуальному, представники злочинного світу користуються не лише класичними способами вчинення злочинів у зазначених сферах, але й вдаються до нових або досі не бачених способів їх підготовки та вчинення. Саме тому ми змушені постійно підвищувати протидію злочинності.

55 років досягнень Дніпропетровського державного університету внутрішніх справ та якісний склад учасників Міжнародної науково-практичної конференції дають нам міцний фундамент для полеміки та успішного розвитку системного наукового та міждисциплінарного підходу до вивчення проблем економічної та інформаційної безпеки.

Ми сподіваємось, що знання, досвід та пропозиції учасників Міжнародної науково-практичної конференції стануть в нагоді на шляху забезпечення економічної та інформаційної безпеки суспільства.

Бажаємо всім плідної співпраці, вагомих результатів на практиці, творчих успіхів та наукових відкриттів!

Приветственное слово ректора Бухарестского университета «ARTIFEX», профессора, доктора философии АЛЕКСАНДРУ-ЛУЧИАН МАНОЛЕ

Уважаемые коллеги! Для меня большая честь участвовать в качестве представителя Бухарестского университета «ARTIFEX» в престижной конференции по экономической и информационной безопасности, организованной уважаемым Днепропетровским государственным университетом внутренних дел. Тема конференции чрезвычайно важна и актуальна, когда экономическая информация является одним из ключей к управлению политическими отношениями. Развитие (и преимущества) компьютерной обработки информации вместе с расширением сетей сопряжено с некоторыми издержками, одна из которых связана с безопасностью информации, которую необходимо защищать любой ценой. Мы можем согласиться с тем, что после компрометации конфиденциальность информации не может быть восстановлена.

От имени академического сообщества Бухарестского университета «ARTIFEX» выражаю самые искренние пожелания, поздравления и уважение организаторам и участникам конференции. Мы считаем, что усилия исследователей должны быть капитализированы в ценной и полезной базе знаний и собрании передового опыта, что будет способствовать усилению безопасности физических и электронных систем обработки информации.

З М І С Т

ТЕЗИ ВИСТУПІВ

КУРСАНТИ ТА СТУДЕНТИ

ТЕЗИ ВИСТУПІВ

Glavan B., Doctor of Law, Associate Professor, Scientific Secretary of the Senate of the Academy "Stefan cel Mare" of the Ministry of Internal Affairs of the Republic of Moldova

ABOUT THE COHERENCE OF THE LEGAL PROVISIONS IN THE FIELD OF SPECIAL INVESTIGATIONS, CRIMINAL LAW AND CRIMINAL PROCEDURAL LAWS RELATING TO THE PROTECTION OF THE INVESTIGATOR UNDER COVERAGE

Today, fighting crime, compared to a few decades ago, has become a much more difficult and risky job. On the one hand, new technologies (mobile communication networks and the Internet) have offered the criminal world new opportunities for crime preparation, commission and camouflage, and the expansion of links between national and international criminal groups. On the other hand, the aspirations of democratization and the rule of law have imposed on our country new requirements for the quality of the normative act meant to fight crime, imposing higher standards in the application of criminal investigation procedures in line with respect for human rights.

Under these conditions, law enforcement agencies in general and operational services in particular face increasingly sophisticated and complex techniques and methods of concealing criminal traces, which require the infiltration of secret agents into various criminal structures to obtain the necessary information. It is no secret that in order for undercover agents to act effectively (to gather information about the plans and intentions of criminal structures, about the ways and means of carrying them out, to influence members of the criminal group or organization to abandon their intentions to commit crimes) must enjoy the trust of the leaders and members of these groups. This in turn involves the adaptation of the agent to the infiltrated environment, which means his real or formal participation in criminal activities. In turn, this is possible only if the infiltrators are protected from criminal liability in connection with the inevitable co-participation in the activity of criminal structures.

This is the explanation and the importance of the legal provisions that refer to the controlled crime stipulated in the Law of the Republic of Moldova no. 50/2012 [1] regarding the fight against organized crime.

According to art.14 of the indicated law "*Controlled crime represents the*

commission by the controlled person in the criminal group or organization of a deed that shows only objective signs of a minor or less serious crime, in a controlled manner and directed by the authority provided in art. 6 para. (1), in order to stop or discover serious, particularly serious and exceptionally serious crimes".

The analysis of these provisions denotes the lack of coherence between the legal norms in the field of special investigations, criminal law and criminal procedural law, which undermines the value of these legal provisions as a guarantor for the undercover investigation.

First of all, the text above talks about the crime that meets only the objective signs of a crime, not the subjective ones. However, the theory of criminal law tells us that if the deed does not meet at least one of the signs of the crime, either objectively or subjectively, then this deed cannot be considered a crime [2, p.104]. Therefore, the legal nature of the deed discussed in the above text is not clear.

Secondly, it is known that any crime is at the same time an illegal act, respectively it is incorrect to talk about legal crimes, or through a controlled crime the lawer try to accredit the idea of legal crimes.

Thirdly, the mechanism for implementing the provisions of art. 14 of Law no. 50/2012 is currently missing. The Code of Criminal Procedure [3] does not provide for such a circumstance as the controlled crime, under which the criminal investigation should not be initiated or should cease (art. 275 CPC).

Fourthly, the Criminal Code of the Republic of Moldova [4] is the only law that establishes which deeds constitute crimes (art. 1 of the Criminal Code) and which are the circumstances in the presence of which the criminal character of the deed is excluded (art. 35 of the Criminal Code). Therefore, it becomes obvious the collision between the criminal law that criminalizes certain facts and Law no. 50/2012 which excludes the criminal nature of those acts committed by the undercover investigator. It would be correct for the place of the legal provisions that would ensure guarantees for the conduct of undercover investigations to be found in the content of the Criminal Code and not of another law.

The problem of inconsistency between the provisions of the criminal law and those concerning special investigations is not limited to the actions of the undercover investigator infiltrated in a criminal group. In addition to the undercover investigation, there are other special investigative measures that involve carrying out certain actions that from the point of view of criminal law are considered crimes. Thus, the criminal law criminalizes the actions of transmission or receipt of money, services or other material or immaterial values claimed, accepted, extorted or offered (art. 324; 325; 333; 334 CP), and the criminal procedural law decriminalizes them if they are performed. within the special measure of investigations – Control of the transmission or receipt of money, services or other material or intangible values claimed, accepted, extorted or offered (art.135 CPP).

At the same time, we notice that only the actions of sending and receiving

money are decriminalized while the other acts of corruption (acceptance, promise, offering of money and other goods) remain incriminated. The problem extends to special investigative measures related to the limited or even prohibited circuit of services, objects and goods (narcotics, psychotropic substances, explosives, radioactive, etc.), especially in the conditions of carrying out these measures outside the criminal process, under the Law no.59 / 2012 [5].

In conclusion, taking into account the experience of other states in solving a similar problem (Ukraine (art. 43 CP) [6], the Republic of Kazakhstan (art. 35 CP) [7], the Republic of Belarus (art. 38 CP) [8]) , as well as the opinions of some experts in the field [9, p.41-46], we propose the inclusion of a new article in the Criminal Code of the Republic of Moldova with the following content:

"Article 40^2 Carrying out special investigative measures:

1) Actions taken within the limits of special investigative measures shall not constitute an offense.

(2) The provisions of paragraph 1 of this Article do not refer to prejudicial actions directed against the life and health of the person, the occurrence of an ecological calamity as well as other serious consequences".

References

1. Legea Republicii Moldova nr.50 din 22.03.2012 privind prevenirea şi combaterea criminalităţii organizate**.** [on-line]. Available: https://www.legis.md/cautare/getResults?doc_id=22943&lang=ro (Visited: 15.10.2021).
2. Botnaru S. şi alţii. Drept penal. Partea generală. Chişinău: Cartier, 2005. 624 p.
3. Codul de procedură penală al Republicii Moldova din 14.03.2003. [on-line]. Available: https://www.legis.md/cautare/getResults?doc_id=113967&lang=ro (Visited: 15.10.2021).
4. Codul penal al Republicii Moldova din Nr. 985 din 18-04-2002 [on-line]. Available: https://www.legis.md/cautare/getResults?doc_id=109495&lang=ro (Visited: 12.02.2021).
5. Legea Republicii Moldova nr.59 din 29.03.2012 cu privire la activitatea specială de investigaţii. [on-line]. Available: https://www.legis.md/cautare/getResults?doc_id=110235&lang=ro (Visited: 15.10.2021).
6. Уголовный кодекс Украины от 05.04.2001. [on-line]. Available: http://continent-online.com/Document/?doc_id=30418109#pos=307;-58 (Visited: 15.10.2021).
7. Уголовный кодекс РК от 03.07.2014. [on-line]. Available: https://online.zakon.kz/Document/?doc_id=31575252#pos=4;-89 (Visited: 15.10.2021).
8. Уголовный кодекс Республики Беларусь от 09.07.1999. [on-line]. Available: https://kodeksy-by.com/ugolovnyj_kodeks_rb.htm (Visited: 15.10.2021).
9. Рахимзода Р. Х. Некоторые проблемы законодательного регулирования оперативно-розыскной деятельности. *Современное состояние науки и законодательства об оперативно-розыскной деятельности* : материалы Международной научно-практ. конф. Душанбе : «Вектор-Принт», 2016. С. 41–46.

Klinytskyi I., Mgr. et Mgr., PhD candidate, Department of Law and Administration, the University of Silesia (Katowice, Republic of POLAND).

CHANGING THE PATTERNS OF RESEARCH ON LANGUAGE RIGHTS PROBLEMS: FIRST DRAFT ON THE NEW METHOD OF DIGITAL RESEARCH.

In this paper, we determine and shape our methodological approach by answering the main question posed by researchers from the social science and legal studies realm: "How to collect accurate and objective empirical data based on social processes?" in a sufficiently equipped way. We have designed our solution for a critically important field of human rights exploration – linguistic (language) rights. In order to fill the gap of empirical data, we demonstrate our scrapper of Sitemap files, which counts the languages of available web-pages for users. This solution should be used for (a) imaging the current intention of organizations in the field of digital accessibility, (b) as a part of more sufficiently constituted instruments for indicating – in accordance with the European directive on accessibility (European Parliament, 2016) – WCAG 2.0 problems, (c) gathering of empirical data for further legal research.

As an entrance to the issue, we start with a short description of current problems in the methodological framework for language rights; especially, from the perspective of modern – not even a "black letter" – legal research. Next, we describe the developed instrument and the reason for its creation. In addition, we summarize our paper making a few suggestions and forming further questions for future exploration.

The discussion on the scientific methodology vs. law is still an ongoing process. However, the article "*The Scientific Method and the Law*" by Bernard L. Diamond will celebrate its 55 years (Bernard L. Diamond, 1967), there is still a great scope of activity ahead in the methodology area. Of course, the sentence "law as a part of science" seems like a great joke[1] in the keen eye of a so-called "Western observer". As a matter of fact, in post-soviet states we have a clear understanding of this concept – thanks to Soviet philosopher Vladik Nersesyants (рус. *Вла́дик Сумба́тович Нерсеся́нц*) and his opening up a new world Libertarian legal theory of law and state (Нерсесянц В. С., 2002) – by the way, following common empirical attention in research we shall highlight an overall need to effectuate the empirical framework of social-based research.

First of all, in order to define the language rights, we take a similar position

[1] See the discussion on ResearchGate <https://www.researchgate.net/post/Is_law_a_science> (date of access: 22.10.2021).

as it was mentioned in (Xabier Arzoz et al., 2009) that linguistic (language) rights have a crossfield definition. Moreover, the same idea exists among the European Court of Human Rights cases, e.g. *Nusret Kaya and Others v. Turkey* and *Mesut Yurtsever and Others v. Turkey*, where the language was perceived by the court as a personal good for the applicant/-s, which is limited by articles of European convention. Indeed, it is not bordered by the occasional area of social life (for example, just by healthcare or rights of national minorities). For our purpose we use the limited essence of this type of rights – accessibility of information on web-page in non-official language.

In accordance with the literature, the most notable examples of discrimination can be found in the public sphere or education (i.e. the limitations in the choice of language for instructions at the university) (Róisín McKelvey, 2021; Stephanie L. Haft et al., 2021). It was also noted that migrants have a vital need in integration into a labour market, and the level of language integration takes an important place here (Calò, Francesca, et al., 2021).

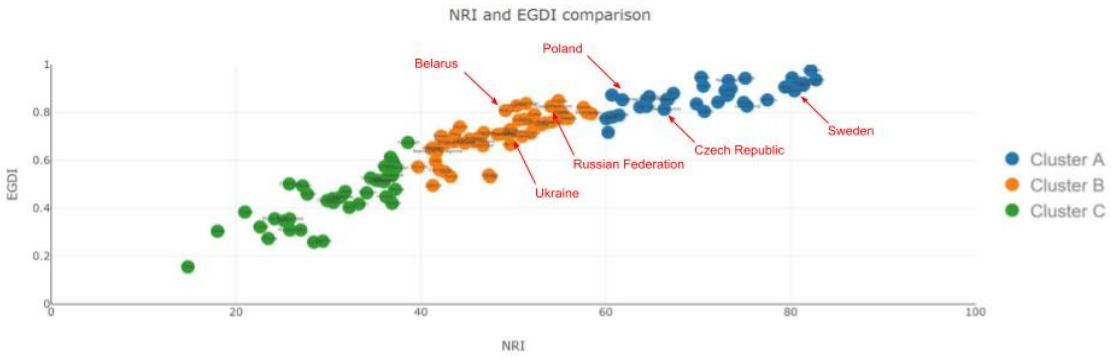


Figure 1. The NRI and EGDI comparison of states (K-Means (k=3) algorithm for clustering method). Source: Illia Klinytskyi[2]

Of course, we should not forget a non-newcomers descrimination by language. As it was pointed out by (Dimitry Kochenov et al., 2013; Dimitry Kochenov 2021), the passport is not a guarantee of being covered by antidiscriminational law and humanism derived practices. We cannot omit the dramatically radical shift in Ukrainian language policy also – which is definitely shameful for a multicultural state accepting the main Sakharov's dream – a state drived by human rights as it is.

Nevertheless, to summarize used methodological pathways, there are no global indicators for social response on language rights (even in the digital measuring). The current digital accessibility framework does not cover the multilingual requirements for web-pages, although it is under ongoing implementation in the multilingual European Union (see: WCAG 2.0). Certainly,

[2] Colleague Klinytskyi clustered gathered data from official sources using K-Means (k=3) algorithm for clustering in order to border states by groups in the context of e-government development for another research on WCAG 2.0 compliance.

the category of people with special needs is not directly connected with people with non-official language preferences.

The main two indices, which indicate current developments in the digital context, can broadly describe the differences between selected jurisdictions (see: Figure 1), but it is not a mapping of WCAG 2.0 implementation or, thinking more deeply, languages support on websites. We pose a hypothesis that businesses and other types of non-governmental organisations are policing more open solutions for their customers in the context of language support. That is why the response of the market on social changes and preferences should be an interesting area of scientific research.

The solution. Taking a step ahead, we come up with a first draft of a solution for further measurements. We have used the PHP programming language for script writing and its CURL library for making cross-server connections using HTTP protocol. The first version of the script is located below.

```
<?php
/*
The script for counting of human related languages based on sitemaps (.xml)
As an input its use the url of sitemap (THE_SITEMAP_URL)
*/
// we use ISO 639-1 for language codes in array below
$language_codes = [
‘ru’,
        ‘en’,
        ‘ua’
];
curl_setopt($ch, CURLOPT_URL, '<THE_SITEMAP_URL>');
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
$data = curl_exec ($ch);
curl_close ($ch);
$xml = new SimpleXMLElement($data);
$result_array = [];
foreach ($xml->url) {
$url = $xml->url->loc;
$urlParts = explode ('/', $url);
$language = $urlParts[1];
if (in_array($language, $language_codes)) {
        if(empty($result_array[$language]){

        $result_array[$language] = 1;
        } else {

        $result_array[$language] += 1;
        }
}
}
// output
print_r($result_array);

?>
```

Our solution is based on Google's main requirement for a web-site: it should have a sitemap in .xml format (as one possible among others) for better indexing[3]. It should be noted that it is not a useful solution for .txt files or for other types of language codes.

As it was mentioned above, we described a script which can be implemented in any other language. To be honest, it is not a final "in-house" solution. Indeed, it implements the main idea – accounting of language versions for web-site pages. Moreover, we do not use natural language processing (NLP) techniques. This attention should be more useful in order to indicate languages directly on selected web-page.

References

1. Нерсесянц В. С. Философия права: либертарно-юридическая концепция. *Вопросы философии.* 2002. № 3. С. 3–15.
2. Kochenov, Dimitry, Vadim Poleshchuk, and Aleksejs Dimitrovs. "Do Professional Linguistic Requirements Discriminate?–A Legal Analysis: Estonia and Latvia in the Spotlight." *A Legal Analysis: Estonia and Latvia in the Spotlight (August 2, 2012)* (2013): 137-187.
3. Kochenov, D. V. (2021). Policing the Genuine Purity of Blood: The EU Commission's Assault on Citizenship and Residence by Investment and the Future of Citizenship in the European Union. EUROPEAN AFFAIRS STUDIES IN, 33.
4. Stephanie L. Haft, Qing Zhoum, "An Outbreak of Xenophobia: Perceived Discrimination and Anxiety in Chinese American College Students before and during the COVID-19 Pandemic – Haft – International Journal of Psychology – Wiley Online Library." Accessed April 30, 2021. https://onlinelibrary.wiley.com/doi/full/10.1002/ijop.12740.
5. McKelvey, Róisín. "Language provision in the Scottish public sector: Recommendations to promote inclusive practice." *Social Inclusion* 9.1 (2021): 45-55.
6. Calò, Francesca, et al. "Regulating Fortress Britain: Migrants, Refugees and Asylum Applicants in the British Labour Market." *Migrants, Refugees and Asylum Seekers' Integration in European Labour Markets: A Comparative Approach on Legal Barriers and Enablers* (2021): 235.
7. Arzoz, Xabier. "Language rights as legal norms." *European Public Law* 15.4 (2009).

[3] See: <https://developers.google.com/search/docs/advanced/sitemaps/build-sitemap> (date: 22.10.2021).

Marinov A.T., Professor of Economics, Ph.D.
Slavyanska V.K., Professor of Administration and Management, D.Sc. (Department of Psychology and Police Management, Police Faculty, Academy of the Ministry of Interior, Bulgaria)

INDICATORS FOR MEASURING ECONOMIC SECURITY AND INNOVATIONS

Economic security of a country is a state of its economy in which there are no threats and there are opportunities to neutralize them when they occur so that the state of dynamic stability is maintained. A highly developed economy is a guarantee of a high level of national security – security cannot be expected in a weak and inefficient economy [1, p. 91].

At the current stage of development of the economy and society, increasing economic potential is impossible without innovations and technologies / inventions. Investments in research and development (R&D) are essential for the transition to a knowledge-based economy, as well as for increasing labor productivity and stimulating economic growth. For this reason, innovations are seen as a prerequisite and criterion for economic security. In turn, this provokes interest in the indicators for their measurement.

1. Indicators for measuring economic security

Historically, economic security has been viewed from the standpoint of three theoretical approaches [2, pp. 45 – 59]: 1) mercantilists – macro level, according to which only the economic security of the state matters; 2) liberals – trans and micro level, according to which the market is the main guarantor of economic security; 3) Marxists – macro- and micro-level. It is noteworthy that none of these approaches combines macro- and meso-security (state and security of companies, corporations, associations).

Currently, economic security can be considered at three levels:

1) international (global and regional);

2) national / state (territorial and by branches within the country);

3) private (of business entities, public organizations and the individual).

In order to better understand the structure of the economic security system, it is necessary to identify the factors / indicators that affect all participants at different levels (macro-, meso- and micro). The reactions of these actors can affect the economic stability of the whole system to varying degrees, respectively causing economic instability and subsequently economic uncertainty.

Table 1. Groups of factors / indicators for economic security

Macrofactors ***Participants: Country, interstate relationships, world***	**Mesofactors** ***Participants: Enterprises, companies, business associations***	**Microfactors** ***Participants: Individuals, families, social groups, society***
• stability of national markets • free trade • competition • sustainable development • gross domestic product growth • productivity • low inflation rates • low unemployment rates • stable exchange rates • balance of payment • government debt • stable supply with production factors • avoiding and responding to speculative attacks • solving problems related to drugs, trafficking, criminal groups, gray economy, etc.	• stability of the macroeconomic environment • innovations and inventions • marketing • solvency and financial discipline • flexibility • stable supply with production factors • technological distribution • flexibility of the administration • stable exchange rates • targeted production • ethical dilemmas • knowledge • minimization of the black market	• stability of the macroeconomic environment • stability of resources – food, water, shelter • housing • stability of employment • stable and "fair" remuneration • trust in institutions • minimizing poverty • limiting social exclusion • education • reduction of fears and diseases • free movement of people • avoiding the "vicious circle" – standard of living and employment

Economic security is an endless and dynamic process, determined in the first place by the macroeconomic environment (macro level), which is connected and affects the meso level (companies and enterprises), and both determine the micro level (individual needs). The stabilization of the macroeconomic environment creates a sense of economic security through "solid macroeconomic indicators" (inflation, employment, etc.). In turn, the micro level affects the macroeconomic environment and thus results in an endless cycle.

2. Indicators for measuring innovations

As mentioned, innovations and inventions are one of the factors / indicators for measuring economic security at the meso level. On the other hand, they are at the heart of gross domestic product growth and sustainable development, which are part of macro level factors / indicators.

The high quality and rate of economic growth presupposes the predominance of the innovation factor in its structure. It is embodied in new types of goods, services, technologies, forms of organization, management methods, change in the quality of the workforce.

Innovations create new potential of the company and opportunities to expand or intensify production, increase sales and increase efficiency and profit. The pace of innovation means constantly updating competitive advantages. Innovation helps to achieve economic growth by increasing labor and capital

productivity and creating jobs. For this reason, governments are trying to create an appropriate macroeconomic and fiscal climate to encourage entrepreneurial initiatives and remove barriers to economic growth.

The European Innovation Assessment Methodology from 2005 includes, for the first time, a sectoral innovation scoreboard. The results of the analyzes show a positive correlation between innovation and the economic characteristics of the sectors, i.e. the better innovation condition of certain sectors has a positive impact on their economic condition. The methodology includes for the first time the construction of a generalized innovation index for 25 sectors in 15 countries. For this purpose, 12 indicators are used, 11 of which are constructed on the basis of data from the Third Monitoring of Innovation in the EU. These indicators are [3, p. 25]:

- share of employees with higher education;
- share of enterprises in which staff training is directly focused on the development and / or implementation of innovations;
- share of enterprises that receive public subsidies to innovate;
- share of enterprises that innovate independently;
- share of small and medium-sized enterprises that cooperate with others to innovate;
- innovation costs as a share of the total turnover of the enterprise;
- share of total sales of new products for the market;
- share of total sales for the sector of new products for the enterprise, but not for the market;
- share of enterprises that patent;
- share of companies that use trademarks;
- share of enterprises that use registered patents.

* * *

Modern economies of developed countries are characterized by a transition to a new quality of economic growth, the intensive nature of which is accompanied by increased production efficiency based on various innovations. Innovation is at the heart of scientific and technological progress. They determine the competitive advantages of both companies and the state as a whole, increasing the level of economic security.

References

1. Marinov, A., An exemplary model of economic security strategy of Bulgaria, Management and Sustainable Development 1/2014 (44).

2. Kopač, Er., The economic dimension of national security and relevant indicators. Varstvoslovje 8 (1), 2006.

3. Bulgarian Industrial Association, Analysis of the possibilities and tendencies for technological development of the Bulgarian enterprises, Sofia, 2010.

Popescu G.-D. – Police Commissione, Police instructor, Chair of Criminal Investigations „Vasile Lascăr" Police Agents School, Câmpina, Romania

SPECIAL TECHNIQUES FOR SURVEILLANCE AND INVESTIGATION REGULATED BY THE ROMANIAN LAW

Special surveillance and investigation methods represent probative procedures which aim at investigating serious crimes in such a manner that the persons in question are unaware of this fact (The Recommendation of the Committee of Ministers from the European Council no. 10/2005). Therefore, although according to article 92 Code of criminal procedure, the rule is that the lawyer of the suspect or of the defendant has the right to participate in the carrying out of any act of criminal investigation, the special surveillance or investigation methods provided for in article 138 Code of criminal procedure represent an exception from it[4].

According to article 138 paragraph 1 Code of criminal procedure, special surveillance or investigation methods are the following:

a) intercept of communications or of any type of distance communication;

b) access to a computerized system;

c) video, audio surveillance or through photographing;

d) localization or tracking through technical means;

e) obtaining data concerning financial transactions of a person;

f) containment, handover or search of postal items;

g) usage of undercover investigators and collaborators;

h) authorized participation in certain activities;

i) monitored delivery;

j) obtaining traffic and localization data, processed by the public networks and electronic communications providers or by the providers of electronic communications services destined for the public.

Global digitalization, which has developed in the last decade in an unprecedented rhythm in the history on humanity, has created the frame for the possession and usage of mobile phones and of other electronic devices at a widespread scale, with including the aim of committing antisocial acts, ranging from the most simple to the most complex, bearing a cross-border character.

In such conditions, the mere ownership of a mobile phone or of another

[4] Code of criminal procedure – Commentary on articles – Second edition, coordinator Mihail Udroiu, C.H.BECK publishing house, page 633.

electronic device, connected to a GSM network, by any individual who is in connection with the criminal area or who enters this area in any way, represents an enormous valorization potential in the course of the criminal investigations.

If the target person uses the respective device in the course of the unraveling of the stages of the crime, the exploitation potential rises proportionally.

Never in the history of evolution of global criminal phenomenon has an extrinsic fact of committing a crime played such an important role, having cascading implications, with regard to the probationary architecture.

Taking photo captures with an incorporated photo camera, capturing audio/video recordings, using applications/online platforms/games through which one can send encrypted data/information, communication through SMS type messages, communication through telephone conversations, tracking the terminal in various moments of the succession of committing the crime, personal notes of the author in the specific applications of the device, relational maps created, have the ability to reveal a series of data and information which cannot remain unseen in the probative management throughout the criminal investigation.

From the perspective of these considerations, the usage at a quasi-generalized scale of probative procedures regulated by article 138 Code of criminal procedure, paragraph 1, letters a) intercept of communications or of any type of distance communication, b) access to a computerized system, c) video, audio surveillance or through photographing, d) localization or tracking through technical means and j) obtaining traffic and localization data, processed by the public networks and electronic communications providers or by the providers of electronic communications services destined for the public, has become a genuine „algorithm" in the mathematics of the evidence, which opens the investigation, apart from other preliminary stages which build the reason for such requests, having a high-level impact of interference with private life, the rights and liberties for the target person.

At the same time, from another perspective, it is observable the fact that the usage of such „algorithms" from the area of probative procedures regulated by article 138 Code of criminal procedure imply a series of advantages as compared to probative procedures bearing a general spectrum, as follows:

The accountability of the judicial police worker is significantly diminished, while the area of classic probative procedures requires the active role of the worker, his actual involvement, which oftentimes raises suspicions of subjectivity/ abuse, potential contestations against the measures and documents issued by him, as well as inherent errors which occur in the elaboration of procedural documents.

In the case of the procedures referred to in article 138 Code of criminal procedure, it is mainly the case of technical evidence, which bear a high level of objectivity, are extremely hard to eliminate following contestations, which are not negligible aspects, from the point of view of the success of the investigation.

Administering the probative procedures requires oftentimes the triggering of other specialized structures, which represent a guaranty for obtaining high quality evidence, both from the point of view of the technicality of the evidence and from that of the high level of qualification in obtaining them.

Most of the times, involving these structures requires, naturally, the „inactivation" of the investigation during the period of time in which the specialized activities are carried out and the transfer of responsibility towards the support structures. Following, the „reactivation" of the investigation is realized, after obtaining the specialized documentation, which will represent the basis for essential decisions in the management of the criminal investigation.

All of these aspects aim, in my opinion, towards a reversal of the proportion of probative procedures used in the course of criminal investigations, in a hardly distant perspective, context in which the center of gravity will be placed on different „algorithms" from the area of procedures stipulated by article 138 Code of criminal procedure, to the disadvantage of classic probative procedures.

Remains to be seen to what extent the balance stipulated by the Code of criminal procedure, between the efficiency of the criminal process and the protection of fundamental rights of the persons targeted by c riminal investigations, manages to maintain itself, under the circumstances of a constantly rising pressure, from the perspective of the use of procedures which represent an intrusion in the private life of these persons and which interfere with the fundamental rights regulated by ECHR.

References

1. Code of criminal procedure – Commentary on articles – Second edition, coordinator Mihail Udroiu, C.H. BECK publishing house.
2. Code of criminal procedure commented – anniversary edition – NICOLAE VOLONCIU – 90 years, HAMANGIU 2017 publishing house.
3. Code of criminal procedure, updated.

Urbanec J., Junková D., Ph.D. Faculty of Security Management The Police Academy of the Czech Republic in Prague

ANALYTICAL STANDARDS IN THE LEGISLATIVE PROCESS (RIA) AS A TOOL FOR INCREASING EFFICIENCY OF THE PUBLIC SECTOR IN THE CZECH REPUBLIC

Introduction

Creating the appropriate quality of the institutional environment and related processes is a prerequisite for the efficient use of public resources, the overall efficiency of the public sector and indirectly for strengthening or at least

maintaining citizens' trust in the public sector (state) and its administration.

In addition to the financial approach to government efficiency, which seeks possible improvements in public finances (and their allocation, redistribution and stabilization functions), considerable room for increasing efficiency in the public sector can also be seen in setting the public choice process and its derivative – legislative process. Legislative process is a kind of state intervention, which can be not only a desirable response to market failures, but also a source of its own failure – if such the intervention is unreasonable, disproportionate to the purpose, discriminatory to regulated subjects or technically inaccurate. An important aspect that forces democratic and market-oriented states to pay attention to the quality of regulatory activity is, in particular, the disruption of the quality of private law relations in the economy (including business relations), the threat of public compensation or threats to security. In this sense, the quality of law can also be considered a tool for achieving social stability and security – see below:

Table 1

The Conceptual Field of Internal and External Security of the State [1]

	1st dimension Ideals, values, mental wealth of man	**2nd dimension** Social influences of the organisation, legal systems	**3rd dimension** Material aspects of the human existence	**4th dimension** Cyberspace
State forms of protection: • Police • Army	• Internal security • External security			
Private forms of protection:	Private/business security services			
The time aspect:	Past – present – future			

The aim of these theses, which are an introduction to further research of the issue using a quantitative analysis of legislative practice in the Czech Republic, is to present initial inputs to assess the benefits and costs of the Regulatory Impact Assessment (RIA) as a specific analytical procedure prescribed for preparing law proposals. The researched issue, i.e. a certain "legislative efficiency" – we define by standard apparatus of inputs and outputs. Inputs can be understood primarily as financial and time costs associated with ensuring a democratic legislative process, while outputs are primarily meant as a stable legal environment and the necessary legal certainty, which are a prerequisite for the quality of the institutional environment and international competitiveness of the country [2].

Briefly on the implementation of the institute of RIA in the Czech Republic and on the properties of the process and its persistent shortcomings

The RIA method is a standardized set of analytical and consulting processes and activities that, using quantitative tools, evaluate the need and possibilities of state intervention in the form of regulation of market and other activities with respect to a defined target state, and provide a qualified basis for subsequent policy decisions. As stated in [3], *"the evaluation process does not replace political decision-making as it only creates the preconditions for its cultivation"*.

The introduction of the obligation to provide (with exceptions) any emerging government legislative proposal with such a justification can be understood as a kind of regulatory reform, which aims to reduce or correct the main negatives of the traditional way of generating legislation – i.e. its redundancy, frequency of changes (regulatory inflation) and underestimating possible negative effects on private entities. However, such a reform will not be possible without the creation of an adequate administrative background, i.e. expert government institutions, which oversee this process and its implementation.

In the Czech Republic, such a body is the Government Legislative Council (by the Office of the Government of the Czech Republic), and its RIA Working Committee, which was established in 2011. However, the initial step in implementing the RIA process in the Czech Republic came several years before (2007), when impact assessment was introduced in the Czech Republic as a mandatory part of the legislative process and when the RIA methodology began to be developed. This was subsequently (2011) materialized in the form of the publication of General Guidelines for Regulatory Impact Assessment.[4] According to Petr Mlsna, then Minister and Chairman of the Legislative Council of the Government, *"the aim of the new RIA implementation methodology was to eliminate the formal RIA process, contribute to a legislative solution that is proportionate to the problem, and place more emphasis on effective control over quality and requisites prepared by the RIA by the submitters"*, in accordance with the recommendations of the Organization for Economic Cooperation and Development." [5]

Thus, the Czech Republic currently has the RIA model firmly integrated into its legislative process with fixed procedures and deadlines defined by the Legislative Rules of the Government. The opinion of the RIA Working Committee is an indivisible and at the same time separate part of the opinion of the Legislative Council of the Government, which represents an aggregated expert basis for the subsequent political decision-making of the Government.

The procedure of the relevant institutions (i.e. ministries and other central state administration bodies) in preparing RIAs is set out in the General Principles for Regulatory Impact Assessments. It is, in fact, a government "cookbook" for how to consult and analyze emerging government legislative proposals. The general principles regulate a) the basic procedural rules used in the elaboration of the RIA and b) the methodological procedure related to it. In some cases, where it

is possible to use an exception, the obligation to perform RIA does not arise.

The RIA is made on the principle of proportionality, i.e. with regard to the extent of the assessed problem and the extent of potential impacts on various groups of addressees of the law. The evaluation method (qualitative vs. quantitative), the scope of consultations and the database, the range of possible variants, etc. are then adapted to this. The submitter is responsible for determining the level of analysis.

The structure of the RIA Final Report, which represents the materialized output of the RIA process, is also standardized. General Guidelines set out its content. The final RIA report is a mandatory part of the draft legislation. It is part of the draft law as it is included in its explanatory memorandum.

If regulator does not fulfill the general principles of the RIA at all, e.g. when he does not fully justifies the need for a new legal regulation at all, the RIA Working Committee should call for the rejection of the material. As the RIA Working Committee annual report states [5], *"the most fundamental shortcoming, which is then reflected in the whole structure and content of the RIA Final Report, is the insufficient definition of the problem and the justification for the need and effectiveness (purposefulness) of adopting new regulation."* Common shortcomings in the preparation of the RIA Final Report include insufficient elaboration of problem-solving options and insufficient evaluation of impacts of the administrative burden type, where regulators focus mainly on qualitative and significantly less on quantitative indicators of benefits and costs of evaluated options.

Final remarks to the challenges of current practice in the Czech Republic

At a time when non-traditional (hybrid) threats "blur and erase the line between peace-crisis-conflict" and seek secrecy and ambiguity, deepen divisions in society, question democratic decision-making processes, disrupt economic processes and seek influence in strategic economic policy processes [6], seems the quality of RIA as a set analytical and evaluation procedures essential. Although it has been operating in the Czech Republic for several years, it still faces a number of challenges, both material and procedural.

An area where there is still great potential for the application of regulatory impact assessments is the area of legislative initiatives other than government ones. The absence of a standardized procedure for evaluating the impacts of regulation has a negative effect, especially in the case of MP´s law proposals or amendments to government ones.

The application of some exceptions from the mandatory processing of RIA to government proposals can also be considered as a negative side. For the purpose of transparency of the government's fiscal intentions and objectives, which are encompassed in state budget proposal, it would be undoubtedly beneficial if at least a basic RIA was to be produced.

It can be also considered desirable that the General Guidelines for RIA provide guidance that is more detailed for regulators on how to deal with the

problem of quantifying some non-monetary assessed benefits and costs, the presence of which in RIA is often required. Asking for the quantification of generally problematic quantifiable benefits and costs, such as citizen safety, consumer protection or social harmony, can lead to undesirable formalization of the whole process and to outputs that will not provide any subsequent usable and relevant information and decision support.

The big procedural challenge is undoubtedly to ensure the adequate functioning of the RIA Working Committee. In particular, it should fully comply with the requirement for transparency of its work vis-à-vis the public and, conversely, rule out any possible doubts about possible conflicts of interest of its members, which may hypothetically take the form of lobbying against an emerging draft regulation by way of "expert opinion" and "conceptual reservations".

References

1. JUNKOVÁ, Dana, KNÝ, Milan. Fuzzy Problems in Security Management: New Threats and the Importance of Tacit Knowledge in the Police of the Czech Republic. In: J. Blažek, J. Piwowarski, J.M. Ramírez (eds), Publication of Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego "Apeiron" w Krakowie, Krakow 2020, pp. 52 – 64. [cit. 20.12.2020] ISBN 978-83-64035-72-2 Dostupné z: http://apeiron-wydawnictwo.pl/wp-content/uploads/2020/12/SECURITY-IN-CENTRAL-AND-EASTERN-EUROPE-proceedings2018.pdf

2. *How do Laws and Regulations Affect Competitiveness: The Role for Regulatory Impact Assessment.* OECD Regulatory Policy Working Papers No. 15. OECD, Paris, France, 2020.

3. *Legislative process (theory and practice).* Prague: Ministry of Internal Affairs, 2011. ISBN 8073120747.

4. *General Principles for Regulatory Impact Assessment (RIA).* Government of the Czech Republic, January 2016.

5. *Annual Report of the Commission for Regulatory Impact Assessment 2012*. Office of the Government of the Czech Republic, Section of the Government Legislative Council. Prague, 2013.

6. POVEJŠIL, Martin. Lecture *Key Security Challenges for the Czech Republic through the Eyes of the Deputy Minister of Foreign Affairs* held online on 15 March 2021 as part of a miniseries of lectures on Czech security on selected security challenges at the Police Academy of the Czech Republic in Prague.

Албул С. В., професор кафедри оперативно-розшукової діяльності Одеського державного університету внутрішніх справ, кандидат юридичних наук, професор

КАТЕГОРІЇ «РОЗВІДУВАЛЬНА ІНФОРМАЦІЯ» ТА «ІНФОРМАЦІЯ РОЗВІДКИ» В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

З погляду тактики розвідка – це продукт добування, аналізу, опрацювання, оцінки та інтерпретації інформації. Саме для того щоб забезпечити вирішення завдань, які стоять перед оперативними підрозділами Національної поліції, останні реалізовують розвідувальну функцію оперативно-розшукової діяльності з метою своєчасного одержання відомостей про злочини, що замислюються, підготовлюються та вчиняються, а також про осіб, причетних до неочевидних злочинів.

Термін інформація походить від латинського слова «informatio», що означає «відомості, роз'яснення, виклад». Інформація – це відомості про об'єкти та явища навколишнього середовища, їх параметри, властивості і стан, які сприймають інформаційні системи (живі організми, керуючі машини тощо) в процесі життєдіяльності та роботи [1, с. 15]. Відповідно до чинного законодавства, інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. В підрозділах Національної поліції України інформаційна діяльність є видом розвідувальної діяльності, яка полягає у здобуванні первинної інформації, її аналітичному опрацюванні та переробленні в інформацію кримінальної розвідки. Первинно отримані з різних джерел відомості – це ще не кінцевий продукт. Первинні відомості можна визначити саме як розвідувальну інформацію. Подальша її перевірка, доповнення та опрацювання – є процес аналітичний. Взагалі, на нашу думку, аналітика у кримінальній розвідці – це цілісна сукупність принципів методологічного, організаційного та технологічного забезпечення індивідуальної та колективної інтелектуальної творчої діяльності співробітників оперативних підрозділів Національної поліції, яке дозволяє ефективно обробляти здобуту інформацію з метою вдосконалення якості наявних та отримання нових знань, необхідних для прийняття оптимальних управлінських рішень. При цьому об'єктами кримінальної розвідки є особи, факти, події, на отримання інформації про яких спрямовується здійснення кримінальної розвідки [2, с. 237].

Залежно від ступеня аналізу й узагальнення розвідувальну інформацію поділяють на:

– первинну розвідувальну інформацію. Вона містить всю доступну для відповідних засобів розвідки об'єктивну інформацію у вигляді якісних та кількісних ознак об'єктів розвідки. Треба зазначити, що якість первинної інформації, з погляду можливості виявлення ознак об'єкта, залежить не лише від технічних характеристик засобів розвідки, а й від властивостей та стану цього об'єкта, а також від умов ведення розвідки;

– інформацію, отриману внаслідок попередньої обробки (матеріали першого рівня аналізу). Така інформація містить результати аналізу даних, отриманих від одного джерела (з допомогою одного засобу розвідки);

– інформацію другого рівня аналізу (комплексна обробка). Обробка інформації, отриманої від різних джерел і різними видами й засобами розвідки. Спільний аналіз різнорідних відомостей, що належать до одного об'єкта, взаємна логічна ув'язка та уточнення, аналітичне визначення характеристик об'єкта, що залежать від сукупності різнорідних відомостей [3, с. 8];

– узагальнену розвідувальну інформацію, яка являє собою розвідувальні зведення, донесення, довідки, аналітичні огляди, технічні описи та інші документи, підготовлені на основі отриманих розвідувальних відомостей для різних категорій споживачів відповідно до їх запитів.

Треба зазначити, що процес аналізу в кримінальній розвідці має взаємопов'язані складові, а саме: добування інформації з різних джерел; оцінювання первинної інформації; систематизації отриманої інформації; встановлення змісту та сутності первинної інформації; виявлення додатково необхідної інформації; опрацювання первинної інформації; отримання та обґрунтування нових знань; формування кінцевого інформаційного продукту (інформації кримінальної розвідки); прогнозування та надання пропозицій. Саме завдяки аналітичному опрацюванню розвідувальна інформація (первинні дані) перетворюється в інформацію кримінальної розвідки – новий інформаційний продукт.

На наше переконанням, кінцевий інформаційний продукт – інформація кримінальної розвідки, як результат творчої інтелектуальної діяльності, має передбачати конкретні рекомендації до подальших дій або описувати декілька варіантів імовірного розвитку подій у майбутньому. Саме в цьому полягає відмінність у сутності категорій «розвідувальна інформація» та «інформація кримінальної розвідки» в контексті реалізації розвідувальної функції оперативно-розшукової діяльності Національної поліції України.

Бібліографічні посилання

1. Рижков Е. В., Вишня В. Б., Гавриш О. С. Основи інформаційної безпеки : навч. посіб. Дніпро : ДДУВС, 2020. 128 с.
2. Захаров В. П. Інформаційна розвідка як перспективний напрям розвитку правоохоронної діяльності у боротьбі зі злочинністю. *Вісник Львівського державного університету внутрішніх справ (юридична серія)*. 2006. № 2. С. 236–242.
3. Никифорчук Д. Й., Бусол О. Ю. Аналітична розвідка як один із напрямів оперативно-розшукової діяльності. *Науковий вісник НАВС*. 2011. № 1. Ч. 2. С. 3–11.

Амеліна А. С., професор кафедри фінансових розслідувань Університету державної фіскальної служби України, кандидат юридичних наук, доцент

ПОНЯТТЯ ТА ЧИННИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Проблеми інформаційної безпеки в сучасних умовах є надзвичайно актуальними і вимагають поглибленого вивчення. Характерною ознакою сучасного етапу науково-технічного прогресу є стрімкий розвиток інформаційних технологій, їх використання як у повсякденному житті, так і в управлінні державою. Інформація та інформаційні технології все більше визначають розвиток суспільства і слугують новими джерелами національної могутності [1, с. 97].

Теоретичні дослідження питань інформаційної безпеки розглядалися у роботах: Д. С. Азарова, В. А. Авраменко, К. І. Бєлякова, П. С. Берзіна, В. Л. Бурячка, В. Д. Гавловського, В. І. Голубєва, О. М. Горбатюка, В. П. Ємельянов, Р. А. Калюжного, А. А. Князєва, Б. А. Кормича, О. І. Крюкова, М. Б, Левицької, В. М. Лопатіна, Ю. Є. Максименко, Г. М. Новицького, В. М. Плугатиря, А. М. Ришелюка, О. А. Сороківської, В. І. Шакуна, Я. Р. Якубовського та інших.

Варто зауважити, що в науковій літературі наявні різні підходи до визначення сутності поняття інформаційна безпека. Розглянемо погляди вчених щодо цього поняття. Зокрема, О. М. Горбатюк вважає, що «інформаційна безпека – стан захищеності потреб в інформації особистості, суспільстві і держави, за якого забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз» [2, с. 47].

Р. А. Калюжний вважає, що «інформаційна безпека держави – це вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для держави безпечних умов існування; суспільних правовідносин, пов’язаних із створенням, розповсюдженням, зберіганням та використанням інформації» [3, с. 237].

У. Ільницька вважає, що «інформаційна безпека є інтегрованою складовою національної безпеки і її розглядають як пріоритетну функцію держави» [4, с. 28]. Тобто робимо висновок, що єдиної думки щодо цієї дефініції немає.

У найзагальнішому випадку інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. Під інформаційним середовищем розуміють сферу діяльності суб’єктів, пов’язану зі створенням, перетворенням і споживанням інформації.

Інформаційне середовище умовно поділяється на три основні предметні частини: створення і розповсюдження вихідної та похідної інформації; формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг; споживання інформації та дві забезпечувальні предметні частини: створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення, а також засобів і механізмів інформаційної безпеки [1, с. 97].

Варто також відмітити, що інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого безпосередньо впливають зовнішні та внутрішні чинники, найважливішими з яких є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх та внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична обстановка в державі. Водночас інформаційна безпека є складною, динамічною, цілісною соціальною системою, компонентами якої є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна інформаційна єдність останніх становить якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх конкурентоздатний, прогресивний розвиток [5, с. 154–157].

У Законі України «Про основи національної безпеки України» до загроз в інформаційній безпеці держави відносять такі: намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної інформації, неповної або упередженої інформації; прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, а також конференційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави [6].

Отже, враховуючи вищевикладене, треба зазначити, що захист інформації повинен здійснюватися комплексно і постійно, за допомогою методів, способів системи захисту, це не можна зробити лише одноразовим актом. При цьому створення безпечної системи інформаційної безпеки є дуже громіздкою роботою, яка вимагає величезних зусиль, способів, методів та засобів.

Бібліографічні посилання

1. Лукянова В. В., Лаутар А. Ю. Інформаційна безпека в умовах розвитку інформаційної системи. *Вісник Хмельницького національного університету*. 2013. № 2. Т. 3. С. 97–101.
2. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть. *Вісник Київського університету імені Тараса Шевченка.* 1999. Вип. 14. Міжнародні відносини. С. 46–48.
3. Калюжний Р. А. Інформаційне право України: концептуальні основи формування. *Науковий вісник Дніпропетровського інституту МВС України*. 2001. № 3(6). С. 234–

244.
4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізм протидії негативним інформаційно-психологічним впливам. *Humanitarian vision*. 2016. Vol 2. Num 1. С. 27–32.
5. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк». 2018. 446 с.
6. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. № 537-V. *Відомості Верховної Ради України*. 2007. № 12. С. 511. Ст. 102.

Архипенко Т. А., аспірант кафедри менеджменту Національного технічного університету «Дніпровська політехніка»

РОЛЬ ДЕРЖАВИ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

У сфері забезпечення економічної безпеки підприємств спостерігається пряма залежність від держави. Одним з найважливіших елементів економічної безпеки держави є правовий захист підприємницької діяльності, що відповідає інтересам держави. З погляду держави підприємство вирішує низку важливих завдань, до числа найважливіших можна віднести: забезпечення доходів держави (податкові надходження до бюджетів усіх рівнів для цілей управління, підтримки та розвитку інфраструктури, оборони); забезпечення зайнятості населення; перерахування коштів для утримання соціальної сфери (пенсійне забезпечення, медичне обслуговування, освіта). Саме тому важливою умовою прогресивного розвитку економічної безпеки є створення зручного та сприятливого клімату для ведення підприємницької діяльності.

Є інструмент державного управління економічною безпекою, який являє собою засоби державного управління, за допомогою яких відбувається забезпечення економічної безпеки. Виділяють дві підгрупи інструментів державного управління економічною безпекою: універсальні та локальні. Під універсальними інструментами управління економічною безпекою розуміють закріплені в правових актах норми й правила управлінської діяльності та ті, що мають низку законів, статутів, інструкцій, обмежень тощо. Під локальними інструментами державного управління економічною безпекою розуміють ті, що мають приватний характер для виконання управлінських рішень та можуть мати низку постанов, наказів, розпоряджень, угод, контрактів, нарад тощо.

Насамперед, можна зазначити закони України, які прямо стосуються регулювання відносин в економічній сфері: «Про Раду національної безпеки і

оборони України» [1], «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом» [2], «Про валюту і валютні операції» [3], «Про приватизацію державного і комунального майна» [4], «Кодекс України з процедур банкрутства» [5], «Про зовнішньоекономічну діяльність» [6], «Кримінальний кодекс України» [7], «Цивільний кодекс України» [8], «Митний кодекс України» [9], «Бюджетний кодекс України» [10], «Господарський кодекс України» [11] та інші.

Крім того, варто виділити Указ Президента України про рішення Ради національної безпеки і оборони України від 11 серпня 2021 р. «Про Стратегію економічної безпеки України на період до 2025 року», в якому визначаються шляхи досягнення цілей і реалізація пріоритетів національних інтересів у сфері забезпечення економічної безпеки [12].

В розрахунках Мінекономіки спостерігається незадовільний стан економічної безпеки України впродовж 2010–2019 років. Особливо небезпечний рівень за всіма економічними складовими досягав у 2014–2015 роках. Проте за цей час середнє значення рівня економічної безпеки дорівнювало 40 %, що відповідає зоні незадовільного стану. Як бачимо, упродовж 10 років економічна безпека України не забезпечувала досягнення національних економічних інтересів. Зокрема, і за підсумками першого півріччя у 2020 р. середнє значення рівня економічної безпеки становить 41 %, що вкотре доводить негативне становище економічної безпеки [13].

Доповнюють негативну статистику дослідження аудиторської компанії PwC, які свідчать, що в Україні за 2019–2020 роки 51 % організацій постраждали від шахрайства. Лідером серед економічних злочинів виявилося незаконне привласнення майна, цей факт підтвердили 47 % опитаних. Також до переліку найпоширеніших економічних злочинів увійшли корупція і хабарництво, шахрайство з боку клієнтів, а також кіберзлочини та шахрайство у сфері закупівель. Зрештою негативні факти економічної безпеки неминуче позначаються на рівні економічного розвитку держави [14].

Нещодавно, в травні 2021 р., Кабінет Міністрів України ухвалив постанову про створення Бюро економічної безпеки для вирішення низки проблем, як-от протидія кримінальних правопорушень у галузі економіки та фінансів. Бюро економічної безпеки отримає статус центрального органу виконавчої влади та буде займатися усіма злочинами у сфері економіки [15].

Отже, підсумовуючи вищевказане, робимо висновок, що основа забезпечення економічної безпеки закладена відповідними документами, що ухвалені й впроваджені в державі. Держава чинить значний вплив на рівень економічної безпеки підприємств. Також можна стверджувати, що економічна безпека, яка регулюється чинним законодавством, є необхідною умовою для життєвого циклу людини, підприємства і держави. Роль державних органів формується для захисту підприємств від різноманітних загроз та забезпечення економічної безпеки. Гарантом економічної безпеки підприємства є держава. Стосовно Бюро економічної безпеки – це нова

сторінка у відносинах держави та підприємницької діяльності.

Тож можемо стверджувати, що для поліпшення економічної безпеки підприємств держава повинна мати чітку стратегію, яка визначає її переваги та спрямована як на її розвиток, так і на реалізацію діяльності підприємств всіх можливостей економічного середовища.

Незважаючи на всі затверджені стратегії та проєкти, статистика показує, що рівень економічної безпеки перебуває на досить низькому рівні протягом 10 років. У цих умовах виникає об'єктивна потреба активізації ролі держави у забезпеченні економічної безпеки підприємництва.

Згідно з аналізом роль держави у забезпеченні економічної безпеки підприємств потребує більш детального вивчення, оскільки питання перевірки запропонованих стратегій держави та комплексного забезпечення економічної безпеки як державних, так і приватних підприємств залишається невирішеним і потребує подальших досліджень.

Бібліографічні посилання

1. Про Раду національної безпеки і оборони України. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text
2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text
3. Про валюту і валютні операції. URL: https://zakon.rada.gov.ua/laws/show/2473-19#Text
4. Про приватизацію державного і комунального майна. URL: https://zakon.rada.gov.ua/laws/show/2269-19#Text
5. Кодекс України з процедур банкрутства. URL: https://zakon.rada.gov.ua/laws/show/2597-19#Text
6. Про зовнішньоекономічну діяльність. URL: https://zakon.rada.gov.ua/laws/show/959-12#Text
7. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
8. Цивільний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text
9. Митний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/4495-17#Text
10. Бюджетний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2456-17#Text
11. Господарський кодекс України. URL: https://zakon.rada.gov.ua/laws/show/436-15#Text
12. Про Стратегію економічної безпеки України на період до 2025 року. URL: https://zakon.rada.gov.ua/laws/show/347/2021#Text
13. Мінекономіка. URL: https://www.me.gov.ua/
14. PricewaterhouseCoopers. URL: https://www.epravda.com.ua/rus/projects/regulation/2021/06/29/675208/
15. Бюро економічної безпеки. URL: https://sluga-narodu.com/beb

Бабакін В. М., викладач кафедри прикладної механіки та технологій захисту навколишнього середовища факультету техногенно-екологічної безпеки Національного університету цивільного захисту України, доктор юридичних наук, доцент

ОКРЕМІ АСПЕКТИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ ЩОДО ПРОТИДІЇ ЗЛОЧИНАМ, ЩО ВЧИНЯЮТЬСЯ МОЛОДДЮ

На сучасному етапі реформування Міністерства внутрішніх справ України та Національної поліції України простежується тенденція активного впровадження і використання цифрових інформаційних технологій у протидії злочинності. На сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційно-аналітичної підтримки. Це є наочним підтвердженням загальновідомої тези «хто володіє інформацією, той володіє світом» [1, с. 202]. Перед науковцями та практичними працівниками поліції постають питання щодо розробки новітніх форм інформаційно-аналітичного забезпечення у сфері протидії молодіжній злочинності. Аналітична робота в поліції – це діяльність, що спрямована на планування роботи, аналізу та оцінки інформації, яка може бути отримана з матеріалів кримінальних проваджень, оперативно-розшукових справ, архівних справ, а також з автоматизованих інформаційно-аналітичних систем оперативно-розшукового призначення, використання форм, методів та засобів для ухвалення управлінських рішень. Метою системи інформаційно-аналітичного забезпечення оперативних підрозділів є інформаційна підтримка їх практичної діяльності у протидії злочинності на підставі застосування комплексу організаційних, нормативно-правових та інших заходів. Таке забезпечення спрямовано на створення, організацію функціонування та удосконалення інформаційних систем, що сприяють успішному виконанню завдань щодо запобігання та припинення злочинів, які вчиняються особами молодого віку. Зокрема, в умовах дії чинного КПК України загалом діяльність оперативних підрозділів пов’язана зі здійсненненням моніторингу злочинності, окремих її видів, із запобіганням та припиненням кримінальних правопорушень, виявленням причин та умов, що сприяють їх вчиненню. Під час протидії злочинності серед молоді першочергового значення набуває отримання первинної оперативно-розшукової інформації про осіб, зокрема молодого віку, що готують, вчиняють, або вже вчинили кримінальне правопорушення. Як зазначає

О. В. Одерій, потреби оперативних підрозділів в отриманні вичерпної інформації спонукають до створення та розробки нових видів обліків, реєстрації об'єктів за новими, раніше не використаними ознаками [2, с. 3]. На нашу думку, ефективне використання оперативних обліків, удосконалення їх змісту та обсягів дасть змогу оперативним працівникам виявляти осіб, які схильні до вчинення кримінальних правопорушень та ухвалювати рішення щодо здійснення відповідних заходів реагування. Зміст інформаційно-аналітичного забезпечення діяльності оперативних підрозділів поліції у протидії злочинності визначається динамікою, характером, детермінованістю, станом оперативної обстановки та тактикою застосування сил, методів та засобів. Серед завдань системи інформаційно-аналітичного забезпечення оперативних підрозділів поліції щодо протидії окремих видів злочинів науковці О. М. Бандурка, В. М. Плішкін називають: 1) інформатизацію оперативно-розшукової діяльності; формування інформаційного середовища оперативними підрозділами, що складається із відомчих інформаційних ресурсів та інформаційної інфраструктури правоохоронних органів [3, с. 219]; 2) забезпечення оперативного отримання інформації; аналіз й результати накопичення, обробки, та узагальнення з метою ухвалення управлінських рішень; 3) забезпечення динамічної та ефективної інформаційної взаємодії всіх галузевих служб поліції України, інших правоохоронних органів і державних установ; забезпечення захисту інформації [4, с. 544]. На нашу думку, завдання інформаційно-аналітичного забезпечення оперативних підрозділів полягає у формуванні єдиних оперативних обліків, збиранні, опрацюванні, аналізі та використанні різноманітної інформації, що має значення щодо виявлення, запобігання та припинення злочинів та належного проведення негласних слідчих (розшукових) дій і оперативного супроводження щодо подальшого досудового розслідування та розгляду їх у суді. Інформаційно-аналітичне забезпечення, як складовий елемент інформаційного забезпечення ОРД, забезпечує здійснення системи заходів, а саме: а) вивчення причин і умов, що сприяли вчиненню злочинів, зокрема особами молодого віку; б) збір і аналіз оперативної інформації про процеси і явища, що відбуваються у молодіжному середовищі та ухвалення рішення для стабілізації оперативної обстановки на певній території оперативного обслуговування чи напрямі; в) проведення спільних заходів щодо виявлення, запобігання та припинення злочинів, до яких готуються чи здійснюють замах особи молодого віку; г) організація щодо забезпечення захисту інформації, що накопичується оперативними підрозділами чи слідчими під час проведення негласних слідчих (розшукових) дій або оперативно-розшукових заходів.

Отже, на нашу думку, використання сучасного інформаційно-аналітичного забезпечення як засіб підвищення ефективності діяльності оперативних підрозділів у протидії злочинам, що вчиняються молоддю, надасть змогу своєчасно проводити роботу з молодими особами, які були

взяті та перебували на профілактичному обліку у зв'язку з високим ступенем імовірності їх схильності до готування або вчинення кримінального правопорушення; здійснювати оперативно-тактичні заходи щодо викриття кримінально активних молодих осіб, членів неформальних молодіжних формувань, раніше засуджених, членів груп з антигромадською спрямованістю, розкриття злочинів, які готуються або вже вчинені ними тощо.

Бібліографічні посилання

1. Танкушина Т. Ю. Автоматизовані інформаційні системи в структурі реєстраційної діяльності міліції: становлення, розвиток, сучасність. *Вісник Запорізького національного університету: збірник наукових праць*. Юридичні науки : у 2 ч. Запоріжжя : Запорізький національний університет, 2011. Ч. І. 224 с.
2. Одерій О. В. Інформаційно-довідкове забезпечення розслідування злочинів. Донецьк : ДІВС, 2001. 20 с.
3. Плішкін В. М. Теорія управління органами внутрішніх справ : підручник / за ред. Ю. Ф. Кравченка. Київ : НАВСУ, 1999. 702 с.
4. Бандурка О. М. Оперативно-розшукова діяльність : підручник. Харків : Нац. ун-т внутр. справ, 2002. Ч. І. 336 с.

Байсеитов Б. Т., начальник Центра по подготовке специалистов по противодействию киберпреступности Алматинской академии МВД Республики Казахстан имени Макана Есбулатова, подполковник полиции

ОСОБЕННОСТИ ТЕНЕВОГО ИНТЕРНЕТА – DEEP WEB И DARK NET

Краткое описание: для многих обывателей термины ***Deep Web и Dark Net (Дип Веб и Даркнет)*** звучат как нечто непонятное или скорее даже пугающее. СМИ, блоги, социальные сети часто описывают их как место, которое кишит наркоторговцами, киллерами, хакерами, нелицензионным контентом и т.п. Однако ***Даркнет*** как концепция приватной сети зародился еще в далеком 1970 году, а сегодня многие ресурсы в темной паутине посещают не только хакеры и преступники, но также журналисты, активисты, простые пользователи из стран, где интернет фильтруется спецслужбами. Но, как и любое благое изобретение, Дарнет можно использовать и не в благородных целях. В ***Даркнете*** безусловно есть площадки, где собираются киберпреступники, покупаются и продаются украденные конфиденциальные денные, различные малвари, нелицензионный контент.

В данной публикации мы постараемся более подробно рассказать о

Deep Web, Dark Net, в чем разница и законно ли подключаться к скрытому интернету, а также о его использовании на хакерском поприще.

Большинство маркетологов говорят, что лучшее место, чтобы спрятать тело, – вторая страница Google. Однако это еще не далеко. Есть черное цифровое кладбище, называемое «Deep web». Это место, до которого Google дотянуться не способен.

Что это вообще такое Deep Web? Он заработал репутацию зловещей бездны, незаконной и вызывающей беспокойство деятельности, о которой можно услышать в СМИ. Но это место называется Dark Net. Термины «Deep Web» и «Dark Net» часто используются как синонимы, однако это не совсем верно. Даркнет – это лишь крошечная часть deep web'а, составляющая всего 0,01 % от него. Все страшное, которые вы слышали о deep web, относились к Dark Net [1].

По большей части, контент в глубоком интернете очень похож на контент обычных сайтов, которые можно найти в Google.

Deep Web – это просто контент, который вы не сможете найти через поисковую систему. К этому контенту относится, например, личная информация в вашей учетной записи в какой-нибудь социальной сети, ваши сообщения на электронной почте, закрытые страницы частных сайтов и т. д.

То, что мы можем найти в поиске, называется surface web, или «поверхностный интернет». Отличия между поверхностным и глубоким интернетом заключается в том, что некоторая защита препятствует к свободному доступу информации из deep web, а к surface web может получить доступ любой пользователь.

Более 96 % контента находится в deep web, т. е. это большая часть информации, к которой мы получаем доступ в интернете только после аутентификации: банковский счет, электронная почта, аккаунт в социальной сети. Представьте только, если бы любой мог получить доступ к этой информации, просто погуглив ваше имя. Ваша личная информация была бы доступна всему миру [2].

Веб-сайты не позволяют индексировать защищенные страницы, потому что лишь определенные лица должны иметь доступ к информации, размещенной на них.

Понятие «скрытой сети», что такое Даркнет. Термин ***Dark Net*** или «***Темная паутина»*** в общем понимании обозначает совокупность веб-сайтов, видимых публично, но при этом имеющих скрытый IP-адрес сервера, на котором они размещаются. Такие сайты общедоступны для всех веб-пользователей, однако выяснить, кто является их автором, очень сложно. Так же стоит сказать, что на подобные сайты невозможно попасть, используя популярные поисковые системы.

По сути ***Dark Net*** это частная сеть, в которой соединения устанавливаются только между доверенными пирами, иногда именующимися как «друзья», и чаще всего с использованием нестандартных протоколов и

портов. ***Dark Net*** отличается от других распределенных одноранговых сетей, так как файлообмен происходит анонимно (вследствии того, что IP-адреса русурсов недоступны публично), и следовательно, пользователи могут общаться без особых опасений и государственного вмешательства.

В виду этого ***Dark Net*** часто воспринимается как инструмент для осуществления коммуникации в запрещенных сообществах, подпольях, а так же для ведения незаконной деятельности. В более общем смысле термин ***Dark Net*** может быть использован для описания некоммерческих «узлов» сети Интернета или относится ко всем «подпольным» интернет-коммуникациям и технологиям, которые в большинстве своем связаны с незаконной деятельностью или инакомыслием.

Можно встретить сравнение ***Dark Net*** и технологий 2p2-обмена, применяемых, например, для распространения торрентов.

Так, наиболее распространенные на сегодняшний день файлообменники, например ***BitTorrent***, на самом деле не являются даркнетами, поскольку пользователи могут связываться с кем угодно в сети [3].

Почти все известные даркнеты децентрализованы, и следовательно, считаются одноранговыми. Также многие даркнеты требуют установки специального программного обеспечения для получения доступа к сети.

Поговорим о истории возникновения *Dark Net.* Термин «***Dark Net***» имеет давнюю историю и появился еще на заре компьютерных технологий в 1970-х годах. В контексте сетевой безопасности использовался для обозначения сетей, изолированных от ***ARPANET.*** Даркнеты могли получать данные от главной сети ***ARPANET***, но имели такие адреса, которые не появлялись в списках сетей и не отвечали на запросы извне [4].

В современном понимании термин ***Dark Net*** получил широкое распространение благодаря публикации «The Darknet and the Future of Content Distribution», опубликованной в 2002 году, группой сотрудников Microsoft в лице Питера Биддла, Пола Инглэнда, Маркуса Пейнаду и Брайана Уиллмана [5].

Авторы данной публикации выдвинули идею ***Dark Net,*** основанную на трех предположениях:

- Любой объект, предназначенный для широкого распространения, будет доступен определенной части пользователей с разрешением на копирование.
- Пользователи будут копировать объекты, если это возможно и если они этого захотят.
- Пользователи соединены каналами с высокой пропускной способностью.

Итак, термин ***Dark Net*** – это файлообменная сеть, которая возникает при появлении общедоступных данных, согласно предположению 1, и при распространении этих данных, согласно предположениям 2 и 3.

С тех пор этот термин часто заимствовался и использовался в таких

крупных СМИ, как ***Rolling Stone*** и ***Wired***.

Специфика Даркнета, как правило, используется в определнных случаях, например, таких как:

- Неприкосновенность частной жизни и страх политических репрессий.
- Преступления в сфере информационных технологий.
- Распространение файлов, защищенных авторскими правами.

Даркнет и анонимные узлы TOR. Практически все сайты, находящиеся в ***Темной паутине***, скрывают свою принадлежность, используя инструмент шифрования ***Tor*** [6].

TOR для тех, кто не знал. *Tor (The Onion Router)* – свободное и открытое программное обеспечение для реализации луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

Так с помощью ***Tor*** пользователи могут сохранять анонимность в Интернете при посещении сайтов, ведении блогов, отправке мгновенных и почтовых сообщений, а также при работе с другими приложениями, использующими протокол TCP. Анонимизация трафика обеспечивается за счет использования шифрованных распределенных сетей серверов – узлов. Технология ***Tor*** обеспечивает защиту от механизмов анализа трафика, которые ставят под угрозу не только приватность в Интернете, но также конфиденциальность коммерческих тайн, деловых контактов и тайну связи в целом.

Tor позволяет скрыть вашу личность и «подменить» ваше местоположение. В случае, когда в управлении сети Tor находится веб-сайт, эффект наблюдается тот же, что и в ситуации с конечным пользователем. Для того чтобы посетить сайт в Темной паутине, который использует инструмент шифрования ***Tor***, веб-пользователь должен также использовать ***Tor.***

Вернемся к даркнетам. Важно сказать, что не все сайты Темной паутины используют ***Tor***. Некоторые используют альтернативные сервисы, как например ***I2P***, но принцип действия остается абсолютно таким же: пользователь должен использовать такой же инструмент шифрования, как и целевой сайт, и, что очень важно, знать, где найти сайт, чтобы посетить его посредством введения конкретного URL. Одним из самых известных примеров сайта Темной паутины остается ***Silk Road («Шелковый путь»)***. Ранее Silk Road долгое время являлся анонимной торговой площадкой для покупки-продажи наркотиков.

Кстати, нужно помнить, что пользователи Tor встречают и некоторые неудобства, например, такие как:

- Так вы можете невольно стать соучастником масштабных преступлений и деятельности хакеров, так как ваш ПК становится частью

сети, что используется другими хостами.

- ***Tor*** разрабатывался военными и спецслужбами, что не исключает его использование в своих целях, несмотря на раскрученный бренд про 100 % безопасность и анонимность использования.
- Это создает неудобства при пользовании «белыми» сервисами, например, почтой. Суть в том, что при работе с Tor у вас постоянно меняется IP-адрес, что приводит к отключению сервисов, которые воспринимают это как попытку внешнего взлома.
- Google часто блокирует поисковые запросы через Tor, поскольку считает, что это хакерская активность.

Белая сторона Даркнета. Компания Trend Micro опубликовала отчет, из которого можно сделать вывод, что не все, что используется в Даркнете, плохо, а именно:

1) на сайты в скрытой сети заходят не только злоумышленники, но и добропорядочные граждане, в том числе журналисты и пользователи из стран с диктаторскими режимами;

2) в торговом ассортименте подпольных магазинов преобладают не сильные, а слабые наркотики, которые и так легализованы на некоторых территориях.

Многие страны лишены того, что соответствовало бы первой поправке к Конституции США. Так сеть Darknet предоставляет всем желающим возможность свободно высказывать свои мысли, не боясь цензуры или преследования. По данным Tor Project, анонимные Hidden Services служат убежищем для диссидентов из Ливана, Мавритании и стран, которые накрыла Арабская весна. Тут же размещаются и зеркала сайтов, вызывающих страх и ненависть у правительств некоторых стран и глобальных корпораций – GlobalLeaks, Indymedia и Wikileaks.

Trend Micro в своем отчете так же отмечает ещё несколько особенностей даркнета. Например, никто не может оценить его размер. Вполне вероятно, что там гигантское количество страниц, но невозможно сказать, сколько из них доступны в каждый момент времени. Информационный ландшафт очень быстро меняется: сайты появляются и исчезают.

Если посмотреть на ассортимент магазинов, то там преобладает марихуана и фармацевтические средства вроде виагры. Так называемая «фарма» – давний предмет купли-продажи на полулегальных сайтах, которые существуют и в открытой Сети. Так же в списке присутствуют видеоигры, аккаунты к разным сайтам, грибы [7].

Даркнет и хакеры. Все в том же отчете Trend Micro упоминает известный факт, что даркнет используется для установки командных серверов в ботнетах и других зловредах. По своей природе Скрытая сеть естественным образом подходит для этого. Один из примеров malware, которая пропускает трафик через Tor, — известный троян-шифровальщик

Cryptolocker.

В июне 2016 года специалисты «Лаборатории Касперского» подготовили отчет и рассказали о подпольной торговой площадке xDedic, на которой злоумышленники продают доступ к взломанным серверам со всего мира. Тогда ресурс, работавший в обычном интернете, а не в зоне .onion, быстро исчез с радаров и прекратил свою деятельность. Теперь исследователи компании Digital Shadows сообщают, что xDedic вернулся в строй, но перебрался в даркнет.

Каким образом попадают в Dark Net. К темной сети (darknet) вы не сможете получить доступ через стандартный браузер (Google Chrome, Safari и т.п.), для этого вам нужно специальное программное обеспечение для шифрования, например, браузер Tor.

Tor сохраняет анонимность, скрывает местоположение и засекречивает передачу данных пользователей, поэтому Dark Net, как правило, используют для преступной деятельности. Согласно исследованию двух экспертов по угрозам кибер-разведки, более половины сайтов из даркнета предлагают незаконные продукты или услуги. И отследить кого-то из преступников, их деятельность попросту невозможно.

Но несмотря на то, что правоохранительным органам почти невозможно поймать преступников, анонимность даркнета полезна для пользователей с точки зрения этики.

Пользователь не оставляет цифрового следа в даркнете. Это спасает политических осведомителей, активистов и журналистов, которые живут в репрессивных странах, где введена цензура и за негативное мнение может последовать наказание. Они используют темную сторону интернета, чтобы заявить о своем истинном мнении, не боясь, что их личность будет раскрыта.

Даркнет имеет две крайности: он защищает людей, чью свободу пытаются ограничить, но с другой стороны он создает огромное поле для незаконной деятельности. Это наводит на один вопрос.

Законен ли Даркнет. Доступ к темной сети не является чем-то незаконным. Несмотря на то, что люди совершают незаконные действия на просторах темного веба, использование его для доступа к скрытому контенту не противоречит закону. На самом деле, Tor, самое популярное программное обеспечение для доступа в даркнет, был создан ВМС США, в настоящее время финансируется правительством США [8].

Они поддерживают Tor, потому что он защищает частную жизнь активистов, которые пытаются поменять тиранические режимы своих стран. От этой технологии зависит жизнь и свобода этих людей.

Почему люди имеют неправильно представление о Deep Web? Глубокая паутина по ошибке связана с незаконной деятельностью даркнета. Это не просто рынок наркотиков и прочих незаконных предметов (это описание даже отдаленно неверно). Deep Web в основном безвреден и необходим нам для защиты нашей личной информации и

конфиденциальности. Он играет огромную роль в нашей повседневной жизни.

Библиографические ссылки

1. https://zen.yandex.ru/media/applespbevent/darknet-deep-web-chto-eto-takoe-v-chem-raznica-i-zakonno-li-podkliuchatsia-k-skrytomu-internetu-5b4f182246ae1500a9379bbf
2. https://zen.yandex.ru/media/applespbevent/
3. https://ru.wikipedia.org/wiki/BitTorrent_(программа)
4. https://ru.wikipedia.org/wiki/ARPANET
5. https://ipiskunov.blogspot.com/2016/08/darknet.html
6. https://www.torproject.org
7. https://ru.wikipedia.org/wiki/WikiLeaks
8. https://safe.cnews.ru/news/top/anonimnaya_set_tor_na_60_finansiruetsya

Бекишев А. К., и.о. начальника кафедры кибербезопасности и информационных технологий Алматинской академии МВД Республики Казахстан имени Макана Есбулатова, доктор философии (PhD) по специальности «Правоохранительная деятельность», майор полиции

НЕКОТОРЫЕ ВОПРОСЫ РЕАЛИЗАЦИИ КОНЦЕПЦИИ «КИБЕРЩИТ КАЗАХСТАНА»

Характерной чертой современного общества является его информатизация – активная разработка и внедрение во все сферы человеческой деятельности информационных технологий и средств.

Информация и информационные ресурсы становятся одним из решающих факторов развития личности, общества и государства. Широкие возможности компьютеров и информационных технологий позволяют автоматизировать процессы мониторинга и управления государственными, экономическими, социальными, оборонными и другими объектами и системами, получать, накапливать, обрабатывать и передавать информацию об этих процессах практически с любой требуемой скоростью, в любом количестве.

На сегодняшний день в международном сообществе вопросы кибербезопасности входят в первый список приоритетов национальной безопасности. Вследствие глобальной информатизации всех сфер деятельности, в том числе государственных и военных структур, сформировалась принципиально новая среда противоборства конкурирующих государств – киберпространство.

Сегодня в определенных субъектов возникает стремление единолично

обладать информационными ресурсами, средствами и технологиями и использовать их для удовлетворения своих интересов и противодействия интересам вероятных конкурентов в экономическом, коммерческом и даже военном противоборстве. Информация и информационные технологии при этом начинают выступать в качестве объектов угроз, что порождает проблему информационной безопасности.

Укажем главные проблемы:

1. Увеличение в нашей Республике и в мире число пользователей Интернет сети.
2. Распространенность вредоносных программ для персональных компьютеров и мобильных устройств.
3. Увеличение количества кибератак.
4. Игнорирование мер безопасности для персональных компьютеров.
5. Не умение большинством пользователей обновления программ и установки антивирусных приложений.
6. Пренебрежение соображениями безопасности при использовании интернет-ресурсов и социальных сетей.
7. Низкая правовая грамотность по вопросам информационной безопасности и отсутствие сформировавшихся потребностей в повышении у населения.
8. Отсутствие знаний о правовых ограничениях в Интернет сети.

7 марта 2017 года была принята Концепция «Киберщит Казахстана» [1]. Данный документ – первая попытка в стране выработать комплексный подход к обеспечению кибербезопасности национального цифрового пространства. Концепция кибербезопасности «Киберщит Казахстана» разработана в соответствии с Посланием Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная конкурентоспособность» с учетом подходов Стратегии «Казахстан-2050» по вхождению Казахстана в число 30 самых развитых государств мира [2].

В данной Концепции дан анализ текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития «цифровой» экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг.

На основе данной программы проходит мониторинг процесса обеспечения информационной безопасности. Необходимо подчеркнуть, что при разработке национальной Концепции кибербезопасности был изучен международный опыт таких стран, как Великобритания, Германия, Чехия, Франция, Литва, Эстония, Финляндия, Швеция, Швейцария, занимающих лидирующие и ведущие позиции в Глобальном индексе кибербезопасности.

Выполнение данной Концепции послужит дальнейшей модернизации казахстанского общества и станет вкладом Казахстана в реализацию Глобальной программы кибербезопасности ООН.

Подведем промежуточные итоги реализации Концепции кибербезопасности. К числу основных итогов относятся формирование законодательства, расширение сферы обязательного использования технических стандартов и требований, утверждение профессионального стандарта, увеличение образовательных грантов по специальности «Системы информационной безопасности» (с 2018 года число грантов увеличено с 60 до 500 ежегодно), организация системной работы по повышению грамотности государственных служащих и информированию граждан о мерах безопасности при использовании информационно-коммуникационных технологий.

В целом основные итоги первого этапа реализации Концепции кибербезопасности свидетельствуют о масштабах работы, проведенной в период 2017–2018 годы. К примеру: в 2017 году в Глобальном индексе кибербезопасности показатель Казахстана составил 0,352 балла, увеличившись по сравнению с 2015 годом с 0,176 баллов.

Также с принятием национальных обязательств по кибербезопасности (Концепция «Киберщит Казахстана» и отдельного плана по ее реализации), наша страна в данном рейтинге была отнесена к категории стран со средней оценкой. Эффективное использование информационных ресурсов в интересах Казахстана, каждого его гражданина невозможно без формирования в стране комплексной системы информационной безопасности, обеспечивающей надежную защиту информации. К таковым относится Концепция «Киберщит Казахстана».

Внедрение программы «Киберщит Казахстана» позволило уменьшить рост угроз со стороны информационных атак недоброжелателей, похищению государственных секретов, защиту банков и т. д.

Рассмотрим угрозы кибербезопасности. Под угрозой информационной безопасности понимается потенциально возможное или реальное нарушение нормального использования информационных ресурсов. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица. К угрозам, создаваемым этими лицами, относятся: кражи или несанкционированное несанкционированное уничтожение документов, ускорение угасания текста или изображения, подмена или изъятие документов, фальсификация текста или его части, несанкционированное копирование бумажных и электронных документов и многие другие. Для электронных документов угрозы особенно опасны, так как часто трудно обнаружить сам факт кражи информации [3].

Как считают исследователи «Лаборатории Касперского», в ближайшие годы мир увидит небывалый «расцвет киберпреступности». Развитие технологий и стирание граней между личными и рабочими устройствами, в основном – смартфонами, ноутбуками и планшетными компьютерами, приведет к тому, что доступ злоумышленников к личным данным, к

корпоративной конфиденциальной и секретной информации существенно облегчится. Гаджеты и умные устройства собирают самые разнообразные сведения о своих владельцах.

Угрозы информационной безопасности обретают совершенно новый облик. Это касается всех трех типов задач, которые должны решать средства защиты, включая угрозы доступности, целостности и конфиденциальности:

– нарушения работы системы и поддерживающей их инфраструктуры;

– подлоги и кража информации;

– опасности, которые таит в себе ненадежная защита конфиденциальной информации, будь то корпоративные данные или информация о частных лицах [4].

Казахстан вошел в список 50 стран по индексу киберготовности. В Казахстане киберпреступление стало равносильно обычному преступлению. Только, естественно, совершается оно в виртуальном пространстве, а потери и последствия, к сожалению, выявляются в реальности. Так, например, к кибератакам можно отнести любые незаконные действия в сети, начиная от взлома личной страницы в социальных сетях, заканчивая кражей больших данных. Чаще всего киберпреступники проникают в устройство, будь то мобильный телефон или компьютер, через специальные вирусные программы. Это легко сделать, если пользователь устанавливает нелицензионное программное обеспечение, скачивает файлы с подозрительных сайтов, куда уже занесен вредоносный вирус. Более профессиональные киберпреступники предпочитают нападать на крупные компании, красть оттуда базы данных клиентов или другую информацию, а затем использовать на свое усмотрение либо просят выкуп. Другие кибермошенники могут вымогать деньги с не опытных интернет пользователей, либо и вовсе умудряются без ведома владельца счета в банке или карты, переводить его деньги или тратить их на онлайн покупки. Так какими же методами и задачами кибербезопасности можно устранить такие виды преступлений.

Отметим, что кибербезопасность – это набор средств, стратегий, принципов обеспечения безопасности, их гарантий, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Основными задачами считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность.

В настоящее время, как отмечают эксперты, ежегодный экономический ущерб от непрофессионального использования и вредоносного воздействия на компьютерные системы составляет сотни миллиардов долларов. Выведение из строя компьютеров только на один час для средней компании обойдется в несколько десятков тысяч долларов, для крупной – в несколько миллионов.

Таким образом, по всему миру предпринимаются определенные меры по борьбе с киберпреступлениями.

Например, Нидерланды создали в рамках государственно-частного

партнерства Национальный центр кибербезопасности для увеличения обмена информацией и сотрудничества в стране.

Израиль предоставляет существенные налоговые льготы компаниям, которые размещают свои офисы в национальном киберпарке в Беер-Шеве, как механизм поощрения научно-исследовательского направления.

Россия разрабатывает средства защиты на случай киберкризиса. Это лишь немногочисленные примеры растущей зрелости государств в конкретных сферах кибербезопасности [5].

В настоящее время в Казахстане действует новое Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан, которое ведет работу по внедрению концепции «Киберщит» [1]. Это большой перечень мероприятий, направленный на безопасное использование информационно-коммуникационных технологий. Но все равно этих мер недостаточно для полной ликвидации данных проблем или непосредственно связанных с ними.

Полагаем, что большую пользу принесет изучение мирового опыта государственно-частного сотрудничества по кибербезопасности. В этих целях предлагаем создать в Республике Казахстан Национальный центр кибербезопасности с использованием механизма государственно-частного сотрудничества.

Таким образом, защита информации должна быть комплексным мероприятием. В совокупности организационные и технические мероприятия позволяют предотвратить утечку информации по техническим каналам, предотвратить несанкционированный доступ к защищаемым ресурсам, что, в свою очередь, обеспечивает целостность и доступность информации при ее обработке, передаче и хранении. Так же техническими мероприятиями могут быть выявлены специальные электронные устройства перехвата информации, установленные в технические средства и защищаемое помещение [6].

Базовые принципы кибербезопасности – то, что должен знать каждый пользователь Интернета.

Библиографические ссылки

1. Концепция кибербезопасности («Киберщит Казахстана») от 30 июня 2017 г. : Постановление Правительства Республики Казахстан от 30.06.2017 г. № 407.
2. Третья модернизация Казахстана: глобальная конкурентоспособность : Послание Президента Республики Казахстан от 31 января 2017 г.
3. Жатканбаева А. Е. К вопросу о системе обеспечения информационной безопасности Республики Казахстан. *Вопросы современной юриспруденции* : сб. ст. по матер. XIX Междунар. науч.-практ. конф. Ч. I. Новосибирск : СибАК, 2012 г.
4. Сачков И. Угрозы безопасности информационным технологиям. Москва, 2016.
5. Махмутов А. Концепция национальной безопасности Казахстана в контексте современных внешнеполитических реалий. *Внешнеполитические перспективы и новые концепты международной стратегии Казахстана* : материалы круглого стола. Институт мировой экономики и политики при Фонде Первого Президента Республики Казахстан – Лидера Нации, 2012 г. URL: // iwep.kz/index

Бобиль В. В.
завідувач кафедри обліку
і оподаткування Дніпровського
національного університету
залізничного транспорту
імені академіка В. Лазаряна,
доктор економічних наук, професор

ВПЛИВ КОРПОРАТИВНОГО УПРАВЛІННЯ НА ЕКОНОМІЧНУ БЕЗПЕКУ АКЦІОНЕРНОГО ТОВАРИСТВА

Корпоративне управління – це певний процес, який використовується для управління діяльністю підприємства з метою забезпечення високого рівня економічної безпеки і підвищення ринкової вартості акціонерного товариства.

Головні переваги ефективного корпоративного управління полягають у наступному:

1. Ріст довіри до акціонерного товариства. Ефективна система корпоративного управління є для зовнішніх стейкхолдерів доказом того, що фінансові ресурси підприємства використовуються в інтересах власників (акціонерів), а не топ-менеджерів.

2. Полегшення доступу до фінансового ринку. Використання міжнародних стандартів корпоративного управління та фінансового обліку відкриває вітчизняним підприємствам доступ до більш дешевого фінансування в західних фінансових інститутах, у тому числі банків.

3. Зменшення величини зовнішніх та внутрішніх ризиків. Пряма відповідальність топ-менеджерів перед акціонерами знижує рівень розбіжностей і протиріч і, таким чином, позитивно впливає на якість управлінських рішень у системі ризик-менеджменту акціонерного підприємства.

Зазначимо, що корпоративне управління пов`язано, в першу чергу, з вирішенням конфлікту інтересів, який у свою чергу впливає на рівень економічної безпеки акціонерного товариства.

Відомо, що конфлікт інтересів ґрунтується на певних протиріччях економічних інтересів внутрішніх та зовнішніх стейкхолдерів акціонерного товариства.

Основним органом, який забезпечує узгодження насамперед внутрішніх конфліктів інтересів, є наглядова рада акціонерного товариства, головне завдання якої – стежити за тим, щоб економічні та фінансові результати діяльності підприємства відповідали очікуванням акціонерів.

Законодавство України не встановлює терміни повноважень членів наглядової ради. Однак у світовій практиці членів наглядової ради прийнято

вибирати на два – три роки і їх неможливо відкликати із посади до закінчення цього терміну без вагомих причин. Практика свідчить, що доцільно не переобирати весь склад наглядової ради одночасно, а керуватися принципом ротації, тобто щорічно заміняти тільки частину від загального складу членів наглядової ради підприємства. Тоді досвідчені члени допомагають недавно обраним членам якнайшвидше ознайомитися з діяльністю і станом справ в акціонерному товаристві. В Україні, на відміну від міжнародної практики, члени наглядової ради можуть переобиратися необмежену кількість разів.

Крім того, чинне законодавство України не передбачає обов'язкової кількості членів наглядової ради (як правило, це залежить від кількості акціонерів і обсягу повноважень, що надаються Раді). Для підприємств з числом акціонерів понад тисячу осіб бажано обирати до складу наглядової ради не менше семи осіб, а якщо кількість акціонерів перевищує десять тисяч – то не менш дев'яти осіб. Як показує вітчизняна практика, наглядова рада, до складу якої входить більше дванадцяти осіб, є малоефективною [1].

Якщо член наглядової ради має економічну зацікавленість в угоді, у якої однієї зі сторін є акціонерне товариство, він зобов'язаний сповістити про свою зацікавленість інших членів наглядової ради і утриматися від голосування за даною угодою. Члени наглядової ради вважаються економічно зацікавленими, якщо вони:

а) є другою стороною в угоді;

б) є представниками другої сторони в угоді;

в) володіють акціями чи є посадовими особами іншої сторони;

г) є кредиторами іншої сторони;

д) мають близьких, родичів чи бізнес-партнерів, які потрапляють під одну з перерахованих вище категорій.

Таку угоду необхідно визнавати дійсною тільки тоді, коли за неї проголосує більшість незацікавлених членів наглядової ради.

Що стосується розв'язання конфлікту інтересів, то Голова наглядової ради має самостійно визначати порядок роботи з урегулювання таких конфліктів.

Основним завданням наглядової ради в процесі врегулювання конфліктів є пошук рішення, яке є законним, обґрунтованим і позитивно впливає на економічну безпеку акціонерного товариства.

Розповсюдженою є практика, коли основні акціонери безпосередньо призначають членів наглядової ради. Ці призначені особи зазвичай виконують свої наглядові та піклувальні обов'язки, керуючись виключно економічними інтересами цих основних акціонерів.

Отже, одним з інструментів поліпшення корпоративного управління (а отже і економічної безпеки підприємства) є збільшення кількості незалежних членів наглядової ради.

Незалежні члени наглядової ради повинні приділяти увагу таким

аспектам системи корпоративного управління, як робота органів управління, стан планування, розробка політики розвитку підприємства, управління персоналом, організаційна структура, системи контролю, системи управлінського інформування.

У підсумку зазначимо, що в умовах кризи та фінансової нестабільності мета корпоративного управління полягає в покращені рівня економічної безпеки акціонерного товариства.

Бібліографічні посилання

1. Дослідження корпоративного управління в банківському секторі України : Міжнародна фінансова корпорація. URL: http://www.ifc.org/ukraine/ucdp/.

Бочковий О. В., завідувач навчально-наукової лабораторії з дослідження проблем превентивної діяльності факультету підготовки фахівців для підрозділів превентивної діяльності Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, старший науковий співробітник, майор поліції

ЕФЕКТИВНІСТЬ ІНФОРМАТИЗАЦІЇ АНТИКОРУПЦІЙНОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

Україна, як і весь світ, є активним учасником загальної інформатизації та діджитилізації. Практично кожна сфера життя суспільства повністю чи частково перенесена до цифрової мережі.

Правоохоронна сфера не виняток. Проте якщо аналізувати антикорупційну діяльність в Україні, то створюється сумнівне враження щодо її ефективності, в основному за рахунок ігнорування сучасних досягнень у сфері інформаційних технологій під час виявлення та документування корупційних проявів.

Антикорупційна діяльність в Україні нагадує вислів з трактату Лао Цзи, який останнім часом став мемом та дещо змінив свою сутність: «у самурая немає цілі, тільки шлях».

Багато років протидія корупції є топовою темою для усіх політиків та службовців, прагнення у подоланні корупції висловлюються під час кожного створення чергового антикорупційного органу чи підрозділу. Проте якщо врахувати інформаційне супроводження антикорупційної діяльності, то її результативність наближається до нуля.

Водночас тема корупції надзвичайно важлива для України: її рівень сягнув загрозливих масштабів і безпосередньо впливає як на економіку країни, так і на її обороноздатність, адже через неї не можуть ефективно здійснювати свою діяльність головні державні інституції.

За об'єктивними оцінками, Україна на 117 місці у рейтингу міжнародної неурядової антикорупційної організації Transparency International за результатами 2020 року серед 180 країн, з показником у 33 бали. Поряд із нами у рейтингу Єгипет, африканська Есватіні (Свазіленд), Непал, Сьєрра-Леоне та Замбія – всі ці країни так само у CPI-2020 набрали по 33 бали. Для порівняння, найближчі сусіди Польща на 45-му місці, Словаччина на 60-му [1]. Корупція справляє нищівний вплив на усі без винятку сфери життя суспільства та зводить нанівець будь-які ініціативи чи спроби щодо поліпшення його життя.

Водночас, крім безпосереднього негативного впливу на ефективність діяльності державних інституцій, корупція здійснює опосередкований, не менш негативний, вплив на свідомість громадян, у тому числі й на молоде покоління, що зрештою негативно впливає на формування їх як свідомих громадян України.

Зокрема, сприйняття протидії корупції в Україні може бути результатом неефективної антикорупційної діяльності, яка справляє враження імітаційного процесу без мети досягнути результату. Україна достатньо активно висвітлює протидію корупції у медіапросторі. Чи не кожний ЗМІ, так само як і стрічка новин у фейсбуці, рясніє повідомленнями про викриття чергового хабарника, створення чергового антикорупційного органу чи видання нормативно-правового акта, який має сприяти протидії корупції. Тим часом ми бачимо неефективність антикорупційної політики, але вперто продовжуємо створювати контролюючі антикорупційні органи, куди призначаються ті самі службовці, які багато років обіймали посади в інших контролюючих чи правоохоронних органах, яких постійно звинувачують у корумпованості. Така собі замкнена система: службовці корумпованих структур влаштовуються на роботу до новостворених антикорупційних структур, щоб протидіяти корупції в тих структурах, в яких вони раніше працювали.

Відбувається своєрідна імітація антикорупційної діяльності. Часто виявлений журналістами чи громадськими активістами факт вчинення корупційних дій чи навіть підозра на них має великий суспільний резонанс, отримує відповідне реагування з боку державних органів. У кращому разі скомпрометованого чиновника звільняють, демонструючи рішучість та безкомпромісність до таких порушень [2, 3]. Проте фактично відбувається лише стримування резонансу шляхом зміни статусу таких осіб, адже до відповідальності нікого не притягують, конфіскації не відбувається, а вплив таких осіб на підконтрольні сфери залишається. Ба більше, через деякий час упійманий на корупції чиновник звертається до суду та поновлюється на

посаді, отримавши значні кошти компенсації за неправомірне звільнення. Тож останнім часом ЗМІ рясніють повідомленнями про виплати мільйонних компенсацій звільненим прокурорам за результатами переатестації.

Така сама ситуація й в інших державних структурах. Зокрема, під час «реформування» МВС заявлялось про зміну підходів та оновлення особового складу, хоча по факту відбулась міграція посадовців між службами. Колишні даішники перейшли на роботу до сервісних центрів МВС або до Укртрансбезпеки та зайняли там керівні посади.

За відсутності дієвих важелів контролю та відсутності автономної системи контролю корупції, зокрема інформаційно-аналітичної, що не є проблемою за сучасного інформаційно-технічного розвитку, запобігати корупційним проявам у діяльності правоохоронних органів надзвичайно проблематично, а часто навіть неможливо.

Незважаючи на усвідомлення важливості ефективної антикорупційної діяльності, не запроваджуються автоматизовані засоби фінансового контролю високопосадовців, а перевірка статків відбувається у ручному режимі, що є нонсенсом, з огляду на цифровізацію усіх сфер життя.

З іншого боку, ведеться активна протидія корупційним проявам найнижчого рівня серед рядових службовців та співробітників правоохоронних структур, що здебільшого є наслідками низького матеріально-фінансового забезпечення цих працівників, й повністю ігноруються багатомільйонні втрати державного бюджету. Адже, наприклад, керівники правоохоронних органів наділені правом підписувати документи на мільйони гривень, маючи при цьому заробітну платню у сотні разів меншу. Чи може потенційно виникнути бажання присвоїти частину таких коштів? Питання риторичне.

У Дніпропетровському державному університеті внутрішніх справ ми готуємо майбутніх правоохоронців, осіб, від яких залежить наше майбутнє та майбутнє наших поколінь. Сьогодні вдалося до мінімуму звести корупційні ризики під час вступу до закладів вищої освіти через запровадження ЗНО, що відкрило шлях у майбутнє для багатьох обдарованих хлопців та дівчат, яким раніше було б надзвичайно важко вступити на навчання без додаткового фінансового стимулювання з боку батьків і які самостійно обрали для себе шлях правоохоронця. Та дуже важко підтримувати їх мотивацію на фоні корупційних скандалів та неефективної антикорупційної політики в державі.

Підсумовуючи викладене, вважаємо за необхідне наголосити на тому, що поки що антикорупційні заходи, які застосовують державні органи України, неефективні й фактично імітують антикорупційну діяльність шляхом заповнення повідомленнями антикорупційного змісту медіапростір. Водночас важливим питанням мінімізації негативного впливу корупції є підвищення рівня соціального забезпечення співробітників правоохоронних органів та одночасного запровадження ефективної системи автоматизованого фінансового контролю їх діяльності та способу життя.

Бібліографічні посилання

1. Індекс сприйняття корупції – 2020. URL: https://ti-ukraine.org/research/indeks-spryjnyattya-koruptsiyi-2020/
2. Зеленский уволил главу СБУ в Николаевской области. *Украинская правда*. URL: https://www.pravda.com.ua/rus/news/2020/11/18/7273989/
3. После скандала с нарушением карантина уволен глава департамента Нацполиции. *Украинская правда*. URL: https://www.pravda.com.ua/rus/news/2020/11/18/7273985/

Бугорська М. Є.,
ад'юнкт Дніпропетровського
державного університету
внутрішніх справ, майор поліції

АКТУАЛЬНІ ПРОБЛЕМИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ДОМАШНЬОМУ НАСИЛЬСТВУ

В умовах сучасного життя глобальною проблемою суспільства та держави загалом є проблема домашнього насилля, насамперед, стосовно неповнолітніх. У нашому суспільстві домашнє насильство переважно не обговорюється та нерідко розглядається як необхідна форма дисципліни чи виховання. Тому інформація про випадки домашнього насильства залишається мінімальною, що призводить до збільшення кількості постраждалих, і як наслідок, відтворення жорстокості в суспільстві, оскільки колишні жертви доволі часто стають кривдниками.

За статистикою, яку оприлюднили під час голосування за Закон України «Про запобігання та протидію домашньому насильству», понад 3 мільйони дітей в Україні щороку спостерігають за актами насильства в сім'ї або є їх вимушеними учасниками, а майже 70 % жінок піддаються різним формам знущань і принижень. Щорічно приблизно 1 500 жінок помирають від рук власних чоловіків. Діти скривджених матерів у 6 разів схильніші до суїциду, а 50 % – до зловживань наркотичними засобами та психотропними речовинами. Майже 100 % вагітних жінок, які зазнали домашнього насильства, народили хворих дітей – переважно з неврозами, заїканням, енурезами, церебральним паралічем, порушенням психіки [1].

07 січня 2018 року набув чинності Закон України № 2229-VIII «Про запобігання та протидію домашньому насильству», яким визначено організаційно-правові засади запобігання та протидії домашньому насильству, основні напрями реалізації державної політики у сфері запобігання та протидії домашньому насильству, спрямовані на захист прав та інтересів осіб, які постраждали від такого насильства [2].

Відповідно до пункту 12 частини 1 статті 1 Закону України «Про запобігання та протидію домашньому насильству», протидія домашньому насильству – це система заходів, що здійснюються органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами та організаціями, а також громадянами України, іноземцями та особами без громадянства, які перебувають в Україні на законних підставах, та спрямовані на припинення домашнього насильства, надання допомоги та захисту постраждалій особі, відшкодування їй завданої шкоди, а також на належне розслідування випадків домашнього насильства, притягнення до відповідальності кривдників та зміну їхньої поведінки.

11 грудня 2018 року наказом Міністерства соціальної політики України № 1852, з метою забезпечення належного реагування на звернення громадян про факти торгівлі людьми, домашнього насильства, насильства за ознакою статі, насильства стосовно дітей, створено Державну установу «Кол-центр Міністерства соціальної політики України з питань протидії торгівлі людьми, запобігання та протидії домашньому насильству, насильству за ознакою статі та насильству стосовно дітей» (далі – Кол-центр) та затверджено Положення про ДУ Кол-центр, яке визначає його основні завдання, функції та права [3].

Кол-центр є неприбутковою державною бюджетною установою, створеною для забезпечення виконання завдань щодо належного реагування на звернення громадян про факти торгівлі людьми, домашнього насильства, насильства за ознакою статі та насильства стосовно дітей.

Звернення до Кол-центру приймаються за скороченими телефонними номерами 1578 (з питань протидії торгівлі людьми) та 1588 (з питань запобігання та протидії домашньому насильству, насильству за ознакою статі та насильству стосовно дітей) або на електронну адресу Кол-центру.

Потерпілі мають змогу скористатися чат-ботами в соціальних мережах МВС України #ДійПротиНасильства у месенджерах:

- телеграм: https://t.me/police_helpbot;
- вайбер: https://tinyurl.com/y8rgatt9.

Зокрема, чат-бот може допомогти викликати поліцію або швидку, або переадресувати на спеціалістів безоплатної правової допомоги.

Крім того, статтею 16 Закону України «Про запобігання та протидію домашньому насильству» запроваджено ведення Єдиного державного реєстру випадків домашнього насильства та насильства за ознакою статі – автоматизованої інформаційно-телекомунікаційної системи, призначеної для збирання, реєстрації, накопичення, зберігання, адаптування, зміни, поновлення, використання, поширення (розповсюдження, реалізації, передачі), знеособлення і знищення визначених цим Законом даних про випадки домашнього насильства та насильства за ознакою статі (далі – Реєстр).

Формування Реєстру здійснюється окремо за кожним випадком

домашнього насильства, насильства за ознакою статі шляхом внесення до нього відповідної інформації.

20 березня 2019 року Кабінет Міністрів України затвердив Порядок формування, ведення та доступу до Єдиного державного реєстру випадків домашнього насильства та насильства за ознакою статті, який, на жаль, на цей час так і не створено [4].

Підсумовуючи, можна зазначити, що домашнє насильство в Україні можна здолати тільки об'єднавши намагання суб'єктів державної влади, органів місцевого самоврядування та суспільства, при цьому шляхом створення в суспільстві нульової толерантності до насильницької моделі поведінки, не нехтуючи використанням сучасних інформаційних технологій. Тільки так можна запобігти та протидіяти домашньому насиллю, а також надати реальну допомогу громадянам, які опинилися в складних, конфліктних та небезпечних життєвих ситуаціях.

Бібліографчні посилання

1. Методичні рекомендації щодо запобігання та протидії насильству : лист Міністерства освіти і науки України від 18.05.2018 р. № v5480729-18. URL: https://zakon.rada.gov.ua/rada/show/v5480729-18#top.
2. Про запобігання та протидію домашньому насильству : Закон України від 07.12.2017 р. № 2229-19. URL: https://zakon.rada.gov.ua/laws/show/2229-19#Text.
3. Про утворення Державної установи «Кол-центр Міністерства соціальної політики України з питань протидії торгівлі людьми, запобігання та протидії домашньому насильству, насильству за ознакою статі та насильству стосовно дітей» : наказ Міністерства соціальної політики України від 11.12.2018 р. № 1852. URL: https://zakon.rada.gov.ua/laws/show/z1458-18#Text
4. Про затвердження Порядку формування, ведення та доступу до Єдиного державного реєстру випадків домашнього насильства та насильства за ознакою статі : Постанова Кабінету Міністрів України від 20.03.2019 р. № 234. URL: https://zakon.rada.gov.ua/laws/show/234-2019-%D0%BF#Text.

Бурбело О. А.,
доктор економічних наук, професор
Бурбело С. О.,
(Інститут економіко-правових досліджень НАН України)

ІНФОРМАЦІЙНА БЕЗПЕКА СУБ'ЄКТІВ БІЗНЕСУ

Сучасній світовій економіці притаманне зростання ризиків у господарській діяльності. Все більшого значення в забезпеченні безпеки суб'єктів бізнесу набуває правова, економічна, політична і соціальна інформація [1, с. 220]. При цьому проблема захисту інформації не є новою.

Вона з'явилася ще задовго до появи комп'ютерів. Стрімке вдосконалювання комп'ютерних технологій позначилося й на принципах побудови захисту інформації.

Принципова особливість сучасної ситуації полягає в тому, що переважна більшість інформації міститься та передається завдяки електронним системам та мережам, а тому найважливішим завданням стає захист інформації саме в таких системах й мережах.

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

Вищевказане доводить необхідність перегляду наявних принципів та підходів до захисту інформації загалом та суб'єктів бізнесу зокрема.

Під інформаційною безпекою будемо розуміти захищеність інформаційних активів як частини інфраструктури бізнес-процесів, від випадкових або навмисних впливів власного або штучного характеру. Останні можуть призвести до нанесення шкоди власникам або користувачам інформаційних активів в бізнес-системі як частини підтримуючої інфраструктури.

Забезпечення інформаційної безпеки має комплексний характер і передбачає необхідність поєднання законодавчих, організаційних та програмно-технічних заходів.

Одним з основних завдань систем інформаційної безпеки суб'єктів господарської діяльності є сервісний супровід бізнес-процесів. Будь-яка використана в бізнесі технічна система, будучи важливим елементом інфраструктури, повинна надавати бізнесу певний тип сервісу. Інформаційна система надає бізнесу інформаційний сервіс, але й сама потребує підтримки та захисту. Сервіс полягає в наданні бізнесу необхідної інформації потрібної якості, в потрібний час і в потрібному місці, тобто, зрештою, інформації для управління самим бізнесом.

По суті, інформація в такому розумінні стає одним з головних елементів інформаційної інфраструктури .

Ще одним бізнес-завданням системи інформаційної безпеки (ІБ) є забезпечення гарантій достовірності інформації, або, інакше кажучи, гарантій довірливості інформаційного сервісу.

У практичному ж плані інформаційна безпека наявна тільки у взаємозв'язку із суб'єктом інформаційного середовища, саме він диктує показники такої безпеки. Це стосується не тільки конкретних суб'єктів, але й особистості, суспільства та держави.

Водночас інформаційні потреби різних суб'єктів не однакові й відсутність можливості отримання необхідної інформації для будь-якого з них може мати негативні наслідки. Вони можуть мати різний характер, їх

важкість залежить від складу неотриманої інформації.

Для задоволення потреб споживачів в інформації вона повинна відповідати певним вимогам. Передусім, інформація повинна бути відносно повною, оскільки абсолютно повної інформації жоден суб'єкт мати не може. Повнота інформації характеризується її достатністю для ухвалення рішення. Також інформація повинна бути достовірною, бо наслідками користування недостовірною інформацією є ухвалення неправильних (деколи катастрофічних) рішень. Крім того, інформація повинна бути своєчасною (актуальною), оскільки необхідні рішення ефективні лише тоді, коли вони ухвалюються вчасно [2, с. 34]. Ухваленню неправильних рішень може сприяти наявність шкідливої, небезпечної для суб'єкта інформації, яка найчастіше цілеспрямовано нав'язується. Це вимагає забезпечення захисту суб'єктів інформаційних відносин від негативного інформаційного впливу, що є ще однією складовою інформаційної безпеки [3, с. 96].

На практиці застосовуються різні способи забезпечення захисту ІТ-систем підприємств, які можна об'єднати в дві групи: організаційні та технічні. Організаційні заходи управління безпекою доцільно реалізовувати за допомогою комплексу заходів, що формується підприємством. У діяльності підприємств його прийнято називати «Політикою інформаційної безпеки організації». Друга група заходів управління (технічні) являє собою налаштування системи і зовнішні контрзаходи (подібно шифруванню). Їх рекомендується використовувати з метою забезпечення аутентифікації, санкціонування, конфіденційності, цілісності, доступності та інших послуг безпеки. Ця сфера бурхливо розвивається, внаслідок чого з'являються нові стандарти і нормативні документи [4, 6].

Після початкового розміщення заходів управління і контрзаходів організація повинна вжити заходів щодо забезпечення їх довгострокового функціонування та підтримки. Інакше, з плином часу, з появою нових уразливостей безпека системи ослабне. Добре діюча програма забезпечення безпеки містить процеси і процедури підтримки. Вони забезпечують наявність необхідних заходів управління та їх постійне оновлення. Захисні заходи апаратних систем у середовищі ІТ є вирішальними для цілісності інформаційних активів. Вичерпний набір заходів цього типу можна знайти в каталогах відповідних стандартів [ISO/IEC 27001:2005]. Каталоги фактично є довідниками для розробників і менеджерів систем управління інформаційною безпекою [7, с. 4].

Конкретні рішення в галузі управління інформаційною безпекою ІТ-компанії почали розробляти з початку 2000-х, коли хакерство поступово перетворювалось на прибутковий бізнес. Наслідком цього явища став величезний збиток, що отримували держави і великі міжнародні корпорації. Протихакерські рішення об'єднували в собі антивірусні програми й утиліти, що займаються моніторингом системних журналів.

Для розробки нових стандартів управління інформаційною безпекою в

США було створено спеціалізоване агентство з кібербезпеки [4].

Комплекс заходів щодо забезпечення інформаційної безпеки на підприємстві, як правило, – це програмні продукти різних типів [8]. Вони містять функції і програмні модулі, які вбудовані безпосередньо в програмне забезпечення (ПЗ). Ними створюються умови для зберігання, обробки і передачі інформації. Сюди відносять операційні системи, системи управління базами даних, системи електронної пошти, MRP / ERP-системи. Сучасні програмні продукти чітко закріплюють права тих чи інших користувачів, регламентують доступ до інформації, розподіляють використання системних ресурсів. Програмні продукти містять і інші обмеження, що забезпечують дотримання встановлених вимог і реалізацію політики інформаційної безпеки на підприємстві.

На практиці застосовується окремий клас спеціальних програмних продуктів, призначених тільки для підтримки процесів розробки політик безпеки і управління ними на організаційному рівні. Основними функціями таких програм є довідково-інформаційна підтримка, допомога під час обробки управлінської інформації, оцінцки ризиків і підготовки необхідних документів [9].

В практиці управління інформаційною безпекою збірники (довідники) містять такі типові документи:

– зразки політик безпеки різних рівнів для підприємств, що функціонують в різних сферах діяльності і ставлять різні вимоги до рівня захищеності інформації;

– зразки (шаблони, бланки) документів, що використовуються в процесах захисту інформації (зобов’язань про нерозголошення інформації, звітів про стан інформаційної безпеки тощо);

– зразки розділів різних договорів (контрактів з різними контрагентами або трудових договорів з працівниками підприємства), що містять вимоги до забезпечення інформаційної безпеки.

Такі електронні довідники можуть випускатися як на основі оригінальних методичних розробок, так і на основі загальновизнаних стандартів (таких як ISO 17799) з метою сприяння проходженню сертифікації на відповідність цим стандартам. Електронні довідники, що випускаються, можуть бути доповнені підручниками, текстами стандартів і іншими методичними матеріалами, виданих у вигляді брошур.

Одним з найбільш повних є електронний довідник «Information Security Policies Made Easy» американської компанії Information Shield, Inc. Дев’ята версія цього довідника містить більше 1 360 зразків і шаблонів різних документів, створених з урахуванням вимог стандарту ISO 17799 і належать до всіх аспектів інформаційної безпеки підприємства.

Концепції більш розвинених програмних продуктів, заснованих на інтерактивному інтелектуальному аналізі та вдосконаленні політики безпеки, припускають, що користувач (менеджер) спочатку внесе всю необхідну

інформацію про стан інформаційної безпеки на своєму підприємстві (відповість на поставлені програмою запитання), а потім отримає детальний звіт про стан інформаційної безпеки, опис рівня відповідності вимогам стандартів, рекомендації щодо вдосконалення чинної політики безпеки та інші звіти. Отже, програмне забезпечення дозволяє пов'язувати в єдиний процес процедури первинного збору інформації про підприємство, аналізу фактичного рівня організаційного забезпечення інформаційної безпеки, розробки документації, адаптації методів управління до певних вимог (наприклад, стандарту ISO 17799) і проведення аудитів інформаційної безпеки.

Одним з таких програмних продуктів є система «COBRA», яку поставляє британська компанія C & A Systems Security Ltd. у двох варіантах: скорочена версія містить у собі модуль «COBRA ISO17799 Consultant», а повна версія, крім того, містить додаткові засоби аналізу ризиків («Risk Consultant») і спеціальний модуль, що дозволяє створювати і модифікувати власні бази знань і набори питань для дослідження стану інформаційної безпеки («Module Manager»). Базовий модуль цієї системи призначений для оцінки того, якою мірою робота щодо захисту інформаційної безпеки відповідає вимогам стандарту ISO 17799. На першому етапі його використання вступає в роботу «Question Module» – Модуль відповідей на запитання, який містить набір запитань, розділених на групи відповідно до структури стандарту ISO 17799: безпека персоналу, політика безпеки, управління доступом, планування безперервної роботи тощо [7].

При цьому формування режиму інформаційної безпеки є комплексною проблемою. Серед засобів для її вирішення, як правило, виділяють п'ять рівнів. Перший – законодавчий (закони, нормативні акти, стандарти тощо); другий – морально-етичний (всілякі норми поведінки, недотримання яких призводить до падіння престижу конкретної людини або цілої організації); третій – адміністративний (дії загального характеру з боку керівництва організації або установи); четвертий – фізичний (механічні, електро- і електронно-механічні та інші перешкоди на можливих шляхах проникнення потенційних порушників); до п'ятого рівня заходів відносять використання електронних пристроїв та спеціальних програм захисту інформації.

Поряд з цим всі структурні елементи інформаційної системи (ІС) і системи захисту на всіх етапах їх життєвого циклу охоплюють організаційні заходи. При цьому вони відіграють двояку роль в механізмі захисту. З одного боку, ці заходи дозволяють повністю або частково перекривати велику частину каналів витоку інформації, а з іншого – забезпечують ефективність об'єднання, узгодженість всіх використовуваних в ІС засобів в цілісному механізмі захисту.

Скоординоване застосування всіх заходів, спрямованих на протидію загрозам безпеці з метою зведення до мінімуму можливої шкоди, утворює в кінцевому підсумку систему захисту.

Фахівці, що мають стосунок до системи захисту, повинні повністю уявляти собі принципи її функціонування і, в разі виникнення скрутних ситуацій, адекватно на них реагувати. Під захистом повинна знаходитися вся система обробки інформації.

Розробники системи захисту не повинні бути в числі тих, кого ця система буде контролювати. Система захисту повинна надавати докази коректності своєї роботи.

Особи, що займаються забезпеченням інформаційної безпеки, повинні нести особисту відповідальність, а найбільш важливі і критичні рішення повинні ухвалюватися людиною.

Отже, результати виконаних досліджень свідчать, що інформація – це один з важливих ресурсів у забезпеченні безпечної діяльності підприємства. Втрата конфіденційної інформації призводить до моральної чи матеріальної шкоди. Умови, що сприяють неправомірному оволодінню конфіденційною інформацією, зводяться до її розголошення, витоку і несанкціонованого доступу до її джерел. У сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації як важливою складовою системи інформаційної безпеки суб'єкта господарської діяльності. Система захисту повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не тільки в повсякденних умовах, але і в критичних ситуаціях.

Бібліографічні посилання

1. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ. *Актуальні проблеми економіки*. 2006. № 10. С. 220–225.
2. Панченко О. А., Панченко Л. В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика*. 2015. № 2 (46). С. 32–38.
3. Сігова В. Актуальні питання забезпечення інформаційної безпеки підприємства : тези доп. студентів і магістрантів на науковій конф. 14 квітня 2016 року. Кіровоград : КНТУ, 2016. С. 96–99.
4. Информационная безопасность. URL: http://protect.htmlweb.ru
5. Невойт Я. В. Метод оцінювання стану захищеності інформаційних ресурсів на основі дослідження джерел загроз інформаційній безпеці : дис. … канд. техн. наук. ДУТ, Київ, 2016. URL: http://www.dut.edu.ua/uloads/ p_1539_26349739.pdf.
6. Управление информационной безопасностью. URL: https://ru.wikipedia.org/wiki/ финансы.
7. Анисимов Александр. Менеджмент информационной безопасности на уровне предприятия: основные направления и структура политики безопасности : лекция. НОУ ИНТУИТ. URL: https://www.intuit.ru/studies/courses/563/419/lecture/ 9585+&cd=2&hl=ru&ct=clnk
8. Силаенков А. Н. Проектирование системы информационной безопасности : учеб. пособ. Омск : Изд-во ОмГТУ, 2009. 128 с.

Варяниченко О. В., доцент кафедри менеджменту, кандидат економічних наук, доцент
Госалов Ю. С., студент 2-го курсу магістратури факультету менеджменту

(Національний технічний університет «Дніпровська політехніка»)

ФОРМУВАННЯ УПРАВЛІНСЬКИХ РІШЕНЬ ЩОДО ЕКОНОМІЧНОЇ БЕЗПЕКИ АТ «НІКОПОЛЬСЬКИЙ ЗАВОД ФЕРОСПЛАВІВ» НА ОСНОВІ SWOT-АНАЛІЗУ

Економічна криза, пандемія й відповідний спад промислового виробництва вплинули на погіршення результатів діяльності й економічної небезпеки багато підприємств, які не змогли чітко виділити головні стратегічні завдання, визначити пріоритети, мобілізувати потенціал для підтримання позицій на ринках.

АТ «Нікопольський завод феросплавів» (АТ «НЗФ») – найбільше в Україні підприємство з виробництва силіко- і феромарганцю, здіснює активну зовнішньоекономічну діяльність, має диверсифіковані ринки для власної економічної безпеки [1]. Зважаючи на важливість цього комплексу для країни, звичайно потрібна розробка управлінських рішень для підвищення ефективності його діяльності.

Економічна безпека має досить суттєві перспективи для впровадження на кожному підприємстві, адже саме вона здатна попередити загрози, створити превентивні заходи щодо вчасного реагування на них [2].

Надійним підґрунтям для формулювання основних положень стратегічного розвитку підприємств та заходів щодо їх реалізації є метод SWOT-аналізу. Цей метод є загальною схемою, яку щоразу необхідно пристосовувати до конкретних умов та до вирішення певних завдань. Найчастіше такими завданнями є формування комплексу дій щодо перетворення слабких сторін підприємства на переваги, загроз на можливості, а також розвитку сильних позицій [3]. Результати SWOT-аналізу для АТ «НЗФ» розглянуто нижче.

Потенційні внутрішні сильні сторони АТ «НЗФ»:

– підприємство працює з 1966 року, має великий досвід роботи ринку, високий імідж як надійний партнер, що випускає високоякісну продукцію, реалізація продукції відбувається як самостійно, так і через посередників;

– злагоджена команда працівників кількістю 5 691 осіб;

– товар на стадії «зрілості» життєвого циклу, продукція відповідає стандартам ДСТУ 3547-97, ДСТУ 35-48-97, сертифікована система менеджменту якості відповідно до ISO 9001:2015, є сертифікат з менеджменту

навколишнього середовища ISO 14001:2015, продукція має порівняні конкурентні переваги за якістю;

– впровадження нових технологій (власні розробки та з залученням фахівців НМетАУ, УкрНДІспецсталь, Механобрчермет, ІЕЗ ім. Є. О. Патона тощо);

– використання імпортної марганцевої сировини австралійського походження, ПАР, Бразилії, Габону та Гани, вітчизняної сировини Марганецького та Покровського ГЗК, контракти на поставку сировини укладаються напряму з постачальниками.

Потенційні внутрішні слабкості АТ «НЗФ»:

– не досконала формалізація довгострокових цілей та стратегії компанії;

– виробничий та збутовий потенціал підприємства не відповідає тенденціям зміни ринку, вузька номенклатура продукції (феросилікомарганець, феромарганець), яка не має конкурентних переваг за ціною;

– низька конкурентоспроможність підприємства через великі витрати на електроенергію та залізничне транспортування, низька рентабельність – за останні 10 років упродовж 6 років було збитковим.

Потенційні можливості зовнішнього середовища: можливість диверсифікації ринків збуту продукції, застосування стратегії «послідовника», інновації в галузі виробництва феросплавів, кредитування ЕБРР.

Потенційні загрози зовнішнього середовища:

– нестабільна політична ситуація та зовнішня політика України, часті та непередбачувані зміни в законодавстві;

– тенденція повільного зростання ВВП та добробуту населення, прогноз зростання ВВП на 2021 рік – 3,8 % та 4 % на 2022–2023 рр., прогноз рівня інфляції на 2021 рік – 9,6 %, слабка платоспроможність населення;

– постійне зменшення кількості населення в Україні;

– нестабільне співвідношення гривні до іноземних валют;

– високі ціни на електроенергію та висока вірогідність їх подальшого зростання, збільшення вартості залізничного тарифу на транспортування товару;

– не визначено тенденції розвитку ринку феросплавів, відкриття 3 нових феросплавних заводів в Малайзії, на ринках Росії, Білорусі та Казахстану запроваджено загороджувальне мито 26,3 %, що унеможливлює експорт в ці країни, відсутність зони вільної торгівлі з Туреччиною;

– більш низькі ціни на аналогічну продукцію в Південній Кореї, Малайзії, Індії, ЄС, Бразилії, ПАР;

– пандемія COVID.

За результатами виконаного SWOT-аналізу для АТ «НЗФ» можна сформувати стратегічну мету: забезпечення довгострокового, орієнтованого на отримання доходу, росту компанії за рахунок управління витратами, впровадження інноваційних технологій та розширення закордонних ринків

збуту. Рекомендується такий стратегічний комплекс:

- глобальна стратегія – інтернаціоналізації;
- базова стратегія – стратегія цінового лідерства через удосконалення технологічного процесу виробництва та відповідного зниження витрат на електроенергію;
- стратегія росту – стратегія розвитку ринку (розвиток продажів наявних товарів на нових ринках, освоєння ринку Норвегії);
- маркетингова конкурентна стратегія – стратегія послідовника та підвищення ринкової частки підприємства внаслідок виходу на новий закордонний ринок збуту Норвегії та наслідування елементів стратегії лідера.

Цей приклад демонструє, що SWOT-аналіз є інструментом, який може застосовуватись підприємством для ринкового аналізу, вибору стратегії розвитку для його економічної безпеки.

Бібліографічні посилання

1. Офіційний сайт АТ «Нікопольський завод феросплавів». URL: http://nzf.com.ua/
2. Зайченко К. С., Діма Н. І. Економічна безпека підприємства: сутність та роль. URL: http://www.economy.nayka.com.ua/pdf/5_2021/92.pdf
3. Носонова Л. В. Застосування SWOT-аналізу для визначення конкурентоспроможності АТ «Сумський завод «Насосенергомаш». URL: http://global-national.in.ua/archive/4-2015/107.pdf

Варяниченко-Гутовская А. О.,
адвокат при Окружной Адвокатской Палате в Варшаве. Юрист in-house (Польша)

ВЛИЯНИЕ ФИНАНСОВЫХ РИСКОВ НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Финансовая деятельность предприятия связана со многими операциями, соглашениями и несет за собой не только возможность развития, но и значительные финансовые риски. Прибыль, как материальный показатель эффективности экономической деятельности предприятия, зависит от многих внутренних и внешних факторов. Именно поэтому для обеспечения финансовой стабильности на предприятии необходимо разрабатывать концепцию безопасности и стратегию управления с учетом рисков, сопровождающих деятельность предприятия.

Риски, связанные с возможностью возникновения неожиданных материальных затрат, снижением или отсутствием прибыли, потерей части капиталовложений для предприятия классифицируются как финансовые риски. Эти риски возникают на любом этапе хозяйственной деятельности, а

также в результате сотрудничества с другими предприятиями.

Причины формирования финансовых рисков разнообразны и они могут возникнуть на любом этапе хозяйственной деятельности предприятия. К основным внешним причинам формирования финансовых рисков можно отнести следующие: слаборазвитую и нестабильную экономику страны; экономический кризис; инфляцию; повышение уровня конкурентной борьбы; снижение цен на мировом рынке; политические факторы и др. Все эти причины имеют внешнее для предприятия происхождение и, поэтому, предприятие их спрогнозировать и контролировать не в состоянии. К внутренним причинам формирования финансовых рисков можно отнести: повышение затрат на производство на предприятии, низкий уровень управления, отсутствие планирования, неудовлетворительную финансовую политику предприятия и др [1].

Для регуляции и нивелирования всех финансовых рисков должна быть налажена внутренняя финансовая политика, которая зависит только от внутренних факторов организации предприятия. Целенаправленное использование ресурсов предприятия, согласование процесса производства и реализации, выполнение актуальных задач в совокупности и представляет собой финансовую политику компании.

На любом этапе выявления потенциальных рисков очень важно принять соответствующие меры обеспечения финансовой безопасности. Концепция финансовой безопасности предприятия должна основываться на:

– обеспечении высокой степени согласования и гармонизации финансовых интересов предприятия с интересами окружающей среды и интересами его персонала;

– наличии на предприятии устойчивой к угрозам финансовой системы, которая способна обеспечивать реализацию финансовых интересов, миссии и задач;

– сбалансированности и комплексности финансовых инструментов и технологий, используемых на предприятии;

– росте постоянства и динамичности развития финансовой системы предприятия.

Итак, финансовые риски могут возникать во многих сферах финансовой деятельности предприятия. И независимо от того, какие риски по состоянию и по времени возникновения – они представляют угрозу и приносят ущерб предприятию в целом. Следовательно, для продуктивной работы и получения максимальной прибыли руководству необходимо разрабатывать стратегию устранения и противодействия рискам методами идентификации, профилактики, оценки и страхования. Для выявления и устранения рисков необходима соответствующая стратегия и тактика в менеджменте предприятия, а также разработанная концепция безопасности предприятия.

Библиографические ссылки

1. Какушкина Г. Р. Финансовые риски и методы управления ими в условиях. URL: http://ieay.ru/nauka-v-ieau/vestnik-ieau/publikacii-zhurnala-vestnik-ieau/vestnik-ieau-n-13/finansovye-riski-i-metody-upravleniya-imi-v-usloviyah-nestabilnoj-makroekonomicheskoj-sredy-predpriyatiya/?wb=off.

Вишня В. Б., професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, доктор технічних наук, професор, почесний професор ДДУВС, заслужений діяч науки і техніки України

ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ЗАСОБАМИ ПАТЕНТНОЇ ДІЯЛЬНОСТІ

У межах діяльності наукових шкіл Дніпропетровського державного університету внутрішніх справ науково-педагогічний колектив постійно здійснює патентну діяльність. Така діяльність є однією із складних напрямів науково-дослідної роботи. Водночас вона є одним із пріоритетів у межах ліцензійних вимог до навчального закладу Міністерства внутрішніх справ України.

За останні роки ця діяльність значно активізувалась. Якщо аналізувати результати і показники патентного фонду університету, то маємо станом на 2006 рік – 1 патент, на 2021 рік – 18 патентів.

Першочергова роль у патентній діяльності належить кафедрі економічної та інформаційної безпеки. Двічі її патентна робота у 2019 році та 2020 році відмічалася першими місцями серед інших ЗВО на конкурсі МВС України. Такі значні результати патентної роботи в університеті (табл. 1), свідчать про те, що на кафедрі створені умови для нормальної роботи як окремих фахівців, так і творчих колективів.

Особливістю патентної роботи в ДДУВС є те, що в університеті виділені напрями (і відповідно організовані авторські колективи під ці напрями) актуальної діяльності боротьби правоохоронних органів. Серед цих напрямів використовуємо:

а) боротьба з крадіжками вантажів на залізниці на зупинках та у русі потягу (куратор – професор В. Б. Вишня);

б) боротьба з несанкціонованим підключенням споживачів до електромережі (куратор – доцент В. О. Мирошниченко);

в) удосконалення технічних рішень в діяльності патрульної служби Національної поліції (куратор – професор Е. В. Рижков).

При цьому куратор напряму підбирає собі співавторів для підготовки заявки.

Відмінною особливістю патентної діяльності в нашому університеті є те, що усі патенти, отримані кафедрою, є власністю університету, тоді як в інших ЗВО автори переважно залишають за собою право на власність.

Таблиця 1

Патенти ДДУВС

№ з/п	**Назва патенту**	**Номер патенту**	**ПІБ автора**	**Дата**
1	Пристрій контролю обліку електроенергії	12568	Шкрабець Федір Павлович; Вишня Володимир Борисович; Мирошниченко Володимир Олексійович; Красовський Павло Юрійович	15.02.2006
2	Пристрій охоронної сигналізації в електричних мережах	70695	Шкрабець Федір Павлович; Мирошниченко Володимир Олексійович; Вишня Володимир Борисович; Остапчук Олександр Володимирович	15.09.2006
3	Пристрій контролю обліку електроенергії	79846	Шкрабець Федір Павлович; Вишня Володимир Борисович; Мирошниченко Володимир Олексійович; Красовський Павло Юрійович	25.07.2007
4	Пристрій контролю споживання електроенергії на ділянці мережі	24136	Шкрабець Федір Павлович; Вишня Володимир Борисович; Мирошниченко Володимир Олексійович; Красовський Павло Юрійович	10.12.2007
5	Радіоканальна система контролю схоронності вантажоперевезень на залізниці	28327	Вишня Володимир Борисович; Вишня Олег Володимирович;	10.12.2007
6	Пристрій контролю споживання електроенергії на ділянці мережі	84472	Шкрабець Федір Павлович; Вишня Володимир Борисович; Мирошниченко Володимир Олексійович; Красовський Павло Юрійович	27.10.2008
7	Пристрій контролю споживання електроенергії	48802	Вишня Володимир Борисович; Мирошниченко Володимир Олексійович;	12.04.2010
8	Пристрій контролю споживання електроенергії у розгалужених мережах	74647	Мирошниченко Володимир Олексійович; Вишня Володимир Борисович; Строжко Сергій Валерійович	12.11.2012
9	Система управління нарядами мобільної	118449	Вишня Володимир Борисович; Глуховеря Віталій Андрійович;	10.08.2017

№ з/п	Назва патенту	Номер патенту	ПІБ автора	Дата
	патрульної служби		Золотоноша Олег Вікторович; Рижков Едуард Володимирович	
10	Пристрій охоронної сигналізації в електричних мережах	119064	Вишня Володимир Борисович; Мирошниченко Володимир Олексійович;	11.09.2017
11	Пристрій охоронної сигналізації в електричних мережах	116869	Вишня Володимир Борисович; Мирошниченко Володимир Олексійович;	10.05.2018
12	Система управління нарядами мобільної патрульної служби	125582	Вишня Володимир Борисович; Фоменко Андрій Євгенович	10.05.2018
13	Пристрій для захисту електричної мережі від несанкціонованого підключення споживачів	134829	Вишня Володимир Борисович; Мирошниченко Володимир Олексійович; Фоменко Андрій Євгенович	10.06.2019
14	Пристрій радіолокаційного розпізнавання об’єктів	139240	Мирошниченко Володимир Олексійович; Фоменко Андрій Євгенович; Рижков Едуард Володимирович; Гавриш Олег Степанович; Махницький Олександр Васильович	26.12.2019
15	Система управління нарядами мобільної патрульної служби	145759	Махницький Олександр Васильович; Фоменко Андрій Євгенович; Вишня Володимир Борисович	07.01.2021
16	Пристрій визначення ділянки електричної мережі з несанкціонованим підключенням електроприймачів	146837	Фоменко Андрій Євгенович; Вишня Володимир Борисович; Мирошниченко Володимир Олексійович; Гребенюк Андрій Миколайович; Прокопов Сергій Олександрович	25.03.2021
17	Навчально-тренувальний комплекс для підготовки фахівців правоохоронної галузі	146878	Фоменко Андрій Євгенович; Вишня Володимир Борисович; Собакарь Андрій Олексійович; Мирошниченко Володимир Олексійович; Конанець Віта Петрівна; Щербина Олександр Вікторович; Лазарев Владислав Олександрович; Неклеса Олександр Вікторович	01.04.2021
18	Навчально-тренувальний комплекс для підготовки фахівців ювенальної превенції	147801	Фоменко Андрій Євгенович; Вишня Володимир Борисович; Бахчев Костянтин Вікторович; Мирошниченко Володимир Олексійович; Рижкова Світлана Анатоліївна	17.06.2021

Як бачимо, велика кількість патентів призначена забезпечити захист економічних відносин в державі щодо конкретних напрямів.

Необхідно відмітити, що у нас вперше розроблені два патенти № 146881, № 146801, які вирішують завдання функціонування спеціалізованих навчальних полігонів, серед яких економічний полігон, призначенням якого є підготовка відповідних фахівців щодо протидії злочинам економічного спрямування.

Усі отримані нами результати є наслідком активної роботи таких співробітників університету: А. Є. Фоменко, ректор університету, д-р юрид. наук, доцент, заслужений юрист України; В. Б. Вишня, професор кафедри Е та ІБ, д-р техн. наук, професор, заслужений діяч науки та техніки України; В. О. Мирошниченко, професор кафедри Е та ІБ, канд. техн. наук, доцент; Е. В. Рижков, завідувач кафедри Е та ІТ, канд. юрид. наук, професор; О. О. Косиченко, доцент кафедри Е та ІБ, канд. техн. наук, доцент; А. М. Гребенюк, доцент кафедри Е та ІБ, канд. техн. наук, доцент; С. О. Прокопов, старший викладач кафедри Е та ІТ; Л. В. Можечук, старший науковий співробітник відділу організації наукової роботи канд. юрид. наук; М. М. Вакуліч, керівник відділу організації наукової роботи, канд. екон. наук, доцент; К. В. Бахчев, декан факультету ПФППД, канд. юрид. наук; В. О. Лазарев, декан факультету ПФПСР, канд. юрид. наук.

У 2021 році від університету подано на розгляд ще 3 заявки на патенти. Сподіваємося, що рішення щодо їх видачі також буде позитивним.

Головін Д. В.,
аспірант кафедри криміналістики та психології Одеського державного університету внутрішніх справ

ОСОБЛИВОСТІ ТА ПОРЯДОК ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ У ПРОЦЕСІ ДОКАЗУВАННЯ ЗЛОЧИНІВ У СФЕРІ ОБІГУ НАРКОТИЧНИХ ЗАСОБІВ

Сьогодні в життя людей в усьому світі широко увійшли інформаційно-телекомунікаційні технології. За останні роки Україна робить великі кроки щодо інформатизації населення. Під час такого зростання ІТ-індустрії закономірно, що набуває нових форм злочинна діяльність. Особливо це спостерігається під час доказування злочинів у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, оскільки здебільшого така діяльність перейшла в онлайн-форму та органи досудового розслідування стикаються з неабиякими труднощами під час збору доказової бази: злочинці використовують анонімні месенджери для зв’язку;

криптовалюти для розрахунку та здебільшого фізично не перебувають в країні, в якій ведуть протиправну діяльність.

Актуалізується зазначене питання ще тим, що приклади використання електронних документів як засобів доказування в конкретних справах свідчать про існування різних підходів до розуміння процесуально-правової сутності електронних документів, особливостей їх збирання, подання та дослідження.

Розглянемо поняття «електронний документ» та «електронний доказ».

Слово документ (лат. documentum зразок, доказ, свідоцтво) походить від дієслова docere вчити, навчати. Документ – це базова теоретична конструкція, яка стосується всього, що може бути збережене або подане, щоб служити як доказ для певної мети [1].

Згідно зі ст. 99 КПК України документом є спеціально створений із метою збереження інформації матеріальний об’єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомостей, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. Відповідно до п. 1 ч. 2 цієї статті до документів, за умови наявності в них відомостей, передбачених ч. 1 цієї статті, можуть належати матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні) [2].

Також відповідно до п. 3 ч. 2 ст. 99 КПК України, до документів можуть належати носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії, якщо вони складені в порядку, передбаченому КПК України. У ч. 4 ст. 99 КПК України зазначено, що дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, що міститься в інформаційних автоматизованих системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід’ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визначаються судом як оригінал документа [2].

Досліджуючи електронний документ як засіб доказування, в юридичній літературі пропонується розуміти під ним відомості про обставини, що підлягають встановленню у справі, які записані на перфокарту, перфоплівку, магнітний, оптичний, магнітооптичний накопичувач, карту флеш-пам’яті чи інший подібний носій, які отримані з дотриманням процесуального порядку їх збирання.

Зокрема, відповідно до ч. 1 ст. 100 ЦПК України електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам’яті, мобільних телефонах тощо), серверах, системах резервного

копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі «Інтернет») [3].

Під формою електронного документа правильно буде вважати набір відповідних реквізитів, які за своїм процесуально-правовим значенням можна поділити на обов'язкові (від наявності або відсутності яких залежить питання юридичної сили документа) та необов'язкові (ті, які мають додатковий характер).

Кожен реквізит, обов'язковість якого встановлена нормативним правовим актом, унікальний і не може бути замінений яким-небудь іншим реквізитом. За відсутності хоча б одного обов'язкового реквізиту електронний документ втрачає юридичну силу. Призначення реквізитів полягає в забезпеченні документа юридичною силою. Реквізит є самостійним щодо мети змісту документа встановлення чи засвідчення документом юридичних фактів. Основними функціями реквізитів в широкому сенсі є інформаційна (ідентифікація, фіксування дати та часу складення документа) та посвідчувальна (автентифікація, достовірність, цілісність) [4, с. 67].

Проблема практичного використання електронних документів зумовлена вразливістю електронного доказу, що полягає у можливості змінювати зміст електронної інформації, її «мобільність» між технічними носіями інформації, відсутність класичних реквізитів письмових документів, які б забезпечували можливість аутентифікації змісту електронного документа та ідентифікації його автора тощо. Тобто загалом проблема практичного використання електронних засобів доказування полягає у забезпеченні допустимості електронного документа як умови використання такого засобу доказування в судочинстві.

Зазначимо процесуальний алгоритм дій щодо виявлення, фіксації та вилучення криміналістично значущої інформації з мобільного пристрою. Вилучення під час огляду (ч. 7 ст. 237 КПК України), затримання (ч. 3 ст. 208 КПК України), обшуку (ч. 7 ст. 236 КПК України) мобільний пристрій вважається тимчасово вилученим. Тож слідчий, відповідно до ч. 5 ст. 171 КПК України, повинен звернутись до слідчого судді з клопотанням про накладання на вказане майно арешту [2]. У разу відмови в задоволенні клопотання такий мобільний пристрій підлягає поверненню. Тобто можна стверджувати, що накладення слідчим суддею арешту на тимчасове вилучене майна (мобільний пристрій) підтверджує законність дій щодо вилучення майна та можливість його використання як джерела доказу. Зважаючи на вищевикладене, надаємо процесуальний алгоритм дій виявлення, фіксації та вилучення криміналістично значущої інформації з мобільного пристрою [5].

Злочини у сфері обігу наркотичних речовин на сьогодні одні з резонансних у суспільстві, насамперед якщо в них брали участь діти. Наведемо основні правила поводження з мобільними пристроями під час виявлення, фіксації та вилучення криміналістично значущої інформації:

– об'єкт обов'язково фотографується та в протоколі описується його

початковий стан та місце виявлення;

– якщо виникне припущення про наявність на мобільному пристрої слідів, які не видно неозброєним оком (сліди пальців рук, сліди біологічного походження тощо), необхідно застосувати спеціальні методи та засоби їх виявлення;

– в разі якщо телефон заблоковано, скористатися методами, які не мають ризику руйнування або пошкодження інформації, що знаходиться на мобільному пристрої. Наприклад, якщо оглядається мобільний телефон під керуванням операційної системи Android, часто виникає спокуса отримати максимально повний доступ до пристрою так званий root-доступ, який дозволить дослідити будь-який Android-телефон, незалежно від його конструктивних інженерних особливостей. Маючи повний доступ до операційної системи Android, можна вносити зміни у файли операційної системи, видаляти стандартні програми операційної системи, запускати будь-які виконавчі файли, призначені для Linux, створювати повну резервну копію встановленої системи з усіма параметрами та додатками, використовуючи додаткові програми. Але виникає ризик пошкодження інформації на мобільному телефоні, оскільки вносяться зміни в пам’ять пристрою шляхом інсталяції спеціальної програми, яка відкриває root-доступ (Unlock Root, z4root, HTC Quick Root, Easy Rooting Toolkit, Gingerbreak, SuperOneClick, Visionary, Unrevoked), а також відбувається втрата заводської гарантії, що пов’язане з можливим пошкодженням операційної системи;

– інформацію, яку неможливо скопіювати на зовнішній носій і проаналізувати за допомогою спеціалізованого програмного забезпечення, бажано зафіксувати будь-яким іншим способом (за допомогою фото- чи відеофіксації).

Виявлення, фіксації та вилучення ідеальних (інформаційних) слідів з мобільного пристрою можна здійснити такими методами, які залежать від стану мобільного пристрою та певними факторами доступу до даних пристрою.

Отже, останнім часом наукові дослідження з тематики електронного доказування стають все частіше предметом дискусій науковців, але досі відсутні науково-практичні напрацювання щодо специфічних методів дослідження електронних доказів. Електронні докази мають широкий доказовий потенціал завдяки шаленим темпам науково-технічного прогресу та стрімкої діджиталізації.

Основними причини скоєння злочинів у сфері незаконного обігу наркотичних засобів є: недостатнє правове регулювання інформаційного простору; відсутність географічних кордонів; неконтрольоване поширення інформації про наркотики в мережі «Інтернет», особливо в Даркнеті; активний розвиток анонімних грошових переказів, зокрема ринку криптовалют.

Бібліографічні посилання

1. Dokument. URL: https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82. (In Ukrainian).
2. *Kryminal'nyy protsesual'nyy kodeks Ukrayiny: Zakon Ukrayiny* № 4651-VI. (2012) [Criminal Procedure Code of Ukraine: Law of Ukraine]. URL: http://zakon. rada.gov.ua/ laws/show/4651-17. (In Ukrainian).
3. T*syvil'no protsesual'nyy kodeks Ukrayiny: Zakon Ukrayiny* № 1618-IV. (2004) [Civil Procedure Code of Ukraine: Law of Ukraine]. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text. (In Ukrainian).
4. Borodin, M.V. (2014) *Priznaki elektronnogo dokumenta kak ob"yekta informatsionnykh pravootnosheniy* [Signs of an electronic document as an object of information legal relations]. *Vestnik YUUrGU* [Bulletin of YUUrGU]. Seriya «Prava». T. 14. №3. P. 66-70. (In Russian).
5. *Vyyavlennya, fiksatsiya ta vyluchennya kryminalistychno znachushchoyi informatsiyi z mobil'nykh prystroyiv pid chas rozsliduvannya kryminal'nykh pravoporushen'* [Detection, fixation and extraction of criminologically significant information from mobile devices during the investigation of criminal offenses] / D.S. Afonin, K.Yu. Ismaylov, D.V. Lisnichenko, O.I. Postol. Odesa: Odes′kyy derzhavnyy universytet vnutrishnikh sprav, 2018. 38 p. (In Ukrainian).

Головкова Л. С.,
доктор економічних наук,
професор кафедри фінансів
та економічної безпеки
Рипюк Д. П.,
здобувач другого (магістерського)
рівня вищої освіти групи УФ-2026
Дніпровського національного
університету залізничного транспорту
імені акад. В. А. Лазаряна

ОРГАНІЗАЦІЯ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ НА ПІДПРИЄМСТВІ

Підприємницька діяльність у всіх сферах нерозривно пов’язана із залученням і використанням різної інформації. У сучасних умовах інформація являє собою особливий товар, який має певну цінність. Для підприємців найбільш цінною є інформація, яку він використовує для досягнення певної мети підприємства та розголос якої може позбавити його можливості реалізувати зазначені цілі. Тобто може створити загрозу безпеці підприємницької діяльності. В таких випадках загрозу являє собою не вся інформація, яка є в наявності у підприємства, а лише її деяка частина.

Актуальністю цієї теми є той факт, що правовий інститут комерційної

таємниці являє собою невід'ємний атрибут ринкової економіки. В процесі підприємницької діяльності відбувається накопичення великої кількості інформації, яка має важливе значення для сталого та успішного розвитку підприємства.

Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона загалом чи в певній формі та сукупності складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних наявним обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію [1].

У промислово розвинених країнах охороною комерційних таємниць підприємства займаються як окремі особи, так і внутрішні підрозділи (власник, керівник підприємства, спеціально створені служби, кадрові служби тощо) [2].

Аналіз чинного законодавства в цій галузі права показує, що майнові інтереси власників виробничих, торгових, ділових секретів, ноу-хау охороняються нормами цивільного, торгового, кримінального, трудового права, законодавства про недобросовісну конкуренцію.

У низці країн (наприклад, США) діє спеціальне законодавство, що об'єднує правила поведінки зацікавлених осіб в галузі використання торгових або ділових секретів. У країнах прецедентного права (Великобританії, США) для вирішення суперечок сторін притягуються прецедентні судові й адміністративні рішення.

Джерела, які утримують інформацію конфіденційного характеру, мають свою визначену специфіку та відповідно потребують окремої уваги під час розробки системи захисту.

З метою захисту комерційної таємниці на підприємстві необхідно забезпечити її захист, при цьому не обмежувати тих осіб, хто її потребує [3]. Є такі правила формування та розповсюдження комерційної таємниці на підприємстві:

– вона повинна мати відповідне місце в організаційній структурі підприємства;

– необхідно розробити систему охорони комерційної таємниці;

– впровадити принципи персональної відповідальності;

– впровадити терміни дії/використання інформації визначеної як комерційна таємниця.

Зазначені складові системи захисту комерційної таємниці повинні бути задіяні та використані у єдності та взаємодії. Якщо одна із складових системи не буде задіяна, то така система не буде працювати повноцінно та виконувати свою функцію, оскільки в такому разі можливий витік інформації, яка належить до комерційної таємниці, та підприємство може втратити провідні позиції на ринку внаслідок неправомірних дій з боку

конкурентів і втратити юридичні підстави для порушення питання щодо відшкодування матеріальних збитків.

Бібліографічні посилання

1. Цивільний кодекс України від 16.03.2003 р. № 435-IV. *Відомості Верховної Ради України*. URL: http:zakon2.rada.gov.ua/laws/show/435-15/conv/page.
2. Мельніков А. М. Основи організації бізнесу : підручник. Київ : Вид-во Центр навчальної літератури, 2017. 200 с.
3. Мойсеєнко І. П., Марченко О. М. Управління фінансово-економічною безпекою підприємства : навч. посіб. Львів, 2011. 380 с.

Горященко Ю. Г.,
доцент кафедри підприємництва
та економіки підприємства
Університету митної справи та фінансів,
кандидат економічних наук, доцент

ГОСПОДАРСЬКО-ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІННОВАЦІЙНОЇ ПОЛІТИКИ ДЕРЖАВИ

Уперше категорія «інноваційна політика» була вжита у 1967 році в США під час доповіді «Технологічні нововведення: управління й умови здійснення» [1, с. 65]. Вітчизняні вчені І. П. Макаренко, О. М. Трофимчук, В. П. Кузьменко та інші трактують цю категорію як «сукупність заходів нормативного і політичного характеру з метою створення сприятливих умов для випереджаючого економічного розвитку шляхом використання інструментів бюджетно-фінансової та грошово-кредитної політики (у тому числі валютної) на основі науково-технічного прогресу» [2, с. 14].

Інноваційна політика (innovatio, novo – змінювати, поновлювати, винаходити; politu – група людей, через яких виявляється воля як діяльність) є планом дій владних структур (основного суб'єкта) щодо організації інноваційної діяльності (об'єкта). Наповнена релевантним і всезагальним інформаційним змістом, з початку свого зародження державна інноваційна політика швидко і часто змінювала свої цілі, завдання і механізми, та головним її спрямуванням, відповідно до Закону України «Про інноваційну діяльність», є «створення соціально-економічних, організаційних і правових умов для ефективного відтворення, розвитку й використання науково-технічного потенціалу країни, забезпечення впровадження сучасних екологічно чистих, безпечних, енерго- та ресурсозберігаючих технологій, виробництва та реалізації нових видів конкурентоздатної продукції» [3].

В Україні звичним є покладання на державну інноваційну політику основ регулювання інноваційних процесів у державі, регіонах і на

підприємствах, проте проведені експертні дослідження щодо рівня інноваційного розвитку підприємництва дають підстави досить критично оцінити засоби регулювання інноваційної політики та фактичні результати. На думку експертів, по-перше, держава засобами розробки стратегій та норм дійсно визначає пріоритетні напрями інноваційної діяльності, проте слабко їх підтримує; по-друге, формуючи державні, галузеві, регіональні і місцеві інноваційні програми, держава реалізує їх не у повному обсязі; по-третє, у нормативно-правовій базі і економічних механізмах для підтримки і стимулювання інноваційної діяльності є суттєві розбіжності; по-четверте, експерти відмічають незадовільний рівень захисту прав та інтересів суб'єктів інноваційної діяльності і фінансової підтримки виконання інноваційних проєктів [3].

В економічно розвинутих країнах застосовуються такі типи державної інноваційної політики [5, с. 126]:

– політика технологічного поштовху (інформаційна, фінансова підтримка інновацій) у США, Великобританії, Франції. Українська бізнес-еліта сподівається на реалізацію саме цього типу державної інноваційної політики;

– політика ринкової орієнтації (обмежене втручання держави) у Німеччині, Японії, частково в США;

– політика соціальної орієнтації (широке залучення громадськості) у Швеції, частково Франції, Японії і Німеччині;

– політика зміни економічної структури господарського механізму (змішаний тип).

Україна керується здебільшого методами прямого регулювання інноваційної діяльності.

В основі інноваційної політики може знаходитись стратегічний інструмент, витканий із сукупності правил і методик для розробки інноваційної політики – інноваційний органон. Розбудова інноваційної інфраструктури повинна відбуватися на його основі, передусім, створення власних наукових центрів, державних та університетських бізнес-інкубаторів на території України. В іншому випадку, повинно забезпечуватися переведення на територію України за певних вигідних та сприятливих умов наукових центрів, або ж навпаки, з України за кордон. В останньому випадку, частково вирішується проблема патентування, оскільки дочірні підприємства патентують інноваційно-технічні рішення за місцем розташування материнської компанії. За розробку інноваційного органону має відповідати управлінський орган, сформований із провідних фахівців та науковців, бізнес- та владних структур, інших стейкголдерів, які мають сформувати ефективні профільні робочі групи і надалі моніторити виконання завдань інноваційної стратегії, презентуючи результати кожного кроку в Інтернеті, через консультації з громадськістю, тематичні семінари. Іншим елементом у структурі інноваційної політики є налагодження інституційних

взаємозв'язків. Не менш важливими є пошук інструментів фінансово-інвестиційної підтримки МСП і розробка механізму спрощеної системи оподаткування для інвесторів МСП.

Бібліографічні посилання

1. Гусєв В. О. Державна інноваційна політика: методологія формування та впровадження : монографія. Донецьк : Юго-Восток, 2011. 624 с.
2. Макаренко І. П., Трофимчук О. М., Кузьменко В. П. Проблеми становлення інноваційної політики в Україні / за ред. І. П. Макаренко. Київ : УІДНСРіР: Ін-т еволюц. економіки, 2004. 123 с.
3. Про інноваційну діяльність : Закон України в поточній ред. від 05.12.2012 р. URL : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=40-15.
4. Horiashchenko Y., Taranenko I., Yaremenko S., Shevchenko V., Mishustina T., Klimova I. Integrated System of Enterprises' Innovative Development Management Under the Conditions of Post-Fordism. Postmodern Openings. 2021. Vol. 12. Issue 3 Sup1. S. 45–60.
5. Юринець З. В. Формування інноваційних стратегій: теорія, методологія, практика : монографія. Львів : СПОЛОМ, 2016. 412 с.

Гребенюк А. М.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу призвели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності [1].

На сьогодні в зв'язку з карантином та дистанційною формою праці з впровадженням хмарних технологій та розвитком торгових платформ кількість кіберзлочинів в Україні за останні два роки збільшилась.

Кіберзлочинці можуть полювати за персональними даними, банківськими рахунками, паролями та іншою інформацією, яка наявна в електронному вигляді, а також, використовуючи різні платформи по продажу товарів та послуг, виманювати гроші. Потерпілими можуть стати як звичайні люди, так і будь-які підприємства.

Кіберзлочини бувають:

- спрямовані на заволодіння коштами;
- спрямовані на заволодіння інформацією (для власного

використання або для подальшого продажу);

– втручання в роботу інформаційних систем (для навмисного пошкодження за винагороду або через хуліганство);

– поширення спаму і вірусних програм тощо.

Всі ми добре пам'ятаємо, як у 2017 році в Україні відбулася масштабна атака вірусом Petya: були вражені енергетичні компанії, українські банки, аеропорт «Бориспіль», аеропорт Харкова, Чорнобильська АЕС, урядові сайти, київський метрополітен тощо. Подібного безпрецедентного масштабного вторгнення в сервери вітчизняних компаній наша країна ще не знала. За даними експертів Міжнародного валютного фонду, економічні втрати від атаки вірусу Petya становили приблизно 850 млн доларів. При цьому заяви потерпілих компаній в кіберполіцію про втрату даних часто залишалися без відповіді, адже знайти і притягнути до відповідальності зловмисника в цьому разі виявилося неможливо. На рис. 1 наведені у відсотках збитки компаній в Україні за 2020 р.

Сьогодні практично всі фахівці у сфері інформаційних технологій визнають, що ситуація з кіберзлочинністю у світі погіршується. Організована злочинність все частіше і частіше використовує Інтернет з метою приховування своєї діяльності. Зараз нікого не здивуєш існуванням мережі «Даркнет», за допомогою якої злочинці фактично створили чорний ринок для збуту наркотиків, зброї, крадених товарів тощо. Завдяки технологіям, які забезпечують мережеву анонімність, ця частина Інтернету залишається абсолютно безконтрольною, а тому безпечної для діяльності різних злочинних угруповань. За даними, наданими Національною поліцією України, кількість організованих груп і злочинних організацій, що здійснюють кримінальні правопорушення з використанням високих інформаційних технологій, за останній рік збільшилася на 36 %.

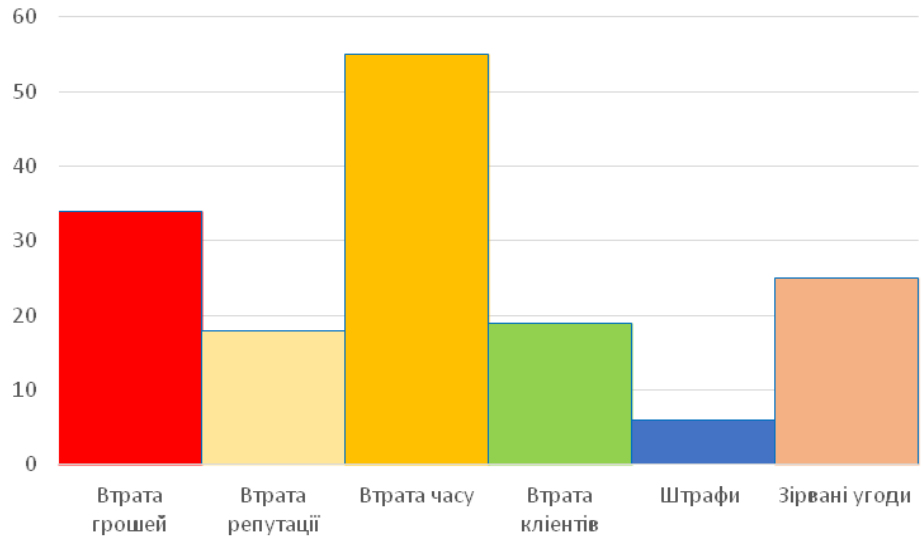


Рис. 1. Збитки компаній внаслідок кіберзлочинів

Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Український Кримінальний кодекс передбачає 4 статті за інформаційні злочини [2]:

– Ст. 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

– Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут незалежно від того, робиться це безкорисливо або за гроші.

– Стаття 361-2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

– Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (якщо ви перед звільненням знищите на своєму службовому комп'ютері важливу інформацію, то ваші дії підпадають під цю статтю).

Збільшення кількості таких злочинів в останні два роки (рис. 2) великою мірою пов'язано з тим, що поступово штат співробітників кіберполіції все-таки розширюється і відповідно більше порушується кримінальних справ. Але, на жаль, левова частина таких справ не доходить до суду або розвалюється в суді через погане збирання доказів слідчими органами [3].

До основних способів допомоги в боротьбі з кіберзлочинністю належать централізоване впровадження основних заходів безпеки, підвищення прозорості з боку організацій та урядів, стандартизація і координація вимог кібербезпеки, навчання співробітників обізнаності про кібербезпеки і розробка планів запобігання і реагування.

Зараз в нашій країні пріоритетними внутрішньополітичними напрямами для розвитку є саме кібербезпека і протидія кіберзлочинності. Тому будемо сподіватися, що рівень безпеки в інтернет-просторі України незабаром підвищиться, а популярні шахрайські схеми в мережі будуть знищені.

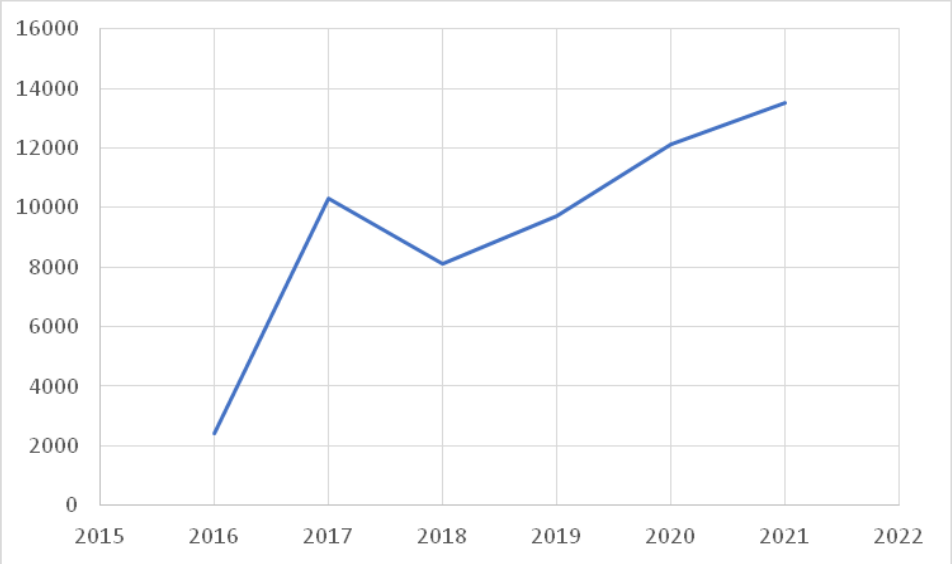


Рис.1. Судові рішення щодо кіберзлочинів в Україні

Але для цього потрібно змінювати та вдосконалювати законодавчу базу для швидкого реагування представників кіберполіції.

Бібліографічні посилання

1. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. 126 с.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T172163.html
3. Кримінальний кодекс України. URL: https://kodeksy.com.ua/kriminal_nij_kodeks_ukraini/statja-361.htm
4. Opendatabot. URL: https://opendatabot.ua/blog/ru/375-hackers
5. Платформа LIGA:ZAKON. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/EA013606.html

Дараган В. В., завідувач кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, доцент

ДЕЯКІ ПРОБЛЕМИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ БЮРО ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

22 березня 2021 року Президент України Володимир Зеленський підписав Закон України «Про Бюро економічної безпеки України» № 1150-IX, який Верховна Рада України ухвалила 28 січня 2021 р. Як зазначив Глава

держави, документ створює інституційні умови для захисту економічних процесів від тиску силових органів, що підтримується міжнародними партнерами України. Основною функцією Бюро економічної безпеки буде аналітична робота, а не силові повноваження. Бюро аналізуватиме бенефіціарів фінансових операцій і визначатиме, чи є порушення закону в обігу коштів тих чи інших бізнесових або державних структур. Бюро економічної безпеки – єдиний орган державної влади, відповідальний за боротьбу з економічними злочинами. Він отримає відповідні повноваження Служби безпеки України та податкової міліції, які будуть переосмислені з тим, щоб це був не стільки силовий, скільки аналітичний орган [1].

Однак аналіз Закону України «Про Бюро економічної безпеки України» вказує на низку суттєвих прорахунків, наявність яких ставить під сумнів виконання того обсягу завдань, заради якого було створено принципово новий правоохоронний орган – забезпечення економічної безпеки України.

Зокрема, одним з основних недоліків сучасної редакції Закону України «Про Бюро економічної безпеки України» є відсутність у Розділі VI «Прикінцеві та перехідні положення» відповідних статей щодо внесення змін у Кримінальний процесуальний кодекс України у ст. 38 «Органи досудового розслідування», ст. 216 «Підслідність» та інших, менш важливих статей. Відсутність вказаних норм унеможливлює здійснення досудового розслідування детективами Бюро економічної безпеки кримінальних проваджень.

Як показує аналіз Положення про Бюро економічної безпеки України, затвердженого постановою Кабінету Міністрів України від 6 жовтня 2021 р. № 1068, у структурі Бюро економічної безпеки також передбачені посади оперуповноважених. Наявність вказаних посад передбачає можливість здійснення вказаними працівниками оперативно-розшукової діяльності. Однак у Розділі VI «Прикінцеві та перехідні положення» не було передбачено відповідних змін до Закону України «Про оперативно-розшукову діяльність» зокрема у ст. 5 «Підрозділи, які здійснюють оперативно-розшукову діяльність».

Відсутність вказаних норм унеможливлює здійснення оперуповноваженими Бюро економічної безпеки оперативно-розшукової діяльності, що знову ставить під сумнів можливість виконання підрозділами Бюро економічної безпеки реальних заходів щодо забезпечення економічної безпеки України.

Крім того, існування в одному правоохоронному органі відповідних посад детективів та оперуповноважених ставить питання щодо їх функцій, адже на сьогодні такої штатної структури не має жоден з правоохоронних органів. Зокрема, підрозділи детективів мають лише підрозділи Національного антикорупційного бюро України. Відповідно до ч. 4 ст. 5 Закону України «Про Національне антикорупційне бюро України» підрозділи детективів здійснюють оперативно-розшукові та слідчі дії.

Інститут поліцейських детективів є в скандинавських країнах, Німеччині, США та інших державах сталої демократії. Між ними є низка відмінностей в обсязі повноважень, моделі взаємодії з прокуратурою тощо. Водночас усіх їх об'єднує те, що збирає докази і фіксує їх у процесуальних документах одна особа, яка несе відповідальність за якість виконаної роботи – підготовку й спрямування обвинувального висновку до суду. Тому детектив зацікавлений у якісній роботі над кримінальним провадженням, на якому він знається від початку до кінця [2].

У такому разі виникає питання, навіщо було передбачати у структурі Бюро економічної безпеки посади оперуповноважених, якщо їх функції можуть виконувати й детективи (якщо брати до уваги їх традиційні функції).

Обсяг тез доповіді не дозволяє зупинитися на усіх наявних у Законі України «Про Бюро економічної безпеки України» прогалинах. Однак вже зараз можна зробити однозначний висновок, що без внесення відповідних змін до Закону України «Про оперативно-розшукову діяльність» та Кримінального процесуального кодексу України працівники Бюро економічної безпеки не матимуть реальної можливості здійснення дієвих заходів щодо забезпечення економічної безпеки України.

Бібліографічні посилання

1. Президент підписав закон щодо створення Бюро економічної безпеки. Президент України : офіц. сайт. URL: https://www.president.- gov.ua/news/prezident-pidpisav-zakon-shodo-stvorennya-byuro-ekonomichnoy-67265 (дата звернення: 25.10.2021).
2. Запровадивши інститут кримінальних проступків, утворивши інститут детективів, ми просунемося на шляху до євроінтеграції. URL: https://dt.ua/internal/reforma-kriminalnogo-bloku-policiyi-problemi-i-perspektivi-247837_.html (дата звернення: 25.10.2021).

Демко І. І.,
кандидат економічних наук,
доцент Університету
банківської справи, м. Львів

ПЕРЕВАГИ АВТОМАТИЗАЦІЇ СИСТЕМИ БУХГАЛТЕРСЬКОГО ОБЛІКУ ПІДПРИЄМСТВА

Неодмінною умовою вдосконалення управління є докорінна реконструкція його технічної та інформаційної бази на основі автоматизованої системи обліку, контролю й аналізу з використанням автоматизованих робочих місць бухгалтера.

Одним з найважливіших завдань у цій справі є подальший розвиток і вдосконалення інформаційних систем підприємств із використанням нових

засобів управління та сучасних технічних засобів. Відповідно до цього має змінитися роль бухгалтерського обліку, а отже, методологічні та методичні його аспекти потребуватимуть коригування.

Бухгалтерський облік і бухгалтерська інформація в умовах автоматизованої системи обробки інформації використовуються значно ширше, ніж у разі ручної обробки даних. Змінюється й цільове призначення бухгалтерського обліку. Він дедалі більше стає складовою управлінської системи підприємства.

Економічна ефективність інформаційної системи виявляється в поліпшенні економічних результатів функціонування об'єкта внаслідок впровадження інформаційної системи.

Створення та використання автоматизованої системи бухгалтерського обліку здатне прискорити процес обробки облікової інформації на підприємствах, на яких бухгалтерський облік організовано ефективно, та суттєво покращити організацію бухгалтерського обліку на підприємствах з низьким рівнем її організації [1].

Як наслідок, застосування комп'ютерних технологій в бухгалтерському обліку значно підвищує продуктивність праці бухгалтерів. Отже, метою створення і запровадження автоматизованої системи бухгалтерського обліку є забезпечення підвищення ефективності виробничо-господарської діяльності економічного суб'єкта (рис.1).

Рис. 1. Мета створення автоматизованої системи бухгалтерського обліку

Економічну ефективність від впровадження комп'ютерної та організаційної техніки поділяють на пряму та непряму.

Як пряму економічну ефективність розуміють економію матеріальних, трудових ресурсів та грошових коштів, отриману внаслідок скорочення чисельності управлінського персоналу, фонду заробітної плати, витрачання основних та допоміжних матеріалів завдяки автоматизації конкретних видів облікових та аналітичних робіт тощо [2].

Непряма економічна ефективність може бути пов'язана, наприклад, з економією робочого часу на ухвалення управлінських рішень внаслідок оперативного отримання необхідної інформації, підвищення іміджу підприємства тощо [2].

За даними закордонних публікацій, впровадження на підприємствах сучасних ERP-систем (систем планування ресурсів підприємства) забезпечує значний економічний ефект внаслідок:

• зростання ефективності виробничих потужностей – до 20 %;

• економії оборотних засобів – до 1–6 % від валютної виручки, що практично відповідає досягненню подвійного прибутку;

• зниження виробничого браку – до 35 %;

• зниження страхових запасів (залишків, що не знижуються) на складах – до 40 %;

• зниження транспортно-заготівельних витрат – до 60 %;

• зниження частки невиконаних у відведений термін платежів – до 35–80 %;

• скорочення затрат на адміністративно-управлінський апарат – до 30 % тощо.

Визначають економічну ефективність за допомогою трудових та вартісних показників. Основним під час розрахунків є метод співставлення даних з базисним періодом. Під час автоматизації окремих робіт порівнюють затрати на обробку інформації до впровадження автоматизованої системи бухгалтерського обліку (під час ручної обробки), і затрати на обробку інформації за досягнутого рівня автоматизації. При цьому користуються абсолютними та відносними показниками. В окремих випадках затрати на впровадження можуть скласти більшу суму, ніж вартість самого програмного забезпечення. Є такий показник, як відношення вартості затрат на впровадження програмного продукту до вартості самого продукту. Числове значення цього показника змінюється, від 1 до 12 – залежно від країни.

Мета створення і запровадження автоматизованої системи бухгалтерського обліку полягає у забезпеченні підвищення ефективності виробничо-господарської діяльності підприємств, досягненні кращих техніко-економічних показників, соціальних умов, підвищення рівня кваліфікації персоналу, підвищення якості управління об'єктами господарювання, підвищення іміджу підприємства та інших результатів.

Бібліографічні посилання

1. Бенько М. М. Інформаційні системи і технології в бухгалтерському обліку : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2010. 336 с. URL: https://knute.edu.ua/file/MTc=/00fe89dcf255176477f44d6060ac7347.pdf
2. Рожелюк В. М. Шляхи вдосконалення організації обліку з використанням сучасних інформаційних систем. URL: http://magazine.faaf.org.ua/shlyahi-vdoskonalennya-organizacii-obliku-z-vikoristannyam-suchasnih-informaciynih-sistem.html

Долженков О. Ф.,
професор кафедри
політичних наук і права
Державного закладу
«Південноукраїнський національний
педагогічний університет
імені К. Д. Ушинського»,
доктор юридичних наук, професор

Корнієнко М. В.,
завідувач кафедри
адміністративної діяльності поліції
Одеського державного
університету внутрішніх справ,
доктор юридичних наук, професор

ІМПЛЕМЕНТАЦІЯ МІЖНАРОДНОГО ДОСВІДУ У СФЕРІ ПРОТИДІЇ ЗЛОЧИНАМ ЩОДО ДІТЕЙ: ІНФОРМАЦІЙНИЙ АСПЕКТ

Розглядаючи імплементацію міжнародного досвіду під час розслідування насильницьких злочинів щодо дітей, варто наголосити, що наявний тісний зв'язок підвищеного рівня вбивств та інших насильницьких злочинів, в тому числі вчинених щодо дітей із соціально-економічним розвитком у різних державах світу.

Особливості розслідування насильницьких злочинів щодо дітей має свою специфіку, що пов'язана із психосоматичними особливостями дитини. Загалом практика розслідування таких злочинів у державах Європи та Сполучених Штатах Америки здійснюється у межах кримінального провадження, однак враховує зазначені психосоматичні особливості дитини. Надзвичайно важливим аспектом, який ураховують передові держави у таких справах, є забезпечення інтересів дитини та її психологічного здоров'я.

Розслідування насильницьких злочинів щодо дітей у державах Європи та Сполучених Штатах Америки (як і в нашій державі) має і певні труднощі, пов'язані з необхідністю удосконалення нормативно-правової бази, прискорення процесу розслідування тощо.

Сучасне правове дослідження в умовах глобалізації та євроінтеграції не може не враховувати порівняльно-правовий аспект. Становлення і розвиток юридичної компаративістики є важливим фактором удосконалення правозастосовної діяльності органів державної влади, у тому числі і у сфері діяльності правоохоронних органів, зокрема протидії насильницьким злочинам проти малолітніх. «Злочини проти малолітніх у останні часи починають набувати міжнародного характеру. Винні особи можуть

переїжджати з держави у державу, зокрема, у країни, що розвиваються, зважаючи на меншу суворість покарання», – наголошує Інтерпол [2].

«Для України за нинішніх умов особливої уваги науковців та практиків у цьому контексті потребує зарубіжний досвід як країн із міцним громадянським суспільством і правовою державою, так і країн, в яких демократичні інститути лише формуються. Держава за допомогою правових норм і застосування владних важелів регулює суспільні відносини, встановлює і підтримує в країні необхідний порядок, проте й сама підпорядковується суспільству, покликана служити йому», – зазначає А. Дакал [3, с. 211].

Водночас треба зазначити, що запозичення досвіду розвинутих країн має певні проблемні аспекти, пов'язані з різним законодавчим регулюванням відповідних суспільних відносин, хоча деякі питання інфоомаційної безпеки у державах Європи та Сполучених Штатах Америки є достатньо прогресивними і можуть бути запозичені.

Превалювання в Україні і до цього часу нормативістського підходу до розуміння права, за якого право і до сьогодні сприймається як система загальнообов'язкових, формально визначених правил поведінки, що приймаються і охороняються державою, зумовлювало розвиток юридичної техніки, тому можна стверджувати, що вітчизняне розуміння насилля у цілому відповідає сучасному стану розвитку соціуму.

Зауважимо, на сьогодні в Англії запроваджено посаду уповноваженого з питань дитинства (так званий «дитячий комісар – Children's Commissioner). Він співпрацює з політиками для того, щоб останні враховували тенденції у сфері захисту дітей під час ухвалення рішень. Уповноважений з питань дитинства проводить дослідження факторів, що впливають на життя дітей. Він також дає поради дітям, які потребують догляду або живуть далеко від дому. Незалежний від уряду та парламенту, уповноважений з питань дитинства має унікальні повноваження, щоб впроваджувати довготермінові зміни та вдосконалення для дітей, зокрема найбільш вразливих дітей, у тому числі тих, що знаходяться під опікою. Він є «очима і вухами» дітей у системі та країні в цілому [4, с. 3]. Однак уповноважений з питань дитинства безпосередньо не бере участь у розслідуванні злочинів проти малолітніх, виконуючи лише превентивну функцію, зокрема, загальної превенції.

Розслідування насильницьких злочинів щодо малолітніх відрізняється від розслідування насильницьких злочинів щодо повнолітніх осіб і частково неповнолітніх. Саме тому в Європейських державах, зокрема Великій Британії, а також Сполучених Штатах Америки, *кожне кримінальне провадження у таких справах щодо малолітніх здійснюється особами, які отримали спеціальні навички, пройшли відповідне навчання*.

Уповноважений з питань дитинства використовував дані Міністерства внутрішніх справ та національних даних з КПС для вивчення термінів, пов'язаних із випадками насильницьких злочинів щодо дітей в Англії у

період 2012/2013 та 2015/2016 років, з позиції початку та кінцевої роботи в суді. Як показали результати дослідження, процес розслідування випадків насильницьких злочинів щодо дітей значно перевищує строк по таких злочинах щодо повнолітніх осіб. У 2015/2016 роках середня тривалість проваджень по насильницьких злочинах проти малолітніх становила 248 дні. Для порівняння – середня тривалість проваджень по насильницьких злочинах проти повнолітніх становила 147 днів, що на 101 день менше, ніж середнє значення для таких злочинів [4, с. 3].

Попередні результати уповноваженого з питань дитинства виявили поширеність та високу латентність насильницьких злочинів проти малолітніх в Англії, а також перешкоди та проблеми щодо виявлення дітей, які стали жертвами насильства. Вирішення таких бар'єрів та проблем може поліпшити ідентифікацію жертв насильницьких злочинів проти малолітніх.

У цей час дані про своєчасність процесу кримінального правосуддя у справах про насильницькі злочини не публікуються, (так званий інформаційній захист). Зважаючи на соціально негативний вплив насильницьких злочинів проти малолітніх жертв та зростаючий попит на відповідні охоронні послуги, дуже важливо регулярно повідомляти про своєчасність процесу розслідування та судочинства, щоб забезпечити перевірку результативності.

Не можна оминути і позитивного досвіду Сполучених Штатів Америки у протидії насильницьких злочинів проти малолітніх. За даними Федерального Бюро Розслідувань, у Сполучених Штатах Америки щороку тисячі дітей стають жертвами насильницьких злочинів, таких як сексуальне насильство та викрадення. Федеральне бюро розслідувань є головною інституцією Міністерства юстиції Сполучених Штатів Америки, відповідальною за розслідування злочинів проти дітей. Міністерство юстиції визначило захист дітей пріоритетом, як це відображено у Стратегічному плані, який містить у собі запобігання, припинення та розслідування злочинів проти дітей та описує свої стратегії для досягнення цієї мети. У Сполучених Штатах Америки визначається захист дітей від злочинів як головний пріоритет, зокрема ініціатива проєкту «Безпечне дитинство», метою якого є посилення національної відповіді на цю зростаючу загрозу для молоді Америки шляхом співпраці правоохоронних органів на всіх рівнях, а також неприбуткових організацій. ФБР є основною ланкою у зусиллях Департаменту по боротьбі зі злочинами проти дітей, тому для ФБР дуже важливо мати добре організований, чіткий та ефективний підхід до розслідування, щоб захистити дітей та оперативно притягувати порушників до кримінальної відповідальності [5].

Пріоритетами в розслідуванні насильницьких злочинів проти дітей для ФБР є: викрадення дітей, включно з викраденням батьками та з батьками; сексуальна експлуатація дітей – організації, що займаються торгівлею дітьми; інтернет-мережі та підприємства, які займаються виробництвом,

торгівлею, розповсюдженням та / або продажем дитячої порнографії; дитячий секс-туризм (міжнародні подорожі з сексуальної діяльності щодо дітей); виробництво дитячої порнографії, в тому числі і примус / заманювання неповнолітнього; торгівля дитячою порнографією – розповсюдження дитячої порнографії; володіння дитячою порнографією.

З 1932 року Конгрес надав ФБР юрисдикцію відповідно до «Закону Ліндберга» негайно розслідувати будь-які повідомлення про таємничі зникнення або викрадення осіб «ніжного віку» – зазвичай 12 років або молодше. При цьому не потрібно чекати вимоги викупу, і дитині не потрібно перетинати державний кордон або пропадати безвісти протягом 24 годин.

Заслуговує на особливу увагу додаток ФБР «Child ID». Безкоштовний мобільний додаток дозволяє батькам зберігати оновлені фотографії та фізичний опис своєї дитини і передавати цю інформацію владі, якщо їх дитина зникла. Інформація зберігається тільки на мобільному пристрої користувача і передається тільки в тому випадку, якщо користувач її відправляє.

Групи для розслідування злочинів проти дітей отримують технічну підтримку в основному з таких чотирьох відділень:

– відділення аналізу поведінки: ФБР має три підрозділи з поведінкового аналізу (BAU), в яких працюють спеціалісти зі спостереження, аналітики розвідки, аналітики з питань злочинності, агенти з інших урядових установ, які проводять дослідження та надають підтримку для проведення спеціальних аґенцій розслідування; BAU призначений для сприяння розслідувань, пов’язаних з викраденням дітей, зниклими без вести дітьми, сексуальними нападами та дитячою порнографією. Крім того, BAU супроводжує спеціальних агентів на місце злочину, консультує з місцевими правоохоронними органами та допомагає в підготовці координаторів та спеціальних агентів;

– відділення цифрових доказів: На цей час дві програми в межах відділення цифрових доказів ФБР проводять криміналістичний аналіз цифрових доказів, виявлених під час розслідувань, включно зі злочинами проти дитини: команди з відстеження комп’ютерних аналізів та регіональні комп’ютерні криміналістичні лабораторії. Комп’ютерні групи з реагування на аналіз мають у своєму складі приблизно 270 криміналістичних екзаменаторів, розташованих у межах 89 відділень місцевого офісу ФБР та агентств-резидентів по всій країні. Ці експерти допомагають спеціальним агентам аналізувати цифрові дані, такі як комп’ютерні жорсткі диски та інші комп’ютерні носії, отримані під час їх досліджень. Крім того, у ФБР є 16 регіональних комп’ютерних криміналістичних лабораторій, які проводять криміналістичний аналіз цифрових доказів місцевим, державним та федеральним правоохоронним органам, які проводять розслідування різних злочинів;

– відділення допомоги жертвам: ФБР створив свій офіс допомоги

жертвам, щоб гарантувати, що жертвам злочинів, що розслідуються ФБР, надається можливість отримувати послуги, що вимагаються федеральними законами та керівними принципами;

– відділення запобіжного захисту: цей підрозділ, до складу якого входять два спеціалісти з питань охорони психічного здоров'я, щороку проводить приблизно 1400 оцінок персоналу ФБР, включно з тими співробітниками, які беруть участь у прихованих дослідженнях сексуальної експлуатації дітей в Інтернеті.

До державних правових основ міжнародного співробітництва належить, насамперед, Конституція України, що містить положення, яке визначає міжнародні договори України частиною її правової системи (ст. 9) та зазначає, що зовнішньополітична діяльність України спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигідного співробітництва з членами міжнародного співтовариства за загальновизнаними принципами і нормами міжнародного права (ст. 18) [1].

Узагальнення сучасних тенденцій і стратегій протидії насильницькій злочинності щодо малолітніх у різних країнах світу дає підстави для здійснення таких висновків:

1) сучасні світові насильницькі злочини щодо дітей характеризуються відносною сталістю кількісних показників за більшістю майнових і насильницьких злочинів;

2) найбільш поширеними прибутковими видами транснаціональної організованої злочинності щодо малолітніх дітей є злочинність у сфері:

– торгівлі дітьми,

– сексуальної експлуатації,

– використання в порнобізнесі,

– вилучення органів, проведення дослідів над дітьми;

3) успішне запобігання більшості злочинам неможливе без широкої участі громадськості;

4) стратегія громадського впливу на злочинність полягає у залученні окремих громадян, громадських організацій правоохоронної спрямованості тощо до охорони правопорядку, участі у програмах профілактики насильницької злочинності щодо малолітніх дітей, надання інформації про вчинені злочини з обов'язковим матеріальним заохоченням цих напрямів роботи з боку держави і приватного бізнесу.

Отже, варто зазначити, що сучасний передовий міжнародний досвід запобігання насильницькій злочинності щодо дітей має враховуватись органами кримінальної юстиції України під час розробки й практичної реалізації стратегій протидії такої злочинності в нашій державі. Розслідування насильницьких злочинів проти дітей є одним з найбільш складних, але важливих обов'язків правоохоронних органів. Аналіз зарубіжного досвіду у цій сфері виявляє проблеми, з якими стикаються

зарубіжні правоохоронці, та окремі заходи, які можна запровадити у національну правову систему.

Відмітимо, що на сьогодні Україна остаточно визначилася з напрямом свого розвитку, яким обрано долучення до європейської правової спільноти. Для входження в європейський простір необхідно не тільки досягти відповідних економічних показників, а й забезпечити дотримання цінностей, що визнані пріоритетними та основоположними, – узгодити національне законодавство з міжнародними стандартами.

Бібліографічні посилання

1. Конституція України. *Відомості Верховної Ради України (ВВР)*. 1996. № 30. С. 141. URL:
2. http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80;
3. Crimes against children. URL: https://www.interpol.int/en/...and.../Crimes-against-children.
4. Дакал А. Зарубіжний досвід формування та реалізації державної політики щодо захисту прав дітей: роль інституту омбудсмана у справах дітей. *Вісник Національної академії державного управління*. 2012. Вип. 4. С. 211–219.
5. Investigating Child Sexual Abuse. The Length of Criminal Investigations. April, 2017. 15 p.
6. The Federal Bureau of Investigation's Efforts to Combat Crimes Against Children. URL: https://oig.justice.gov/reports/FBI/a0908/final.pdf.

Долженков О. Ф.,
професор кафедри
політичних наук і права,
доктор юридичних наук, професор

Чебан О.Є., студентка

(Державний заклад «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»)

ДЕЯКІ АСПЕКТИ ЗАСТОСУВАННЯ НА ПРАКТИЦІ ЕЛЕКТРОННИХ ДОКАЗІВ

На сьогодні в Україні розвиток інформатизації розглядається в числі національних пріоритетів, прикладом тому служить мобільний застосунок, вебпортал і бренд цифрової держави, який розроблений Міністерством цифрової трансформації України – ДІЯ. Але водночас із безумовно необхідними інформаційними змінами в суспільному житті кожної людини, природно, що з’являються нові схеми протиправної поведінки кримінальних елементів, на які правоохоронній системі потрібно реагувати, і така реакція повинна бути нарівні з сучасними інформаційними технологіями, що, на жаль, практично ніколи не відбувається, і це проблема

не тільки України, а й світова проблема. Можна констатувати, що у кримінальних елементів у перших з'являється саме передове програмне забезпечення, вони мають можливість наймати найбільш фахових працівників, а також діяти в різних правових системах різних країн.

У сучасних реаліях типової схеми скоєння злочинів за останні 10 років відбулися суттєві зміни. Результати людської діяльності дедалі більше відображаються в електронному (цифровому) вигляді, у тому числі й ті, що набувають значення юридичних фактів. Наприклад, для збуту наркотичних речовин, використовується інтернет, а саме месенджери (Telegram, Viber, WhatsApp, Signal), соціальних мереж (ВКонтакте, Одноклассники, Instagram, Facebook, Twitter) та інші ресурси.

В. В. Мурадов зазначає, що через відсутність базового обсягу знань у галузі ІТ та повноцінно сформованої методики збирання та використання таких доказів доводиться залучати спеціалістів (та призначити експертизи), вилучати велику кількість обладнання або ж витрачати багато часу на їх пошук та фіксацію [1, с. 314].

Отже, для електронних доказів можна виділити такі ознаки: існування в нематеріальному вигляді; необхідність використання певних технічних засобів для відтворення; можливість перенесення чи копіювання на різні пристрої без втрати характеристик; оригінал електронного доказу може існувати в багатьох місцях одночасно.

На нашу думку, немає потреби виділяти електронні докази як самостійне процесуальне джерело доказів, а необхідно чітко визначити електронну форму фіксації, яка буде цілісна та незмінна, а отже, потрібно визначити в нормативно-правових актах алгоритм отримання, фіксації, використання, зберігання та аналізу. Крім того, визначені алгоритми миттєво ввести у навчальні плани підготовки здобувачів вищої освіти для формування якісних сучасних знань та вмінь у сфері інформаційно-телекомунікаційного обороту.

Наведемо приклад справи Верховного Суду судової палати Касаційного цивільного суду №753/10840/19, в якій досліджувалось питання, чи може скріншот повідомлень з телефону бути належним доказом. Позивач зазначала, що в листуванні, яке веде її колишній по телефону з приводу організаційних побачень з сином, він вдавався до відкритих погроз, образ, приниження честі та гідності, застосовував нецензурну лайку, називав непристойними словами заявницю, її родичів, вживав лексику, недопустиму в нормальному людському спілкуванні.

Суд першої інстанції позов задовольнив частково. Видано обмежувальний припис. Встановлено такі заходи тимчасового обмеження прав терміном на 6 місяців: заборонено вести листування, телефонні переговори та у будь-який спосіб спілкуватися або контактувати через інші засоби зв'язку із заявником та дитиною особисто і через третіх осіб. Апеляційний суд залишив рішення суду першої інстанції без змін. Не

погоджуючись із таким рішенням судів, колишній чоловік подав касаційну скаргу. Розглядаючи справу, Верховний Суд послався на ч. 1,3 ст. 100 ЦПК України, яку ми раніше наводили, та додатково зазначив, що такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі «Інтернет»). Учасники справи мають право подавати електронні докази в паперових копіях, посвідчених у порядку, передбаченому законом (Цивільно процесуальний кодекс України, 2004). Паперова копія електронного доказу не вважається письмовим доказом. Зокрема, ВСУ наголосив, що на підтвердження заявлених вимог заявниця надала скріншоти повідомлень з телефону та планшету, роздруківки з Viber, які суд першої інстанції, з яким погодився апеляційний суд, вважав належними та допустимими доказами, які досліджені судами у їх сукупності та яким надана належна правова оцінка.

Встановивши, що зміст конкретних фраз, лексики та характеру використання мовних засобів, які колишній застосовує у переписці з колишньою дружиною та малолітнім сином, дає підстави для висновку, що його дії треба кваліфікувати як домашнє насильство, судом обґрунтовано заборону йому вести листування, телефонні переговори та у будь-якій спосіб спілкуватись або контактувати через інші засоби зв'язку з колишньою та постраждалою дитиною особисто і через третіх осіб. Отже, Верховний Суд залишив касаційну скаргу без задоволення, а рішення суду першої та апеляційної інстанції без змін, визнавши скріншоти повідомлень доказами по справі (справа ВСУ №753/10840/19 від 13.07.2020 року) [2].

Листування за допомогою месенджерів (у вигляді текстових та мультимедійних повідомлень) повністю відповідає вимогам електронного доказу. Відповідач вказував на те, що позивачем на підтвердження своїх доводів надано суду електронне листування, скріншоти, копії документів, які не можна вважати належними доказами.

В умовах сьогодення питання використання електронних засобів доказування, їх допустимість та доказова сила стають все актуальнішими. На практиці, а особливо під час доказування злочинів у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, оскільки цей вид незаконної діяльності практично повністю перейшов в онлайн форму, виникає чимало питань щодо можливості використання як доказів інформації з месенджерів, соціальних мереж, мережевих ігор або пропрієтарних програм. На сьогодні питання електронних доказів слабко врегульовані законодавством, а особливо Кримінальним процесуальним кодексом.

Бібліографічні посилання

1. Мурадов, В. В. Електронні докази: криміналістичний аспект використання. *Порівняльно-аналітичне право*. 2013. № 3–2. С. 313–315.

2. Постанова Верховного Суду України від 13.07.2020 р. №753/10840/19. URL: https://reyestr.court.gov.ua/Review/90385050

Дронь М. А.,
аспірантка кафедри обліку
і оподаткування Дніпровського
національного університету
залізничного транспорту
імені академіка В. А. Лазаряна

СИСТЕМА УПРАВЛІННЯ РИЗИКАМИ ЯК ЕЛЕМЕНТ ЕКОНОМІЧНОЇ БЕЗПЕКИ БАНКУ

На сучасному етапі розвитку банківської системи України, що відбувається на фоні нестабільності національного та світового ринкового середовища, зростаючої волатильності фінансових ринків, появи нових форм конкурентної боротьби та зменшення чистої процентної маржі, надзвичайно актуальним постає завдання покращення рівня економічної безпеки банку, яке неможливе без організації ефективної системи управління ризиками.

У процесі динамічного розвитку системи українських банків протягом останніх років все більше уваги приділяється питанням ідентифікації, оцінки й управління ризиками з боку керівництва банківських установ, їх акціонерів, аудиторів, клієнтів і контрагентів, і насамперед – Національного банку України як державного регулятора, що сприяє дотриманню стабільності банківської системи України [1].

Однак за наявності великої кількості досліджень з теми ризик-менеджменту поза увагою залишились проблеми створення якісно нового механізму управління банківськими ризиками, який має бути ефективним в умовах значних змін чинників зовнішнього середовища. Не всі аспекти управління банківськими ризиками достатньо досліджено, а деякі й досі залишаються дискусійними. Більшість науковців подають або загальну характеристику банківських ризиків, або зосереджуються на одному з них. Поверхово розглянуто комплексний вплив різних видів ризиків на економічну безпеку банку. Майже відсутні дослідження специфіки становлення сучасної системи управління ризиками у вітчизняних банках, її взаємозв’язку з корпоративним управлінням та економічною безпекою банку. Недостатньо повно вивчено проблему управління банківськими ризиками в умовах сучасної фінансової кризи, причини її виникнення; відсутній системний підхід до аналізу таких інноваційних інструментів управління, як банкашуренс та сек’юритизація банківських активів; мало уваги приділяється аналізу впливу макроекономічного середовища на банківську систему (нагляд національного регулятора, грошово-кредитна та валютна політики, система гарантування вкладів, глобалізаційні процеси, стратегічні цілі іноземних банків, масштаби неформальної

економіки).

Категорія «економічна безпека» з'явилася в понятійному апараті економічної науки порівняно недавно і тому ще не має загальновизнаного тлумачення. Більшість дослідників розуміють «економічну безпеку» як інтегральну оцінку ресурсного потенціалу і ступеня захищеності підприємства від негативної дії зовнішнього середовища.

Взявши до уваги специфіку банківської діяльності, пропонуємо під «економічною безпекою» розуміти відповідний фінансовий стан банку, який гарантує:

1. Збереження безпечного функціонування (своєчасно й адекватно реагувати на зміну чинників внутрішнього та зовнішнього середовища).

2. Подальший стійкий розвиток (певний стан динамічної рівноваги, за якого банк здатний розвиватися навіть за наявності впливу несприятливих факторів внутрішнього і зовнішнього середовища).

3. Підвищення ринкової вартості банку (підтримка прибутковості акціонерного капіталу) [2, с. 15].

Зважаючи на зазначене тлумачення «економічної безпеки», сформуємо таке визначення «системи управління ризиками банку», а саме: це сукупність методів та інструментів, що забезпечують здатність банку протистояти зовнішнім і внутрішнім загрозам, збереження безпечного функціонування, подальший розвиток та підвищення ринкової вартості банку.

Відзначимо, що становлення системи управління ризиками в банківських установах відбувається в три етапи [3, с. 88]:

1. Підготовчий етап: формалізація системи бізнес-процесів банку; опис процедури контролю та ухвалення рішень; складання карт ризиків за підрозділами (напрямами) і в цілому для банку; розробка методики оцінки та прогнозування ризиків. На цьому етапі також вирішується питання, яка структура системи управління ризиками буде використовуватися, – централізована чи децентралізована.

2. Процедурний етап системи управління банківськими ризиками містить у собі розробку: процедур встановлення лімітів; концепції мінімізації банківських ризиків; процедур перегляду основних параметрів лімітної політики банку; процедур страхування, хеджування тощо.

3. Інтеграційний етап містить у собі аналіз вимог до кількості й якості інформації, що надходить в автоматизовану систему управління ризиками, опис можливостей наявної корпоративної системи, розробку рекомендацій щодо впровадження системи управління банківськими ризиками в корпоративну інформаційну систему, розробку поетапного плану впровадження.

Звертаємо увагу на те, що якість управління ризиком та рівень економічної безпеки мають оцінюватися незалежно одна від одної.

Бібліографічні посилання

1. Методичні вказівки з інспектування банків «Система оцінки ризиків» : Постанова Правління НБУ від 15.03.2004 р. № 104. URL: http://zakon2.rada.gov.ua/laws/show/v0104500-04.
2. Бобиль В. В. Фінансові ризики банків: теорія та практика управління в умовах кризи : монографія. Дніпропетровськ : Дніпропетр. націон. ун-т залізничного транспорту ім. акад. В. Лазаряна, 2016. 298 с.
3. Бобиль В. В., Дронь М. А. Нова концепція антикризового управління банківськими ризиками. *Банківська справа*. 2017. № 2 (143). С. 87–101.

Дубровіна В. В.
ад'юнкт кафедри
кримінального процесу
Дніпропетровського державного
університету внутрішніх справ

УДОСКОНАЛЕННЯ МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

У сучасному суспільстві розроблення та удосконалення управлінських рішень у сфері забезпечення інформаційної підготовки працівників Національної поліції України містить у собі систему заходів, що спрямовані на забезпечення попередження злочинності в суспільстві. Вказаний напрям потребує постійного удосконалення, контролю та подальшого розвитку для підвищення ефективної діяльності. Вказана тема є актуальною для дослідження, оскільки наявна система реєстрації інформації, що становить оперативний інтерес, та інформації органів досудового розслідування Національної поліції України фактично недосконало адаптована і малоефективна для застосування в розкритті та процедурі розслідування кримінальних правопорушень та проступків. Проте проблема отримання необхідної інформації на всіх стадіях кримінального провадження є однією з найбільш значних і актуальних.

На цей час важко уявити діяльність кожного з підрозділів Національної поліції України без інформаційно-аналітичної підтримки та інформаційного забезпечення, накопичення та процедури систематизації інформації в наявних базах даних [4].

Для вирішення розшукових заходів нині накопичений чималий досвід застосування новітніх технологій у процесі попередження, виявлення та розслідування злочинів, розшуку підозрюваного та обвинуваченого, провадження окремих слідчих (розшукових) дій, здійснення судових

експертиз [1].

Очевидно, що однією з важливих умов підвищення рівня протидії злочинності є широке використання сучасних досягнень науково-технічного прогресу, які останніми роками зробили прорив у сфері інформаційних технологій.

Інформаційні технології – це сукупність методів, інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість оброблення даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця розташування [6, с. 82].

Сутність інформаційного забезпечення оперативно-розшукової діяльності можна визначити як доцільну діяльність людини, спрямовану на вихідні фактичні дані з тим, щоб, використовуючи відповідні технічні засоби, перетворити їх форму, придатну для вирішення управлінських або конкретних завдань виявлення, попередження, припинення і розкриття злочинів, розшуку зниклих злочинців, безвісти зниклих громадян [2].

На пріоритетність і необхідність модернізованих інформаційних технологій вказують також норми положення кримінального процесуального законодавства України, в якому визначається неможливість оперативності і ефективності процесу без бази даних, яка укомплектована за допомогою інформаційного простору [3].

Основоположними напрямами подальшого розвитку, удосконалення та забезпечення інформаційно-аналітичної підготовки працівників Національної поліції України є:

1) розроблення пропозицій щодо подальшого удосконалення методів управління системами інформаційно-аналітичного забезпечення в системі МВС України;

2) модернізація комп’ютерних баз даних;

3) введення сучасних комп’ютерних інформаційно-аналітичних технологій для підвищення ефективності ведення обліків Національної поліції України;

4) впровадження ефективних комп’ютерних мереж;

5) використання надійних спеціалізованих засобів захисту інформації в системі МВС України;

6) запровадження методів для ефективного обміну кримінологічною інформацією на міждержавному рівні.

Отже, проаналізувавши вищезазначене, можна узагальнити, що застосування та використання новітніх інформаційних технологій в діяльності підрозділів Національної поліції України поліпшує та підвищує ефективність роботи підрозділів. Основною тенденцією удосконалення та поліпшення методичного інформаційного забезпечення органів та підрозділів внутрішніх справ є саме впровадження та ефективне функціонування новітніх систематизованих обліків, систем, баз даних та забезпечення

надійного доступу кожного із співробітників до вказаних систем.

Отже, інформаційні технології є налагодженим механізмом, що забезпечує якісне функціонування органів внутрішніх справ, які необхідні для виконання їх службових завдань. З розвитком комп'ютерних технологій створюються нові методи роботи, що здатні підвисити професіональні якості працівників [5].

Бібліографічні посилання

1. Рогатюк І. В. Використання інформаційних технологій у досудовому розслідуванні: сучасний стан і перспектив розвитку. *Науковий вісник Національної академії внутрішніх справ*. 2013. № 3. С. 312–320.

2. Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційне забезпечення професійної діяльності : навч. посіб. Дніпро : ДДУВС, 2018. 220 с. URL: http://er.dduvs.in.ua/handle/123456789/3718

3. Правоохоронна діяльність, керована аналітикою: передова методика сучасної правоохоронної діяльності. URL: http://euam.php7.postbox.kiev.ua/ua/news/opinion/intelligence-led-policing-the-cutting-edge-ofmodern-law-enforcement/

4. Возможности использования аналитических программ в борьбе с организованной преступностью. URL: https://articlekz.com/article/11838

5. Мельник В., Некрасов В. Як подолати ворога, багатшого за транснаціональні корпорації? URL: http://n-v.com.ua/yak-podolaty-voroga-bagatshogo-za-korporatsyi/

6. Інформаційно-аналітичне забезпечення діяльності підрозділів кримінальної поліції : зб. наукових статей за матеріалами доп. Всеукр. науково-практ. семінару 23 березня 2018 року / упоряд.: А. В. Баб'як, В. В. Сеник, Т. В. Магеровська. Львів : ЛьвДУВС, 2018. 209 с.

Ефременко Е. М.,
профессор кафедры гражданского
и трудового права учреждения
образования «Академия Министерства
внутренних дел Республики Беларусь»,
кандидат юридических наук, доцент

О ПРАВЕ НА ИЗОБРАЖЕНИЕ СОТРУДНИКА ОРГАНОВ ВНУТРЕННИХ ДЕЛ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ И ЗАЩИТЫ ГРАЖДАНСКИХ ПРАВ

В настоящее время необходимо совершенствование правовой регламентации использования и защиты изображения физического лица (в том числе сотрудников органов внутренних дел) как объекта гражданских прав в целях модернизации правового регулирования, направленного на обеспечение и защиту прав и законных интересов субъектов гражданско-правовых отношений. В современной цивилистической доктрине содержание используемых понятий «изображение» и «внешний облик» является

дискуссионным, не выработаны единообразные подходы к их пониманию и судебной практикой, поэтому субъекты правоприменительной деятельности используют доктринальные определения, что не способствует единообразию их толкования. В современном и динамично развивающемся информационно-цифровом обществе, где личные нематериальные права (блага) имеют важное значение, споры об их защите будут приобретать все большую актуальность. Современный запрос правоохранительных систем направлен на устранение правовой неопределенности и выработке правового механизма защиты сотрудников органов внутренних дел от противоправных действий.

Внешний облик сотрудника органов внутренних дел является его неотчуждаемым личным нематериальным благом и способом идентификации. Следует обратить внимание на важность разграничения внешнего облика человека и его изображения. Последнее, по мнению В. С. Толстого, представляет собой информационный объект [1, с. 81]. Л. О. Красавчикова справедливо отмечает, что «право на собственное изображение – это не право автора и вообще не авторское право, а личное неимущественное право гражданина, направленное на обеспечение неприкосновенности его личной жизни» [2, с. 82]. Таким образом, внешний облик сотрудника органов внутренних дел и его изображение, позволяющее его идентифицировать, следует рассматривать как два самостоятельных объекта гражданских прав, относящихся к личным нематериальным благам и имеющих различный правовой режим.

В настоящий момент в Гражданском кодексе Республики Беларусь отсутствует нормативное закрепление как права на внешний облик (на неприкосновенность внешнего облика) сотрудника органов внутренних дел, так и на его изображение, соответственно, не раскрыто содержание этих прав, не отражены их признаки [3]. Для устранения указанного пробела предлагается, во-первых, с целью нормативного закрепления права на изображение физического лица внести дополнения в п. 1 ст. 151 Гражданского кодекса Республики Беларусь путем включения в перечень нематериальных благ, перечисленных в данной норме относительно-определенного содержания, внешнего облика физического лица и его изображения как поименованных нематериальных благ. В настоящее время внешний облик физического лица и его изображение рассматриваются как элементы частной жизни, что порождает трудности в правоприменительной деятельности, поскольку содержание понятия «частная жизнь» также не конкретизировано в белорусском законодательстве. Следует отметить, что в Гражданском кодексе Украины право гражданина на изображение получило нормативное закрепление (ст. 307, ст. 308) [4].

Актуальной проблемой в настоящее время выступает использование изображения сотрудников органов внутренних дел без их согласия: в том числе освещение профессиональной деятельности, если это не затрагивает их

частной жизни и связанных с ней нематериальных благ. В последнем случае публичные лица имеют возможность запрещать обнародование и использование своих изображений, полученных при обстоятельствах, не связанных с их служебной деятельностью. Однако на практике возникают вопросы разграничения частной и публичной жизни указанных лиц, поскольку все фактические обстоятельства невозможно предусмотреть. Кроме того, было бы необоснованно сложно и нецелесообразно испрашивать согласия изображаемого сотрудника органов внутренних дел в случаях, когда оно получено при съемке, которая проводится в местах, открытых для свободного посещения либо на публичных мероприятиях, если данное изображение является центральным объектом. Вместе с тем важно учитывать, что подобные действия могут быть направлены на дискредитацию сотрудника, на формирование негативного общественного мнения о нем и т. д. Поэтому в случае обнародования и использования такого изображения с нарушением установленных законодательством либо сторонами порядка, способов, целей, пределов и сроков, действия противной стороны следует рассматривать как злоупотребление правом с наступлением предусмотренных актами законодательства правовых последствий.

В данном контексте представляется обоснованным дополнить ст. 35 «Правовая защита сотрудников органов внутренних дел» Закона Республики Беларусь от 17 июля 2007 г. № 263-З «Об органах внутренних дел» Республики Беларусь» [5] включением в нее нормы следующего содержания: «запрещается опубликовывать и использовать изображение внешнего облика или другого элемента идентификации сотрудника органов внутренних дел с целью причинения вреда его имущественным и (или) неимущественным правам (благам). Несоблюдение указанного требования влечет ответственность, предусмотренную законодательными актами Республики Беларусь». Это обеспечит защиту изображения сотрудника органов внутренних дел, а также станет сдерживающим фактором для граждан, желающих злоупотребить своим правом на распространение информации о деятельности государственных органов путем опубликования и использования изображения сотрудника органов внутренних дел по противоправным мотивам.

Библиографические ссылки

1. Толстой В. С. Личные неимущественные правоотношения : учеб. пособ. Млсква : ООО «Издательство Элит», 2006. 198 с.
2. Красавчикова Л. О. Авторское право и право гражданина на собственное изображение. Проблемы современного авторского права : Изд-во УрГУ. Свердловск, 1980. С. 76–90.
3. Гражданский кодекс Республики Беларусь: 07 декабря 2008 г. № 218-З : принят Палатой представителей 28 окт. 1998 г.; одобр. Советом Респ. 19 нояб. 1998 г. *КонсультантПлюс. Беларусь*. ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2021.
4. Гражданский кодекс Украины : 16 янв. 2003 г. № 435-IV. ООО «СоюзПравоИнформ». URL: http://base.spinform.ru /show_doc.fwx?rgn=8896. (дата обращения: 25.10.2021).

5. Об органах внутренних дел Республики Беларусь : Закон Респ. Беларусь от 17 июля 2007 г. № 263-З (изм. и доп. Закон Респ. Беларусь от 30 июля 2019 г. № 231-З). *Консультант Плюс: Беларусь*. Технология 3000. ООО «ЮрСпектр». Нац. центр правовой информ. Респ. Беларусь. Минск, 2021.

Зачек О. І.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ АНТИВАКЦИНАТОРІВ У ПЕРІОД ПАНДЕМІЇ COVID-19

У цей час ми найчастіше спілкуємося через Інтернет та отримуємо більшість новин через соціальні мережі. Однією з важливих тем інформаційного простору є зростання захворюваності на COVID та необхідність масової вакцинації. Позиція ВООЗ полягає у необхідності створення колективного імунітету шляхом вакцинування. Але цій позиції опонують антивакцинатори. Вони наводять аргументи, які ґрунтуються на фейках та маніпуляції, та швидко поширюються через значний вплив соціальних мереж. Це сприяє зменшенню обсягів вакцинації та зростанню захворюваності, що може створювати загрозу національній безпеці України.

Значну загрозу становить поширення дезінформації через соціальні мережі Російською Федерацією з метою дестабілізації ситуації в Україні та світі. Згідно з дослідженням компанії Facebook Росія посіла перше місце як виробник неправдивих новин серед країн світу, а Україна посіла п’яте місце в цьому рейтингу. Також Україна визнана другою після США серед країн, які найбільше постраждали від зовнішніх фейків [1]. На думку Центру стратегічних комунікацій та інформбезпеки, п’яте місце України в рейтингу осередків дезінформації від Facebook означає, що інформаційне поле нашої держави є під значним впливом Росії зовні та її агентів всередині України [2].

Одним з напрямів дезінформації є поширення фейків про шкідливість визнаних світових вакцин від COVID-19 з метою їх дискредитації та просування на світовий ринок російської вакцини Sputnik V. Зокрема за даними, які надає Укрінформ з посиланням на TheWallStreetJournal, французька контррозвідка розслідує можливість компрометації з боку Російської федерації вакцини від COVID виробника Pfizer-BioNTech шляхом пропозиції французьким блогерам розмістити за оплату в розмірі до 2500 євро критичних матеріалів про цю вакцину в соціальних мережах. І французька контррозвідка підозрює саме Російську Федерацію в таких діях [3].

Також на Всеукраїнському форумі «Україна 30. Коронавірус: виклики та відповіді», який відбувся 10.02.2021 р., в межах панельної дискусії «Дезінформація і міфи про вакцинацію та COVID-19 – аналіз даних та масштаб інфодемії» доповідач повідомив про факти формування російськими ЗМІ та українськими проросійськими медіа та блогерами негативної думки про вакцину компанії «Pfizer» шляхом перебільшення новин про летальні випадки після щеплення та поширення інформації про вакцину Sputnik V лише в позитивному спрямуванні [4].

Значна частка фейків про коронавірус в усьому світі походить з Росії та початково поширюється та роздувається кремлівськими джерелами, зокрема з пулу пропагандистських каналів RT, Sputnik тощо [5].

Найбільша тенденція поширення фейків про COVID-19 та вакцинацію є у Facebook, де групи та сторінки антивакцинаторів налічують понад 31 мільйон підписників, але їх вже почала обмежувати жорстка політика боротьби Facebook з фейками та дезінформацією. Антивакцинаторські облікові записи мають також приблизно 17 мільйонів підписників на YouTube. В Instagram акаунти противників вакцинації мають приблизно 7 мільйонів підписників [5].

Facebook вже давно запроваджує механізми боротьби з недостовірним контентом, який блокується, а облікові записи, які систематично його поширюють, видаляються. З початком пандемії COVID-19 Facebook поставив фейки про COVID-19 в один ряд з такими темами, як пропаганда насильства чи торгівля людьми [6].

Також інколи негативне ставлення до вакцинування викликають публікації українських ЗМІ, де поширюються новини про смерть громадян, які перед тим щепилися. І хоча це був трагічний збіг обставин, та не було встановлено зв'язку між щепленням та летальними випадками, гучні заголовки стали черговими аргументами для противників вакцинації [6].

Отже, ми бачимо, що поширення дезінформації щодо COVID-19 та вакцини і вакцинування є значною проблемою і може мати безпосередню загрозу національній безпеці України. Тому є доцільним запровадження відповідальності за поширення такої інформації та залучення Департаменту кіберполіції Національної поліції України до боротьби з цим явищем.

Бібліографічні посилання

1. Facebook назвав найбільших «виробників» фейків, Росія – на першому місці. *Укрінформ*. URL: https://https://www.ukrinform.ua/rubric-world/3253944-facebook-nazvav-najbilsih-virobnikiv-fejkiv-rosia-na-persomu-misci.html (дата звернення: 20.10.2021).
2. «Зради немає»: фахівці пояснили, чому Україна опинилася в ТОП-5 рейтингу Facebook про фейки. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-society/3253961-zradi-nemae-fahivci-poasnili-comu-ukraina-opinilasa-v-top5-rejtingu-facebook-pro-fejki.html (дата звернення: 20.10.2021).
3. У Франції розслідують, чи платила Росія блогерам за наклеп на вакцину Pfizer. *Укрінформ*. URL: https://www.ukrinform.ua/ rubric-world/3253086-u-francii-rozsliduut-ci-

platila-rosia-blogeram-za-naklep-na-vakcinu-pfizer-wst.html (дата звернення: 20.10.2021).
4. Прохоренко Є. Поширення дезінформації та фейків про вакцинацію має на меті ослаблення України – експерти. *Аптека online*. 2021. № 7. URL: https://www.apteka.ua/article/584491 (дата звернення: 20.10.2021).
5. Коронавірус і соцмережі: як антивакцинатори використовують пандемію для просування своїх ідей. *Новинарня.* URL: https://novynarnia.com/2020/07/20/antivaxx/ (дата звернення: 20.10.2021).
6. Рєпік О. COVID-19, антивакцинаторство та як Facebook протидіє дезінформації про пандемію. URL: https://www.oporaua.org/article/vybory/ disinformation/23078-covid-19-antivaktsinatorstvo-ta-iak-facebook-protidiie-dezinformatsiyi-pro-pandemiiu (дата звернення: 20.10.2021).

Зачосова Н. В.,
доктор економічних наук, професор
Черкаського національного
університету імені Б. Хмельницького

УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ЯК СУЧАСНИЙ ЕЛЕМЕНТ МЕНЕДЖМЕНТУ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ

Останнім часом у вітчизняній науковій думці усе частіше лунають ствердні докази того, що підприємства усіх форм власності та видів економічної діяльності повинні мати у своєму управлінському арсеналі інструментарій безпеко орієнтованого менеджменту. Незважаючи на обмеженість фінансових, матеріальних, кадрових ресурсів вітчизняних суб'єктів господарювання, експерти наполягають на тому, що їх частина має бути спрямована на виявлення, протидію та мінімізацію негативного впливу внутрішніх і зовнішніх загроз на фінансово-господарський стан бізнес-структур. Ці завдання вирішуються на практиці шляхом використання механізмів управління фінансово-економічною безпекою. Отже, для зручності роботи управлінського персоналу та враховуючи специфіку безпеко орієнтованого менеджменту, необхідно виділити цей управлінський напрям в окремий, незалежний від фінансового або кадрового менеджменту вектор. Це не означає, що управління фінансово-економічною безпекою має бути автономним, і не інтегруватись у корпоративну систему менеджменту. Однак йому мають бути притаманні власний інструментарій, технології, індикатори рівня ефективності та досяжності поставлених цілей тощо. Також доцільною є розробка окремої стратегії забезпечення фінансово-економічної безпеки з можливістю інтеграції її як складового елементу загальної корпоративної стратегії суб'єкта господарювання.

Важливість управління фінансово-економічною безпекою у сучасних умовах господарювання визнається на державному рівні. Зокрема, 27 вересня

2021 року Президентом України було підписано Указ «Про запровадження національної системи стійкості», яку мають реалізувати у період з 2021 по 2025 роки. Як зазначається в документі, «система стійкості» спрямована на забезпечення здатності своєчасно ідентифікувати загрози та виявляти уразливості у сфері національної безпеки, запобігати або мінімізувати їх негативні впливи на сферу нацбезпеки» [1]. У контексті управління фінансово-економічною безпекою як на макро-, так і на мікрорівні, особливо цікавими є положення щодо функціонування системи державних органів, до завдань яких, вочевидь, буде віднесено моніторинг та протидію загрозам національній безпеці, частина з яких, безперечно, матиме деструктивний вплив і на стан фінансово-економічної безпеки окремих або усіх без винятку учасників національної господарської системи. Також порушується питання організації захисту об'єктів критичної інфраструктури, які представлені суб'єктами господарювання, безперервна та ефективна діяльність яких є запорукою функціонування державних механізмів і систем життєзабезпечення населення. Окремими категоріями, вартими пильної уваги з боку владних структур, визначено «кібербезпеку та фінансово-економічну стійкість, зокрема, безперервність основних бізнес-процесів» [1]. Таким способом встановлено тісний зв'язок між системою стійкості держави та фінансово-економічною безпекою мікро та макрорівневих господарських систем.

Отже, метою управління фінансово-економічною безпекою суб'єктів господарської діяльності має бути ухвалення рішень щодо виявлених загроз їх поточній та перспективній діяльності, визначення тактик ризик-менеджменту, до яких варто вдатись, зважаючи на наявні фінансово-економічні обставини функціонування бізнес-структур, розробка заходів компенсації втрат від дії неоптимізованих загроз і ризиків на корпоративні ресурси суб'єктів господарювання, формування безпечного інформаційного простору функціонування підприємств, забезпечення надійності персоналу та контроль кадрових ризиків в умовах віддаленої роботи у режимі онлайн, оцінка рівня безпечності та ризиковості нових напрямів діяльності підприємств або переоцінка традиційних господарських рішень із урахуванням нових обставин внутрішнього та зовнішнього середовища. Також пропонується запровадження практики формування каталогів управлінських рішень, які належить ухвалювати залежно від цільових орієнтирів діяльності суб'єкта, його мети та видового різноманіття, видів і сили впливу загроз і ризиків фінансово-економічної природи походження на стан ресурсів підприємства, установи або організації.

Бібліографічні посилання

1. Зеленський затвердив національну «систему стійкості» до загроз нацбезпеки. URL: https://detector.media/infospace/article/192371/2021-09-28-zelenskyy-zatverdyv-natsionalnu-systemu-stiykosti-do-zagroz-natsbezpeky/ (дата звернення: 14.10.2021).

Каркоцький І. О.,
директор Запорізького
науково-дослідного експертно-
криміналістичного центру
МВС України

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ПРИНЦИПУ ОБ'ЄКТИВНОСТІ ТА ПОВНОТИ ДОСЛІДЖЕННЯ В СУДОВО-ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

Одним із джерел інформації, що сприяє встановленню істини під час розслідування злочинів, є численні інформаційні системи, в яких концентрується інформація про різноманітні об'єкти матеріального світу. На сьогодні, незважаючи на використання в розслідуванні даних, отриманих з різноманітних за цільовим призначенням та відомчою належністю систем, теорія спрямована на осмислення лише криміналістичних. Практика ж свідчить, що криміналістичного значення, в певній ситуації, набуває інформація, отримана з будь-яких систем [1, с. 252].

Провадження судово-експертної діяльності пов'язане з необхідністю забезпечення доступу до значного обсягу інформації та роботи з нею. Ця робота передбачає можливості нагромадження, зберігання, систематизації, копіювання, перетворення, пошуку, отримання, відтворення інформації, використання її для порівняння, створення спеціалізованих банків даних тощо. Без інформаційного забезпечення судово-експертна діяльність нині була б неможливою.

М. Я. Сегай уважав, що інформаційне забезпечення судової експертизи являє собою науково організований і безперервний процес накопичення, підготовки й надання систематизованої науково-технічної інформації, необхідної для вирішення судово-експертних завдань. Відомості, що є в інформаційній системі, повинні бути актуальними, тобто відповідати сучасному стану науки й техніки в певній галузі. Повнота інформації забезпечується охопленням усіх необхідних даних [2, с. 9].

Зокрема, статтею 20 Закону України «Про судову експертизу» від 25 лютого 1994 року передбачено, що підприємства, установи, організації незалежно від форми власності зобов'язані надавати безоплатно інформацію, необхідну для проведення судових експертиз, державним спеціалізованим установам, а також, за згодою, натурні зразки або каталоги своєї продукції, технічну документацію та іншу інформацію, необхідну для створення й оновлення методичної та нормативної бази судової експертизи [3].

Основними напрямами розвитку системи інформаційного забезпечення фахівці вважають: упровадження єдиної політики інформаційного забезпечення; створення багатоцільових інформаційних систем діяльності

органів виконавчої влади; оснащення інформаційних підрозділів сучасною потужною комп'ютерною технікою; створення умов для ефективного функціонування інформаційних обліків, забезпечення їх повноти, актуальності та безпеки; упровадження сучасних інформаційних технологій та багато ін. [4, с. 107–108].

Зазвичай в науково-дослідних інститутах судової експертизи Міністерства юстиції України та в експертних службах різних відомств для розробки нових, удосконалення вже розроблених експертних методик та їх адаптації до завдань правосуддя, інвентаризації й паспортизації методик створюються наукові лабораторії або спеціальні підрозділи.

Методи і методики вирішення експертних завдань є невід'ємним елементом інформаційного забезпечення судово-експертної діяльності, зокрема у зв'язку з процесом уніфікації і паспортизації наявних типових судово-експертних методик.

Такі відомості, що становлять інформаційну базу для проведення експертних досліджень, містяться в спеціальній та загальнонауковій літературі, в наукових звітах і архівах експертних висновків.

Зазначені інформаційні фонди повинні створюватися за кожним родом і видом судових експертиз, як перелік методів та методик з вказівкою на галузь застосування і коло вирішуваних завдань.

Наявні на цей час інформаційні ресурси щодо судово-експертної діяльності являють собою розрізнені сховища інформації, які є як на паперових носіях, так і у вигляді електронних копій.

Треба зазначити, що інформаційне забезпечення судово-експертної діяльності дедалі зростає. Наприклад, на сьогодні в Реєстрі методик проведення судових експертиз зареєстровано 1307 методик дослідження [5]. Велика кількість інформаційних джерел, їх видів за формами подання інформації та використовуваних технологій диктує необхідність створення єдиного інформаційного ресурсу, що містить інформаційні джерела з різних аспектів судово-експертної діяльності.

Цілком очевидно, що лише підвищення рівня інформаційного забезпечення судово-експертної діяльності в кінцевому підсумку повною мірою сприятиме об'єктивності та повноти проведених експертом досліджень.

Бібліографічні посилання

1. Бірюков В. В. Інформаційно-довідкове забезпечення розслідування злочинів: поняття, система, завдання. *Право і суспільство*. Дніпропетровськ, 2012. № 2. С. 252–255.
2. Сегай М. Я. Типология экспертных задач. *Криминалистика и судебная экспертиза*. Киев, 1988. Вип. 37. С. 9–18.
3. Про судову експертизу : Закон України від 25.02.1994 р. № 4038-XII (зі змінами та доповненнями). URL: http://zakon5.rada.gov.ua/laws/show/4038-12
4. Пясковський В. В., Чорноус Ю. М., Іщенко А. В., Алєксєєв О. О. Криміналістика : підручник. Київ : «Центр учбової літератури», 2015. 544 с.
5. Реєстр методик проведення судових експертиз URL: https: //rmpse.minjust.gov.ua/page/66.

Карчевський М. В.,
доктор юридичних наук, професор
Луганського державного університету
внутрішніх справ імені Е. О. Дідоренка

ПРОТИДІЯ ЗЛОЧИННОСТІ В УКРАЇНІ У ФОРМАТІ DATA SCIENCE

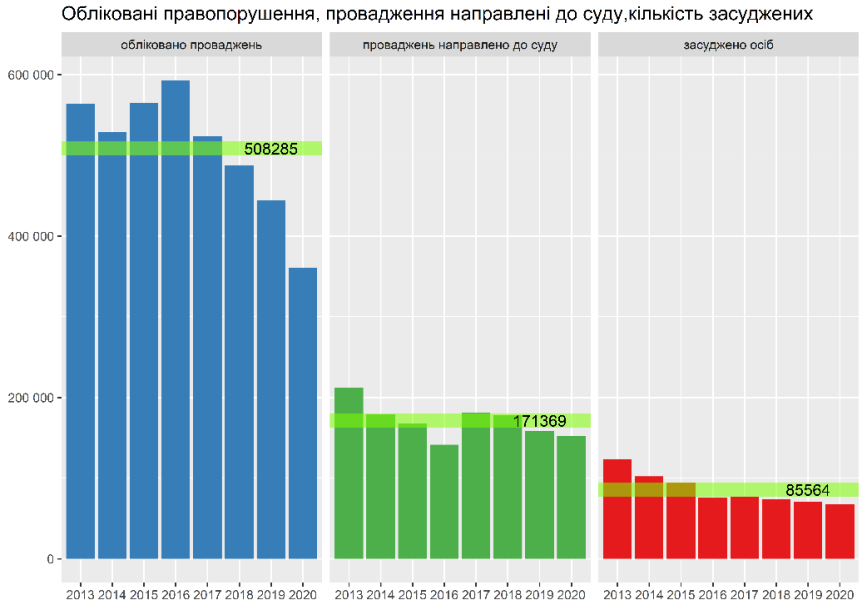
Статистичні дані дають змогу отримати уявлення щодо закономірності й тенденцій протидії злочинності. Їх аналіз є важливим складником процесу ухвалення рішень у галузі кримінально-правового регулювання. Водночас однією з актуальних проблем сучасної науки про суспільство є криза реплікації. Результати багатьох досліджень неможливо отримати в спосіб їх повторення. Це ставить під сумнів зміст і обсяг знань про суспільство. Зараз такі проблеми більше трапляються в психології та медицині. Можливість працювати з великими обсягами даних створила новий вид спокуси для дослідників, що полягає в недобросовісній добірці даних для аналізу. Як убачається, обираються тільки дані, які підтверджують гіпотези. У такий спосіб творяться дослідження, що відповідають формальним вимогам методології, пропонуючи нібито чіткі відповіді, але які, по суті, є хибними. Такі розвідки потрапляють до видань, що індексуються, отримують значний рейтинг цитування, але це не змінює їх підробленої суті.

Головним наслідком кризи реплікації є втрата довіри до науки як такої. Неможливість відтворити дослідження нівелює якість наукових аргументів у суспільному дискурсі, бере під сумнів доцільність їх використання. З іншого боку, процеси, скеровані на подолання проблем, зумовлених кризою реплікації, можуть розглядатися як шлях науки до нових репутаційних переваг. Подолавши недовіру до результатів дослідження, наука спроможна закріпити позиції в соціальному дискурсі. Якісно новий рівень довіри до наукових розвідок здатна забезпечити можливість відтворення результатів дослідження, що досягається через використання відповідної методології.

Доступність інформаційних технологій та даних офіційної кримінальної статистики дають нагоду використовувати методологію Data Science, здійснюючи цілком відтворювані кримінологічні дослідження. Саме таке дослідження нами виконано [1]. Отримані візуалізації дають змогу охарактеризувати зміст даних щодо протидії злочинності в Україні, що містяться у звітах Офісу Генерального прокурора України та Державної судової адміністрації за 2013–2020 роки. Результати роботи можуть бути використані для формулювання висновків щодо загальних тенденцій протидії злочинності в Україні, а також як емпірична база й підґрунтя побудови гіпотез подальших досліджень. Усі дані оброблялися лише автоматизовано. На їх підставі, знову ж таки програмним способом, будувалися візуалізації,

що використовуються для формулювання висновків. В онлайн-додатках до цієї розвідки наведено вихідні дані, дані, придатні до автоматизованої обробки, програмні коди для отримання первинних даних, їх обробки й візуалізації, графічні файли візуалізацій [2].

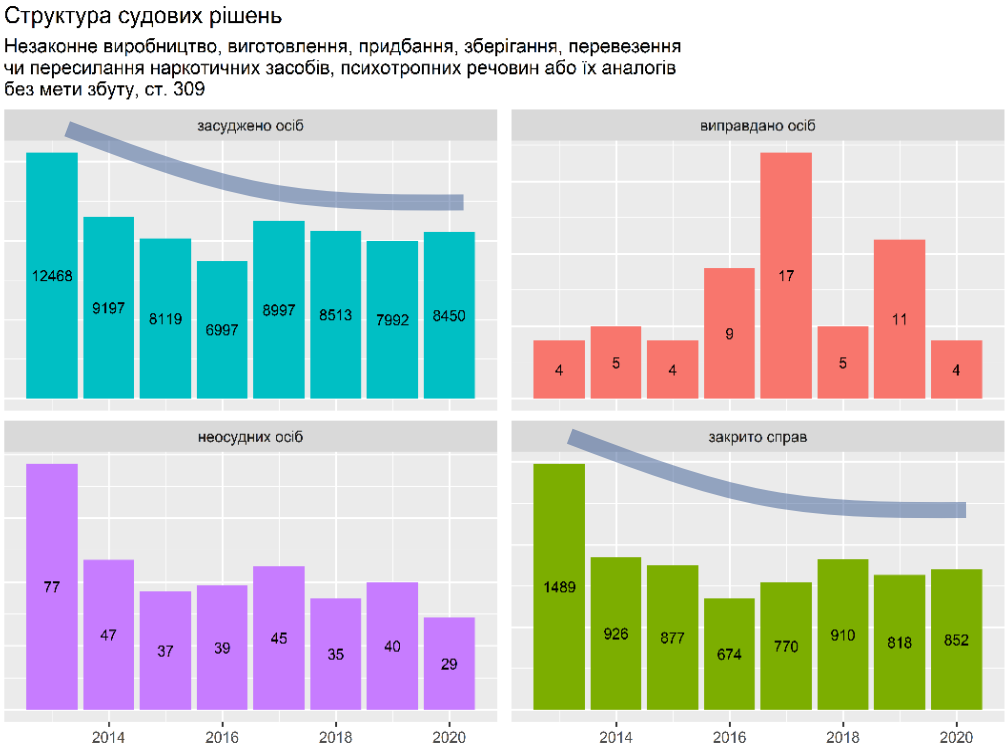
Основні зроблені нами висновки такі. Головні тенденції, що характеризують кримінально-правове регулювання в Україні в період із 2013 по 2020 роки, такі: зменшення кількості облікованих проваджень і засуджених осіб, зменшення суворості покарань, що призначаються.

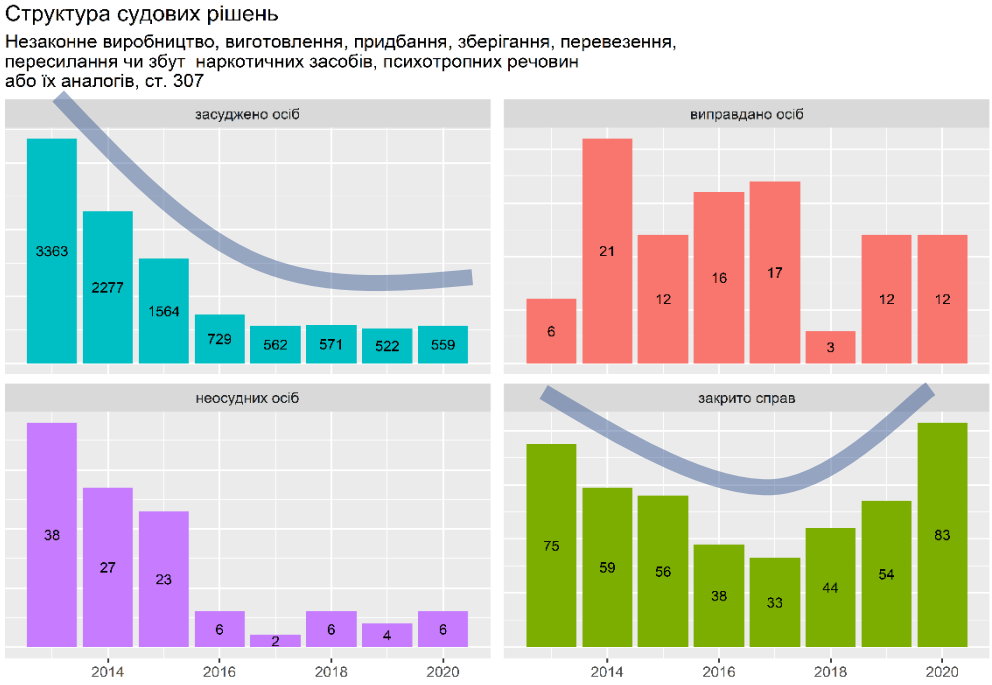


Можна вважати, що все означене свідчить про стійке зростання ефективності національного кримінально-правового регулювання. Менш суворі покарання забезпечують більш результативну протидію злочинності. Є підстави прогнозувати подальше стабільне зменшення злочинності.

Водночас така гіпотеза пояснює далеко не всі встановлені характеристики національного кримінально-правового регулювання.

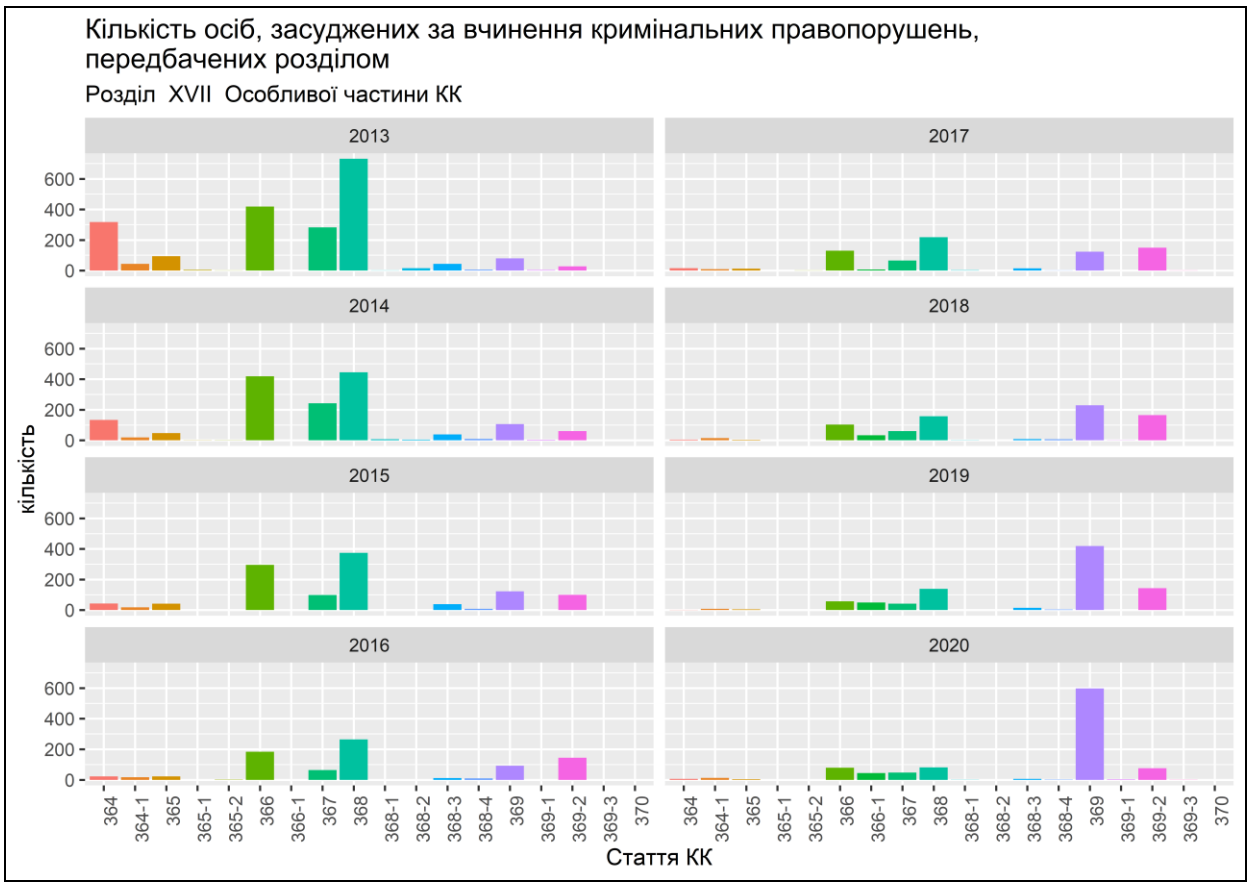
По-перше, кількість облікованих проваджень щодо кримінальних правопорушень, передбачених розділом XIII Особливої частини КК, із 2014 по 2016 роки зменшується з 30 до 23 тисяч, а з 2017 по 2020 роки становить майже 28, 29 тисяч [1, 105]. Подібну динаміку повторює і кількість засуджених осіб, яка з 2014 по 2016 роки зменшується з 14 до 9 тисяч, а з 2017 року тримається на середньому рівні – майже 10 тисяч. Видається, що означені коливання пов'язані радше з процесами реформування підрозділів Національної поліції щодо протидії незаконному обігу наркотиків, а загальне падіння показників обліку й засудження не свідчить про те, що відповідна соціальна проблема набула меншої гостроти. Такий висновок підтверджує і динаміка засудження за кримінальні правопорушення, передбачені статтями 307 та 309. У 2014 році за незаконні дії, пов'язані зі збутом наркотиків, було засуджено 2271 особу, а за подібні дії, але не пов'язані зі збутом – 9197 осіб [1, с. 162, 228]. У 2020 році показники становили 8450 та 559 осіб відповідно. Тобто, якщо в 2014 році на один розглянутий у суді факт збуту наркотиків припадало чотири факти незаконних дій, не пов'язаних зі збутом, то у 2020 році відповідне співвідношення становило 1 до 15. Зрозуміло, що засудження за збут наркотичних засобів потребує якісно іншого рівня складності досудового розслідування та судового розгляду. З огляду на зазначене визнаємо, що динаміка протидії другій за поширеністю групі кримінальних правопорушень є такою, що свідчить радше про недостатню реалізацію публічного інтересу в належній кримінальній юстиції, ніж про зниження рівня відповідної злочинності.





По-друге, протидія кримінальним правопорушенням у сфері службової діяльності. Було встановлено, що протягом досліджуваного періоду суттєво змінилася структура засуджених осіб за кримінально-правовою кваліфікацією. Якщо до 2018 року більшість осіб засуджували за отримання неправомірної вигоди, то починаючи з 2018 року – за пропозицію неправомірної вигоди. Абсолютні значення ще більш промовисті: у 2014 році за отримання неправомірної вигоди засуджено 445 осіб, за пропозицію – 106; у 2020 році за отримання неправомірної вигоди засуджено 81 особу, за пропозицію – 598 [1, с. 132]. До того ж процес був поступовим, відповідні тенденції зменшення / збільшення кількості засуджених осіб прослідковувалися протягом усього періоду спостережень. Чи означає це, що головною проблемою протидії корупції в Україні стала пропозиція неправомірної вигоди? Чи відповідає офіційна статистика реальній соціальній ситуації?

Для відповіді на поставлені запитання ми виконали розвідувальний контент-аналіз обвинувальних вироків за ст. 369 КК, які було винесено в 2020 році та наведено в базі інформаційно-аналітичної системи «Закон-онлайн». За названими ознаками було встановлено 404 судові рішення. Перші п’ять мали майже тотожні обставини та стосувалися пропозиції неправомірної вигоди поліцейським (прикордонникам) під час виконання ними службових обов’язків у складі добових нарядів (охорона громадського порядку, виконання обов’язків на пункті пропуску через державний кордон тощо). У всіх судових рішеннях йшлося про угоду щодо визнання винуватості. Вироки ухвалили судді судів Чернігівської, Сумської, Луганської, Волинської та Рівненської областей [3]. Тотожність обставин і географічний розподіл дають змогу розглядати отриману добірку судових рішень як репрезентативну для розвідувального аналізу.



Що ж до сформульованих запитань про відповідність фактичної судової практики соціальному запиту протидії корупції, вважаємо, що було отримано досить даних для негативної відповіді. Навряд чи сукупність актів застосування кримінального права, майже 4/5 якої являє собою засудження по угоді за пропозицію правоохоронцеві в складі добового наряду незначної неправомірної вигоди є такою, що відповідає соціальній потребі протидії корупції. У такому контексті зменшення кількості осіб, засуджених за кримінальні правопорушення у сфері службової діяльності, навряд чи свідчить про високу ефективність кримінально-правової протидії корупції.

По-третє, не менш болісна соціальна проблема кримінально-правового регулювання у сфері безпеки дорожнього руху. За даними Національної поліції, із 2017 року в ДТП гине майже дев'ять–десять осіб щодня. За даними Державної судової адміністрації, аналогічний період характеризується зменшенням кількості засуджених осіб із 2300 до 1721 особи та збільшенням закритих справ із 1772 до 2191 [1, с.186]. Майже дзеркальна та з огляду на специфіку показників «герметична» зміна. Знову ж таки можна сформулювати непросте запитання: зафіксована статистикою зміна тактики кримінально-правового забезпечення безпеки дорожнього руху – це соціальний тренд, що свідчить про більшу схильність потерпілих від ДТП до примирення, чи статистика відображає зростання непрофесійності досудового розслідування та впливу неформальних практик під час судового розгляду?

По-четверте, наведені дані не вичерпують прикладів неоднозначних тенденцій фактичної практики кримінально-правового регулювання в контексті наявних соціальних потреб. Згадаймо й збільшення кількості засуджених за злочини проти основ національної безпеки з одночасним збільшенням майже до 90 % звільнення від покарання за найбільш поширені злочини цієї групи в умовах гібридної війни [1, с. 29], і зменшення кількості засуджених за незаконне поводження зі зброєю з одночасним збільшенням кількості закритих справ в умовах «чорного» ринку зброї, що зростає [1, с. 180] тощо. Водночас звернемо увагу на загальну характеристику професійного дискурсу у сфері кримінальної юстиції. Досить усталеною є думка про те, що працівники правоохоронних органів проводять тривалу роботу щодо документування злочинних дій, а коли матеріали опиняються в суді, то використання неформальних практик дає змогу уникнути покарання. Не менш поширеною є й оцінка діяльності працівників правоохоронних органів як непрофесійної. Якість проведення досудового розслідування постійно падає, суди отримують такі матеріали, які унеможливлюють притягнення до відповідальності й призначення справедливого покарання. Тобто професійна комунікація фокусується на перекладанні відповідальності за неефективні дії щодо протидії злочинності між суб'єктами кримінально-правового регулювання. Водночас виконане дослідження об'єктивно показує поступове зменшення суворості покарання, зменшення частки обвинувальних вироків і кількості облікованих кримінальних проваджень, які не завжди зумовлені об'єктивними процесами зменшення злочинності.

Отже, як антитеза до висловленої попередньо гіпотези про загалом позитивну оцінку тенденцій та прогнозу протидії злочинності, може бути сформульована така інтерпретація результатів дослідження: через відсутність конструктивної професійної комунікації правоохоронних органів, прокуратури та судів публічний інтерес у належному функціонуванні системи кримінальної юстиції реалізовується не цілком. Непрофесійні дії під час обліку кримінальних проваджень, досудового розслідування та судового розгляду істотно зменшують ефективність протидії злочинності. Поширення непрофесійних дій створює широке корупційне поле, критично збільшуючи можливість уникнення покарання. Є підстави прогнозувати падіння рівня суспільної довіри до соціальних інститутів, які забезпечують дотримання законів, та, як наслідок, зростання злочинності.

На наше переконання, реальний стан справ почасти передають як перша, так і друга гіпотези. Дійсно, спостерігається певне зменшення рівня злочинності, але водночас фактично існують означені негативні процеси у сфері кримінальної юстиції. Мінімізація ризиків розвитку цих процесів, окрім традиційних заходів (законодавчих, організаційних, адміністративних, технічних, інфраструктурних тощо), передбачає передусім зміну фокусу професійної комунікації, що має бути скерована не на пошук «слабких

ланок», а на ефективну реалізацію публічного інтересу належного функціонування кримінальної юстиції.

Бібліографічні посилання

1. Карчевський М. В. Протидія злочинності в Україні (2013–2020): інфографіка. Київ : ВАІТЕ, 2021. 312 с.
2. Репозитарій онлайн додатків. URL: http://github.com/Nickolay78/Combating-crime-in-Ukraine-2013-2020
3. Вирок від 06.05.2020 р. у справі № 733/359/20 Бахмацький районний суд Чернігівської області. Вирок від 22.09.2020 р. у справі № 585/1976/20 Роменський міськрайонний суд Сумської області. Вирок від 03.11.2020 р. у справі № 423/2591/20 Лисичанський міський суд Луганської області. Вирок від 17.12.2020 р. у справі № 162/686/20 Любешівський районний суд Волинської області. Вирок від 17.07.2020 р. у справі № 566/1640/19 Млинівський районний суд Рівненської області.

Каткова Т. Г.,
доцент кафедри земельного
та аграрного права Державного
біотехнологічного університету,
кандидат юридичних наук, доцент

АДМІНІСТРАТИВНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Ст. 32 Конституції України передбачено, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією. Не допускається збирання, зберігання, використання й поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Закон України «Про захист персональних даних» у ст. 6 визначає, що обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством України. Згідно з ч. 1 ст. 24 Закону України «Про захист персональних даних» володілець персональних даних зобов'язаний забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

Закон України «Про захист персональних даних» у ст. 28 передбачає настання відповідальності відповідно до Закону. Отже, ця стаття є бланкетною та відсилає до положень Кодексу України про адміністративні правопорушення ст. 188-39, яка передбачає відповідальність за:

– неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей;
– невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних;
– недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних.

Аналіз судової практики свідчить, що найчастіше притягнення до адміністративної відповідальності та накладання штрафу в розмірі 5 100 грн відбувається за ч. 4 ст. 188-39 «Недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних».

Аналіз судової практики дозволяє виділити такі порушення під час роботи з персональними даними:

1. Розміщення персональних даних у вільному доступі. Зокрема, 21 травня 2020 року ОСОБА_1, перебуваючи на посаді віце-президента Національної академії державного управління при Президентові України, за місцем роботи допустила розголошення персональних даних, внаслідок опублікування на вебсайті Національної академії наказу від 30.04.2020 р. № 81 «Про затвердження Плану заходів щодо погашення заборгованості в гуртожиток готельного типу Національної академії», у додатку до якого викладено список мешканців гуртожитку, із зазначенням їх прізвищ та ініціалів, місця роботи і місця проживання, що проживають у ГГТ № 2 Національної академії та мають заборгованість за фактично надані послуги з проживання станом на 29.04.2020 р.

2. Розголошення персональних даних у відповіді на запит без згоди суб'єкта персональних даних.

Не поодинокі випадки, коли медичні персональні дані розголошуються під час відповіді на адвокатський запит або на запити лікарень. Наприклад, Комунальна установа Запорізька багатопрофільна клінічна лікарня № 9 зробила запит до Міської клінічної лікарні екстреної та швидкої медичної допомоги міста Запоріжжя щодо громадянина. Міська клінічна лікарня в особі головного лікаря надала відповідь про факт звернення особи за медичною допомогою та результатами його медичного обстеження, вказав його діагноз, ступінь тяжкості одержаної травми, групу крові і резус фактор.

3. Протиправна відмова в наданні соціальної допомоги у разі не отримання згоди на обробку персональних даних.

Треба відмітити, що така відмова може бути зумовлена релігійними

переконаннями особи. Наприклад, ОСОБА_1 є матір'ю шести дітей та подавала необхідний пакет документів для призначення цих видів допомоги. Але керуючись своїми релігійними православними переконаннями, не надала згоду на обробку своїх персональних даних. Управління праці та соціального захисту населення Бориславської міської ради повідомленням відмовлено в наданні державної допомоги (малозабезпеченій сім'ї та до 3-х років) у зв'язку з тим, що заявник не надав згоду на збір інформації та обробку персональних даних відповідно до Закону України «Про захист персональних даних». Суд дійшов висновку, що письмової згоди на обробку персональних даних для призначення державної соціальної допомоги законом не вимагається, оскільки дозвіл на обробку персональних даних наданий Управлінню праці та соціального захисту населення Бориславської міської ради Законом: ч. 2 ст. 32 Конституції України, п. 2 ст. 11 Закону України «Про захист персональних даних», тобто Управління за законом має право на використання даних без згоди суб'єкта персональних даних. Отримання від суб'єктів персональних даних письмової згоди на обробку їх персональних даних у сфері призначення допомоги не є обов'язковим, оскільки дозвіл на обробку їх персональних даних наданий законом виключно для здійснення його повноважень у сфері їх призначення.

4. Передача персональних даних фінансовими державними органами та установами третім особам.

Наприклад, між Державним підприємством «Головний проектно-виробничий і сервісний центр комп'ютерних і фінансових технологій» Міністерства фінансів України та ТОВ «Дельта М Юкрейн» було укладено договір про закупівлю послуг. На виконання вказаного договору Міністерство фінансів України в особі начальника відділу верифікації Управління верифікації та моніторингу виплат передало Державному підприємству «Головний проектно-виробничий і сервісний центр комп'ютерних і фінансових технологій» Міністерства фінансів України в особі заступника директора – головного інженера, яке передало директору ТОВ «Дельта М Юкрейн» оптичний носій CD з інформацією щодо фізичних осіб, які отримують соціальні виплати, пільги, субсидії за рахунок коштів державного та місцевого бюджетів, коштів Пенсійного фонду України. ТОВ «Дельта М Юкрейн» з метою проведення верифікації та подачі уточненої інформації до Міністерства фінансів України здійснювало телефонні дзвінки за вказаною базою даних. Суд дійшов висновку, що ТОВ «Дельта М Юкрейн» не може бути розпорядником персональних даних, тому що не належить до сфери управління Міністерства фінансів України. Отже, заступник директора Державного підприємства порушив вимоги Закону України «Про захист персональних даних», не забезпечивши належний рівень захисту персональних даних осіб, які отримують державні виплати.

Основною проблемою притягнення до адміністративної відповідальності є архаїчність та застарілість положень КУпАП – п. 7 ст. 247,

оскільки суд має ухвалити рішення щодо притягнення до відповідальності в межах 3 місяців з моменту вчинення правопорушення, а за триваючого правопорушення – не пізніш як через 3 місяці з дня його виявлення. Виходить, що особі досить часто вдається уникнути досить солідних штрафів.

Отже, адміністративна відповідальність за порушення законодавства у сфері захисту персональних даних в Україні потребує свого перегляду. Щодо цього європейський досвід та вимоги General Data Protection Regulation (GDPR) будуть доречними для удосконалення механізму адміністративної відповідальності за правопорушення у сфері захисту персональних даних в Україні.

Климюк І. М.,
викладач кафедри
адміністративного і кримінального
права Дніпровського національного
університету імені Олеся Гончара,
доктор філософії

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

У сучасному світі інформаційний простір має вагоме значення для людей та держав. Особливо у період пандемії коронавірусу, коли країни переходять на електронний документообіг, кожен замислювався над конфіденційністю власної інформації.

Безумовно, перехід до електронного обігу документів є закономірним процесом глобалізації та має позитивні і негативні сторони. До позитивних аспектів переходу держави в електронний документообіг належать: зручність використання; швидкість отримання інформації; відсутність зв’язку між людьми, що запобігає зараженню хворобами тощо. Зручно не виходячи з дому замовити певні документи та не гаяти час, який краще приділити більш важливим моментам. До того ж це знижує «бюрократичні окови» у суспільстві.

Проте є й негативні моменти, які здебільшого зводяться до нерозуміння населенням, як користуватися такими технологіями та можливості виходу приватної інформації до загального інформаційного простору.

Візьмемо як приклад соціальні мережі. Інколи їх «зламують», отримуючи доступ до приватної інформації – повідомлень (переписок). Але це не найстрашніше. Набагато гірше, коли «зламують» банківські системи, отримуючи доступ до коштів людей. Подібна ситуація може трапитись і

стосовно більш глобальних аспектів. Наприклад, якщо хакери «зламають» державні реєстри України або ж заволодіють інформацією, яка становить державну таємницю.

Вищезазначені приклади демонструють вже кримінально-карані діяння від шахрайства до шпигунства.

Саме тому економічна безпека країни нерозривно пов'язана з інформаційними технологіями, їх розвитком, використанням та охоронюваністю. Адже попереду нова епоха вже навіть не інформатизації, а роботизації та штучного інтелекту.

Коваленко А. О.,
аспірант кафедри менеджменту
та економічної безпеки Черкаського
національного університету
імені Богдана Хмельницького

РОЛЬ КАДРОВОГО ПОТЕНЦІАЛУ СУБ'ЄКТІВ ГОСПОДАРЮВАННЯ В УПРАВЛІННІ ЇХ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ

Кадрова безпека є однією з найважливіших складових комплексної системи економічної безпеки, тому безпеко орієнтований менеджмент неодмінно має поєднувати у собі підходи та інструментарій управління кадровими або інтелектуально-кадровими ризиками. Проблемні аспекти управління економічною безпекою висвітлені у публікаціях вітчизняних вчених [1–3]. Водночас мінливість умов функціонування бізнес-структур в Україні вимагає постійного перегляду канонів управління економічною безпекою як важливою характеристикою фінансово-господарського стану бізнес-структур.

Глобальна пандемія вкотре довела важливу роль персоналу підприємств у процесі реалізації функцій забезпечення їх економічної безпеки. Зокрема, під час переходу на дистанційну форму роботи сумлінне виконання кадровим складом своїх обов'язків без традиційних форм контролю, нагляду, неухильного дотримання трудового розпорядку – стало важливою конкурентною перевагою, а у окремих випадках – єдиною можливістю для виживання бізнесу, робота якого могла б бути повністю паралізованою через зупинку в карантин. Отже, все більше уваги управлінців має бути зосереджено на формуванні кадрового потенціалу суб'єктів господарювання з такими якісними характеристиками та у такій кількості, щоб ефективно та своєчасно організувати роботу віддалених команд у разі чергового переходу до дистанційної форми роботи.

Стрімке входження вітчизняних господарських структур до реалій роботи у режимі онлайн продемонструвало низький рівень готовності персоналу більшості суб'єктів господарювання до організації віддаленого робочого місця. Особливо важкими трансформації робочих процесів стали для осіб, старших за 50 років, оскільки для них користування всілякими технологічними пристроями, гаджетами для виконання своїх професійних обов'язків стало надскладним, а іноді взагалі неможливим для виконання завданням.

Розширення меж використання техніки та технологій, особливо персональних електронних пристроїв для робочих цілей, спровокувало збільшення кількості загроз для економічної безпеки господарських структур, пов'язаних із втратою інформації, несанкціонованим доступом до неї сторонніх осіб, її спотворення, використання не за призначенням тощо. Належний рівень знань і компетентностей персоналу щодо захисту інформаційних ресурсів і безпечної передачі даних міг би попередити названі негативні явища. Отже, виникає необхідність у оцінці кадрового потенціалу підприємств на предмет здатності до швидкої адаптації до нових умов праці, безпечного використання технічних пристроїв для виконання своїх посадових обов'язків, здатності до самоорганізації, дисципліни, ефективного тайм-менеджменту. Щодо останнього, то вважаємо, що питання раціонального управління часом дарма залишаються поза увагою управлінського персоналу, адже час уже давно визнається одним із важливих ресурсів сучасних підприємств, а для низки видів бізнесу – особливо інноваційних, різноманітних стартапів, тощо – це взагалі пріоритетний актив, що може забезпечити суттєві конкурентні переваги суб'єкту господарювання на ринку. Якщо працівник ефективно керує власним часом, розуміє, як краще організувати робочий день, вміє визначати пріоритети і своєчасно робити паузи для професійного «перезавантаження», концентрація його уваги буде високою, що не дозволить йому допуститись прорахунків і помилок, які можуть мати негативні наслідки для стану економічної безпеки суб'єкта господарювання. Рівень ефективності працівників, що не нехтують правилами тайм-менеджменту, зазвичай, набагато вищий, ніж у їх колег. А в ситуації, коли працівник має самостійно організувати свій робочий день із використанням дистанційних технологій, часто в умовах, не зовсім для цього придатних (наприклад, удома, де є інші мешканці зі своїми потребами та інтересами), навик управління часом стає просто необхідним.

Наявність кадрового потенціалу є необхідною для підтримки належного рівня економічної безпеки бізнес-структури, оскільки гарантує безперервність реалізації господарських процесів без вимушених зупинок, внаслідок яких підприємство може зазнати збитку, втрат ділової репутації, клієнтів і партнерів. Водночас кадровим потенціалом повинні бути особи, свідомі у питаннях економічної безпеки, що мають навички роботи в умовах

наявності численних внутрішніх і зовнішніх ризиків і знають, як себе поводити у різних виробничих обставинах.

Бібліографічні посилання

1. Зачосова Н. В., Шостак А. В. Концептуальні засади формування комплексної системи забезпечення фінансово-економічної безпеки підприємств та фінансових установ України. *Економіка та держава.* 2016. № 7. С. 80–83.
2. Зачосова Н. В. Механізм створення Фонду гарантування інвестицій як суб'єкта захисту економічної безпеки компаній з управління активами та торговців цінними паперами в Україні. *Економічний часопис-XXI.* 2010. № 5–6. С. 18–23.
3. Занора В., Сільченко Б. Управління системою економічної безпеки підприємства на основі проектного підходу. *Економічний вісник Запорізької державної інженерної академії.* 2017. № 5(11). С. 130–133.

Коваль О. В.,
аспірант кафедри менеджменту
та економічної безпеки Черкаського
національного університету
імені Богдана Хмельницького

ФАКТОРИ ВПЛИВУ НА ВИБІР СТРАТЕГІЇ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ СУБ'ЄКТА ГОСПОДАРЮВАННЯ

У практиці діяльності європейських та американських компаній стратегічне управління вважається важливим елементом менеджменту, тоді як в Україні цей аспект лише декларується як управлінська традиція, але фактично розроблені вітчизняними підприємствами стратегії залишаються тільки на папері. Причиною тому, з-поміж іншого, є неможливість точного прогнозування експертами тих умов, у яких підприємство провадитиме свою діяльність у довгостроковій перспективі через наявні реалії вітчизняного бізнесу. Нестабільність правового поля, залежність економіки від рішень і бажань міжнародних фінансових організацій і фондів, мінлива податкова політика, надмірна забюрократизованість організації та реалізації господарських процесів, залежність фінансової системи від іноземних валют, непотизм у владних колах – формують середовище господарської невизначеності та ускладнюють планування діяльності суб'єктів господарювання на тривалий період часу.

Управління економічною безпекою є одним із напрямів сучасного менеджменту. Загалом проблематика безпеко орієнтованого управління уже тривалий час знаходить відображення у публікаціях вітчизняних вчених [1–3], однак останнім часом вона усе частіше досліджується з позиції управління. Зважаючи на важливість стратегічного бачення бізнесом своїх

цілей в умовах постійних трансформацій господарського середовища, появи все нових форм і видів ризиків для нормальної діяльності підприємств, установ, організацій, виникає необхідність поєднання стратегій управління з управлінням економічною безпекою з метою недопущення їх суперечності одне одному, що неодмінно призведе до проблем у розподілі ресурсів, обранні пріоритетів, визначенні тактик поводження підприємства на ринку тощо.

Отже, робимо висновок щодо необхідності розробки топ-менеджментом підприємств стратегій забезпечення економічної безпеки та управління нею. Вважаємо за доцільне розпочинати цей процес із виявлення, уточнення та конкретизації факторів впливу на вибір стратегії управління економічною безпекою суб'єкта господарювання. Виконане дослідження дозволило запропонувати такий перелік факторів:

– розмір суб'єкта господарювання, кількість персоналу (чим більшим за розміром буде підприємство, тим більш узагальненими мають бути цілі його економічної безпеки, однак чим більшою є кількість персоналу, тим більш конкретними мають бути завдання щодо управління економічною безпекою, які адресуватимуться відповідальним особам);

– вид економічної діяльності суб'єкта господарювання, тривалість його виробничого та/або операційного циклу (наведені фактори формують перелік конкретних ризиків, які є характерними для підприємства, а тому мають бути враховані під час формування стратегії забезпечення його економічної безпеки як у довгостроковій, так і у поточній перспективі);

– базові стратегічні цілі функціонування суб'єкта господарювання (визначені генеральною стратегією підприємства за її наявності – йдеться про те, що цілі стратегії забезпечення або управління економічною безпекою мають ґрунтуватися на загальних цілях підприємства, сприяти їх досягненню і в жодному разі їм не суперечити; наприклад, якщо стратегічною ціллю є захоплення нових сегментів ринку та досить агресивне нарощення впливу у конкурентному середовищі, у такому випадку і стратегія економічної безпеки має бути агресивною, спрямованою на усунення наявних ризиків, подолання їх негативного впливу чи повну компенсацію їх наслідків у разі визнання невідворотності їх впливу на стан корпоративних ресурсів суб'єкта господарської діяльності);

– підприємницький клімат середовища функціонування суб'єкта господарювання (зовнішні загрози та виклики, ідентифіковані на момент розробки стратегії, мають допомогти визначити, чи буде стратегія економічної безпеки спрямована на їх уникнення, подолання, мінімізацію їх негативного впливу на результати діяльності підприємства у майбутньому, чи стратегія вирізнятиметься пасивним ставленням керівництва суб'єкта господарювання до наявних загроз, а також викликів, які ідентифікуються у цей конкретний момент часу, а також можуть з'явитися в перспективі);

– наявне ресурсне забезпечення (у тому випадку, коли суб'єкт

господарювання відчуває потребу у додаткових ресурсах, вільних активів для організації роботи по управлінню економічною безпекою у нього немає, стратегія має будуватись із мінімальними допустимими витратами на заходи безпеки; водночас, якщо підприємство має достатню кількість ресурсів, безпеко орієнтовані заходи мають бути комплексними, з обов'язковим контролем їх результативності та ефективності, а також економічного ефекту; не буде зайвим розрахунок, який зиск отримало б підприємство у випадку обрання альтернативного варіанту використання ресурсів, які були спрямовані на заходи забезпечення економічної безпеки суб'єкта господарювання.

Виявлені фактори необхідно покласти в основу розробки набору стратегій забезпечення економічної безпеки, з якого керівники вітчизняних підприємств у майбутньому могли б обрати шаблони, внести до них корективи і використати як власну безпеко орієнтовану стратегію.

Бібліографічні посилання

1. Зачосова Н. В. Механізм створення Фонду гарантування інвестицій як суб'єкта захисту економічної безпеки компаній з управління активами та торговців цінними паперами в Україні. *Економічний часопис-XXI*. 2010. № 5–6. С. 18–23.
2. Зачосова Н. В., Шостак А. В. Концептуальні засади формування комплексної системи забезпечення фінансово-економічної безпеки підприємств та фінансових установ України. *Економіка та держава.* 2016. № 7. С. 80–83.
3. Занора В., Сільченко Б. Управління системою економічної безпеки підприємства на основі проектного підходу. *Економічний вісник Запорізької державної інженерної академії.* 2017. № 5 (11). С. 130–133.

Користін О. Є.,
головний науковий співробітник
Державного науково-дослідного
інституту МВС України,
доктор юридичних наук, професор

РИЗИК-ОРІЄНТОВАНИЙ ПІДХІД У СТРАТЕГІЧНОМУ ВИМІРІ ВНУТРІШНЬОЇ БЕЗПЕКИ УКРАЇНИ

Безпековий зміст правоохоронної діяльності на сьогодні в Україні становить:

– Національна поліція України (поліція) – центральний орган виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку [1];

– Служба безпеки України – державний орган спеціального

призначення з правоохоронними функціями, який забезпечує державну безпеку України [2];

– Бюро економічної безпеки України – завданням якого є участь у забезпеченні економічної безпеки [3].

Безпекові складові правоохоронної діяльності:

а) досудове розслідування:

– закони про кримінальну відповідальність;

– закони щодо кримінальної процесуальної діяльності: обшуки, допити, арешти майна, вилучення носіїв інформації тощо;

б) інформаційно-аналітична складова:

– інформаційно-пошукова;

– розвідка;

– формування компетенцій.

Стратегічний вимір спрямовується на забезпечення уявлення щодо загроз у сфері внутрішньої безпеки, розуміння тенденцій злочинності та системи причинно-наслідкових зв'язків порушення правопорядку, а також є внеском у розроблення широких стратегій щодо правоохоронної політики та використання ресурсів)

За сучасних умов безпекознавчий підхід стає ризик-орієнтованим підходом у таких напрямках:

– безпечне середовище;

– рівень безпеки;

– оцінка загроз, ймовірність, наслідки;

– оцінка ризиків, критерії ризиків, профіль ризиків;

– уразливість, спроможність, стійкість.

Вільної від ризику поведінки не існує, якщо рішення не приймається і суб'єкт утримується від дій, то все одно ризику він не уникає

Відповідно до Стратегії національної безпеки України, Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме:

– оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей;

– поширення необхідних знань і навичок у цій сфері [4].

У секторі громадської безпеки гібридні загрози класифікуються так:

– інформаційні гібридні загрози;

– гібридні загрози, пов'язані з кібернетами;

– гібридні загрози, пов'язані зі злочинністю;

– гібридні погрози, пов'язані з провокацією громадянської непокори, порушенням громадського порядку;

– гібридні загрози, пов'язані з об'єктами критичної інфраструктури;

– гібридні загрози, пов'язані з корупцією.

Кримінальна ситуація в Україні у 2013-2020 рр. характерихується тим,

що на сьогодні помітна тенденція до постійного скорочення чисельності кримінальних правопорушень у сфері господарської діяльності – зменшення у 2,1 раза з 11 104 у 2013 р. до 5342 у 2020 р., зокрема:

– злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів – у середньому 23,7% від усіх таких злочинів;
– крадіжки – 9,0%;
– розбої – 4,6%;
– привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем – 4,5%;
– незаконне виготовлення, зберігання, збут або транспортування з метою збуту підакцизних товарів – 2,4%;
– хабарництво та отримання неправомірної вигоди – 2,4%;
– грабежі – 1,8%;
– вимагання – 1,7%;
– незаконний обіг зброї – 1,6%.

Організована злочиність у фіскальній сфері має на сьогодні такі ознаки:

– характеристика за видами злочинів, податків та галузей економіки
– «професіоналізація» кримінальної діяльності ОЗУ
– способи вчинення злочинів
– можливості ОЗУ використовувати фінансові та ін. ресурси їх обсяги
– використання ОЗУ осіб із спеціальними навичками й знаннями
– полікримінальна діяльність
– адаптивність та гнучкість
– здатність ОЗУ відмивати доходи від протиправної діяльності
– кримінальна інфраструктура
– контрзаходи
– корупційні зв'язки
– озброєність
– кримінальний досвід
– транснаціональні зв'язки
– фактори, які сприяють злочинній діяльності
– попит і пропозиція

Викладене зумовлює констатувати таке:

– необхідність формування нового рівня мислення в правоохоронних органах на основі адекватного сприйняття ризику як особливого методу пізнання та управління;
– існує проблема фактичної недостатності знань та систематизації реалізації державної правоохоронної політики на всіх рівнях управління, навіть у разі відвертого бажання передбачити майбутні умови та наслідки реалізації;
– наявність системи необхідних знань не завжди є гарантією компетентності та вміння прогнозувати на основі прогнозування ризиків;

– процес управління ризиками має стати невід'ємною частиною загальної стратегії розвитку.

Бібліографічні посилання

1. Про Національну поліцію: Закон України від 02 липня 2015 року (зі змінами і допов.) Відомості Верховної Ради України. 2015. № 40-41 Ст.379.
2. Про Службу безпеки України : Закон України від 25.03.1992 року (зі змінами і допов.). Відомості Верховної Ради України. 1992. №27. ст. 382.
3. Про Бюро економічної безпеки України : Закон України від 28.01.2021. Відомості Верховної Ради (ВВР), 2021, № 23, ст.197.
4. Стратегія національної безпеки України «Безпека людини – безпека країни» : затв. Указом Президента України від 14.09.2020. URL : https://zakon.rada.gov.ua/ laws/show/392/2020#Text.

Корнейко О. В.,
завідувач кафедри інформаційних технологій та кібербезпеки НАВС, кандидат технічних наук, професор

Школьніков В. І.,
старший викладач кафедри інформаційних технологій та кібербезпеки НАВС

ДОСВІД ОСВІТНЬО-НАУКОВОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ У СФЕРІ КРИМІНАЛЬНОЇ АНАЛІТИКИ

На цей час інформаційно-аналітичні технології знаходять достатньо широке використання під час попередження, розслідування, розкриття та прогнозування кримінальних правопорушень, забезпечення ведення оперативно-розшукової діяльності (ОРД) правоохоронними органами України, зокрема підрозділами кримінального аналізу, кіберполіції, стратегічних розслідувань й інших структур кримінального блоку Національної поліції (НП) України.

Тому вивчення та розвиток новітніх технологій та методик здійснення кримінального аналізу (КА), інформаційно-пошукової та аналітичної роботи є одним із важливих напрямів освітньої та наукової діяльності Національної академії внутрішніх справ (НАВС) під час підготовки, перепідготовки та підвищення кваліфікації працівників НП України.

Вперше планова підготовка в НАВС фахівців у сфері КА для підрозділів НП України розпочалась у 2017 році на базі кафедри фінансової безпеки та фінансових розслідувань, де вивчались теоретичні основи та

загальна методологія ведення КА, особливості здійснення оперативного, тактичного та стратегічного аналізу під час розслідування кримінальних правопорушень. І сьогодні кафедра продовжує надавати такі знання всім здобувачам вищої освіти, що навчаються в НАВС і здобувають освітній рівень бакалавра та магістра.

Починаючи з 2018 року з метою надання здобувачам вищої освіти НАВС практичних навичок застосування сучасних інформаційних технологій (ІТ) та програмних засобів під час здійснення інформаційно-пошукової та аналітичної роботи до підготовки фахівців у сфері КА приєдналась і кафедра інформаційних технологій та кібербепзеки НАВС. Для цього кафедрою були розгорнуті сучасні комп'ютерні класи, розроблені нові авторські курси та методики у сфері технологій КА, в тому числі для ведення ОРД в кіберпросторі.

У 2018–2019 та 2019–2020 навчальних роках на кафедрі проводилась планова підготовка курсантів, які навчались в НАВС для комплектування органів досудового розслідувань НП України, з розширенням їх фахових компетенцій у сфері інформаційно-аналітичної підтримки слідчої діяльності. А починаючи з 2020–2021 навчального року підготовка фахівців у сфері сучасних технологій КА здійснюється на кафедрі вже для здобувачів НАВС, які навчаються для подальшого комплектування підрозділів кримінальної поліції.

Під час навчання на кафедрі інформаційних технологій та кібербезпеки НАВС, опановуючи традиційні дисципліни для майбутніх працівників аналітичних та оперативних підрозділів поліції, курсанти навчаються:

– особливостям організації та здійснення оперативно-розшукової, інформаційно-пошукової та аналітичної роботи в підрозділах кримінальної поліції за допомогою технологій ILP (англ. Intelligence Led Policing, поліцейська діяльність керована аналітикою) та OSINT (англ. Open Source INTelligence – розвідка на основі відкритих джерел інформації);

– застосовувати під час здійснення ОРД спеціалізовані програмні засоби та сервіси для пошуку та аналізу за допомогою технологій OSINT оперативної інформації про фізичних та юридичних осіб, необхідні документи та зображення в поверхневій (Surface Web), глибинній (Deep Web) та темній (Dark Web) частинах мережі «Інтернет», в соціальних мережах, в державних реєстрах та інформаційних системах, в системах електронного банкінгу тощо;

– здійснювати заходи щодо забезпечення анонімної ОРД в мережі «Інтернет»;

– використовувати технологію ILP та основні функції програмних засобів Microsoft Word, Excel, Power BI та IBM i2 Analyst's Notebook для обробки та кримінального аналізу здобутої оперативної інформації;

– застосовувати програмний засіб Belkasoft як інструментарій для збирання, обробки та аналізу електронних (цифрових) доказів з мережі

«Інтернет», персональних комп'ютерів, мобільних пристроїв тощо;

– використовувати основні функції програмного продукту ArcGIS для геоінформаційного відображення оперативної інформації на електронних картах місцевості;

– здійснювати візуалізацію великих обсягів здобутої та проаналізованої оперативної інформації та інші заходи щодо інформаційно-аналітичної роботи тощо.

Для забезпечення цієї освітньої діяльності в НАВС є відповідна сучасна матеріально-технічна база. Зокрема, академія зареєстрована на відповідних освітніх порталах (Octopus Cybercrime Community, «SPACE» – The Secure Platform for Accredited Cybercrime Experts) та бере участь у навчальних програмах (Microsoft Office for Education, Gsuit for Education, IBM Academic Initiative), які дозволяють отримувати ліцензоване програмне забезпечення та проводити освітній процес на високому методологічному рівні.

Для підтримки цієї освітньої діяльності кафедри на підставі рішення Вченої ради НАВС від 07.07.2020 р. та за підтримки керівництва Департаменту кримінального аналізу НП України в НАВС як самостійний структурний підрозділ був створений відповідний Центр кримінальної аналітики. Основними завданнями цього Центру є здійснення науково-освітньої діяльності у сфері кримінального аналізу, впровадження разом з кафедрою новітніх ІТ в практичну діяльність НП України, підтримання курсантської молоді НАВС в задоволенні їхніх наукових інтересів у сфері КА та кіберрозвідки.

Хоча Центр тільки розпочав свою діяльність, але за час свого функціонування його співробітниками разом з науково-педагогічними працівниками кафедри інформаційних технологій та кібербезпеки:

– було проведено на платформі Google Classroom онлайн тренінги «MS Excel у кримінальному аналізі» та «Аналітичні програмні продукти в кримінальному аналізі (Microsoft Excel, IBM i2 Analyst's Notebook, Power BI, ArcGIS)» для співробітників підрозділів кримінального аналізу, внутрішньої безпеки, кіберполіції, карного розшуку, оперативно-технічних заходів, оперативної служби, протидії наркозлочинності та боротьби зі злочинами, пов'язаними з торгівлею людьми НП України;

– були організовані та проведені курси підвищення кваліфікації для працівників практичних підрозділів кримінального аналізу НП України, де розглядались новітні методики та технології здійснення КА із застосуванням сучасного програмного забезпечення;

– підготовлено низку практичних посібників, що детально розкривають специфічні методики та технології проведення КА, серед яких, наприклад, такі: «Кластерний аналіз інформації про телефонний трафік»; «Обробка та аналіз за допомогою MS Excel та IBM i2 Analyst's Notebook інформації щодо одночасного перетину кордону декількома особами»; «Обробка та аналіз інформації з Державного реєстру нерухомого майна Міністерства юстиції

України»; «Обробка та аналіз інформації з інформаційно-аналітичного комплексу “Безпечне місто”»; «Встановлення місцезнаходження та маршруту руху особи чи транспортного засобу за допомогою геоінформаційного програмного продукту ArcGIS»;

– здійснюється науково-аналітичне опрацювання результатів проведеного онлайн курсу з кібергігієни для працівників апарату МВС України (у межах спільного проєкту Консультативної місії Європейського Союзу й української компанії з кібербезпеки ISSP), а також підготовка відповідних методичних рекомендацій тощо.

Отже, можна стверджувати, що стрімкий розвиток сучасних інформаційно-аналітичних технологій зумовлює переосмислення змісту поліцейської діяльності, а теоретичні та практичні наробки науковців та викладачів НАВС у сфері кримінальної аналітики дозволяють підготувати нову генерацію працівників поліції, що здатні виконувати складні інформаційно-аналітичні завдання для ефективного попередження, розслідування, розкриття та прогнозування кримінальних правопорушень.

Косиченко О. О.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІЗУАЛІЗАЦІЇ ДАНИХ У БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ

Максимально повна картина того, що відбувається на основі даних, є ключем до своєчасного втручання та ефективному запобіганню злочинів. Правоохоронні органи по усьому світу усе більше використовують технології візуалізації даних [1–3]. Тож поліцейські у всьому світі активно працюють із системами відеоспостереження, які в реальному часі збирають зведення про злочини, відомості про дорожню ситуацію, геопросторові, метеорологічні та інші дані. Рішення ухвалюються на основі достовірних і надійних відомостей, що дозволяє вчасно виділяти необхідні ресурси для результативного втручання та попередження злочинів. Візуалізація даних відкриває широкі можливості. Зібравши всі дані в загальну картину, можна ефективніше виявляти та запобігати злочинам. Але якщо даних занадто багато, ефект може бути зворотним. Обсяг даних зростає по експоненціальному закону, причому більша частина інформації надходить у неструктурованому (текстовому) вигляді, що ускладнює обробку, аналіз та

використання.

Якщо ви не здатні сформувати загальну картину, то можете не помітити критично важливу інформацію, а отже, ухвалити неправильне рішення або зовсім не діяти. Це може загрожувати суспільній безпеці. Технології візуалізації даних допомагають упоратися з цією проблемою, формуючи наскрізний ланцюжок, від доступу до даних до їхньої візуалізації, пошуку й аналізу в єдиному середовищі.

Візуальна аналітика допомагає оперативно аналізувати дані з різних джерел і готовити тактичні та стратегічні звіти для нарад керівництва. Ці звіти можуть поставлятися в декількох форматах, у тому числі на веб- і мобільні платформи.

Такий підхід дозволяє швидко обробляти накопичені великі дані й знаходити відповіді на головні питання. Він допомагає виявляти тенденції й інтерпретувати візуальні шаблони в даних, регулярно формувати тактичні й стратегічні звіти в різних форматах і розподіляти ресурси для ефективного попередження й втручання. Візуальна аналітика доповнює цей підхід: завдяки їй правоохоронці можуть виконувати поглиблений аналіз даних, виявляти приховані можливості, визначати головні взаємини та швидше ухвалювати точні рішення.

Крім прямого аналізу інформації, на який поліцейські традиційно покладалися під час розслідувань, візуальна аналітика дозволяє простежити більш складні взаємозв’язки в цих даних. У результаті можна буде виявити кореляцію між збільшенням кількості злочинів, пов’язаних з наркотиками, і тим, як розподіляються співробітники по напрямах боротьби зі злочинністю.

Візуальна аналітика також допомагає поліції краще служити суспільству. Наприклад, збиток від автомобільних аварій становить приблизно 800 млрд доларів у рік, а пов’язані з цим людські страждання зовсім не піддаються оцінці. Використовуючи візуальну аналітику, поліцейські зможуть установлювати причини аварій, визначати ділянки концентрації дорожньо-транспортних випадків тощо, тобто сприяти поліпшенню ситуації на дорогах і порятунку багатьох життів.

Ще один найважливіший аспект: інструменти візуальної аналітики призначені для самостійної роботи користувачів. Фахівці It-підрозділів можуть відчувати деяке занепокоєння щодо збільшення навантаження. Однак вони повинні знати, що візуальна аналітика – це інтуїтивно зрозумілі інструменти. Співробітники поліції зможуть самостійно створювати візуальні звіти без допомоги It-підрозділів.

Технології візуалізації даних будуть необхідні практично всім співробітникам поліції, а потенційні вигоди поширюються на усе населення. Крім того, зміщається акцент самих правоохоронних органів; вони все частіше прагнуть не просто розслідувати злочини, а вживати профілактичних заходів. Чим більше поліцейських зможуть побачити загальну картину, тим вища ймовірність швидкого та результативного попередження та розкриття

злочинів. У цей час формуються всі умови для активної реалізації цієї концепції. Саме такого підходу сьогодні очікує суспільство.

Бібліографічні посилання

1. Косиченко О. О., Дисковський О. А. Використання методів візуалізації в інформаційно-аналітичній діяльності. *Використання інформаційних технологій в діяльності Національної поліції України* : зб. наукових статей за матеріалами доп. учасників науково-практ. семінару (м. Дніпро, 23 лист. 2018 р.). Дніпро : ДДУВС, 2018. С. 25–27.
2. Kosychenko O. O. Peculiarities of the use of visual means of time analysis as a tool of investigations in law enforcement. *International and national security: theoretical and applied aspects* : theses of the IV-th International scientific practical conference (Dnipro, March 13, 2020). Dnipro : Dniprop. State Univ. of Int. Aff, 2020. S. 144–146.
3. Кирилова З. Crystal – инструмент для расследования махинаций с криптовалютами. URL: https://hightech.fm/2018/01/31/crystal (https://crystalblockchain.com/about)

Крамаренко Ю. М.,
доцент кафедри
кримінально-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ОКРЕМІ ТЕНДЕНЦІЇ У СФЕРІ ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ (за матеріалами Європолу)

Організована злочинність є тим соціальним явищем, що не тільки негативно впливає на рівень добробуту суспільства та безпеки держави, а й відображає вразливість системи управління соціальними та державними процесами. Орієнтація організованої злочинності на отримання надприбутку та легалізацію доходів, в тому числі внаслідок створення законних бізнес-структур, призводить до прагнення таких структур до зменшення або ухилення від сплати податків за рахунок злочинних схем чи преференцій від держави. Це пов’язано не лише прагненням до надприбутку, а й тим, що організовані злочинні організації, які в змозі легалізувати кошти, отримані злочинним шляхом, мають низку додаткових витрат – корупція, підтримання вигідної суспільної думки, витрати на консультантів тощо. Як наслідок, державний та місцеві бюджети недоотримують кошти, а реформи та інвестування в різні сфери життєдіяльності не мають очікуваних результатів.

Відповідно до Стратегії економічної безпеки України на період до 2025 року, введеною в дію Указом Президента України № 347/2021 від 11 серпня 2021 року, до основних викликів та загроз у сфері фінансової безпеки віднесено «високий рівень тінізації економіки», «втрата доходів бюджету

внаслідок поширених явищ «сірого» імпорту та контрабанди, схем ухилення від оподаткування, розмивання бази оподаткування шляхом використання «низькоподаткових» юрисдикцій», «непослідовність правового регулювання відносин у податковій сфері» та «поширення явища легалізації (відмивання) доходів, одержаних злочинним шляхом» [1].

З огляду на суттєвий негативний вплив організованої злочинності на державні та соціальні процеси демократичні країни всього світу прагнуть до протидії цьому явищу. Одним із показових та зразкових засобів моніторингу тенденцій у сфері організованої злочинності є методологія «Оцінки загрози серйозної та організованої злочинності» – SOCTA (Serious and organised crime threat assessment), що є складовою чотирирічного циклу політики ЄС стосовно організованої та серйозної міжнародної злочинності (EU POLICY CYCLE – EMPACT). Такі періодичні звіти відображають основні тенденції у сфері злочинності, що можуть братися за основу в інших країнах. Тож серед висновків, наданих у звіті 2021 року (EU SOCTA 2021), можна виділити такі тенденції:

– організована злочинність (далі – ОЗ) є головною загрозою внутрішній безпеці ЄС;

– ОЗ має «мережеву» побудову з високим рівнем внутрішньої взаємодії та орієнтацією на прибуток;

– серцевину (ядро) злочинної мережі становлять управлінські рівні та «польові ділки», що оточені різними фахівцями, пов’язаними із злочинною інфраструктурою, які відіграють забезпечуючу роль;

– висока адаптація ОЗ до середовища та отримання вигоди від змін;

– застосування корупційних механізмів (майже 60 % злочинних груп вдаються до корупції);

– наявність «паралельної» фінансової системи, що дозволяє «відмивати» злочинні доходи у великих масштабах;

– створення, контроль або проникнення в легальні бізнес-структури (понад 80 % злочинних мереж використовують легальні бізнес-структури);

– активне використання нових технологій для здійснення злочинної діяльності, в т. ч. використовують різні засоби комунікації для швидкого та широкого охоплення «аудиторії» під час просування реклами нелегальних товарів та поширення дезінформації;

– висока причетність ОЗ до незаконного обігу наркотиків (38 % злочинних мереж);

– висока світова розгалуженість злочинних мереж (майже 70 % діють у більше ніж трьох країнах) [2].

Аналізуючи статистичні дані щодо ОЗ в Україні, можна помітити темпи зростання кількісних показників. Зокрема, у 2016 р. в Україні виявлено 136 організованих груп та злочинних організацій, у 2017 р. – 210, у 2018 р. – 288, у 2019 р. – 293, у 2020 р. – 377, а за 9 місяців 2021 р. – 460 [3]. Зважаючи на загальносвітові тенденції, що передбачають взаємопроникнення

інформації, технологій та ресурсів, під час дослідження та протидії організованій злочинності в Україні треба враховувати не тільки наявні «привабливі» ресурси та залученість нашої країни до економічних і соціальних процесів Європи та світу, а й особливість формування вітчизняної політичної та економічної еліти. Вказане дозволяє припустити, що прагнення отримання ОЗ контролю над управлінням легальними бізнес-структурами в Україні, органами влади та соціально-економічними процесами буде постійно зростати. Вкладення коштів суб'єктами ОЗ у нові суб'єкти господарської діяльності, окремі сфери економіки чи технології матиме швидкоплинний ефект для соціально-економічного стану країни, оскільки сама суть та специфіка злочинного середовища орієнтована на швидке збагачення, експлуатацію, експансію та суперництво. Тому об'єктами моніторингу для правоохоронних органів (в т. ч. об'єктами оперативно-розшукових заходів) повинні бути саме новостворювані суб'єкти господарювання або «ключові гравці» в пріоритетних сферах економіки та особи, що залучені до процесів реформування соціальних, правових та економічних інститутів.

Бібліографічні посилання

1. Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року «Про Стратегію економічної безпеки України на період до 2025 року» : Указ Президента України № 347/2021 від 11 серпня 2021 року. URL: https://www.president.gov.ua/documents/3472021-39613
2. European Union serious and organised crime threat assessment. Report Serious Organised Crime (SOCTA/OCTA). URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment
3. Офіційний сайт Офісу Генерального прокурора. Статистика. URL: https:// https://www.gp.gov.ua/ua/1stat

Куценко Д. М.,
аспірант кафедри менеджменту
та економічної безпеки Черкаського
національного університету
імені Богдана Хмельницького

ПЕРЕДУМОВИ ВИКОРИСТАННЯ КОМПЛЕКСНОГО ПІДХОДУ ДО ФОРМУВАННЯ МЕХАНІЗМУ УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ

Традиційні механізми управління економічною безпекою, які зводяться до попередження збитковості підприємства за будь-яку ціну та забезпечення отримання його власниками прибутку або досягнення іншого економічного чи соціального ефекту з мінімальними ризиками, продовжують доводити

свою неефективність у контексті нових викликів для вітчизняних суб'єктів господарської діяльності. Тільки за останні роки (2019–2021) відчутними стали такі інноваційні загрози для нормального функціонування бізнесу, як карантин (примусове припинення діяльності через епідеміологічну ситуацію або з інших причин), проблеми організації роботи в онлайн форматі (дистанційно), проблеми контролю результатів роботи віддалених команд або окремих працівників, необхідність організації фінансової роботи та розрахункових операцій повністю у безготівковому форматі. З огляду на перераховані проблемні аспекти, природа походження яких є різноманітною – і кадри, і інформаційне поле, і фінанси підприємств – виникає необхідність у використанні комплексного підходу до формування механізму управління економічною безпекою підприємств України різних видів економічної діяльності. Це не означає, що потрібно з нуля вибудовувати системи забезпечення економічної безпеки господарських структур – як свідчать виконані науковцями дослідження [1–3], такі системи у різному функціональному стані є притаманними для вітчизняного бізнесу. Водночас необхідно оновити, модернізувати, трансформувати підходи до управління економічною безпекою, запропонувати інноваційний інструментарій для оцінювання досягнутого у процесі менеджменту рівня захищеності корпоративних ресурсів підприємств від внутрішніх і зовнішніх загроз, ризиків тощо.

За даними статистики, місцеві господарські суди у 2020 році розглянули 73,1 [74,6] тис. господарських справ. Кількість справ про банкрутство становила 13414 (18,34 % від усіх справ) у 2020 році та 14140 (18,96 % від усіх справ) у 2019 році [4]. Тож хоча спостерігається зменшення кількості розглядів судових справ про банкрутство підприємств, все ж випадки втрати фінансової стійкості та ліквідності, що є передвісниками банкрутства і ліквідації суб'єкта господарювання у перспективі, важко назвати поодинокими. І причиною їх стабільної тенденції є, з-поміж іншого, низько ефективні механізми забезпечення економічної безпеки, у межах яких мають реалізовуватись управлінські завдання ризик-менеджменту, забезпечення надійності персоналу, раціонального управління часом (особистого тайм-менеджменту працівників і корпоративного тайм-менеджменту). Розбалансування роботи елементів механізму управління економічною безпекою призводить до того, що підприємство отримує збиток. Відомості Державної служби статистики України містять інформацію про те, що за січень-червень 2021 року 26,1 % усіх підприємств в Україні одержали збиток у загальному розмірі 63791,6 млн грн. Отже, можемо говорити про те, що понад чверть суб'єктів підприємницької діяльності у державі потребують негайної ініціації змін у будові та/або функціонуванні їх механізмів управління економічною безпекою.

Застосовуючи комплексний підхід, пропонуємо механізм управління економічною безпекою будувати з врахуванням:

– досягнутого рівня економічної безпеки (дасть змогу зробити висновок, чи була на підприємстві практика управління економічною безпекою, які недоліки мав наявний механізм, чи є взагалі необхідність щось поліпшувати і в якій управлінській площині);

– наявного кадрового потенціалу (необхідно розуміти, чи має управлінський персонал необхідні знання і навики для безпеко орієнтованого менеджменту, чи краще передати ці функції на аутсорсинг);

– масштабів і рівня складності фінансово-господарських операцій (необхідно враховувати розміри підприємства, вид економічної діяльності, набір активів, функціональний стан яких потрібно стабілізувати або захищати);

– обов'язковості ефективного захисту ресурсів підприємства за умови його переходу до роботи у режимі онлайн;

– інтеграції або розширення меж використання прийомів і інструментарію ризик-менеджменту системі забезпечення економічної безпеки підприємства;

– стратегічних цілей, визначених керівництвом підприємства, для різних напрямів його роботи (управління економічною безпекою має всіляко сприяти успішній реалізації стратегії діяльності суб'єкта господарювання, а не відволікати надмірні ресурси від цільових операцій, що приносять підприємству прибутки).

Такий підхід дозволить побудувати ефективний механізм управління усією системою забезпечення економічної безпеки підприємства.

Бібліографічні посилання

1. Зачосова Н. В. Механізм створення Фонду гарантування інвестицій як суб'єкта захисту економічної безпеки компаній з управління активами та торговців цінними паперами в Україні. *Економічний часопис-XXI.* 2010. № 5–6. С. 18–23.
2. Зачосова Н. В., Шостак А. В. Концептуальні засади формування комплексної системи забезпечення фінансово-економічної безпеки підприємств та фінансових установ України. *Економіка та держава.* 2016. № 7. С. 80–83.
3. Занора В., Сільченко Б. Управління системою економічної безпеки підприємства на основі проектного підходу. *Економічний вісник Запорізької державної інженерної академії.* 2017. № 5 (11). С. 130–133.
4. Огляд даних про стан здійснення правосуддя у 2020 році. URL: https://court.gov.ua/userfiles/media/new_folder_for_uploads/main_site/ogl_2020.pdf (дата звернення: 14.10.2021).

Кушнір Л. П.,
завідувач кафедри історії України,
економічної теорії та туризму,
кандидат економічних наук, доцент
Гримак О. Я.,
декан факультету
економіки та менеджменту,
кандидат економічних наук, доцент
Калайтан Т. В.,
доцент кафедри історії України,
економічної теорії та туризму,
кандидат економічних наук, доцент
*(Львівський національний
університет ветеринарної
медицини та біотехнологій
імені С. З. Гжицького)*

ФАКТОРИ ФОРМУВАННЯ ТІНЬОВОЇ ЕКОНОМІКИ В ІНДУСТРІЇ ГОСТИННОСТІ

Тіньова економіка – це незареєстрована в установленому порядку економічна діяльність суб'єкта господарювання, яка характеризується мінімізацією витрат на виробництво товарів, виконання робіт та надання послуг, ухиленням від сплати податків, зборів (обов'язкових платежів), статистичного анкетування та подання статистичної звітності, наслідком якого є порушення законодавчо встановлених норм (рівень мінімальної заробітної плати, тривалість робочого часу, умови і безпека праці тощо) [1].

Тіньова економіка наявна в кожній країні, а в середині країни – в кожній галузі економіки. Різниця полягає у розмірах її поширення. В країнах з розвиненою економікою рівень тіньового сектора є нижчий. Незважаючи на це, тіньова економіка не зникає зовсім з ростом ВВП на душу населення. До того ж зарубіжні вчені виявили, що рівень неформальності знижується по мірі росту ВВП на душу населення лише до певної критичної межі, після чого він починає зростати.

Як в розвинених країнах, так і в країнах, що розвиваються, розмір тіньової економіки неоднаковий для різних галузей. Це, насамперед, пов'язано з економічними особливостями функціонування цих секторів економіки. Світова наукова спільнота до найбільш «тінізованих» галузей майже одностайно відносить будівництво, сільське господарство, торгівлю, тимчасове розміщування та організацію харчування. При цьому методи оцінки розміру тіньової економіки є приблизними, що цілком логічно, оскільки якщо б можна було точно оцінити її розмір, то легко би було

подолати це явище. Важливість здійснення навіть приблизної оцінки тіньового сектора у галузевому розрізі не викликає ніяких сумнівів, оскільки вказує на проблемні сфери економіки, які потребують особливої уваги. Рівень тіньової економіки в Україні оцінюють Державна служба статистики України, Міністерство економічного розвитку і торгівлі, а також міжнародні експерти. Розрахунки деяких експертів показують, що в «тіні» знаходиться не менше ніж 50 % ВВП [2].

Традиційними проявами тіньової економіки в індустрії гостинності є: (1) зарплата в «конвертах», (2) неофіційне працевлаштування, (3) фіктивна самозайнятість, (4) заниження транзакцій з метою ухилення від сплати податків. Дослідження, виконане за фінансової підтримки ЄС та Міжнародної Організації Праці, показує, що в Україні сектор «Тимчасове розміщування та організація харчування» належить до видів економічної діяльності з високим рівнем неофіційної роботи. Зокрема, в 2016 році у секторі «Будівництво» неофіційна зайнятість становила 32 % (1-ше місце), а в секторі «Тимчасове розміщування та організація харчування» – 29,4 % від кількості працюючих у відповідних секторах (2-ге місце) [3]. У 2020 році за офіційними даними Державної служби статистики України, відсоток неформальної зайнятості у сфері гостинності становив 33 % від загальної кількості зайнятих в цьому секторі, поступаючись при цьому лише сільському господарству та будівництву.

Серед факторів, що сприяють формуванню неформального сектора, науковці виділяють: психологічні, фактори політичної активності громадян, якості державних послуг та інші. Але найбільш вагомим фактором впливу, на думку багатьох дослідників, є високий податковий тиск. Менеджери готельного та ресторанного бізнесу серед факторів, що заважають їх діяльності, на перше місце ставлять високі ставки податків.

В Україні на цей час є достатньо високе податкове навантаження на працю – 41,5 %, з них 22 % – єдиний соціальний внесок (ЄСВ), 18 % – податок на доходи фізичних осіб, 1,5 % – військовий збір. Таке навантаження посилюється тим, що підприємства індустрії гостинності переважно є невеликими, а отже, їх витрати вище, ніж в тих галузях діяльності, які належать до великого бізнесу. Підприємницька діяльність у сфері гостинності може здійснюватись як юридичними особами, так і фізичними-особами підприємцями (ФОП). ФОПи, як правило, застосовують у своїй діяльності спрощену систему оподаткування. Мінімальний обов'язковий розмір ЄСВ повинен сплачуватись навіть у разі відсутності діяльності в розмірі, зважаючи на дві мінімальні заробітні плати. Враховуючи, що індустрія гостинності має достатньо виражену сезонність, сплата ЄСВ, особливо для ФОПів у сфері розміщування туристів, створює відчутне навантаження і спонукає їх працювати в «тіні».

Треба зазначити, що в Україні сфера туризму немає жодної податкової пільги. Однак більшість країн Євросоюзу всіляко підтримують туризм

шляхом стимулювання туристичних потоків, а також наданням суб'єктам господарювання цієї сфери різноманітних податкових преференцій. Серед них скасування або зниження стандартної ставки ПДВ на внутрішні і міжнародні пасажирські перевезення, зниження ставки ПДВ (порівняно зі стандартною) для закладів розміщування та організації харчування. Крім сприяння легалізації економіки, запровадження такої практики позитивно впливає на стабільність цін, забезпечення зайнятості населення, зростання інвестицій. Досвід Європи це підтверджує. Наприклад, після введення зниженої ставки ПДВ для готельного бізнесу Німеччини у 2010 р. обсяг капітальних вкладень в цьому секторі зріс в 2,7 раза. У Франції в 2009 р. зниження ставки ПДВ на послуги ресторанів знизило на 17 % кількість банкрутств, що дозволило зберегти 18 000 підприємств та 30 000 робочих місць. Зниження ставки ПДВ на послуги ресторанів у Швеції (2012 р.) вплинуло на додаткове середньорічне зростання обороту на 5,6 %, зарплати на 4,9 %, зайнятості на 5 % [4, 5].

Отже, в Україні з метою зниження розміру тіньової економіки в секторі «Тимчасове розміщування та організація харчування», на нашу думку, необхідно запровадити низку заходів щодо зниження податкового тиску. По-перше, реформування потребує спрощена система оподаткування у напряму нейтралізації наявних суперечностей фіскального стимулювання малого бізнесу [6], оскільки суб'єкти підприємницької діяльності індустрії гостинності функціонують в основному у сфері малого бізнесу. По-друге, необхідним є запровадження податкових пільг, зокрема зниження стандартної ставки ПДВ, а також перегляд механізму нарахування та сплати ЄСВ для ФОПів, які здійснюють свою діяльність у сфері розміщування туристів.

Бібліографічні посилання

1. Методичні рекомендації розрахунку рівня тіньової економіки : затв. наказом Мінекономіки України від 18.02.2009 р. № 123. URL: https://zakon.rada.gov.ua/rada/show/v0123665-09#Text
2. Vox Ukraine. Серая зона: 5 мифов украинской теневой экономики. URL: https://voxukraine.org/longreads/1/shadow.html
3. Undeclared Work in Ukraine: Nature, Scope and Measures to Tackle It. Working paper. International Labour Organization, 2018. URL: https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---lab_admin/documents/projectdocumentation/wcms_630068.pdf
4. Калайтан Т. В., Гримак О. Я., Кушнір Л. П. Шляхи нейтралізації наслідків кризи COVID-19 для індустрії гостинності на макро- та мікрорівні. *Трансформація податкової та обліково-аналітичної систем в контексті сучасних кризових явищ* : матеріали Міжнар. науково-практ. конф., м. Чернівці (Україна), 20 травня 2021 р. Чернівці : Технодрук, 2021. С. 321–325.
5. Temporarily reduced VAT rates for hospitality services. URL: https://www.hotrec.eu/wp-content/customer-area/storage/567b52abba7d6ff356cbaa210e841180/D-1020-371-Position-Paper-Temporarily-reduced-VAT-rates-for-hospitality-services-21102020.pdf
6. Yaroshevych N. B., Cherkasova S. V., Kalaitan T. V. Inconsistencies of small business fiscal stimulation in Ukraine. *Journal of Tax Reform.* 2019. 5 (3). S. 204–219. DOI: 10.15826/jtr.2019.5.3.068

Легеза Є. О.,
професор кафедри адміністративного
та митного права Університету
митної справи та фінансів,
доктор юридичних наук, професор

ПРАВОВЕ РЕГУЛЮВАННЯ ПОНЯТТЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Прогресивний розвиток України в умовах сьогодення залежить насамперед від здійснення ефективної політики у сфері захисту національних інтересів та територіальної цілісності.

Велике значення має безпека держави, яка дає змогу попередити та нейтралізувати будь-які загрози знищенню інтересів громадян, їх майна, а також життя та здоров'я. Зміст поняття «національна безпека» детермінується історичними та соціально-політичними умовами держави, в яких вона народжується, функціонує та розвивається.

Треба акцентувати, що розуміння сутності національної безпеки різниться серед різних верств населення. Зокрема, її переважно пов'язують з діяльністю спеціальних служб або ототожнюють з обороною держави.

Аналіз вітчизняної наукової літератури дає змогу виокремити різні підходи до розуміння поняття національної безпеки.

З документів ООН випливає підхід, відповідно до якого національна безпека розуміється як безпека держави в усіх сферах життєдіяльності народу, як єдиного носія суверенітету та джерела державної влади.

Наприклад В. А. Ліпкан, під національною безпекою розуміє сукупність офіційно прийнятих поглядів на цілі і державну стратегію у сфері забезпечення безпеки особистості, суспільства і держави від зовнішніх і внутрішніх загроз політичного, економічного, соціального, військового, техногенного, екологічного, інформаційного та іншого характеру з урахуванням наявних ресурсів і можливостей [1, с. 132].

Я. Ю. Кондратьєв визначає, що національна безпека – це здатність нації задовольняти потреби, необхідні для її самозбереження, самовідтворення і самовдосконалення з мінімальним ризиком збитку для базових цінностей її нинішнього стану [2].

М. О. Косолапов стверджує, що національна безпека – це стабільність, яка може підтримуватися протягом тривалого часу, стан досить розумної динамічної захищеності від найбільш істотних з реальних загроз і небезпек, а також здатність розпізнавати такі виклики і своєчасно вживати необхідні заходи щодо їх нейтралізації [3, с. 68].

Варто зазначити, що традиційно вважається, що основою основ національної безпеки будь-якої країни в будь-який час є збереження держави

в тих кордонах, в яких вона існує на цей історичний момент. Тому загроза державній «цілісності» є нібито універсальною та позаідеологічною характеристикою. Особливо яскраво ця загроза виявляє себе під час війни, внаслідок чого остання завжди є приводом для національної консолідації (тобто емоційного переживання єдності поза всіма соціальними та класовими розбіжностями) та національної мобілізації [4, с. 83].

Отже, можна стверджувати, що дійсно підходів до розуміння поняття національної безпеки досить багато і всі вони певною мірою різняться, проте можна констатувати, що все ж таки тут йдеться про цілий комплекс політичних, економічних, соціальних, з охорони здоров'я, військових і правових заходів, які спрямовані на забезпечення нормальної життєдіяльності нації та усунення можливих загроз для держави.

Отже, система забезпечення національної безпеки має свої складові, до яких відносять: захист державного суверенітету та територіальної цілісності; гарантування конституційного ладу; створення умов для політичної та економічної незалежності; забезпечення громадського порядку; боротьбу зі злочинністю тощо.

Зрозуміло, що всі ці дії здійснюються уповноваженими на те органами, які відповідно до власної компетенції реалізують різні програми держави, положення, директиви та міжнародні договори, а також норми вітчизняного законодавства. Варто зазначити, що до основних органів, які забезпечують національну безпеку держави, належать насамперед Збройні Сили країн та усі силові структури держави. Усі вони мають основне завдання, яке покладає на них держава – забезпечення високого рівня захищеності національних інтересів, у контексті чого створюються належні умови для стабільного розвитку кожної особистості, суспільства та держави. Треба наголосити на тому, що умовою ефективності цієї політики є пріоритет несилових шляхів захисту національних інтересів та цінностей.

Бібліографічні посилання

1. Ліпкан В. А., Ліпкая О. С., Яковенко О. О. Національна і міжнародна безпека в визначеннях та поняттях. Київ : Текст, 2006. 256 с.
2. Кондратьєв Я. Ю., Ліпкан В. А. Концепція національної безпеки України: теоретико-правові аспекти зарубіжного досвіду. Київ : Нац. акад. внутр. справ України, 2003.
3. Косолапов Н. Национальная безопасность в меняющемся мире (К дискуссии о содержании понятия). *Мировая номика и международные отношения.* 1992. № 10. С. 67–75.
4. Андрєєва О. М. Національна безпека в контексті національної ідентичності і взаємовідносин з Росією. Київ : Парламентське вид-во, 2009. 360 с.

Лізунов С. І.,
доцент кафедри захисту інформації
Національного університету
«Запорізька політехніка»,
кандидат технічних наук, доцент

АКТИВНЕ ПРИДУШЕННЯ ЗВУКОВОЇ ІНФОРМАЦІЇ

Захист акустичної інформації з обмеженим доступом потребує постійного вдосконалення з урахуванням сучасних засобів та методів її несанкціонованого зняття зловмисниками.

Раніше в [1] описувалася система активного придушення звуку (САЗ), яка має підвищену ефективність за рахунок врахування різниці швидкостей поширення акустичного та електричного сигналів. Ця система має підвищену швидкодію через поліпшену синхронізацію сигналу придушення з джерелом звуку. Схему такої системи зображено на рис. 1.

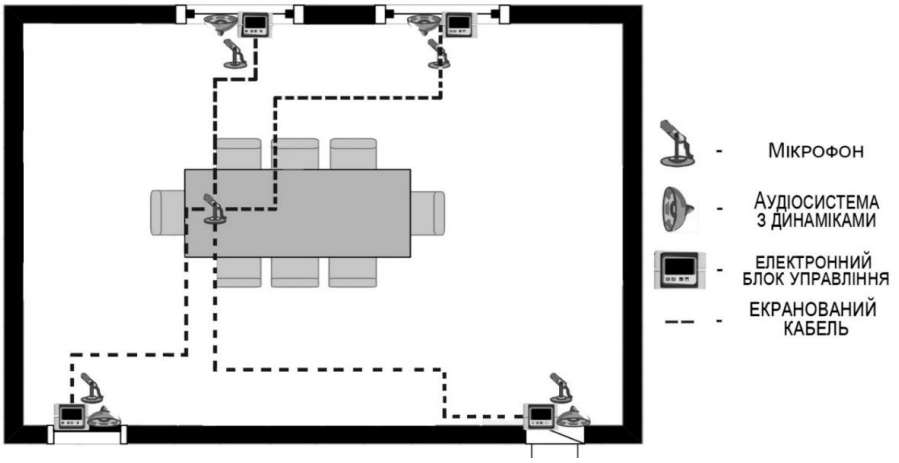


Рис. 1. Схема САЗ з підвищеною синхронізацією

Як видно, система містить мікрофон біля джерела звуку (наприклад, доповідач) і мікрофони по кожному каналу витоку інформації на границі контрольованої зони.

Автором пропонується подальше удосконалення цієї системи з метою:

– підвищення ефективності придушення звуку,
– прихованості факту та місця проведення перемовин,
– спрощення апаратної частини,
– зменшення енергоспоживання системи.

Таке вдосконалення системи активного придушення звуку можливе з урахуванням акустичних характеристик приміщення [2–4].

Якщо врахувати всі суттєві для конкретного випадку технічні канали витоку акустичної інформації [5], а також такі залежності (характеристики)

приміщення між точкою розташування джерела звуку, що придушується (доповідач), і точками каналів витоку акустичної інформації на границях контрольованої зони:

– часові (час поширення акустичної хвилі);

– частотні (АЧХ і ФЧХ);

– реверберaційні (відбиття звукових хвиль від перешкод),

то можна, в принципі, відмовитися від використання додаткових мікрофонів біля кожного каналу витоку мовної інформації. Це спрощує апаратну частину системи та процес її встановлення.

Вказані вище характеристики можуть бути зняті завчасно і внесені в електронні блоки управління, які вироблятимуть пригнічуючі сигнали. У цьому випадку кожен блок заздалегідь готовий до перетворення отриманого від мікрофона електричного сигналу з метою вироблення максимально ефективного сигналу придушення.

Крім того, в такій системі будуть придушуватися тільки звуки, які існують біля основного мікрофона, не порушуючи решту звукової «картини». Ці сторонні звуки також будуть ускладнювати зловмисникам зняття інформації, що приховується. Оскільки природний звуковий фон при цьому не порушується, то сам факт та місце проведення перемовин будуть замасковані. Також не будуть витрачатися ресурси системи на придушення цих «зайвих» звуків і зменшиться споживання електроенергії. Вимоги до максимальної потужності випромінювачів теж можуть бути знижені, оскільки звукові коливання, які треба погасити на границях контрольованої зони, часто бувають значно нижчі, ніж сторонні звуки, які інші системи придушують без потреби.

Процедуру попереднього налаштування системи можна спростити, використовуючи налаштування за допомогою тестових сигналів в автоматичному режимі.

Бібліографічні посилання

1. Лізунов С. І., Філобок Є. В. Захист мовної інформації з використанням систем активного звукопридушення. *Захист інформації*. 2021. № 1. Т. 23. С. 20–25. ISSN 2410-7840. URL: http://jrnl.nau.edu.ua/index.php/ZI.
2. Как звук распространяется в пространстве? URL: http://information-technology.ru/sci-pop-articles/23-physics/265-kak-zvuk-rasprostranyaetsya-v-prostranstve.
3. Основы распространения звука в свободном и замкнутом пространстве. URL: http://jcs.com.ua/news/osnovy-rasprostraneniya-zvuka-v-svobodnom-i-zamknutom-prostranstve
4. Звуковые волны. Источники звука. Характеристики звука (Иванова М. Г.). URL: https://interneturok.ru/lesson/physics/9-klass/mehanicheskie-kolebaniya-i-volny/zvukovye-volny-istochniki-zvuka-harakteristiki-zvuka-ivanova-m-g
5. Технические каналы утечки акустической (речевой) информации. URL: http://www.bnti.ru/showart.asp?aid=957&lvl=04.02.

Лопатка К. А.,
аспірант кафедри економіки
та підприємництва ДВНЗ
«Придніпровська державна
академія будівництва та архітектури»

АНАЛІЗ ВЗАЄМОЗВ'ЯЗКУ СТРАТЕГІЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ Й ЗАГАЛЬНОЇ СТРАТЕГІЇ ПІДПРИЄМСТВА

Незалежно від того, якою мірою ефективними здаються на перший погляд проєкти тих чи інших управлінських рішень у сфері поточного захисту економічних інтересів організації від різних загроз, їх треба відхилити, в тому разі, якщо вони суперечать напрямам економічного розвитку організації з погляду тривалої перспективи, а також суперечать стратегічним цілям підприємства, підривають здатність щодо реалізації заходів, спрямованих на забезпечення економічної безпеки з погляду тривалої перспективи. Реалізація цього принципу забезпечується також з огляду на загальну філософію розвитку організації, яка висуває на перший план саме стратегічні параметри економічного розвитку економічного суб'єкта і формування механізмів захисту пріоритетних господарсько-економічних інтересів у тривалій перспективі [1].

Забезпечення стратегічної економічної безпеки підприємства – це система методів і принципів розробки та реалізації управлінських рішень, які пов'язані із забезпеченням захисту компанії від потенційних і реальних внутрішніх і зовнішніх загроз її функціонуванню, що дозволяють їй досягати поставлених цілей і стабільно розвиватися в довгостроковому періоді [1].

В економічній літературі є безліч різноманітних підходів у сфері класифікації стратегії організацій, зважаючи на різні ознаки. Наприклад, залежно від того рівня, на якому ухвалюються стратегічні рішення, виділяють корпоративні та функціональні стратегії.

Корпоративні (або базові, загальні) стратегії стосуються загального розвитку організації або інтегрованої (або корпоративної) економічної системи. Метою базової стратегії є, насамперед, вибір елементів і орієнтирів системи, в які необхідно спрямувати наявні інвестиції і ресурси, а також вибір набору інструментів управлінської діяльності, що дозволяють досягти належного рівня з позиції стійкості та ефективності. Функціональні ж стратегії приймаються, зважаючи на інтереси служб і відділів організації. Кожна з функціональних структур (наприклад, фінанси, маркетинг, виробництво, персонал тощо) планує власний інструментарій управління і рівень фінансування як спосіб досягнення локальної мети процесу, функції відповідного підрозділу.

Досить важливим аспектом розробки загальної (базової) і функціональних стратегій підрозділів є те, що вони, врешті-решт, зливаються в єдину систему управління підприємством (орієнтир розвитку). Інакше

кажучи, інструментарій, за допомогою якого реалізується моніторинг і ретранслювання стратегій на всі рівні управління організацією (наприклад, стратегічна карта або система показників безпеки), повинні бути взаємопов'язані для полегшення впровадження (як своєрідних інновації), а їх розробка повинна являти собою ітераційний процес [2].

Необхідно акцентувати, що загальна (базова) стратегія містить у своєму складі стратегію підтримки безпеки, фінансову та інші функціональні стратегії підрозділів організації. Отже, загальна система показників повинна містити в собі всі ті показники, які використовуються для моніторингу і транслювання функціональних стратегій (стратегій підрозділів).

Можуть бути виділені такі основні типи стратегій економічної безпеки організацій: спрямованість на зниження наявних або можливих (потенційних) загроз стану економічної безпеки; спрямованість на усунення шкоди від впливу реалізованих, наявних, а також можливих загроз економічній безпеці організації; спрямованість на компенсацію завданої шкоди економічній безпеці компанії.

Безумовно, перший з наведених вище видів стратегій економічної безпеки найбільш радикальний, але і дає найкращі результати. Однак його реалізація можлива тільки тоді, коли організація дійсно здатна знизити або ж запобігти загрозі. Як правило, це можливо, коли йдеться про внутрішні загрози економічній безпеці організації, та й то не в усіх випадках. Зовнішні загрози, в основному, непідвладні підприємству, тому що зумовлені зовнішніми причинами.

Бібліографічні посилання

1. Іванюта Т. М., Заїчковський О. А. Економічна безпека підприємства : навч. посіб. Київ : Центр учбової літератури, 2009. 256 с.
2. Черевко О. В. Стратегічне управління фінансово-економічною безпекою підприємства. URL: http://www.economy.nayka.com.ua/?op=1&z=3302 (дата звернення: 24.09.2021).

Марценюк Л. В.,
професор кафедри економіки
та менеджменту Дніпровського
національного університету
залізничного транспорту
імені академіка В. А. Лазаряна,
доктор економічних наук, доцент

НАПРЯМИ ПІДВИЩЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ЗАЛІЗНИЧНОГО ТРАНСПОРТУ УКРАЇНИ

Відповідно до Закону України «Про інноваційну діяльність» інновації – це новостворені (застосовані) і (або) удосконалені конкурентоспроможні технології, продукція чи послуги, а також організаційно-технічні рішення

виробничого, адміністративного, комерційного чи іншого характеру, що істотно поліпшують структуру і якість виробництва і (або) соціальної сфери [1].

У сучасних ринкових умовах практично всі галузі потребують розробки та впровадження інновацій для забезпечення потреб споживачів та власних очікувань в контексті позитивного фінансового результату. Інновації дозволяють суб'єктам господарювання підвищувати свою конкурентоспроможність та отримувати відповідні бонуси.

Якщо говорити про залізничний транспорт, то тут вже давно назріла необхідність ввести різні інновації, починаючи від зміни структури управління до допуску приватних інвесторів до локомотивної тяги та використання сучасного рухомого складу чи впровадження залізничного туризму.

В умовах інноваційного розвитку дуже важливим аспектом є забезпечення економічної безпеки залізниць та держави загалом. На нашу думку, потрібно дуже обережно та виважено підходити до питань призначення керівниками Укрзалізниці та її структурних підрозділів іноземних громадян; до участі іноземних приватних інвесторів у концесії вокзалів та інших інфраструктурних об'єктів залізниць, а також до роботи компаній-операторів вантажних перевезень, до локомотивної тяги.

Важливо, аби амбітні плани іноземців не йшли в розріз із потребами громадян України та враховували соціально-економічну ситуацію в країні.

Під економічною безпекою треба розуміти практичне використання такої засади сучасного управління, як своєчасна реакція на зміни в зовнішньому середовищі, яка визначається швидкістю та адекватністю реакції підприємства на збудники зовнішнього середовища [2].

Вважаємо, що для посилення економічної безпеки Укрзалізниці доцільно якомога більше залучати саме українських науковців, фахівців, практиків та інвесторів до розробки інновацій на залізничному транспорті, а саме: нового рухомого складу, сучасних інфраструктурних об'єктів, різноманітних цифрових послуг тощо.

Головним завданням, що є загальним для всієї транспортної системи держави, нині є визначення цілей підходів до управління та стратегії державного регулювання економічної безпеки галузі національної економіки. Воно полягає у створенні таких умов для Укрзалізниці, які б дозволили виконувати її основне завдання – перевезення. При цьому конкурентну перевагу залізничний транспорт порівняно з іншими видами транспорту зможе отримати лише у разі комплексного оновлення інфраструктури, рухомого складу, підвищення рівня та розширення спектра послуг пасажирам та вантажовідправникам.

Бібліографічні посилання

1. Про інноваційну діяльність : Закон України. URL: https://zakon.rada.gov.ua/laws/show/40-15#
2. Синиця С. М., Вакун О. В. Особливості управління економічною безпекою підприємств залізничного транспорту. *Причорноморські економічні студії*. 2020. Вип. 51. С. 112–117.

Матусевич О. О.,
доцент кафедри обліку і оподаткування,
кандидаит економічних наук, доцент

Постільженко Г. С.,
магістрант кафедри обліку
і оподаткування Дніпровського
національного університету
залізничного транспорту
ім. академіка В. Лазаряна

ДЖЕРЕЛА ФІНАНСУВАННЯ КАПІТАЛЬНИХ ВКЛАДЕНЬ АТ «УКРЗАЛІЗНИЦЯ»

Для суттєвого оновлення основних засобів, фізичний знос яких перевищує 60 %, АТ «Укрзалізниця» необхідні великі капітальні вкладення (інвестиції) у заміну морально та фізично застарілих основних засобів та впровадження нової техніки і технологій, що передбачає перехід до нових підходів фінансування оновлення основних засобів.

Основними і законодавчо визначеними варіантами отримання фінансових ресурсів для АТ «Укрзалізниця» є такі:

1. Власні внутрішні джерела фінансування АТ «Укрзалізниця» у вигляді прибутку товариства та накопичених амортизаційних відрахувань.

2. Власні зовнішні джерела фінансування АТ «Укрзалізниця» – кошти, отримані від емісій акцій, а також цільове фінансування.

3. Позикові ресурси АТ «Укрзалізниця» – блок різноманітних кредитних програм фінансування проєктів оновлення об’єктів його основних засобів.

4. Змішане фінансування, оновлення об’єктів основних засобів АТ «Укрзалізниця» як певне поєднання вищенаведених джерел фінансування [1, с. 71].

В економічно розвинених країнах базовими внутрішніми джерелами фінансування господарської діяльності акціонерних товариств, зокрема їх інвестиційної діяльності, є суми нерозподіленого прибутку та накопиченої амортизації [2, с. 137]. Однак на цей час в АТ «Укрзалізниця» як прибуток, так і накопичена амортизація не можуть бути використані як основне джерело фінансування капітальних вкладень. Це зумовлено тим фактом, що господарська діяльність АТ «Укрзалізниця» не забезпечує необхідного рівня прибутковості його операційної діяльності, внаслідок чого значно зменшується частка прибутку, яку можна направити на фінансування капітальних вкладень товариства, та яка є недостатньою для здійснення необхідних на цей час інвестиційних витрат. Наявні амортизаційні відрахування також неспроможні покривати необхідні витрати на

відновлення об'єктів основних засобів товариства, які експлуатуються вже більше встановленого терміну і вимагають значних додаткових витрат на поточний ремонт.

Можливості значного фінансування капітальних вкладень за рахунок власних зовнішніх джерел фінансування АТ «Укрзалізниця», наприклад, шляхом додаткового акціонування, на цей час також обмежені внаслідок практично повної відсутності подібних джерел фінансування господарської діяльності акціонерного товариства, в якому всі 100 % акцій належать державі.

Отже, перспективними видами фінансування капітальних вкладень АТ «Укрзалізниця» є позикові ресурси та змішане фінансування.

На сьогодні кредитний рейтинг АТ «Укрзалізниця» – це кредити банків, єврооблігації, фінансова оренда (лізинг), а також корпоративні облігації. В країнах ЄС банки, як інвестори, забезпечують значні обсяги позикових фінансових ресурсів, але в Україні можливості банківської системи обмежені. АТ «Укрзалізниця» вже має велику заборгованість за кредитами, що призводить до значних сум фінансових витрат на обслуговування зовнішнього боргу. При високих ставках процента за банківський кредит та низьких рівнях рентабельності операційної діяльності товариства це призводить до поступового додаткового зниження рентабельності власного капіталу, внаслідок чого використання банківських кредитів стає проблематичним [2, с. 34].

Оскільки існуючі можливості фінансування господарської діяльності залізниць за рахунок власних джерел та банківських кредитів значно обмежені, для додаткового фінансування господарської діяльності товариству доцільно використовувати емісію корпоративних облігацій (лише у випадках, коли рентабельність проєктів капітальних вкладень суттєво перевищує процентну ставку за облігаціями). Крім того, в АТ «Укрзалізниця» під емісію корпоративних облігацій доцільно залучати кошти фізичних осіб.

Іншим варіантом використання позикового капіталу є фінансова оренда (лізинг), яка має більш високу, ніж у банківського кредиту, ціну капіталу, але не вимагає застави як у разі отримання банківського кредиту [1, с. 75].

Отже, базовим джерелом фінансування АТ «Укрзалізниця» доцільніше вибрати змішане фінансування з основним акцентом на кредитні програми у формі фінансової оренди (лізингу) і емісії корпоративних облігацій.

У випадках, коли обмежені фінансові ресурси АТ «УЗ» не дозволяють забезпечити оновлення основних засобів шляхом закупівлі нового рухомого складу у необхідних обсягах, першочергового значення набувають питання фінансування капітального ремонту основних засобів.

Бібліографічні посилання

1. Lomtieva I. M., Snachov M. P., Toporkova O. A., Shylo L. A. Formation peculiarities of financial resources of PJSC «Ukrainian railway». *Science and Transport Progress. Bulletin*

of Dnipropetrovsk National University of Railway Transport. 2018. Vol. 3(75). S. 67–77. doi: 10.15802/stp2018/133380.
2. Атрилл П., МакЛейни Э. Финансовый менеджмент и управленческий учет для руководителей и бизнесменов; пер. с англ. Москва : Альпина Паблишер, 2012. 648 с.
3. Васильєв О. Л. Джерела фінансування інвестиційної діяльності залізниць. *Міжнародний науковий журнал «Інтернаука».* Серія : Економічні науки. 2018. № 7(15). С. 31–36.

Махницький О. В.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

РИЗИКИ ВИКОРИСТАННЯ СТАРИХ ОПЕРАЦІЙНИХ СИСТЕМ НА ПРИКЛАДІ WINDOWS XP

Нещодавно операційній системі Windows XP виповнилося 20 років, і хоча підтримка цієї операційної системи припинилася в 2014 році, багато людей продовжують використовувати небезпечну версію Windows.

Windows XP була випущена 25 жовтня 2001 р. і вважається однією з найулюбленіших версій Windows завдяки простоті використання, високій продуктивності і стабільності. Сьогодні, після того, як Microsoft випустила Windows 7, 8, 10 і 11, невелика, але пристойна кількість людей все ще використовує стару операційну систему.

Таке постійне використання свідчить про його успіх, але також викликає побоювання щодо відсутності безпеки. Основна підтримка Windows XP закінчилася 14 квітня 2009 р., а розширена підтримка триватиме ще п’ять років. Це означає, що будь-хто, хто все ще працює з Windows XP, не отримував підтримки від Microsoft протягом приблизно 7,5 років, включно з майже всіма оновленнями безпеки та виправленнями вразливостей, які могли бути виявлені.

Це величезна кількість часу для технічних фахівців, і цього більше ніж достатньо, щоб перетворити операційну систему на жах безпеки з великою кількістю незахищених вразливостей. Хоча корпорація Майкрософт зробила виправлення для деяких, найбільш серйозних уразливостей у Windows XP, таких як EternalBlue і BlueKeep, є набагато більше вразливостей, якими можуть скористатися зловмисники. Це робить підключення пристрою Windows XP до Інтернету ризикованою справою, тому всі фахівці з безпеки рекомендують користувачам перейти на підтримувану версію Windows.

Чому застаріла операційна система й досі використовується?

Тим часом як Vista здавалася експериментальним випуском для бета-версії, Windows 7 була відмінним та вдосконаленим випуском, як і Windows

10. Отже, чому в деяких системах досі використовується застаріла версія XP?

Перша категорія систем, які ще використовують Windows XP, – це системи державного сектора, відомі своєю повільною швидкістю оновлення і нерішучістю у використанні нових технологій. Для багатьох державних структур бюрократія, пов'язана із затвердженням закупівель ліцензій на нові системи, оновленням обладнання та навчанням всього державного сектора, є надто складною та дорогою.

Сумісність спеціально створених 32-бітних програмних інструментів – ще одна важлива причина того, що XP все ще зустрічається у багатьох місцях, таких як промислові підприємства, лікарні тощо. Переважно нових версій цих критично важливих інструментів немає або компаніям доводиться платити великі гроші за їх перенесення на нові системи. Потім є категорія людей, які використовують занадто старе та слабке обладнання для правильного запуску нової версії Windows, і вони не бачать вагомих причин змінити те, що все ще (технічно) працює.

Перехід на Linux тільки для кращої підтримки та безпеки не є варіантом для більшості цих людей, тому що, простіше кажучи, Windows XP – це те, до чого вони звикли вже стільки років.

Скільки ще комп'ютерів працює під керуванням Windows XP?

Відповідно до StatCounter, відсоток користувачів Windows, які використовують версію ОС XP у вересні 2021 року, становить 0,59 %, що є великою кількістю, якщо врахувати, скільки систем Windows розгорнуто у всьому світі. Платформа NetMarketShare дає операційній системі Windows XP примітну частку ринку 0,26 % на вересень 2021 року. Якщо перевірити аналітику BleepingComputer, лише за останній місяць маємо 19 000 унікальних відвідувачів, які підключилися до сайту з системами Windows XP. Якщо взяти, наприклад Вірменію, то там Windows XP є найпопулярнішою ОС, на яку припадає 53,5 % користувачів Windows.

Рівень заробітної плати за три з половиною роки зріс на майже 40 %, але все одно перебуває в межах рівня мінімальної оплати праці по країні. Це є одним з головних стримуючих факторів щодо створення привабливого іміджу організації для потенційних майбутніх наукових працівників. Причому ця проблема не має очевидного вирішення у найближчій перспективі через вплив низки як внутрішніх, так і зовнішніх факторів.

До внутрішніх варто віднести відсутність нагальної потреби в залученні молоді до виконання науково-дослідних робіт через майже відсутність нових замовлень та перспективних ринків як всередині, так і поза межами України. Відповідно наявний обсяг робіт цілком спроможні виконати наявні штатні працівники ДП «НДТІ». Також останніми роками спостерігається чітка тенденція до зменшення кількості випускників технічних вузів, які здатні замінити працюючих в науковій установі співробітників пенсійного віку. І йдеться не стільки про низький рівень заробітної плати, скільки про фізичну відсутність молодих фахівців як таких.

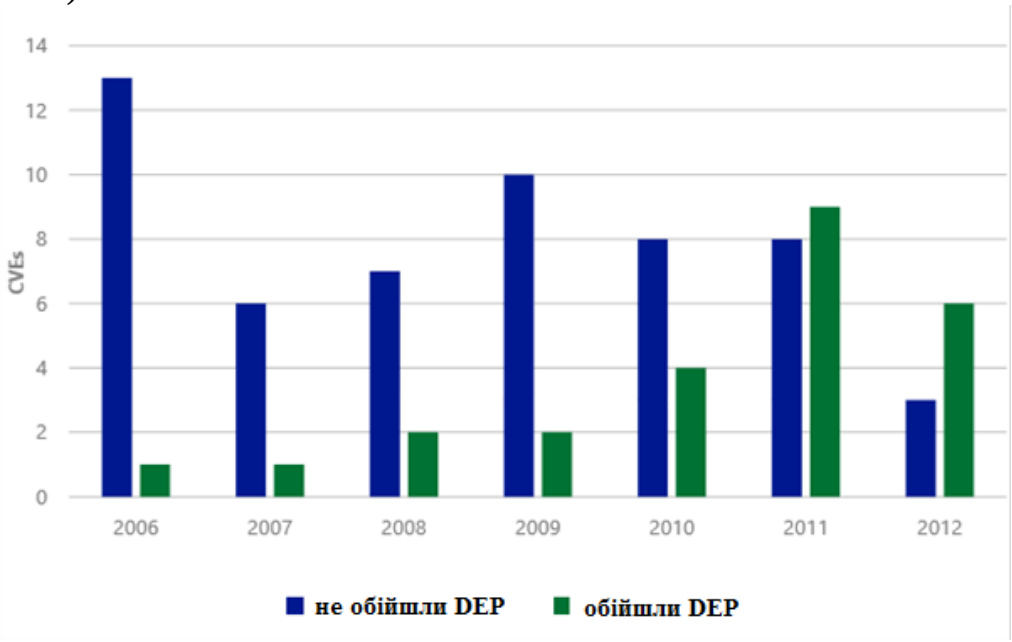
Половина всіх комп'ютерів у Вірменії працює під керуванням Windows XP.

Хоча ринкова частка Windows XP відносно невелика, надто багато організацій та користувачів все ще використовують цю застарілу версію Windows.

Оскільки кібератаки і програми-вимагачі є загрозою, що постійно розвивається, використання застарілих і непідтримуваних систем – занадто великий ризик для організацій, особливо якщо ці пристрої живлять критично важливі системи.

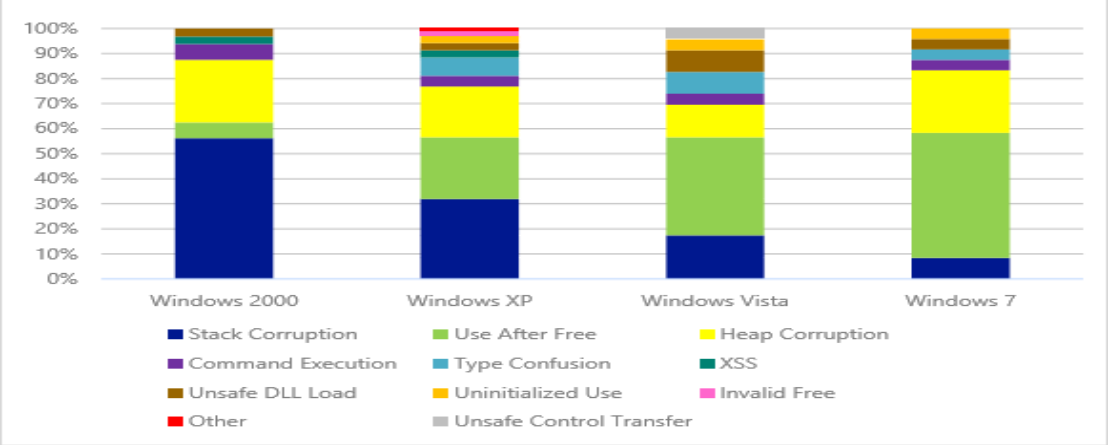
У чому ризик роботи у застарілій операційній системі?

З часом корисність старих захисних механізмів знижується, але не тому, що вони стають менш ефективними власними силами. Справа в тому, що зловмисники навчаються обходити їх, адаптуючись до умов, у яких ці механізми працюють. Хорошим прикладом цієї тези є DEP (Data Execution Prevention).



На діаграмі вище синім кольором позначені вразливості, для яких були випущені експлойти, чия дія звелася б нанівець включеним DEP. Зеленим кольором позначені вразливості, експлуатації яких DEP перешкодити не зміг. Ці дані Microsoft показують, що починаючи з 2009 року все більше і більше вразливостей експлуатується в обхід DEP. Компанія також спостерігає схожий тренд з механізмом ASLR, який обходиться за рахунок атак на ресурси, що не сховалися під парасолькою. Останні 12 місяців у нових клієнтських операційних системах Microsoft було закрито значно менше вразливостей, ніж у попередніх. Звичайно, нові ОС менше поширені, а тому не мають такого гострого інтересу для зловмисників. Однак Microsoft напевно посилює захист, беручи до уваги напрямки атак на свої продукти, що ускладнює експлуатацію вад у безпеці.

Компанія класифікує вразливості за типом експлуатації, і на діаграмі нижче наведено розподіл цих класів у клієнтських ОС, для яких були випущені експлойти з 2006 до 2016 року.



Тут добре видно, що увага зловмисників зміщується у бік експлуатації уразливостей двох класів:

Use after free. Вразливість експлуатується, коли до об’єкта відбувається звернення після звільнення. Зловмисники використовують такі вразливості, щоб змусити програми використовувати свої значення, домагатися падіння програм чи віддаленого виконання коду. Саме цей клас найчастіше експлуатується в атаках Internet Explorer. У Windows 8 на боротьбу з цим відряджена технологія Virtual Table Guard.

Heap Corruption. Вразливість експлуатується шляхом пошкодження стану даних додатків, які зберігаються у його купі (heap). Нерідко це досягається шляхом переповнення буфера купи, що дозволяє взяти під контроль роботу програми. У Windows 8 для протидії таким атакам передбачено механізм Heap Hardening.

Цілком очевидно, що нові захисні заходи є наслідком перегонів озброєнь між виробниками програмного забезпечення та зловмисниками.

Підтвердження цієї тези ви побачите далі. Порівняємо захисні

механізми Windows XP та Windows 8 (див. табл. 1)

Дуже часто один бюлетень стосується всіх продуктів лінійки, випущених у різні роки (наприклад, від Windows XP до Windows 8). Зрозуміло, що підготовка виправлення та його тестування на різних продуктах можуть займати різний час, але бюлетені та латки виходять лише в один день. Тим самим Microsoft нівелює ефект від зворотної розробки виправлень, яка неминуче починається після їх виходу у світ.

Інакше кажучи, якщо випускати, наприклад, виправлення для Windows 7 через місяць після латок для Windows 8, то на цей момент експлойт для вразливостей Windows 7 з XI = 1 вже буде давно готовий.

Таблиця 1

Порівняльний аналіз захисних механізмів Windows XP та Windows 8

	Windows XP SP3 Internet Explorer 8	Windows 8 Internet Explorer 10
SEHOP	No	Yes
Protected Mode	No	Yes
Enhanced Protected Mode (EPM)	No	Yes
Virtual Table Guard	No	Yes
ASLR	Limited	Extensive
Stack randomization	No	Yes
Heap randomization	No	Yes
Image randomization	No	Yes
Force image randomization	No	Yes
Bottom-up randomization	No	Yes
Top-down randomization	No	Yes
High entropy randomization	No	Yes
PEB/TEB randomization	Yes	Yes
Heap hardening	Limited	Extensive
Header encoding	No	Yes
Terminate on corruption	No	Yes
Guard pages	No	Yes
Allocation randomization	No	Yes
Safe unlinking	Yes	Yes
Header checksums	Yes	Yes
/GS	Yes	Yes
Enhanced /GS	No	Yes
SafeSEH	Yes	Yes

На закінчення повторимо деякі тези цієї статті:

– зловмисники навчилися обходити старі захисні механізми;

– до багатьох уразливостей експлойти виходять протягом місяця після випуску виправлень, чому сприяє їхня зворотна розробка;

– нові експлойти для XP обов’язково включатимуться до наборів для атаки;

– захищати стару систему потрібно не безкоштовним антивірусом, а як мінімум, комплексним захисним рішенням (ще краще – SRP чи EMET).

У нових ОС закривається менше вразливостей, тому що їх захисні механізми удосконалюються з урахуванням напрямків атак. Слід завжди користуюся найновішими програмними продуктами Microsoft, у тому числі й тому, що це є безпечнішою практикою. Однак будь-яку ОС та все популярне

ПЗ необхідно оновлювати максимально швидко. Можна рекомендувати включити автоматичне оновлення Windows, а Java та Adobe Reader не встановлювати, щоб зменшити поверхню атаки.

Бібліографічні посилання

1. Microsoft: Software Vulnerabilities Exploitation Trends (PDF).
2. Microsoft Security Intelligence Report: Exploitation Trends.
3. Kaspersky Security Bulletin 2016. Основна статистика за 2016 рік.

Мироненко М. А.,
учений секретар ДП «НДТІ»,
кандидат технічних наук, доцент

Король Р. М.,
директор ДП «НДТІ»,
кандидат технічних наук

АНАЛІЗ ДЕЯКИХ ПОКАЗНИКІВ КАДРОВОГО ТА ФІНАНСОВОГО СТАНУ НАУКОВО-ДОСЛІДНОЇ УСТАНОВИ ДЕРЖАВНОЇ ФОРМИ ВЛАСНОСТІ У 2018 – ІІ кв. 2021 РОКІВ

Державне підприємство «Науково-дослідний та конструкторсько-технологічний інститут трубної промисловості ім. Я. Ю. Осади» (ДП «НДТІ») є розробником технологій виробництва усіх видів труб та балонів, що впроваджені на заводах колишнього СРСР та деяких інших країн.

До складу інституту входять: адміністративно-управлінські підрозділи; 3 науково-дослідних підрозділи; міжрегіональний науково-інженерний центр обґрунтування вимог до якості труб, балонів, іншої металопродукції та забезпечення їх нормативною документацією; науково-інженерний центр з випробування труб, балонів, іншої продукції і матеріалів; центр технічного забезпечення євроінтеграції в металургійній та енергетичній галузях України ENtoUA-VNITI; сектор технології і виробництва виробів спеціального призначення.

У табл. 1 наведено деякі показники кадрового та фінансового стану ДП «НДТІ» за період 2018 – І півріччя 2021 років.

Як випливає із наведеної у табл. 1 інформації, за проаналізований період в інституті відбулося скорочення кількості працівників на 12,5 %. Водночас кількість працівників пенсійного віку збільшилась майже на 30 %, а тих, хто має повну вищу освіту, скоротилась на 5 %.

Таблиця 1

Деякі показники кадрового та фінансового стану ДП «НДТІ» за період 2018 – ІІ кв. 2021 рр.

Показник кадрового складу, осіб	на 31.122018	на 31.12.2019	на 31.12.2020	ІІ кв. 2021 р.
Середня кількість працівників, із них:	64 ос.	62 ос.	60 ос.	56 ос.
Чоловіків	26 ос.	26 ос.	24 ос.	22 ос.
Жінок	38 ос.	36 ос.	36 ос.	34 ос.
Кандидатів наук	3 ос.	3 ос.	3 ос.	3 ос.
Середній вік працівника	53 р.	56 р.	57 р.	55 р.
Кількість молодих працівників (віком до 35 років)	10 ос.	4 ос.	2 ос.	1ос.
Беруть участь у виконанні НДР	25 ос.	21 ос.	21 ос.	30 ос.
Із них винахідників та раціоналізаторів	18 ос.	18 ос.	18 ос.	21 ос.
Загальна кількість пенсіонерів	24 ос.	29 ос.	35 ос.	31 ос.
Мають повну вищу освіту	45 ос.	44 ос.	43 ос.	43 ос.
Кількість керівників наукових підрозділів	8 ос.	8 ос.	8 ос.	9 ос.
Середньомісячна заробітна плата	4823,1 грн	6597,2 грн	6390,3 грн	6744,0 грн
Загальна сума виплат на користь держави, із них:	4012 тис. грн	5855 тис. грн	3582 тис. грн	927 тис. грн
ПДВ	1289 тис. грн	1762 тис. грн	1503 тис. грн	463 тис. грн
Податок на прибуток	20,0 тис. грн	-	-	-
Місцеві податки та збори	1764 тис. грн	2951 тис. грн	1036 тис. грн	205 тис. грн
Соціальне страхування	939 тис. грн	1142 тис. грн	1043 тис. грн	259 тис. грн

До зовнішніх чинників насамперед належить шалена конкуренція за молоду робочу силу, особливо через відкриття кордонів із більш заможними країнами ЄС: Польщею, Словаччиною, Чехією тощо. Наявна зараз в Україні атмосфера нагнітання нагальної потреби човникової еміграції – тимчасового

від'їзду за кордон на термін до півроку – не сприяє закріпленню кваліфікованих кадрів всередині держави. Водночас приватний сектор пропонує більш високі заробітні плати потенційним новим молодим працівникам, аніж це можливо нині у ДП «НДТІ».

З огляду на тематику конференції, присвяченої зокрема висвітленню питань економічної безпеки держави та підприємств, працівники яких створюють матеріальне підґрунтя для її існування, варто зазначити таке.

По-перше, органи влади мають більш свідомо підходити до питань управління державною власністю. По-друге, варто використовувати більш гнучку фіскальну політику як на рівні місцевого самоврядування, так і на рівні загальнодержавних контролюючих органів. По-третє, захист національного ринку від недоброчесної зовнішньої конкуренції має стати наріжним каменем побудови усієї системи вертикалі влади в Україні.

Мирошниченко В. О.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ВІДЕОТЕХНОЛОГІЇ: МОЖЛИВОСТІ ТА ПРОБЛЕМИ ВИКОРИСТАННЯ

У цей час в багатьох країнах, в тому числі і в Україні, відеоспостереження широко використовується як дієвий інструмент для зниження рівня злочинності та тероризму. Доступність, простота використання відеотехнологій і тенденції світової спільноти до вирішення проблем, що виникають, силовими методами через не вирішення юридичних питань та правового нігілізму суспільства призводять до їх широкого використання. Зараз підраховано, що у Великобританії налічується приблизно 5,2 мільйона камер відеоспостереження, по одній камері на кожні 13 осіб – ця кількість охоплює всі: від громадського спостереження до камер, використовуваних приватним бізнесом, і навіть камер для дверних дзвінків [1].

За останнє десятиліття можливості систем відеоспостереження кардинально змінилися внаслідок фундаментального розвитку технологій збору, аналізу, передачі і зберігання цифрових даних. Використання штучного інтелекту стає все більш поширеним явищем, наслідком чого відеокамери можуть більш точно збирати дані і робити прогнози на основі розробленого виробниками інтегрованого аналітичного програмного забезпечення. Прикладом може бути продукція фірми Hikvision з

вбудованими смарт функціями [2]. З бурхливим розвитком технологій розпізнавання осіб з використанням відеокамер, використанням дронів, натільних камер, відеоаналітики і багато чого іншого сучасні системи тепер мають феноменальні можливості.

Люди звикли бачити камери відеоспостереження практично на кожній вулиці. Такі системи, як і раніше, користуються широкою суспільною підтримкою. Потенційна цінність технологій громадського спостереження була неодноразово продемонстрована і підтверджена ще в далекому квітні 2013 року, коли поліція ідентифікувала двох підозрюваних у вибуху бомб на Бостонському марафоні після перегляду відеозображень, знятих міськими камерами [3].

Є безліч аргументів на користь камер відеоспостереження:

– камери спостереження в громадських місцях забезпечують громадську безпеку. Рідко хто спробує завдати шкоди, якщо знає, що його дії записуються на камеру;

– за допомогою камер спостереження поліція може не тільки запобігти правопорушенням, а й швидко розкрити злочини з використанням речових доказів;

– камери спостереження захищають від крадіжок майна та вандалізму. Досить складно уникнути відповідальності, якщо злочинні дії зафіксовані камерою. Камери відеоспостереження фіксують правопорушника до і в процесі вчинення злочину;

– у разі відсутності свідків під час вчинення злочинів камери відеоспостереження дозволяють ефективно розкривати багато злочинів, тому що запис із камер відеоспостереження завжди є важливим елементом доказів під час поліцейського розслідування;

– злочинці з меншою ймовірністю здійснять злочинні дії в районі, де ведеться відеоспостереження, якщо знають, що їх весь час будуть знімати на відео. Недобросовісні дії, такі як крадіжка в магазинах, навряд чи варті того, щоб потрапити до в’язниці;

– люди відчувають себе в більшій безпеці, знаючи, що потенційного грабіжника або зловмисника відлякує присутність камери;

– розвиток систем розпізнавання осіб і аналітичного програмного забезпечення дозволяє набагато краще прогнозувати злочинну поведінку і робити більш точні висновки.

Якщо з технічного погляду впровадження таких технологій вирішується досить успішно, то з морального і законодавчого боку виникає багато питань, особливо в країнах з розвиненими демократичними традиціями. Світова демократична спільнота все частіше ставить подібні питання: хто проводить межу між суспільним інтересом і зловмисним використанням таких технологій? Яку мету має розміщена камера? А як щодо приватної камери, розміщеної зі злим умислом? Хто регулює правовий статус відеокамер приватної власності? Так, камери

спостереження важливі для запобігання злочинів, однак важливо знати, хто перебуває на іншому кінці камери. Хто насправді спостерігає за тобою, хто в кінцевому підсумку бачить те, куди спрямований об'єктив камери? Як вирішити ситуацію, коли приватна камера відеоспостереження спрямована неправильно або зловмисно, наприклад, у вікна приватного будинку? Кому взагалі належить камера? Як довго зображення має зберігатися після того, як особу було знято й ідентифіковано як таку, що «не становить загрози»? І хто несе відповідальність за видалення такого контенту з системи? Де зберігаються зібрані дані, як довго і хто має до них доступ?

Особливу занепокоєність викликають IP-камери, підключені до Інтернету. Такі системи легше «зламати», ніж замкнуті відеосистеми, і занепокоєність щодо кібербезпеки використання таких камер продовжує зростати. На думку деяких, поліція повинна виходити на вулиці, намагаючись запобігти злочинним проявам. Камери відеоспостереження – просто менш ефективна альтернатива тому, щоб поліція ходила вулицями. Крім того, камери відеоспостереження можуть дати помилкове відчуття безпеки і є менш ефективною заміною поліцейської діяльності у публічних місцях. На цей час на більшість поставлених запитань ніхто не може дати чіткої відповіді.

На закінчення необхідно відзначити, що в таких дебатах прихильникам по обидва боки необхідно розумно враховувати наведені вище аргументи, які є далеко не повним переліком, і рішення поставлених питань вимагає якнайшвидшого законодавчого вирішення.

Бібліографічні посилання

1. URL: https://www.cctv.co.uk/number-of-cctv-cameras-in-the-uk-reaches-5-2-million (дата звернення: 23.10.2021).
2. Кочеткова І. Б., Махницький О. В., Мирошниченко В. О. Використання відеоаналітики у роботі Національної поліції : метод. рекомендації. Дніпро : Дніпропетр. держав. ун-т внутр. справ, 2020. 34 с.
3. URL: https://www.ifsecglobal.com/video-surveillance/london-2012-boston-marathon-securing-large-scale-events (дата звернення: 23.10.2021).

Мішкевич Ж. В., старший інспектор
з особливих доручень відділу
уповноважених з контролю
за дотриманням прав людини
в поліцейській діяльності
(з дислокацією в Одеській області)
Управління дотримання прав людини
Національної поліції України

Рудой К. М., професор кафедри
адміністративного права
та адміністративного процесу
Одеського державного
університету внутрішніх справ,
доктор юридичних наук, доцент

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ «CUSTODY RECORDS» У ДІЯЛЬНІСТЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Інформаційна підсистема «Custody records» призначена для покращення стандартів захисту прав затриманих осіб шляхом запровадження обов'язкового інтерв'ю під час доставляння до органу поліції, електронної фіксації всіх дій щодо затриманого (фіксації, накопичення, зберігання) та перебування особи під контролем поліції з моменту фактичного затримання [1].

Метою зазначеної підсистеми є:

– зменшення навантаження на поліцейських, задіяних у роботі із затриманими особами;

– захист прав поліцейських від неправдивих звинувачень у неправомірних діях щодо затриманих осіб;

– здійснення дистанційного зовнішнього контролю за дотриманням прав затриманих осіб уповноваженими УДПЛ НПУ;

– електронна фіксація всіх дій щодо затриманої особи з моменту її фактичного затримання і до поміщення в СІЗО або звільнення з-під варти [2].

Ефективність функціонування інформаційної підсистеми «Custody records» зумовлюється забезпеченням таких елементів, а саме:

– Інститут інспекторів з дотримання прав людини (відповідний досвід та кваліфікація поліцейських).

– Єдина електронна база обміну всіх дій щодо затриманих (належне інформаційне забезпечення поліцейської діяльності).

– Зонування приміщень підрозділу поліції (відповідне матеріально-технічне забезпечення відділів поліції).

– Система зовнішнього контролю (доступ до електронної бази та віддалене відеоспостереження) (централізована система контролю) [3].

Першочергові заходи щодо впровадження інформаційної підсистеми «Custody records»:

1. Розробка проєкту Технічного паспорта першого поверху територіального органу поліції в частині вимог до розміщення та облаштування приміщень, де можуть перебувати учасники кримінального провадження, а також відвідувачі (хол територіального органу, кімната для прийому громадян, кімната для затриманих, кімната для проведення слідчих дій, кімната для конференційного побачення з адвокатом, чергова частина та робоче місце інспектора з дотримання прав людини).

2. Затвердження Технічного паспорта відповідно до нормативно-правових актів (в т.ч. ДБН), а також відомчих нормативно-правових актів МВС та НПУ.

3. Аналіз інфраструктури облаштування територіальних органів поліції на предмет їх відповідності новому Технічному паспорту та підготовка й затвердження за результатами аналізу відповідного Плану заходів щодо проведення інфраструктурних змін [4].

На виконання Плану заходів щодо масштабування пілотного проєкту запровадження системи «Custody records» в територіальних підрозділах поліції, який затверджений 31.07.2020 р. міністром внутрішніх справ України, та підпункту 4 пункту 4 наказу голови Національної поліції України від 28.12.2020 р. № 1041 «Про впровадження пілотного проєкту «Інформаційна підсистема «Custody records», інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» Управлінням дотримання прав людини Національної поліції України здійснюється постійний моніторинг та аналіз стану упровадження пілотного проєкту ІП «Custody records» [5].

Отже, впровадження інформаційної підсистеми «Custody records» в діяльність Національної поліції спрямоване насамперед на дотримання прав людини в поліцейській діяльності, а також забезпечення законності та дисципліни поліцейськими під час спілкування з особами, які перебувають у відділі поліції. Ефективність заходів впровадження інформаційної підсистеми «Custody records» в поліцейській діяльності залежить від забезпечення певних вимог: наявності відповідної кваліфікації поліцейського у сфері дотримання прав людини в поліцейській діяльності (досвід роботи в практичних підрозділах поліції, підвищення рівня професійної підготовки), забезпечення фінансування заходів, матеріально-технічного оснащення відділів поліції, інформаційного забезпечення та підтримки, належних контрольних заходів за впровадженням цієї підсистеми.

Бібліографічні посилання

1. Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису : наказ МВС від 18.12.2018 р. № 1026.

2. Система Custody Records: новий рівень забезпечення прав затриманих. URL:

https://www.legalaid.gov.ua/novyny/systema-custody-records-novyj-riven-zabezpechennya-prav-zatrymanyh/ (дата звернення 20.10.2021)

3. Технічне завдання із впровадження системи «Custody Records» у територіальних органах поліції: Національна поліція, Міжнародний Фонд Відродження, Українська Фундація Правової Допомоги, Експертний центр з прав людини. URL: http://www.custodyrecords.com/index.php/ (дата звернення: 20.10.2021).

4. Технічне завдання із впровадження системи Custody records у територіальних органах поліції. Київ : Міжнародний фонд «Відродження», 2021. 102 с.

5. Методичні рекомендації для інспекторів з дотримання прав людини в ізоляторах тимчасового тримання: Національна поліція, Міжнародний Фонд Відродження, Українська Фундація Правової Допомоги, Експертний центр з прав людини. Київ, 2019.

Мордвинцев М. В.,
провідний науковий співробітник,
кандидат технічних наук, доцент

Хлєстков О. В.,
старший науковий співробітник

Ницюк С. П.,
старший науковий співробітник
науково-дослідної лабораторії з
проблем розвитку інформаційних
технологій Харківського національного
університету внутрішніх справ

ТЕХНІЧНІ ПРОБЛЕМИ, ПОВ'ЯЗАНІ ЗІ СТРІМКИМ РОЗВИТКОМ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ, Й СПОСОБИ ЇХ ВИРІШЕННЯ

У світі спостерігається стрімкий розвиток систем відеоспостереження, які використовуються в сучасному мегаполісі. Зростає кількість завдань, які покладаються на системи відеоспостереження, кількість камер, їх роздільна здатність, обсяги оброблюваної інформації і швидкість, необхідна для її обробки [1]. При цьому виникають технічні і фінансові труднощі під час вирішення цих проблем. Сервера, задіяні під час обробки відеопотоків, мають дуже великі обсяги пам'яті і велику вартість. Продуктивності обчислювальних систем не вистачає для обробки потокової інформації. Кількість завдань, що покладаються на системи, постійно зростає, відповідно збільшується вимоги до показників обсягів і швидкості обробки інформації.

Для вирішення цих проблем виробники технічного обладнання та програмного забезпечення використовують розподілені системи обробки відеоінформації, штучний інтелект безпосередньо в камері відеоспостереження, хмарне відеоспостереження.

Під час використання розподілених систем обробки відеоінформації виникають деякі особливості, а іноді і проблеми з їх налаштуванням і

використанням: це адміністрування, єдиний протокол подій, єдиний пост спостереження, міжсерверна автоматика, відеостіна, відеоаналітика, інтелектуальний пошук, резервування.

Технології штучного інтелекту (ШІ) перетворюють звичайну камеру відеоспостереження в розумний пристрій, здатний навчатися і надавати корисні дані в реальному часі [2]. Тобто обробка здійснюється не на сервері, а в самій камері відеоспостереження.

Раніше більшість встановлених відеокамер використовувалися тільки для запису величезних обсягів даних, проте більшість відеозаписів не являли собою ніякого практичного інтересу. Знайти конкретну подію у відеоархіві було вкрай складно: для обробки гігантських обсягів відеоінформації були потрібні високопродуктивні комп'ютери. Тепер відеокамери можуть навчатися на розмічених даних, а також на нових даних, що підвищує точність відеоаналізу і дозволяє виявляти саме ті події, які цікавлять користувача.

Хмарне відеоспостереження – це відеоспостереження через інтернет, що дозволяє зберігати, переглядати і аналізувати відео в хмарній інфраструктурі. Також відмінною рисою хмарного відеоспостереження є можливість об'єднувати територіально розподілені камери в одну систему і управляти доступом до їх відеоархіву та до бази подій. Відеоінформація при цьому зберігається в потужних і надійних дата-центрах компанії – організатора хмари в зашифрованому вигляді.

До основних переваг хмарного відеоспостереження можна віднести [3]:

– спрощення доступу до камери й архіву (хмарне відеоспостереження надає змогу перегляду онлайн відео і архіву з будь-якої точки світу, де є підключення до мережі «Інтернет»);

– забезпечення безпеки зберігання даних (відео зберігається на потужних серверах у географічно розподілених дата-центрах, весь трафік повністю шифрується спеціалізованим процесором на самому пристрої, забезпечується багаторазове дублювання даних);

– додаткові можливості хмарних систем (передача прав доступу до відео іншим особам, повідомлення про рух в зоні спостереження тощо);

– можливість організації територіально віддалених відеосистем (географічно розподілені камери об'єднуються в одному кабінеті користувача, можна розмістити об'єкти на карті GoogleMaps для візуалізації);

– відсутність капітальних витрат (не потрібно жодних витрат на сервери, їх утримання та обслуговування, виникає змога оперативно збільшувати необхідний обсяг сховища).

Отже, використання розподілених систем обробки відеоінформації, штучного інтелекту безпосередньо в камерах відеоспостереження, які можуть навчатися на розмічених та нових даних, хмарного відеоспостереження дозволяють записувати, обробляти і зберігати великі обсяги інформації та вирішувати велику кількість різноманітних завдань користувача.

Бібліографічні посилання

1. Коршенко В. А., Чумак В. В., Мордвинцев М. В., Пашнев Д. В. Стан систем безпеки з використанням технічних засобів відеозапису та відеоспостереження: зарубіжний досвід, перспективи впровадження в діяльність Національної поліції України. *Право і безпека*. 2020. № 2 (77). С. 86–92. URL: https://www.secuteck.ru/articles/iskusstvennyj-intellekt-nauchit-kamery-dumat
2. Ма Стив. Искусственный интеллект научит камеры «думать». *Системы безопасности*. 2018. № 4 (142). С. 36–37.
3. Пальцева Вера. Облачные технологии в видеонаблюдении. *Технологии защиты*. 2015. № 6. URL: http://www.tzmagazine.ru/jpage.php?uid1=1348&uid2=1474&uid3=1490

Насонова С. С., доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СКЛАДНИХ СИСТЕМ З ВИСОКИМ СТУПЕНЕМ ВІДПОВІДАЛЬНОСТІ

Системи з високим ступенем відповідальності – це системи, аварії яких призводять до величезних економічних витрат, екологічних і соціальних проблем. Аварії таких систем прийнято відносити до розряду катастроф державного масштабу. Системами з високим ступенем відповідальності є, зокрема, АЕС і нафтові резервуари. Ці технічні системи належать до споруд, безпека експлуатації яких є безумовно головною умовою. Під безпекою тут розуміється властивість системи в разі відмови не створювати загрозу для життя і здоров'я людей, а також для навколишнього середовища [1].

У цій роботі об'єктом дослідження є сталеві вертикальні циліндричні резервуари наземного типу (РВС) для довгострокового зберігання нафти і нафтопродуктів. У процесі експлуатації РВС відчувають вплив механічних і температурних навантажень, агресивних середовищ і інших негативних чинників, які діють спільно і нерідко в найнесприятливіших поєднаннях. Наслідком такого впливу є поступова деградація (фізичний знос, накопичення дефектів і пошкоджень) сталевих конструкцій РВС, погіршення їх технічного стану. Треба зазначити, що деградація є об'єктивною складовою процесу експлуатації нафтових резервуарів і починається з перших днів їх служби. Якщо процесом деградації кваліфіковано не управляти, то з часом технічний стан РВС може тільки погіршуватися. Рано чи пізно споруда деградує настільки, що подальша його експлуатація стає небезпечною або взагалі неможливою. Все це викликає необхідність організації заходів щодо забезпечення безпечної експлуатації резервуарних

парків.

Проблема планування таких заходів за своєю природою є завданням оптимального управління, яке ставиться не в сенсі максимального підвищення безпеки РВС в процесі експлуатації, а в межах економічного підходу і полягає в забезпеченні безпечної роботи споруди при мінімізації сумарних експлуатаційних витрат. Останнє означає, що ухвалення рішення повинно бути мотивоване аналізом витрат і прогнозуванням ризику відмови РВС. При цьому мета управління полягає в забезпеченні прийнятного рівня експлуатаційної надійності резервуара, а основним способом здійснення цього управління є періодичні ревізії технічного стану, які являють собою виконання технічних обстежень і ремонтів, спрямованих на відновлення технічних кондицій споруди.

Зміст і періодичність виконання технічних обстежень РВС регламентуються чинними нормативними документами [2]. Не ставлячи під сумнів правомірність існування і корисність загальних рекомендацій з технічного діагностування РВС, що перебувають в експлуатації, відзначимо про те, що рекомендовані плани-графіки виконання технічних обстежень визначено досить орієнтовно, а з позицій економічної ефективності витрат на ревізію і прогнозування ризику відмови відповідні питання стосовно конкретного резервуару (або парку резервуарів) в умовах конкретної нафтобази вимагають подальшого дослідження. Це зумовлює актуальність розробки нових математичних моделей, методів і алгоритмів, які адекватно відображають концепцію безпечної експлуатації розглянутих споруд в межах економічного підходу.

Згідно з [3–5] нафтовий резервуар розглядається як складна система, що має чотири логічно послідовно з'єднані підсистеми: днища, покрівлі, циліндричної стінки і вузла сполучення стінки з днищем (уторного вузла). Структурну схему надійності резервуара зображено на рис. 1.

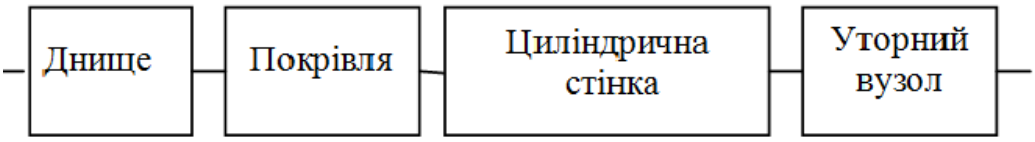


Рис. 1. Структурна схема надійності РВС

Вважається, що резервуар виконує властиві йому функції з приймання, зберігання та відпуску нафтопродуктів у нормальних режимах роботи відповідно до чинних нормативних документів і з проєктним рівнем затоки. Основним механізмом відмов резервуара вважається корозійний знос, який розглядається в контексті комбінованого впливу поверхневої і локальної корозії. Технічний стан РВС описується в термінах випадкових функцій корозійного зносу, що залежать від часу, як від параметра. Приймається, що усунення незворотного зносу конструктивних елементів вимагає

відповідного капітального ремонту, а локальні корозійні пошкодження усуваються на основі поточних ремонтів, що виконуються в межах системи технічного обслуговування і ремонтів. Критерієм відмови резервуара вважається порушення хоча б одного з нормативних вимог ненастання граничних станів, а також умов герметичності.

У роботі сформульовані модель експлуатаційного стану та ймовірні критерії часткового і повного відновлення РВС. Запропоновано модель раціонального забезпечення надійності РВС в період експлуатації з урахуванням відновлення. Розроблені алгоритми її чисельної реалізації на комп'ютері. Стосовно до типового проєкту резервуара об'ємом 5 000 м^3 досліджено вплив величини необхідного рівня надійності на стратегії відновлення конструктивних елементів. Отримані відповідні плани-графіки відновлення.

Бібліографічні посилання

1. Рябинин И. А. Надежность и безопасность структурно-сложных систем. Санкт-Петербург : Политехника, 2000. 248 с.
2. Правила технічної експлуатації резервуарів та інструкції по їх ремонту від 03.07.1999 р. : (змінені розділи та пункти розділів) : ДПІ УкрДНІПРОнафтотранс. Київ : Укрнафтопродукт, 1997. 297 с.
3. Семенец С. Н., Насонова С. С. Управление эксплуатационным состоянием нефтяных резервуаров по экономическим критериям. *Інформаційні технології в освіті, науці та управлінні*. Дніпропетровськ : ПДАБА, 2012. С. 184–187.
4. Семенец С. Н., Насонова С. С., Власенко Ю. Е., Кривенкова Л. Ю. Расчетные модели надежности нефтяных резервуаров. *Вісник ПДАБА*. Дніпропетровськ : ПДАБА, 2018. № 1. С. 60–67.
5. Семенець С. М. Насонова С. С., Олевський В. І., Волчок Д.Л. Управління проектною надійністю нафтових резервуарів. Опір матеріалів і теорія споруд. Київ : КНУБА, 2019. Вип. 103. С. 165–176.

Охрименко С. А.,
доктор экономических наук, профессор
Бортэ Г. Р.,
кандидат экономических наук
Черней В. А., аспирант
(Лаборатория информационной безопасности, Молдавская экономическая академия, г. Кишинев, Республика Молдова)

ТЕНЬ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Процессы цифровизации экономики связаны с появлением качественно новых угроз. Теневая деятельность привлекает внимание специалистов во многих странах и является предметом научных исследований. В настоящей

работе предпринимается попытка очертить ландшафт теневой цифровой экономики, выделить ее основные сегменты и описать новое поле для противодействия, какими являются криминальные операции с информационными продуктами и услугами.

Настоящая работа является логическим продолжением публикаций авторов по теме исследований, связанных с определением категории теневая цифровая экономика (ТЦЭ), сегментации сфер противоправной деятельности, построением моделей и др.

В результате проведенных исследований, авторы предлагают следующие определения теневой цифровой экономики [1–4] :

– теневая цифровая экономика – специфическая сфера экономической деятельности с присущими ей структурой и системой экономических отношений. Специфичность задается нелегальностью, неофициальностью, а также криминальным характером экономической деятельности и сокрытием доходов;

– с экономической точки зрения – сектор экономических отношений, охватывающих все виды производственно-хозяйственной деятельности, которые по своей направленности, содержанию, характеру и форме противоречат требованиям существующего законодательства и осуществляются вопреки государственному регулированию экономики и в обход контроля над ней;

– с технологической точки зрения – это индивидуальная и коллективная деятельность, являющаяся незаконной, связанная с проектированием, разработкой, распространением, поддержкой и использованием компонент информационных и коммуникационных технологий, скрываемая от общества.

Таким образом, ТЦЭ – это все незаконные и скрываемые продукты и услуги, использующие и основывающиеся на информационных технологиях. В качестве наиболее важных экономических элементов данной сферы выделяются следующие: незаконные экономические взаимоотношения, незаконная деятельность, связанная с производством, распространением и использованием запрещенных продуктов и услуг.

Достижения в области информационных технологий порождают также новые угрозы:

– атаки становятся все более изощренными за счет автоматизации и использования методов искусственного интеллекта и машинного обучения;

– подключение огромного количества новых незащищенных устройств (промышленный интернет или интернет вещей, как сеть передачи данных между физическими объектами, которые оснащены встроенными средствами и технологиями взаимодействия друг с другом или с внешней средой).

Хакеры используют для входа в сеть такие устройства, как видеокамеры, кофемашины и др., в результате резко возрастает количество целей для атак;

– раскрытие персональных данных;

– социально-опасный контент: кибербулинг, призывы к суициду и др;

– вмешательство в выборы, атаки на электронные системы голосования и обработки информации;

– атаки на электронные системы, которые обслуживают физическую инфраструктуру поставок различных товаров.

Авторы изучили состав основных продуктов и услуг криминальной направленности, относящихся к ТЦЭ. Но их спектр постоянно изменяется, появляются новые сегменты, требующие исследования и описания. В докладе будут рассмотрены следующие основные сегменты: кибероружие, как сосредоточение всех достижений информационных и коммуникационных технологий на уровне противодействия между государствами; целенаправленные атаки и АТР-группы или киберкриминал; кража личных данных. В качестве нового сегмента выделена деятельность криминальных групп по отношению к криптовалютам и нападение на криптобиржи. Следует отметить, что технология блокчейн внушает доверие клиентам и доказывает безопасность криптовалютных транзакций. Но развитие криптовалютного бизнеса не обошло пристальным вниманием компьютерных мошенников. Они обратили внимание и усилия на деятельность бирж, которые специализировались на покупке, продаже и хранении виртуальных валют.

Библиографические ссылки

1. Borta, G. (2015). The Dark Side of Information Economics. Economica (An. XXIII, nr2. (92)).
2. Охрименко, С., & Бортэ, Г. (2018). Тень цифровой экономики. ГОДИШНИК ТОМ CXXI, АКАДЕМИЧНО ИЗДАТЕЛСТВО „ЦЕНОВ”,СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ”. № 121.
3. Охрименко, С., & Бортэ, Г. (2019). Новое наполнение науки секьюритологии. В Nauka i praktyka bezpieczeństwa (стр. 112-147). Krakow: WYDAWNICTWO EAS.
4. Ohrimenco, S. & Borta, G., (2021). The nature of shadow digital economics. MEST Journal, 15 January, 9(1), pp. 146-156.

Панченко Л. В., викладач кафедри загальноправових дисциплін Дніпропетровського державного університету внутрішніх справ

МУЛЬТИСТЕЙКХОЛДЕРСЬКА МОДЕЛЬ УПРАВЛІННЯ ІНТЕРНЕТОМ

В наш час розвитку інформаційних технологій відбувається зростання кіберзагроз та їх вплив на функціонування національних та транснаціональних структур, що сприяє формуванню нової глобальної

ситуації в безпеці.

Між світовими центрами відбувається поділ сфер впливу у кіберпросторі, внаслідок цього посилюється їх прагнення до забезпечення власних геополітичних інтересів, що впливає на рівень розвитку інформаційного суспільства держав. Посилюється маніпулювання громадською думкою та використання кібератак як інструменту спеціальних інформаційних операцій.

Необхідним фундаментом інформаційного суспільства є проголошене у *ст. 19 Загальної декларації прав людини* право кожного на свободу переконань, що серед іншого включає свободу переконань та свободу шукати, отримувати та поширювати інформацію та ідеї будь-якими засобами та незалежно від державних кордонів.

За результатами всесвітньої зустрічі з питань інформаційного суспільства *в Женеві 2003 р.* була розроблена *Декларація принципів інформаційного суспільства (Туніс),* що визначила основні завдання побудови інформаційного суспільства у світі та *План дій.* Також було затверджено щорічне проведення форуму з питань управління Інтернетом та визначено, що політичні повноваження питань регулювання Інтернету є суверенним правом кожної держави [1].

Основними підходами до управління Інтернетом є такі:

- технологічна координація елементів (розподіл IP-адрес);
- створення протоколів і стандартів;
- управління системою доменних імен тощо;
- розробка урядами принципів, норм, правил, програм та процедур ухвалення рішень.

У сферу забезпечення інтересів кожної держави входить: забезпечення кібербезпеки та встановлення режиму регулювання Інтернету. Крім того, виявленню кіберзагроз сприяє Інтерпол.

Платформа Інтерполу використовується як централізований портал для забезпечення координації силових структур у боротьбі з кіберзлочинцями, у своєму складі має 194 країни, що створюють своєрідну глобальну систему поліції, яка співпрацює з Генеральним секретаріатом для обміну даними під час поліцейських розслідувань. Для цього в кожній країні створено національне центральне бюро Інтерполу (NCB), яке пов’язує національну поліцію з глобальною мережею [5].

Законодавством України, яке регулює Інтернет, є Конституція України, закони України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», Конвенція про захист прав людини і основоположних свобод, Конвенція про кіберзлочинність, Стратегія національної безпеки України, Концепція боротьби з тероризмом в Україні, тощо. В глобальному контексті пр*отидії кіберзагрозам була прийнята Стратегія кібербезпеки України.*

З огляду на протидію злочинам в інформаційному полі національного

законодавства 15 жовтня 2021 року РНБО затвердила Стратегію інформаційної безпеки України на період до 2025 року.

Основними завданнями стратегії визначено: захист інформаційного простору України, протидію поліцією поширенню незаконного контенту; інформаційну реінтеграцію громадян, підвищення рівня медіакультури та медіаграмотності; забезпечення захисту прав працівників інформаційної сфери тощо [1].

Стратегія визначає підтримку *мультистейкхолдерської моделі* управління Інтернетом. Мультистейкхолдерська модель управління містить у собі багатостороннє управління Інтернетом.

Стейкхолдери – це фізичні та юридичні особи, зацікавлені у фінансових та інших результатах діяльності певної організації та здатні здійснювати на неї вплив, що пояснює та формує стратегію розвитку з врахування інтересів зацікавлених сторін [3].

Відповідно до *мультистейкхолдерської моделі* для досягнення цілей управління Інтернетом потрібно брати до уваги різні інтереси *стейкхолдерів* (представників держав, урядових та міжурядових організацій), які будуть представляти певний тип неформальної коаліції.

Ще в березні 2021 року для протидії дезінформації, пропаганді, реагування на кіберінциденти та кібератаки в Україні створено спеціальні органи: *Міжнародний центр протидії дезінформації* та *Центр стратегічних комунікацій та інформаційної безпеки*. Відповідно до Стратегії 15 жовтня 2021 року утворюється *Національний центр резервування державних інформаційних ресурсів, урядова команда – CERT-UA, Національний координаційний центр кібербезпеки.*

Загалом Консорціум Всесвітньої мережі «Інтернет» містить у собі 350 організацій, що займаються розробкою та поширенням стандартів Інтернет.

На виконання цілей Україною планується: формування системи дієвої кібероборони, забезпечення у протидії розвідувально-підривній діяльності у кіберпросторі, завершення імплементації міжнародного законодавства; удосконалення системи розвідувального забезпечення та низка інших заходів. [1].

Отже, *мультистейкхолдерської моделі* управління Інтернетом – це *моделі* управління для досягнення цілей з урахуванням інтересів зацікавлених сторін.

Бібліографічні посилання

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021р. № 447/2021.
2. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/7-R. Тунисское обязательство. Тунис, 2005. URL: www.itu.int/wsis/docs2/tunis/off/7-ru.doc
3. Гурова А. Р., Морозова В. К. Стейкхолдерский подход к управлению предприятием-

субъектом ВЭД. URL: /donampa.ru/images/document/repablic_o/1/9.pdf
4. Декларація принципів побудови інформаційного суспільства. URL: /www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf.
5. Innovation to beat cybercrime acceleration the theme of 2021 Europol-INTERPOL Cybercrime Conference. 11 November 2021. Cybersecurity innovation the backbone of digital transformation. URL: https://www.interpol.int/News-and-Events/News/2021/Innovation-to-beat-cybercrime-acceleration-the-theme-of-2021-Europol-INTERPOL-Cybercrime-Conference

Паршин Ю. І.,
професор кафедри фінансових
та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

ВПЛИВ ПОДАТКОВИХ СХОВИЩ НА ЕКОНОМІКУ ДЕРЖАВИ

Глобалізація світової економіки сприяє зростанню міжнародного співробітництва, торгівлі, а економіки країн стають більш взаємозалежними одна від одної, що змушує країни поступово уніфіковувати податкові системи з метою формування сприятливого середовища для розвитку бізнесу.

Зазначимо, що в кожній країні своя система валютного регулювання, а також своя система оподаткування. Такі обставини можуть бути використаними нерезидентами країн для отримання додаткового прибутку, часткової нейтралізації вимог валютного законодавства країни, де базується організація в умовах «переміщення» її в іншу юрисдикцію. Це стосується також і конкуренції між валютними ринками держав за схемою торгів, де наявні кращі умови для ведення бізнесу, а зважаючи на динамічний інформаційно-технологічний розвиток світової економіки, такі питання і процеси не є проблемними. Ці та інші фактори і призвели до активного розвитку офшорного бізнесу в кінці минулого століття.

Податкове сховище, або інша його назва офшор – це фінансовий центр, основу якого становить спеціалізація на залученні іноземного капіталу [1]. Основою діяльності таких податкових зон є надання податкових пільг для іноземних компаній, які зареєстровані в країні, де вони розташовані, але з управлінням ними з-за кордону. У різних країнах є різне податкове навантаження на компанії, від помірного до такого, що компанії повністю звільняються від оподаткування, під час здійснення їх діяльності за межами місця реєстрації.

Необхідно також зазначити, що одним з найбільш привабливих критеріїв є анонімність фактичних власників компаній. Реєстрація компаній в податкових сховищах дозволяє компаніям більш ефективно планувати свою

діяльність, і особливо розподіляти фінансові кошти та оптимізувати податкові зобов'язання. Тобто такі сховища є одним з основних способів ухилення від оподаткування.

Якщо розглянути фактори, які є домінуючими під час використання компаніями таких схем, то можна виділити такі [2]:

– важке податкове навантаження, неефективна фінансова політика держави;

– клімат для інвестицій є несприятливий;

– великі ризики з інвестиційної діяльності;

– анонімне володіння інвестиційними об'єктами.

– легалізація доходів, отриманих злочинним шляхом.

Зважаючи на ці та інші фактори, офшорні юрисдикції є привабливими зонами та мають такі відмітні ознаки: податкові переваги; високий ступінь конфіденційності інформації про клієнта (банківська і комерційна таємниця); розвинена фінансова інфраструктура; історично сформований центр концентрації капіталу; політично нейтральна юрисдикція; сприятливий інвестиційний клімат та наявність розгорнутої системи угод про уникнення подвійного оподаткування.

За оцінками різних експертів, недоодержуючи доходи від податків, держави втрачають на рівні 500–600 мільярдів доларів США на рік. На частку країн з низькими доходами припадає приблизно 200 мільярдів доларів США, а їх питома вага в обсягу ВВП більше, ніж у розвинутих країн [3]. Наприклад, тільки американські компанії, що входять в рейтинг топ-500 журналу Fortune, тримали в офшорах приблизно 2,6 трильйона доларів США, таке можна сказати за будь-яку країну.

Проблема є, тож фахівці різних країн пропонують різні підходи щодо зменшення впливу цього явища (використання податкових сховищ) на економічну систему кожної країни окремо.

Зокрема, на початку жовтня 2021 р. країни Організації економічного співробітництва і розвитку досягли домовленості щодо запровадження єдиного податку на діяльність глобальних корпорацій. Країнами, які брали участь, було ухвалено рішення про 15 % збір і з цим погодилось зі 140 країн 136, а це становить понад 90 % світового ВВП. Також зазначається, що така реформа торкнеться багатьох компаній та призведе до перерозподілу 125 мільярдів доларів США.

Стосовно таких кроків міністр фінансів Франції Брюно ле Мер сказав: «Угода відкриває дорогу до справжньої податкової революції XXI століття. Це революція, оскільки назад ми вже не повернемося. Це податкова революція, оскільки вона зробить оподаткування більш справедливим. Цифрові гіганти нарешті будуть вносити справедливий податковий внесок у ті країни, де вони заробляють» [4].

Бібліографічні посилання

1. Офшор. Класичні офшорні схеми. URL: https://ru.wikipedia.org/wiki/%D0%9E%D1%84%D1%88%D0%BE%D1%80 (дата звернення: 08.10.2021 р.).
2. Офшоризація та деофшоризація економіки: міжнародний досвід та особливості. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2021. № 2. С. 294–301. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2021/09/21_2_ua/2-2021-294-301.pdf (дата звернення: 08.10.2021 р.).
3. Оффшоры, схемы, отмывание средств и оптимизация налогов: что об этом надо знать. URL: https://www.epravda.com.ua/rus/publications/2020/12/12/669095/ (дата звернення: 10.10.2021 р.).
4. 136 стран мира согласились на «глобальный налог». URL: https://ru.euronews.com/2021/10/09/oecd-world-global-corporate-taxagreement-criticism (дата звернення: 11.10.2021 р.).

Пекарський С. П., доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ, кандидат юридичних наук

ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПІД ЧАС РОЗШУКУ ТРАНСПОРТНИХ ЗАСОБІВ У ЗВ'ЯЗКУ З НЕЗАКОННИМ ЗАВОЛОДІННЯМ

Статтею 289 Кримінального кодексу України визначені підстави кримінальної відповідальності за незаконне заволодіння транспортним засобом. Незаконне заволодіння транспортним засобом – це діяння, яке вчинене умисно, з будь-якою метою протиправне вилучення будь-яким способом транспортного засобу у власника чи користувача всупереч їх волі [1, ст. 289]. З метою своєчасного виявлення інформації про осіб, які готують та вчиняють кримінальні правопорушення, та їх розкриття підрозділи кримінальної поліції використовують інформаційно-аналітичне забезпечення.

Статтею 25 Закону України «Про Національну поліцію» зазначено, що поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень. Зокрема, поліція уповноважена наповнювати та підтримувати в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України [2, ст. 26]. Відповідно до положень статті 27 Закону України «Про Національну поліцію» поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням вимог Закону України «Про захист персональних даних».

Пунктом 18 статті 8 Закону України «Про оперативно-розшукову діяльність» підрозділам кримінальної поліції, для виконання завдань

оперативно-розшукової діяльності надається право створювати і застосовувати автоматизовані інформаційні системи [3, ст. 8].

Наказом МВС України від 13.06.2018 р. № 497 затверджена Інструкція з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України. Ця Інструкція визначає порядок формування та ведення інформаційної підсистеми (далі ІП – *прим. автора*) «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (система ІПНП), призначеної для обробки відомостей про транспортні засоби (ТЗ) усіх типів (автомобілі, автобуси, мотоцикли всіх типів, марок і моделей, самохідні машини, причепи та напівпричепи до них, мотоколяски, інші прирівняні до них ТЗ та мопеди) та номерні знаки ТЗ, що розшукуються у межах кримінального, виконавчого проваджень, проваджень у справах про адміністративні правопорушення, оперативно-розшукової діяльності, а також за ухвалою слідчого судді, суду.

Метою ІП «Гарпун» є:

– об’єднання інформації про розшук ТЗ та номерних знаків в єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп’ютерного та телекомунікаційного обладнання;

– забезпечення оперативного реагування та прийняття управлінських рішень посадовими особами органів (підрозділів) поліції щодо розшуку ТЗ та номерних знаків;

– моніторинг тимчасових потоків даних про номерні знаки, що надходять із систем відеофіксації, на предмет їх розшуку, одночасного перебування на різних ТЗ (номерні знаки – двійники), використання номерних знаків, що за даними Єдиного державного реєстру Міністерства внутрішніх справ України (ЄДР МВС) знищено;

– забезпечення взаємодії з державними та приватними виконавцями під час розшуку ТЗ боржника у виконавчому провадженні [4].

Обліку в ІП «Гарпун» за категоріями «орієнтування про незаконне заволодіння ТЗ», «орієнтування про залишення ТЗ місця дорожньо-транспортної пригоди», «орієнтування про залишення ТЗ місця вчинення іншого правопорушення» та «орієнтування оперативне про ТЗ» підлягають відомості про розшук ТЗ, які стали засобом, предметом кримінального чи адміністративного правопорушення або місцезнаходження яких встановлюється під час здійснення оперативно-розшукової діяльності.

Під час внесення інформації до ІП «Гарпун» зазначаються:

– підстава внесення інформації до обліку;

– номер і дата реєстрації заяви (повідомлення, рапорту);

– вид правопорушення (кримінальне, адміністративне);

– прізвище, ім’я, по батькові поліцейського, який є ініціатором розшуку ТЗ;

– найменування органу (підрозділу) поліції;

– реєстраційний номер, вид, марка, модель та колір ТЗ;

– відомості про водія, власника (співвласника) ТЗ (прізвище, ім'я, по батькові, дата та місце народження, місце проживання та реєстрації, для юридичної особи зазначаються її найменування, код за ЄДРПОУ, місцезнаходження);

– місце події;

– стислий опис події та первинні дії поліцейських під час виявлення ТЗ, що розшукується (надання інформації ініціатору розшуку про осіб, що перебували в ТЗ, опитування водія і пасажирів, з'ясування необхідних анкетних даних та контактних телефонів, у разі наявності підстав – вжиття заходів щодо затримання та доставляння до найближчого органу (підрозділу) поліції тощо);

– підстава та дата зняття інформації з обліку [4].

Підставою для внесення відомостей є заява (повідомлення) особи про вчинене кримінальне правопорушення чи іншу подію або рапорт поліцейського, що надійшли до органу (підрозділу) поліції, із зазначенням інформації про ТЗ. Зазначаємо, що під час здійснення оперативно-розшукової діяльності інформація за категорією «орієнтування оперативне про ТЗ» вноситься до ІП «Гарпун» поліцейським оперативного підрозділу на підставі рапорту.

ІП «Гарпун» має відповідне програмне забезпечення створене для запобігання вчиненню правопорушень, аналізу тимчасового набору даних про номерні знаки, що надходять із систем відеофіксації, на предмет їх розшуку, одночасного перебування на різних ТЗ (номерні знаки – двійники), використання знищених знаків, а також для автоматизованого інформування про такі факти диспетчерів, оперативних чергових, нарядів поліції органів (підрозділів) поліції та ініціаторів розшуку [4]. Використання сучасних технологій надає можливість встановити місцезнаходження транспортного засобу, який перебуває в розшуку у зв'язку із незаконним заволодінням.

Наприклад, зазначаємо, що у м. Маріуполі 24 грудня 2016 року було відкрито Єдиний аналітичний сервісний центр поліції Донеччини, який побудований на технологіях «смарт-сіті». До цієї системи були підключені різні міста Донецької області. Поліцейські постійно бачать відео з камер не тільки м. Маріуполя, але й з усієї території Донецької області, що підконтрольна Україні. До системи UASC під'єднані і прифронтові райони. Встановлені камери на межі з Харківською, Дніпропетровською та Запорізькою областями, на КПВВ, а також на трасах міжнародного та державного значення та аварійно небезпечних ділянках.

У системі UASC працюють: служба 102 та диспетчерський центр, система інтелектуального відеоспостереження, мобільні додатки «Поліція 102» та «My Pol». Ці сервіси допомагають контролювати оперативний стан та підвищувати безпеку громадян. Програма розпізнає номер, марку, модель, колір автомобілів, а також здатна здійснювати переслідування автомобілів в

реальному часі. Камери налаштовані і на ідентифікацію людей та можуть розпізнавати вік, етнічне походження, вираз обличчя, наявність окулярів, навіть колір одягу. За інформацією ГУНП в Донецькій області за перші три роки (2016–2019) з використанням «розумних» камер затримано приблизно 500 транспортних засобів, зокрема ті, що були викрадені або залишили місце ДТП.

UASC надає можливість оперативно реагувати на події та правопорушення. Усі дзвінки зі всієї області надходять до кол-центру 102. Із впровадженням централізованого прийому викликів оперативне реагування на повідомлення громадян поліпшилося. Програма має 700 функцій, за 15 секунд камера розпізнає небезпеку та надсилає до центру сигнал тривоги, обробка виклику та спрямування на допомогу наряду поліції займає 3–5 хвилин.

У 2020–2021 роках UASC встановлені в Донецькій області додаткові відеокамери, які спостерігають за місцями концентрації правопорушень. Також розширено функціонал програмного комплексу. Зокрема, до камер підключені функції розпізнавання залишених речей та їх власників (для можливого виявлення вибухових та інших небезпечних речовин), нетипової поведінки людей (для своєчасного реагування на дестабілізацію ситуації).

Отже, первинна інформація, яка надходить до кол-центру, обробляється та вже опрацьована спрямовується до патрульної поліції. Патрульні, виїжджаючи на виклик, вже мають усю інформацію про людей, які перебувають за вказаною адресою, якщо вони є у базі. Крім того, патрульні отримують інформацію з камер відеоспостереження. Якщо камера зафіксує автомобіль, який перебуває у розшуку, або людину, яка в невідведеному місці переходить дорогу та багато іншого, ця інформація негайно передається патрульним для швидкого реагування.

Викладені міркування дозволяють зробити висновок, що використання підрозділами кримінальної поліції інформаційно-аналітичного забезпечення під час розшуку транспортних засобів у зв’язку із незаконним заволодінням має правове регулювання та практичне використання.

Бібліографічні посилання

1. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III (редакція від 04.10.2021). *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
2. Про Національну поліцію : Закон України від 2 липня 2015 року № 580-VIII (редакція від 08.08.2021). *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.
3. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 року № 2135-XII (редакція від 15.03.2021). *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.
4. Інструкція з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України : затв. наказом МВС України від 13 червня 2018 року № 497. *Відомості Верховної Ради України.* URL: how/z0787-18#Text.

Пефтієв Д. О.,
начальник відділу Управління
оперативної підтримки
Національної поліції України

ПРОБЛЕМНІ ПИТАННЯ ПОБУДОВИ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ, ЩО БАЗУЮТЬСЯ НА ЗБОРІ ТА АНАЛІЗІ ДАНИХ (ILP)

Поліцейську діяльність, що базується на зборі та аналізі даних, все частіше використовують у багатьох країнах світу для реагування на зростаючі виклики. Стратегія розвитку системи Міністерства внутрішніх справ України до 2020 року передбачала ухвалення поліцейської діяльності, що базується на зборі та аналізі даних, у вигляді методології та набору інструментів для підвищення аналітичного потенціалу Національної поліції України.

Започаткована у Великобританії така концепція поліцейської діяльності мала за основу визнання того факту, що поліція витрачала занадто багато часу та ресурсів на розслідування злочинів, а не протидію злочинності в цілому. У 1993 році Аудиторська комісія Великобританії виступила за посилення використання розвідки, спостереження та інформаторів для боротьби з основними порушниками, щоб поліція стала більш ефективною у боротьбі зі злочинністю, а не займалася лише реагуванням на вже вчинені злочини.

Поліцейська діяльність, що базується на зборі та аналізі даних, сприяє проактивному підходу в поліцейській діяльності, доповнюючи традиційну модель (реагування). Безсумнівно, що це ефективний інструмент для боротьби з організованою злочинністю, більш ефективного використання ресурсів, а також для цільового визначення та вирішення пріоритетних завдань по боротьбі із злочинністю в стратегічному руслі. Випереджаючий і орієнтований на майбутнє підхід такої поліцейської діяльності полегшує роботу із запобігання, зменшення та ліквідації злочинності.

Аналіз проблем. В умовах складної соціально-економічної ситуації в країні, яка у тому числі продиктована тривалим військовим конфліктом, бюджет Національної поліції України навряд чи є достатнім для ефективної поліцейської діяльності щодо забезпечення профілактики та безпосередньо боротьби із злочинністю на усіх напрямах одночасно.

Тому у керівництва Національної поліції України є потреба визначати найбільш актуальні напрями поліцейської діяльності для ефективного розподілу ресурсів. Впровадження поліцейської діяльності, що базується на зборі та аналізі даних (не плутати з аналізом статистичних показників результатів виявлення та розкриття злочинів та правопорушень), надає

можливість ранжування пріоритетів та напрямів, які найбільш гостро потребують першочергового забезпечення такими ресурсами.

Поліцейська діяльність, що базується на зборі та аналізі даних, у тому числі оперативної інформації про злочинну діяльність, є динамічною діяльністю, що складається з таких 6 етапів: завдання й планування, збір та оцінювання інформації, систематизація й обробка, аналіз, звітність і розповсюдження інформаційних матеріалів, зворотний зв'язок та подальші дії.

Кожен із зазначених етапів залежить від аналітичних можливостей персоналу, залученого до процесів роботи з інформацією, наявності технологій (як програмного забезпечення, так і обладнання) і, нарешті, обґрунтованої методології, необхідної для того, щоб досягнути більшої ефективності аналітичної діяльності.

Незважаючи на те, що концепція поліцейської діяльності, що базується на зборі та аналізі даних, є досить новою, вона вже існувала в певній формі в Національній поліції України, зокрема в напрямі розкриття та розслідування злочинів.

Кримінальний аналіз традиційно є складовою частиною окремих видів діяльності структурних підрозділів НПУ як на центральному, так і на регіональному рівні. Цей підхід дотепер впроваджується різними суб'єктами поліцейської діяльності. Проте сьогодні немає єдиної методології та концепції суцільного впровадження, а види аналітичних продуктів відрізняються залежно від служби або підрозділу, що їх розробляють.

Окрім вищезазначених відмінностей, треба зосередитись на проблематиці усвідомлення способу та кінцевої мети проведення кримінального аналізу.

Попри те, що кримінальний аналіз покликаний розвивати та впроваджувати горизонтальний та вертикальний обмін інформацією, а також обмін аналітичними даними між поліцейськими підрозділами з тим, щоб керівники вищої ланки мали змогу будувати ефективні стратегії розслідування та профілактики злочинності, все відбувається навпаки.

На жаль, кримінальний аналіз, що зараз проводиться в Національній поліції України, насамперед, впливає безпосередньо на боротьбу з конкретними злочинами, що фактично позбавляє його можливості проактивного впливу на оперативну ситуацію. Крім того, він має обмежені можливості для розроблення довгострокової стратегії поліцейської діяльності, і як наслідок, купірування та ліквідації певних видів злочинної діяльності.

Конфігурація кримінального аналізу, що наявна сьогодні в Національній поліції України, не заохочує (а подекуди здійснює спротив) перехід накопичених знань та інформації про кримінальний світ та способи боротьби з ним від індивідуального знання (аналітика, сектору, відділу, управління, департаменту) до інституційної бази знань Національної поліції

України загалом. Зазначена ситуація знижує цінність цих знань для досягнення стратегічних довгострокових результатів.

Дотепер не викорінена, а інколи і заохочується помилкова та руйнівна для правоохоронної системи парадигма – «моя інформація, лише мій досвід», так би мовити комплекс «бункерності». Згаданий підхід руйнує ланцюг передачі інформації та досвіду, нівелює інститут наставництва та зводить нанівець інституційну спроможність правоохоронних органів.

Нарешті, за умови відсутності загальноприйнятої методології, наявності застарілих технологій та відсутності єдиної системи накопичення та обробки результатів аналітичних досліджень, потенціал суб'єктів кримінального аналізу в Україні не відповідає ступеню значущості та викликам кримінального світу.

Аналіз варіантів вирішення:

Варіант 1. «Пряме» перенесення досвіду передових країн. Цей варіант передбачає переведення системи кримінального аналізу, що наявна на сьогодні, у формат поліцейської діяльності, що базується на зборі та аналізі даних, з використанням методології, програмного забезпечення та організаційної розбудови, подібних до тих, що вже використовуються у країнах, які свого часу успішно впровадили відповідні системи (наприклад, Великобританії). У такому разі робота буде зосереджена на впровадженні готового «з коробки» спеціалізованого програмного забезпечення (наприклад, I2) для аналізу даних, контролю кіл підозрюваних, підвищення оперативної ефективності та покращення міжвідомчої співпраці. Перевагою цього підходу є те, що I2 – готовий продукт, що довів свою ефективність у багатьох країнах; система є модульною, тож її структурні компоненти можуть бути підібрані відповідно до нагальних потреб; насамкінець, воно може надати необхідну підтримку багатьом групам користувачів, у тому числі керівному складу поліції, аналітикам, слідчим і рядовим поліцейським. З погляду реалізації це відносно простий варіант.

Серед недоліків цього варіанта треба відзначити його високу вартість, з урахуванням обмеженості ресурсів та наявності інших потреб і пріоритетів. Тому виникає питання щодо можливості продовження дії ліцензій користувачів, а також придбання необхідних оновлень.

Варіант 2. Індивідуальне технологічне рішення для впровадження в Україні формату поліцейської діяльності, що базується на зборі та аналізі даних. Цей варіант передбачає розроблення і подальше впровадження індивідуального програмного забезпечення, що відображатиме нагальні потреби щодо збору та аналізу даних, а також розвитку інституційного потенціалу та закупівлі необхідного обладнання, що забезпечить вільний горизонтальний і вертикальний обмін інформацією. Пропоноване рішення є комплексним аналітичним інструментом (програмним забезпеченням), яке

об’єднає в одному місці бази даних, що вже є, та дозволить використовувати «відкриті ресурси» (соціальні мережі, сервіси обміну повідомленнями, записи камер спостереження тощо, які є загальнодоступними). Простіше кажучи, рішення об’єднає великі масиви даних. Загальна мета рішення – аналіз зібраних даних для підтримки розслідувань, які проводить НПУ, планування внутрішніх ресурсів установ та управління відповідними рішеннями.

Складність реалізації цього варіанта набагато вища за попередній, однак цей варіант є більш комплексним. Саме тому другий варіант може стати більш дієвим, ніж, наприклад, використання традиційного програмного забезпечення I2.

Філософія підходу до впровадження діяльності поліції, керованої аналітикою (ILP), дещо глибша, ніж просто закупівля окремих програмних продуктів для вирішення або автоматизації окремого виду поліцейської діяльності.

Це зміна парадигми світосприйняття взагалі аналітичної роботи в нашій державі та перехід від окремих розрізнених програмних продуктів, застарілих логістичних підходів з обміну інформацією, стандартизації та уніфікації наборів даних та підходів до їх аналізу.

У підсумку пропонується розробити та затвердити концепцію та дорожню карту розвитку кримінального аналізу в Україні, реалізація якої б не залежала від організаційно-штатних та кадрових змін, що відбуваються в окремих підрозділах та системі загалом.

Покраса К. В., ад’юнкт кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ ПІД ЧАС ПРОВЕДЕННЯ ОГЛЯДУ МІСЦЯ ПОДІЇ УМИСНОГО ЗНИЩЕННЯ АБО ПОШКОДЖЕННЯ ЧУЖОГО МАЙНА ШЛЯХОМ ПІДПАЛУ

У сучасних умовах розвитку інформаційних систем та технологій актуальним постає питання щодо використання новітніх досягнень науки та техніки під час здійснення досудового розслідування та проведення окремих слідчих (розшукових) дій.

Одним з ефективних шляхів збирання доказів сторонами кримінального провадження, зазначених у ст. 93 Кримінального

процесуального кодексу України, під час розслідування кримінальних правопорушень, пов'язаних з умисним знищенням або пошкодженням чужого майна шляхом підпалу – є огляд місця події [1].

Огляд, як і багато інших слідчих дій, є дією пізнавальною, оскільки проводиться за допомогою різних методів пізнання. Тому під час проведення огляду слідчий не тільки спостерігає, але й здійснює різні вимірювання та обчислення, в тому числі із застосуванням інноваційних сучасних технологій.

Останнім часом поряд із традиційними засобами виявлення, фіксації, вилучення, а також дослідження матеріально фіксованих слідів та обстановки місця події в цілому інноваційним і досить перспективним напрямом стає активне застосування сучасних тривимірних цифрових технологій і штучного інтелекту, метою якого є створення візуалізації й реконструкція обставин і картини злочину або окремих його епізодів (деталей) за допомогою використання 3D-моделей. Практика показує, що правоохоронці все частіше стикаються з необхідністю дослідження й фіксації матеріальних об'єктів, розташованих на великих територіях (зокрема внаслідок кримінальних вибухів, пожеж, аварій і катастроф на різних видах транспорту, техногенних катастроф). Для реконструкції місця події все більшого поширення набуває метод лазерного сканування певних об'єктів і відтворення їх у вигляді систем 3D-візуалізацій, що дає змогу зафіксувати й реконструювати в міліметрових деталях місце події та його окремі об'єкти у тривимірному просторі, що не є можливим за використання звичайних засобів і методів дослідження цих об'єктів. Це дає змогу досліджувати й використовувати важливу криміналістичну інформацію під час розслідування злочинів й у судовому розгляді. Використання технології лазерного сканування місцевості та об'єктів, у результаті чого виготовляється 3D-модель, дає змогу в кілька разів збільшити інформативність зібраних на місці події даних, надає наочну візуалізацію в тривимірному вигляді, що забезпечує ілюстративність [2, с. 159].

Фіксацію обстановки значного за розміром місця події на відкритій місцевості (наприклад, місця пожежі чи аварії) можна здійснити за допомогою мультикоптерів (квадрокоптерів), оснащених відеокамерами з відповідним програмним забезпеченням [3, с. 30–34].

В Україні досить швидкими темпами розвивається впровадження безпілотних літальних апаратів (далі – БПЛА), а зокрема квадрокоптерів у різні сфери суспільного життя.

У межах діяльності органів національної поліції БПЛА можна використовувати під час проведення оглядів місць подій з різних видів злочинів на ділянках місцевості великої площі, межі огляду якої визначені слідчим або обмежені висотою і дальністю польоту використовуваного БПЛА, а також у важкодоступній місцевості.

Зважаючи на специфіку таких місць подій, застосування БПЛА для аерофотовідеозйомки деталей місця події може бути не тільки додатковим до традиційних технікокриміналістичних засобів фіксації місця події, а й

єдиним сучасним, самостійним засобом у конкретній ситуації, здатним виконувати традиційні види фотозйомки, що застосовуються під час огляду місця події: орієнтуючої – для фіксації загального вигляду місця події з прив'язкою до навколишньої території; оглядової – для фіксації безпосередньо самого місця події; вузлової – для фіксації крупним планом, наприклад, місця зіткнення транспортних засобів, що зіткнулися; детальної – для фіксації безпосередньо самих слідів зіткнення [4, с. 117–125].

Зокрема, англійськими фірмами Polyciano Foster+Freeman, SUPERfume Foster+Freeman і Natural l Foster+Freeman розроблені технології обкурювання слідів флуоресцируючим реагентом, використання ціанакрилату і ІК-флуоресцентного дактилоскопічного порошку. Німецькою фірмою Nincha Attestor Forensics і англійськими фірмами TFD-2 Foster+Freeman і Crime-Lite Imager Foster+Freeman запропоновані відповідно технології виявлення слідів у кліматичних камерах у низькотемпературному режимі після обробки поверхні розчином нінгідрину, високотеплової обробки слідів на паперових носіях, а також система напівавтоматичного і автоматичного поліпшення якості слідів. Такі технології дають змогу значно розширити наявні можливості виявлення папілярних візерунків на різних поверхнях, зокрема на поліетилені, шкірі, металі, пінопласті тощо [5, с. 59–60].

Отже, аналізуючи рівень наукових досягнень вітчизняних та зарубіжних фахівців у галузі науки та техніки, вивчення сучасних технологій, важливу роль в успішному, якісному та швидкому проведенні слідчих (розшукових) дій та досудового розслідування загалом відіграє наявність та використання сучасних наукових приладів, які застосовуються спеціалістами під час проведення окремих слідчих дій, в тому числі під час проведення огляду місця події щодо умисного знищення або пошкодження чужого майна шляхом підпалу. З огляду на викладене виникає необхідність оптимізації, осучаснення та оснащення слідчих підрозділів Національної поліції вказаними технічними розробками.

Бібліографічні посилання

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 29.10.2021).

2. Павлюк Н. В. Фіксація доказової інформації за допомогою систем 3D-візуалізації : матеріали наукової конференції за результатами роботи фахівців НДІ ім. акад. В. В. Сташиса НАПрН України за фундаментальними темами у 2018 р., м. Харків, 26 березня 2019 р. Харків : Право, 2019. С. 158–160.

3. Пиріг І. В. Організація і тактика проведення огляду місця події в сучасних умовах розвитку науки і техніки. *Криміналістичний вісник*. 2019. № 2 (32). С. 30–34.

4. Семенов В. В., Терешкевич А. І. Використання новітніх технологій та досягнень науки й техніки в кримінальному провадженні. *Криминалистика и судебная экспертиза*. 2015. Вып. 60. С. 117–125.

5. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів : ЛьвДУВС, 2020. С. 59–60.

Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ВИКОРИСТАННЯ ПОЛІЦЕЙСЬКИХ КВЕСТІВ У НАВЧАЛЬНОМУ ПРОЦЕСІ ДНІПРОПЕТРОВСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ

Минуло майже п’ять років з моменту розроблення та впровадження у навчальний процес Дніпропетровського державного університету внутрішніх справ професійно-ділової гри «Лінія 102». Інформаційно-технічна платформа квесту «Лінія 102» розроблена викладачами кафедри економічної та інформаційної безпеки [1]. За розпорядженням керівництва Національної поліції ця технічна платформа впроваджена в усі навчальні заклади МВС. Це підтверджує необхідність вивчення цієї інформаційно-технічної платформи курсантами-поліцейськими.

У доповіді буде надана увага новітнім методикам викладання навчального матеріалу для отримання знань та практичних навичок роботи з інформаційно-телекомунікаційною системою «ЦУНАМІ», емулятором якої є інформаційно-технічна платформа професійно-ділової гри «Лінія 102».

У тематичному плані вивчення дисципліни «Інформаційне забезпечення професійної діяльності», яка викладається на другому курсі факультетів підготовки фахівців для підрозділів кримінальної поліції, підготовки фахівців для підрозділів превентивної діяльності, підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ на вивчення теми «Інформаційно-технічна платформа оперативно-тактичних навчань «Лінія 102» заплановано два заняття по 2 години. Інформаційно-технічна платформа «Лінія 102» складається з сімох навчальних місць.

На першому практичному занятті курсанти вчаться кваліфіковано готувати повідомлення-фабули довільних подій та вмінню професійно вносити відомості повідомлень заявників в електронну картку системи «Лінія 102» (емулятор «ЦУНАМІ»). На початку заняття викладач мотивує курсантів щодо необхідності отримання навичок професійного передавання опису подій оператору 102 ситуаційних центрів ГУНП, які знадобляться в разі звернення до поліцейських громадян, яким необхідна допомога правоохоронців. Наводиться методика підготовки повідомлень про події, в яких обов’язково повинна міститись така інформація:

- що за подія трапилась;
- місце скоєння події;

- детальний опис осіб, які брали участь у події;
- наслідки події;
- детальний опис підозрюваних тощо.

Рис. 1. Інформаційно-технічна платформа «Лінія 102»

Після цього наводяться приклади навчальних повідомлень-фабул. Далі курсанти самостійно готують довільне повідомлення, яке будуть передавати під час виконання ролі заявника, та занотовують його у конспект.

Наступний крок заняття – курсантам пропонується перегляд навчальних відеороликів, які розміщені на вебресурсі 102.dduvs.in.ua як мультимедійні рекомендації (рис. 2, 3) [2].

Далі курсанти самостійно заходять на робоче навчальне місце оператора 102 і викладач ще раз за допомогою мультимедійного проєктора показує дії, які їм необхідно буде виконати під час квесту щодо внесення необхідної інформації для створення електронної картки події (рис. 4).

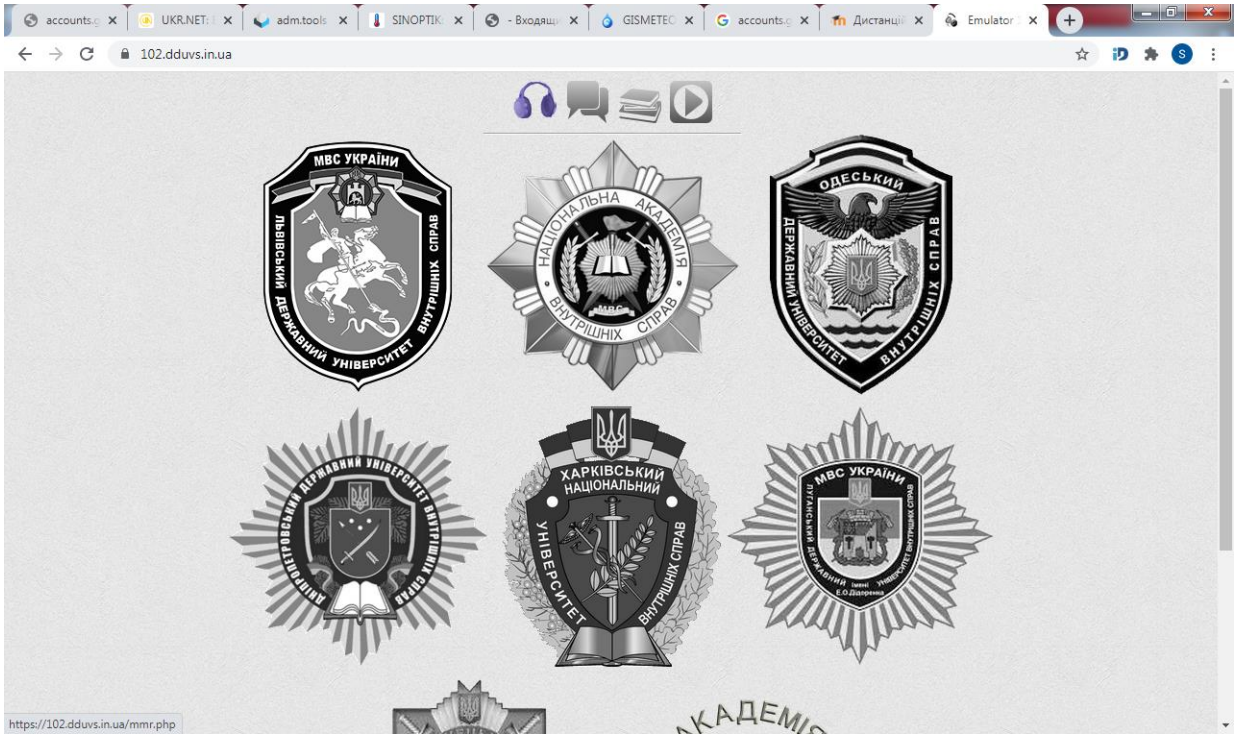


Рис. 2. Загальний вигляд вебресурсу «Лінія 102»

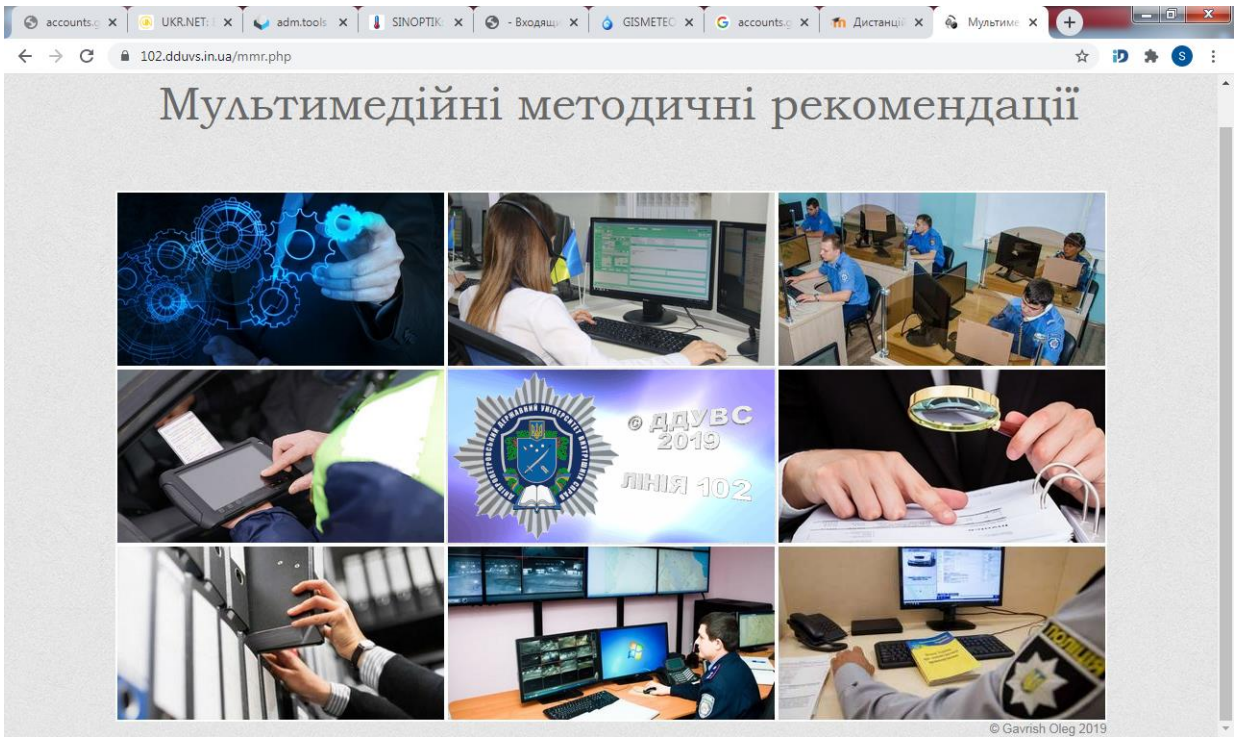


Рис. 3. Мультимедійні методичні рекомендації «Лінія 102»

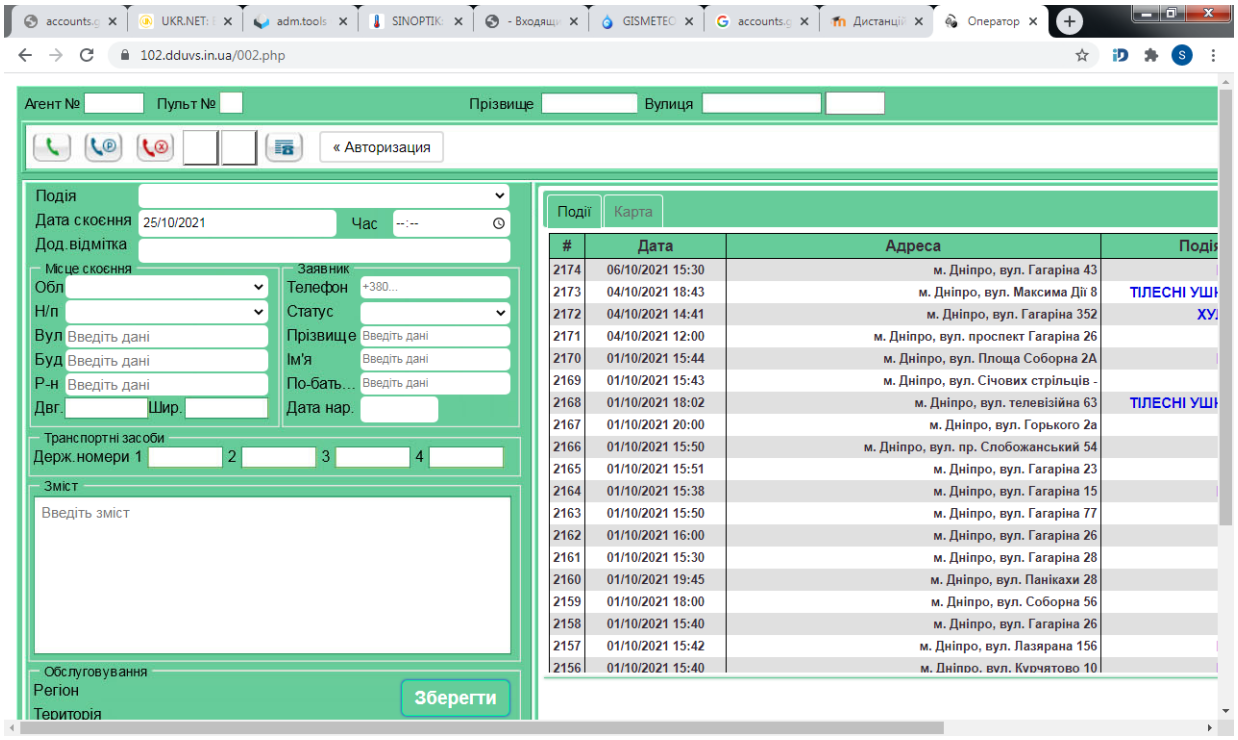


Рис. 4. Робоче навчальне місце оператора 102

Для проведення рольової гри курсантів поділяють на пари «заявник» та «оператор 102». Вони обмінюються мобільними телефонами. «Оператори 102» залишаються в навчальній аудиторії за комп'ютерами, на яких завантажені навчальні робочі місця операторів 102, а «заявники» залишають приміщення аудиторії і переміщуються на територію плацу або коридору університету, де розосереджуються, щоб не заважати один одному, і передають розроблені та занотовані повідомлення своїм напарникам. Під час прийому повідомлень «оператори 102» ставлять навідні запитання заявникам і відповідають за якість внесеної інформації в створену ними картку події, в спеціальному полі якої вводиться їхнє прізвище, ініціали та номер групи.

Після введеної у повному обсязі інформації електронна картка спеціальною кнопкою «Зберегти» записується і попадає в базу даних. Оператору 102 необхідно запам'ятати порядковий номер збереженої картки 102, яка знадобиться для наступного заняття і виконання поліцейського квесту. По завершенню епізоду квесту курсанти міняються ролями і виконують дії, описані вище.

По закінченню заняття викладач підбиває підсумки, вказує на типові помилки та оголошує оцінки за виконані практичні вправи.

Під час другого заняття з вивчення інформаційно-технічної платформи професійно-ділової гри «Лінія 102» курсанти детально ознайомлюються з навчальними робочими місцями патрульного поліцейського [3] та диспетчера (чергового відділу поліції).

На початку заняття курсантам викладається навчальний матеріал. Після цього за допомогою мультимедії та інтерактивної дошки демонструються навчальні відеофільми можливостей робочих місць патрульного поліцейського та диспетчера (чергового відділу поліції), рис. 5, 6.

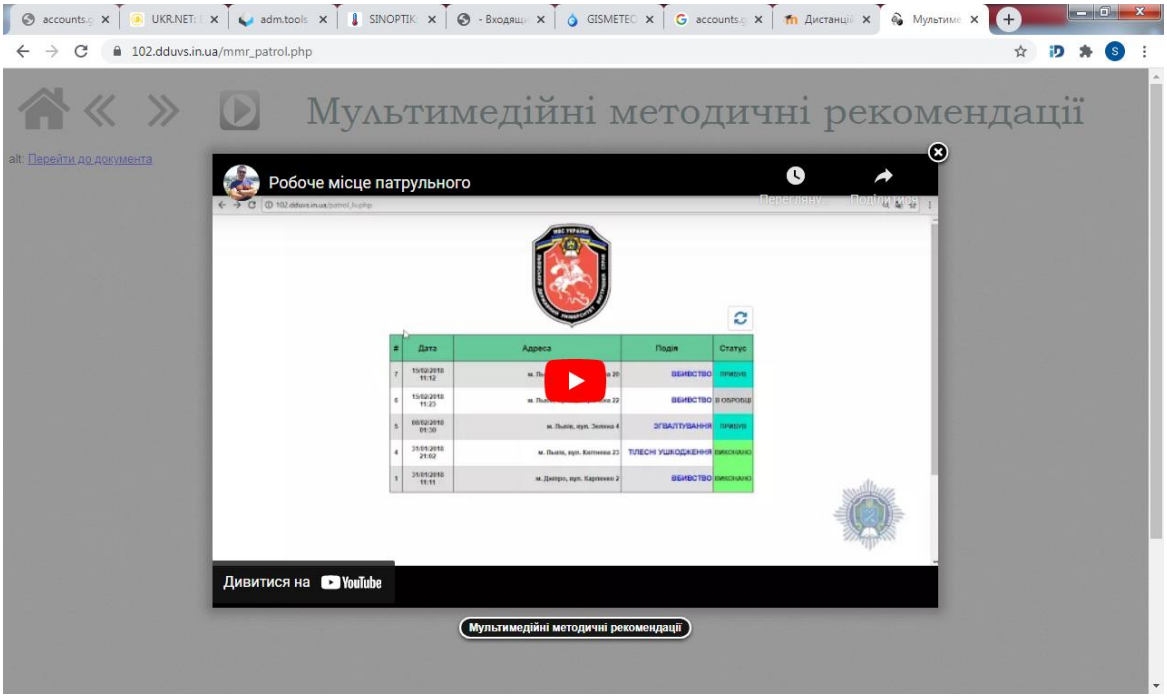


Рис. 5. Навчальний відеофільм робочого місця патрульного поліцейського

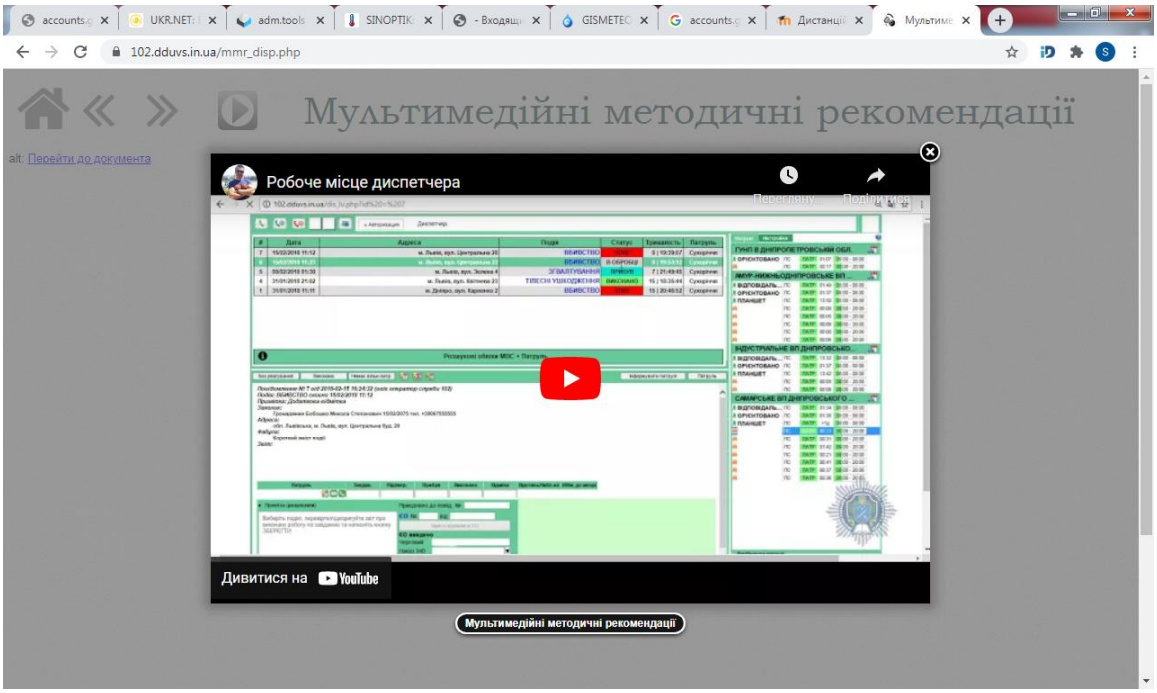


Рис. 6. Навчальний відеофільм робочого місця диспетчера

Далі викладач ще раз за допомогою мультимедійного проєктора показує дії, які їм необхідно буде виконати під час квесту вже безпосередньо з реальної навчальної оболонки «Лінія 102». Курсанти також заходять на робочі місця диспетчера на комп'ютерах навчальної аудиторії. Навчальні робочі місця патрульних поліцейських відкривають на своїх смартфонах, які імітують планшети патрульної поліції.

Поліцейський квест виконується у парі, де один курсант грає роль патрульного поліцейського і відпрацьовує матеріали електронної картки на підставі події, яку він придумав та передав, виконуючи роль «заявника». Наприкінці виконання практичних завдань складається детальний звіт щодо реагування на зазначену подію, до якого додаються фотографії з місця події (рис. 7). Звіт про виконану роботу надсилається диспетчеру.

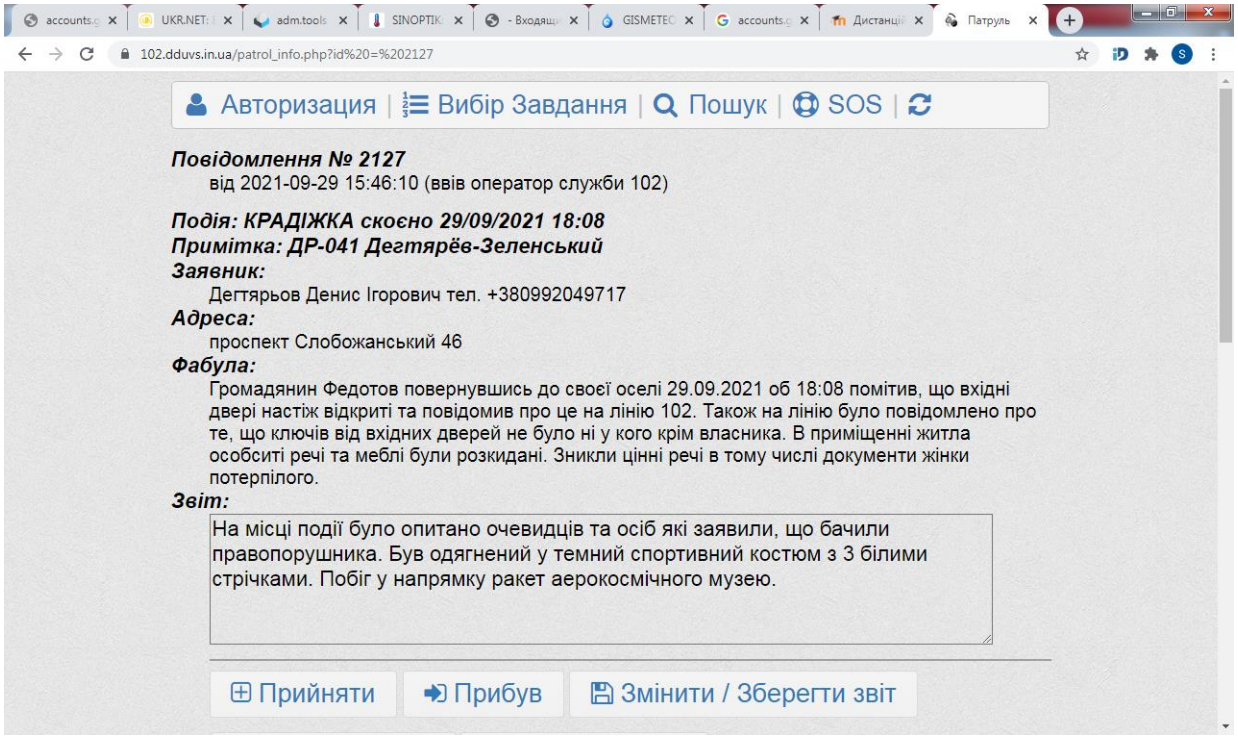


Рис. 7. Звіт про виконану роботу патрульного поліцейського

Другий курсант виконує роль диспетчера (чергового відділу поліції). Він на своєму робочому місці спостерігає як змінюється статус виконання завдання патрульним поліцейським «Нове», «В обробці», «Прибув», «Виконано», рис. 8. Перевіряє звіт напарника-патрульного поліцейського і в разі потреби вимагає від нього необхідних уточнень стосовно осіб, обставин та фото з місця події.

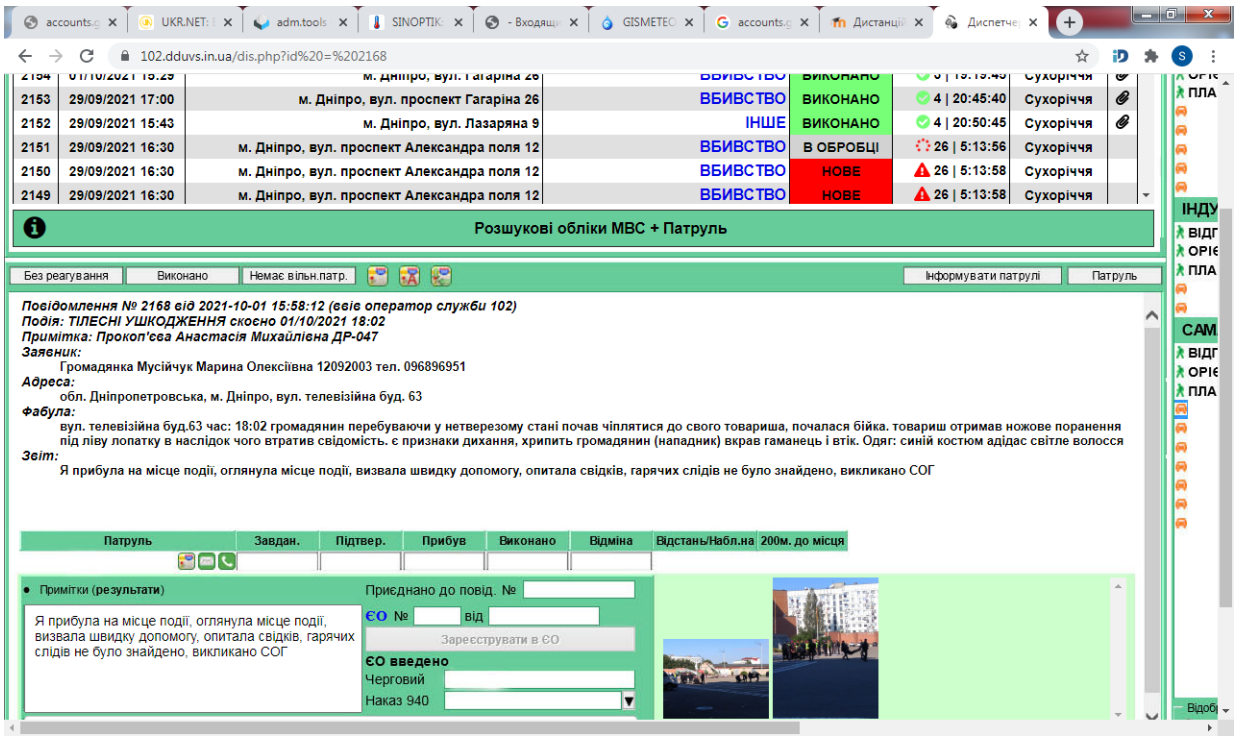


Рис. 8. Навчальне робоче місце диспетчера (чергового відділу поліції)

По закінченню відпрацювання завдання патрульним поліцейським на підставі електронної картки події та схвалення його звіту диспетчером курсанти міняються ролями і виконують кожен своє завдання поліцейського квесту.

Наприкінці заняття для закріплення теоретичних знань курсанти виконують загальний тест на тему «Інформаційно-технічна платформа оперативно-тактичних навчань «Лінія 102». Викладач підбиває підсумки заняття та оголошує оцінки.

Наведена вище методика проведення практичних занять методом поліцейського квесту дозволяє курсантам, окрім теоретичних знань, отримати практичні навички та компетенції, необхідні правоохоронцям, зрозуміти інформаційні потоки та дії поліцейських по реагуванню на події громадян. Це безсумнівно впливає на мотивацію курсантів щодо опанування навчальної дисципліни «Інформаційне забезпечення професійної діяльності» і подальшого навчання у поліцейському ЗВО.

Бібліографічні посилання

1. Акімова О. О., Гавриш О. С., Махницький О. В., Прокопов С. О., Рижков Е. В., Тюря Ю. І. Методичні рекомендації проведення оперативно-тактичних навчань на основі інформаційного моделювання дій нарядів та інших підрозділів Національної поліції. Дніпро : ДДУВС, 2017. 37 с. URL: http://er.dduvs.in.ua/handle/123456789/939
2. Прокопов С. О. Інформаційне забезпечення професійно-орієнтованої ділової гри

«Лінія 102». *Актуальні питання протидії злочинності в сучасних умовах: вітчизняний та зарубіжний досвід* : матеріали ІІ Міжнар. науково-практ. конф. (м. Дніпро, 15 березня 2018 р.). Дніпро : ДДУВС, 2018. С. 439–443. URL: http://er.dduvs.in.ua/handle/123456789/1348

3. Прокопов С. О. Навчальне автоматизоване робоче місце патрульного поліцейського в інформаційно-технічній платформі інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників національної поліції у ДДУВС. *Економічна та інформаційна безпека: проблеми та перспективи* : матеріали Всеукр. науково-практ. конф. (м. Дніпро, 14 квітня 2017 р.). Дніпро : ДДУВС, 2017. С. 151–157. URL: http://er.dduvs.in.ua/handle/123456789/3317

Прокопович-Ткаченко Д. І.,
в.о. завідувача кафедри кібербезпеки,
Університету митної справи
та фінансів, м. Дніпро,
кандидат технічних наук

НОВІТНІ ТЕХНОЛОГІЇ ХМАРНИХ ІНФОРМАЦІЙНО-ТЕХНІЧНИХ СИСТЕМ

Останнім часом хмарні постачальники продемонстрували рух до консолідації технологій навколо інфраструктурних платформ, баз даних і навіть додатків. Поряд з цією тенденцією іншим помітним напрямом, який демонструють постачальники хмарних послуг, є інтеграція «кількох нових технологій», таких як операційні навантаження та галузеві стандарти.

Завдяки останнім досягненням у технології тунелювання постачальники хмарних послуг з метою вдосконалення разом сервісів з локальними центрами обробки даних, імовірніше, позиціонують «гібридну хмару» з найвищою технологією управління пакетами, для чого використовуються нейромережі та квантові технології. Ця пропозиція, ініційована у 2021 році, може продовжувати змінювати маркетинг та менеджмент для постачальників хмарних послуг та постачальників послуг коммунікацій.

Іншим прикладом консолідації платформи є «мультихмара» або гібридна хмара, де наскрізне хмарне середовище може містити принаймні дві загальнодоступні та одну приватну хмару згідно з різноманітними типами хмарних обчислень [1].

До 2021 року архітектура загальнодоступних хмар буде відрегульована відповідно до зростаючих потреб клієнтів, і багато приватних хмар будуть перетворені в гібридні хмари, що дозволить їм зв’язуватися та взаємодіяти з загальнодоступними хмарами. Управління мультихмарного середовища можуть бути наділені або оператором бізнесу, або зовнішнім постачальником послуг. Найбільша перевага багатохмарного середовища – це відсутність

залежності від одного (дорогого та технологічно обмежувального) постачальника хмар [2].

Стандартизація та підвищена сумісність – це дві ознаки зрілої технології, яка зараз оточує світ хмарних обчислень [3]. Як і будь-яка зріла технологія, вона використовує безліч суміжних технологій, призначених для роботи з основною технологічною платформою.

Можна виділити кілька таких нових технологій, призначених для роботи з хмарою:

- Операційні навантаження хмарного сервісу дозволяють зробити навантаження більш портативними, а потоки даних – більш мобільними. Ця еластичність публічної хмари є вимогою конкурентоздатності хмарного сервісу.
- Хмарне середовище з широкомасштабними технологічними функціями буде існувати, зберігаючи при цьому безпеку та конфіденційність приватної хмари згідно із загальними стандартами.
- Багатохмарність (multi-cloud) поєднує в собі додаткові технологічні переваги публічної хмари з аспектами безпеки приватної хмари [4].
- Квантові обчислення дозволяють здійснювати аналітику в режимі реального часу дуже близько до джерела вбудованих даних [5].
- Технологія нейронавчання, що забезпечує високопродуктивну обробку бізнес-даних без необхідності в дорогих серверах. Оскільки постачальник хмарних послуг керує усіма обчислювальними ресурсами, власникам бізнесу стає легше «будувати свої хмарні системи». Найбільша перевага безсерверності – хмарний хост виконує «фрагменти коду» без участі розробників [6].
- Контейнерами даних легко переносити програми та операційне навантаження між двома по-різному налаштованими хмарами [7], якщо загальне припущення полягає в тому, що управління контейнерами та використання контейнерних технологій – це дві різні бізнес-практики, то впровадження хмарних сервісів може збільшитися за допомогою сервісів Amazon EKS, Microsoft Azure AKS або Google GKE, які активно використовують концепції контейнерних даних [8].

Впровадження контейнерних технологій значно пришвидшило обмін інформацією, при цьому приблизно 60 % користувачів скористалися Kubernetes, системою керування контейнерами, розробленою Google.

З огляду на безліч елементів хмарного середовища, яке зображено на рис. 1, не дивно, що воно створює широкий спектр нових технологій [9].

Декілька нових технологій для хмари запропонував Amazon:

– сервіс кібернетичної безпеки з підтримкою штучного інтелекту для аналізу даних кібербезпеки;

– система підтримки прийняття рішень, що активується голосом (DSS), що стимулює продажі та маркетингові функції та може значно вдосконалити державні сервіси цифрових послуг [10].

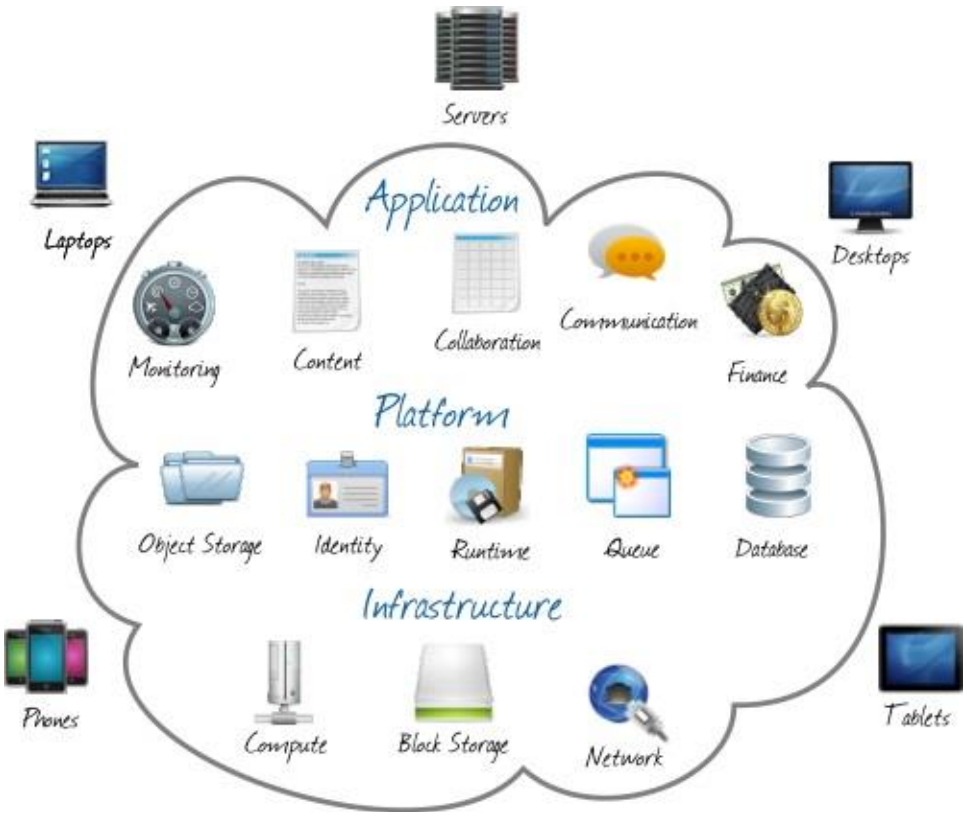


Рис. 1. Структура хмари

Огляд нових технологій для хмар та аналіз інформації вказує на появу багатохмарного середовища, що охоплює різні хмарні інфраструктури для обміну операційним навантаженням, програмами та технологічними ресурсами. А також розвиток технологій захисту даних в багатохмарному середовищі, оскільки нещодавно «Загальний регламент захисту даних» (GDPR) ЄС стимулював розвиток технологій захисту даних у хмарі, бо невідповідність призводить до серйозних штрафів для підприємств. Найближчим часом хмарні послуги матимуть безліч технологічних функцій, доступних за низькою вартістю.

Бібліографічні посилання

1. Облако за малые деньги. URL: https://www.vxchnge.com/blog/different-types-of-cloud-computing
2. Hybrid Cloud vs. Multi-Cloud Architectures. URL: https://www.dataversity.net/hybrid-cloud-vs-multi-cloud-architectures/
3. 10 Emerging Cloud Computing Trends To Watch In 2020. URL: https://www.crn.com/news/cloud/10-emerging-cloud-computing-trends-to-watch-in-2020
4. Cloud Computing Challenges: Navigating the Multi-Cloud Landscape. URL: https://www.dataversity.net/cloud-computing-challenges-navigating-the-multi-cloud-landscape/
5. The Different Types of Cloud Computing and How They Differ. URL: https://www.vxchnge.com/blog/different-types-of-cloud-computing
6. Google Merges AI, IoT With New Chips And Machine Learning Platform. URL:

https://www.crn.com/news/internet-of-things/300107041/google-merges-ai-iot-with-new-chips-and-machine-learning-platform.htm
7. Data Topics. URL: https://www.dataversity.net/what-is-a-data-container/
8. Kubernetes Craze: 8 Hot Offerings Now On The Market. URL: https://www.crn.com/slide-shows/cloud/300105761/kubernetes-craze-8-hot-offerings-now-on-the-market.htm
9. Top Six Emerging Technologies in Cloud Computing. URL: https://www.datamation.com/cloud/top-six-emerging-technologies-in-cloud-computing/
10. Amazon GuardDuty. URL: https://aws.amazon.com/ru/guardduty/

Разумова Г. В.,
професор кафедри аналітичної
економіки та менеджменту,
доктор економічних наук, доцент
Усатенко А. Г.,
слухач магістратури факультету СПОУ
Дніпропетровського державного
університету внутрішніх справ

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

На сьогодні важливим елементом функціонування ринкової економіки є діяльність підприємств. Основними факторами, які впливають на якісний результат їх діяльності, є конкурентне середовище, циклічність розвитку економіки, розвиток інформаційної бази, рівень захищеності персональних даних, наявність кваліфікаційного менеджменту тощо [1].

Економічна безпека – це найважливіша якісна характеристика економічної системи, яка визначає її здатність підтримувати нормальні умови функціонування, стійке забезпечення ресурсами та здатність до розвитку, а також послідовну реалізацію економічних інтересів.

У науковій літературі часто поняття «безпека» пов’язують з поняттям стійкості, стабільності як необхідної умови безпеки економічних систем [2]. Без фінансово-економічної безпеки бізнесу не можна подолати кризу та створити ефективний механізм введення бізнесу.

Для сучасного світу в умовах цифровізації економічна безпека поєднує в собі не лише показники фінансового стану підприємства, а й збереження даних, тобто кібербезпеку підприємства.

Найпоширенішою проблемою в сучасний час – є втрата кадрів (трудова міграція) та інформації. Це відбувається тоді, коли стратегія управління не відповідає внутрішньому середовищу підприємства, як наслідок, велика плинність кадрів, які поширюють внутрішню інформацію в процесі своєї міграції [3].

Актуальною проблемою сьогодення є пандемія. В таких умовах базові ринкові механізми не працюють, а довгострокові прогнози та цілі стають менш достовірними. Але, проаналізувавши два роки від початку карантинних обмежень, можна виявити сезонність цього явище. В процесі формування управлінських рішень необхідно враховувати, що зовнішні загрози матимуть сезонність, наприклад, політична нестабільність призведе до сезонного дефіциту на ресурси та відповідного стрибка цін [4]. Зі свого боку, певні обмеження призводять до внутрішніх конфліктів на підприємстві, наприклад, обмеженість транспорту призводить до труднощів у працівників бути присутніми на робочому місці, що знижує мобільність передачі інформації.

На нашу думку, одними з головних напрямів адаптації підприємства до сучасних умов під час збереження своєї внутрішньої фінансово-економічної безпеки, є:

1. Розвиток інтернет-платформ для обміну інформації. На сьогодні однією з таких є Біктрекс24. Завдяки цьому ресурсу кожен з працівників зможе отримати потрібну інформацію, перебуваючи не на своєму робочому місці. Також це забезпечує максимально зручний та повний доступ до інформації.

2. Головною ознакою 2021 року є мобільність та дистанційність. Тому необхідним є збільшення кількості проведення онлайн конференцій для співробітників, щоб стабільно нарощувати кваліфікаційний рівень на підприємстві. Розширення практик використання інтернет-платформ на підприємстві сприятиме збільшенню штату, що дозволить залучити до роботи нових професійних працівників по всій Україні.

3. Для безпечного функціонування підприємства доцільно використовувати сучасні програмні продукти. Наприклад, необхідним є використання найновітнішої бази для введення господарських операцій, яка забезпечує максимально комфортну та коректну роботу всіх ланок організації.

Підбиваючи підсумки за результатами виконаного дослідження, можна стверджувати, що головною проблемою сучасного підприємства є застарілі технології та обмеженість ресурсів, що призводить до зниження економічної безпеки підприємства. Досягнення цільових орієнтирів діяльності будь-якого підприємства та безпосередньо забезпечення його економічної безпеки буде залежати від результативності процесу своєчасної ідентифікації та мінімізації ризиків зовнішнього та внутрішнього середовища. Використання новітніх технологій на підприємстві сприятиме зростанню його можливостей, а саме розширенню штату, ринків збуту тощо.

Тобто головним на сьогодні є вчасно розпочати використовувати новітні продукти, ефективно уникати реальних загроз і ліквідувати шкідливі наслідки впливу окремих негативних складових зовнішнього і внутрішнього середовищ [5].

Бібліографічні посилання

1. Вівчар О. І. Інтеґраційні процеси логістики у контексті забезпечення фінансово-економічної безпеки бізнесу. *Глобальні та національні проблеми економіки*. 2015. Вип. 5. URL: http://global-national.in.ua/archive/5-2015/66.pdf.
2. Вівчар О. І. Концептуальні підходи SPACE-методики при діагностиці та оцінці економічної безпеки підприємств. *Virtus*. 2016. № 5. С. 231–235.
3. Колесніков А. П. Засади механізму забезпечення стійкого розвитку підприємств. *Інноваційна економіка*. 2013. № 1. С. 97–100.
4. Нескеренко Л. А., Рибалка Ю. М. Складові управління фінансовою безпекою підприємств. URL: http://www.pdaa.edu.ua/sites/default/files/nppdaa/162.pdf.
5. Черевко О. В. Принципи управління фінансовою безпекою підприємства. *Ефективна економіка*. 2014. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=3303.
6. Иванов С. В., Вишневский А. С. Электронные платформы как инструмент модернизации экономики Украины. *Вісник економічної науки України.* 2017. № 1 (32). С. 47–53.

Рибальченко Л. В.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

КІБЕРЗЛОЧИННІСТЬ ТА ЇЇ ВПЛИВ НА ЕКОНОМІЧНУ БЕЗПЕКУ КРАЇНИ

Рівень інформаційних та економічних злочинів у світі залишається високим, що вказує на негативний вплив для держави, підприємств, установ, компаній та громадян.

Стрімкий розвиток інформаційних технологій супроводжується динамічним розвитком злочинності як в інформаційному середовищі, так і в економіці. Рівень цифрових технологій щороку зростає, а з ним і кіберзлочини, що є негативним явищем для суспільства та держави.

Щороку в Україні збільшується кількість жертв кіберзлочинів, що внесла корективи в діяльність організацій на місцевому та державному рівнях.

Економічний статус країни є головним критерієм оцінки розвиненого суспільства, оскільки економіка забезпечує гідний рівень життя, існування країни та її стратегічний розвиток.

Для забезпечення стратегічного розвитку економіки держави необхідно створити потужну виробничу базу з надійною та ефективною системою захисту від можливих загроз. Досягнення належного рівня захисту

економічної безпеки України неможливе без забезпечення високого рівня захисту від кіберзлочинності.

За даними Національного індексу кібербезпеки (National Cybersecurity Index 2020), Україна у 2020 році піднялася на чотири позиції та посіла 22-ге місце серед 160 країн світу.

У першій десятці рейтингу у 2020 році опинилися Греція (96,1), Чехія (96,21), Естонія (90,91), Португалія (89,61), Литва (88,31), Іспанія(88,31), Польща (87,01), Бельгія (85,71), Фінляндія (85,71) та Франція (84,42) (рис. 1).

Поряд з Україною (75,32) у рейтингу Швейцарія (76,62) та Болгарія (74,03) (21-ше та 23-тє місця відповідно). На останніх позиціях Соломонови острови, Тувалу (тихоокеанська країна в Полінезії) та Південний Судан (Африка).

Цікавим є показник рівня цифрового розвитку, який в Україні становить 52,81, а найбільший належить Данії 84,64, яка у рейтингу посідає11-те місце.

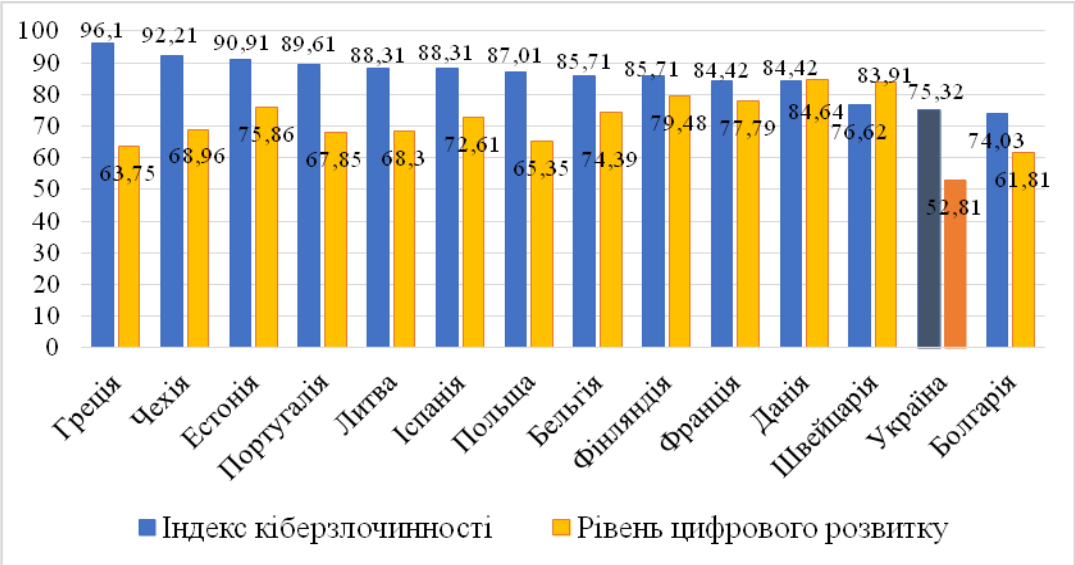


Рис. 1. Рівень кіберзлочинності у світі у 2020 році

За даними Державної служби спеціального зв'язку та захисту інформації України, у цьому рейтингу експерти аналізували такі напрями:

- законодавство у сфері кібербезпеки;
- аналіз кіберінцидентів;
- освіта у сфері кібербезпеки;
- забезпечення захисту цифрових та основних послуг;
- електронна ідентифікація та довірчі послуги;
- захист персональних даних;
- заходи щодо реагування на кібератаки та кіберінциденти;
- боротьба із кіберзлочинністю.

Поліпшення позиції України відбулося через ухвалення законодавчих актів у галузі кібербезпеки та кіберзахисту.

Міністерство цифрової трансформації України та Державна служба спеціального зв'язку та захисту інформації проводять роботу щодо посилення захисту від кіберзлочинності через оновлення та реформування законодавчої бази, вдосконалення механізму кіберзахисту органів державної влади, їх інформаційно-телекомунікаційних систем, проведення аналізу стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

Але сучасний розвиток цифрових технологій відбувається дуже швидко і сприяє поширенню кіберзлочинності, на відміну від наявного нормативно-правового законодавства, яке спрямоване на врегулювання цього виду економічної злочинності.

До основних нормативно-правових документів та законів щодо інформаційної безпеки України належать: Конституція України, Кримінальний кодекс України, Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», Закон України «Про національну безпеку України» та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згоду на обов'язковість яких надала Верховна Рада України.

Бібліографічні посилання

1. Report To The Nations. 2020 Global Study On Occupational Fraud And Abuse. URL: https://www.acfe.com/report-to-the-nations/2021/#download (дата звернення: 10.10.2021).

Рижков Е. В.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ВИКОРИСТАННЯ ІНФОТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ЗАХИСТУ ЕКОНОМІКИ

Україна переживає черговий процес реформування своєї правоохоронної сфери. На цей раз зміни стосуються органів, підрозділів та служб, призначенням яких є протидія економічним злочинам [1]. Етап характеризується стрімким вдосконаленням злочинних схем та їх переходом у віртуальний інформаційний простір. При цьому неухильно зростає

кількість випадків використання під час вчинення економічних злочинів сучасних інформаційно-телекомунікаційних технологій [2]. Особливу небезпеку в контексті появи нових видів злочинів у сфері економіки становить поява віртуальних форм розрахунків із використанням криптовалют. Більшість фінансових операцій, учасниками яких є як фізичні, так і юридичні особи, сьогодні відбувається за допомогою Інтернету. Електронні системи кредитно-фінансових установ і банків, як потенційні об'єкти злочинного посягання, а також активне користування цими системами фізичними особами, стали природною причиною виникнення, існування та збільшення економічних злочинів з використанням сучасних інфотелекомунікаційних технологій.

Водночас більшість методик щодо протидії економічним злочинам, які за останні роки були напрацьовані відповідними оперативними підрозділами Національної поліції та Служби безпеки України, нереалізовані через ліквідацію останніх у зв'язку зі створенням Бюро економічної безпеки України [3].

Тактика отримання економічної інформації оперативного характеру зумовлена як специфікою завдань відповідних підрозділів, так і особливостями економічної інформації, що становить оперативний інтерес, що відрізняють її від оперативної інформації про злочини загальнокримінальної спрямованості.

Отримання інформації, що утворюється під час використання сучасних інформаційно-телекомунікаційних технологій, передбачає застосування спеціальних технічних засобів та дотримання певного процесуального порядку, що забезпечує її доказове значення. Процесуальною формою пізнавальної діяльності негласного характеру під час розслідування кримінального правопорушення є негласні слідчі (розшукові) дії (далі – НСРД), які згідно з ч. 2 ст. 246 КПК проводяться у випадках, якщо відомості про злочин та особу-злочинця неможливо отримати в інший спосіб. НСРД «зняття інформації з транспортних телекомунікаційних мереж» (ст. 263 КПК) та «зняття інформації з електронних інформаційних систем» (ст. 264 КПК) в частині дій, що проводяться на підставі ухвали слідчого судді, проводяться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів [4].

Незалежно від тяжкості злочину проводиться установлення місцезнаходження радіоелектронного засобу без розкриття змісту повідомлень, що передаються, якщо внаслідок його проведення можна встановити обставини, які мають значення для кримінального провадження (ст. 268 КПК), а також зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний з подоланням системи логічного захисту (ч. 2 ст. 264 КПК України) [5].

Зазначене положення цілком кореспондується з вимогами Закону

України «Про телекомунікації», в ч. 4 ст. 39 якого передбачено, що оператори телекомунікацій зобов'язані за власні кошти закуповувати та встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення. Оператори телекомунікацій зобов'язані забезпечувати захист зазначених технічних засобів від несанкціонованого доступу [6].

Треба додати, що оператори телекомунікацій під час виконання своїх службових обов'язків мають доступ до інформації про персональні дані, переміщення (місцезнаходження), контакти (особисті зв'язки) користувачів тощо, яка може бути цінною під час розслідування економічних злочинів.

Наприклад, операторами систем мобільного зв'язку обробляються (приймається, реєструється, зберігається тощо) такі відомості: 1) розрахункові дані – відомості, на основі яких системами операторів здійснюється облік наданих послуг і наступні розрахункові операції з абонентами; абонентські номери, що беруть участь у з'єднанні, отриманні послуг (MSISDN); вид послуги, напрям з'єднання тощо; час початку, завершення та тривалість з'єднання, надання послуги тощо; телекомунікаційні картки, що використовувалися для розрахунків із оператором; 2) службові дані – відомості суто технічного характеру, що забезпечують функціонування систем операторів і терміналів щодо надання та споживання послуг, підтримки з'єднання тощо: міжнародний ідентифікаційний номер рухомого абонента (IMSI); міжнародний ідентифікаційний номер терміналу (IMEI); постійне місцезнаходження споживача відносно підсистеми базових станцій (BSS) оператора [7, с. 7].

Тому важливим і актуальним завданням для фахівців по боротьбі з економічною злочинністю є виявлення метаслідів, а особливо слідів метадезінформування у сфері економічної діяльності, утворених внаслідок використання інформаційно-телекомунікаційних технологій.

Автоматизовані комп'ютерні системи оперують у своїй роботі інформацією в бінарному вигляді, багаторазово змінюючи її форму та зміст. Саме через те, що інформація не є матеріальним об'єктом, а лише може бути матеріально зафіксована у різній формі, класичне розуміння слідів та процесу слідоутворення, у розрізі злочинів, що вчиняються в інформаційно-телекомунікаційній мережі, не є співвідносним. При цьому визначальна роль у процесі слідоутворення в комп'ютерній мережі належить процесу інкапсуляції – важливому інструменті об'єктно-орієнтованого програмування, що обмежує доступ до компонентів (методів і властивостей), які становлять об'єкт, та робить їх приватними (доступними лише всередині об'єкта).

Під час вчинення економічного злочину за допомогою застосування

інформаційно-телекомунікаційних технологій відбувається зміна матеріального стану елементів телекомунікаційної системи мобільного зв'язку або Інтернет, що утворює системи електронних слідів-відображень, придатних до сприйняття за допомогою відповідних програмно-технічних засобів. Це вказує на корисну властивість телекомунікаційних систем (мереж) щодо фіксації обліково-звітних даних про факт передачі та зміст переданої телекомунікаційними мережами інформації у формі електронного документа, завдяки чому цей процес можна назвати унікальним способом виявлення, попередження та припинення сучасних способів учинення злочинів у сфері економіки.

Зазначені технології мають перевагу в отриманні фахівцями по боротьбі з економічною злочинністю криміналістично значущої інформації під час оперативно-розшукового документування та розслідування кримінальних правопорушень, а тому повинні використовуватись під час виявлення, попередження та припинення злочинів цими підрозділами за конкретними напрямами, зумовленими виконанням завдань кримінального провадження, згідно з визначеною КПК процедурою шляхом зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем, а також встановлення контролю за місцезнаходженням злочинців з урахуванням специфіки протидії злочинам економічної спрямованості [8, с. 204].

З урахуванням термінів запуску нового державного органу (мінімум до одного року) та фактичною ліквідацією вказаних попередників маємо тимчасову відсутність в державі ефективно працюючих правоохоронних структур щодо протидії економічній злочинності.

За вказаних обставин питання вдосконалення підготовки відповідних кадрів, проведення прикладних наукових досліджень, організація спеціалізованих науково-практичних заходів та запозичення міжнародного досвіду є вкрай актуальними та перспективними [9].

Ефективний запуск Бюро економічної безпеки України можна здійснити шляхом використання в його діяльності наукомістких інноваційних методик, інформаційно-аналітичних продуктів, сучасних інформаційно-телекомунікаційних технологій та обов'язковим запровадженням кримінального аналізу на етапах оперативно-розшукового документування та розслідування кримінальних проваджень.

Бібліографічні посилання

1. Бюро економічної безпеки: коли запрацює новий орган і чим він відрізняється від фіскалів. URL: https://biz.ligazakon.net/analitycs/205046_byuro-ekonomchno-bezpeki-koli-zapratsyu-noviy-organ--chim-vn-vdrznyatsya-vd-fskalv
2. Всесвітнє дослідження економічних злочинів та шахрайства 2020. URL: https://www.pwc.com/ua/uk/survey/2020/gecs-ua-2020-ukr.pdf
3. Закон України Про Бюро економічної безпеки України. URL: https://ukurier.gov.ua/media/files/2021-4/1_P6-10.pdf

4. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI. *Голос України*. 2012. № 90–91.
5. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : затв. спільним наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Міністерства фінансів України, Адміністрації Державної прикордонної служби України, Міністерства юстиції України від 16.11.2012 р. № 114/1042/516/1199/936/1687/5.
6. Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.
7. Сулацький Д. В., Маркарян Г. О. Відомості щодо наданих телекомунікаційних послуг як предмет інформаційної безпеки людини та джерело оперативно значимої інформації : науково-практ. рекомендації. Донецьк : ДЮІ МВС України, 2011. 28 с.
8. Рижков Е. В. Отримання підрозділами ОВС по боротьбі з економічною злочинністю інформації про злочини у сфері економіки за допомогою сучасних інфотелекомунікаційних технологій. *Митна справа. Науково-аналітичний журнал*. Одеса. 2014. № 2 (92). Ч. 2. К. 2. С. 194–205.
9. Рижков Е. В. Інформаційні технології як засіб підготовки фахівців з економічної безпеки правоохоронних органів. *Економічна та інформаційна безпека: проблеми та перспективи* : матеріали Всеукр. науково-практ. конф. (27 квітня 2018 р., м. Дніпро). Дніпро : Дніпропетр. державний ун-т внутр. справ. 2018. С. 176–178.
10. Рыжков Э. В., Бортэ Г. Р., Охрименко С. А., Чобан Г., Шквир В. Д. Вызовы цифровой экономики. *Landmarks and Challendgts of the Sosial-Ekonomic Development* : Internetional Symposium (24–25 мая 2018 г., бухарест, Румыния). С. 497–504.

Рижкова С. А., старший викладач
кафедри адміністративного права,
процесу та адміністративної діяльності
Дніпропетровського державного
університету внутрішніх справ

AMBER ALERT В УКРАЇНІ: СИСТЕМА ОПЕРАТИВНИХ СПОВІЩЕНЬ ПРО ЗНИКЛИХ ДІТЕЙ ЗА ДОПОМОГОЮ FACEBOOK

Відповідно до статистичних даних МВС України з початку 2021 року органи та підрозділи Національної поліції зареєстрували понад 12 тисяч звернень про зниклих дітей, з них – 98 % дітей були знайдені протягом доби [1]. Окрім позитивної динаміки щодо оперативного встановлення місцезнаходження зниклої дитини, органами та підрозділами Національної поліції у 2 % випадків, які мають найвищий ступінь загрози життю та здоров'ю дитини, є такі, що потребують залучення та допомоги населення в районі, де саме зникла дитина.

У контексті зазначеного науковий та практичний інтерес має впровадження системи пошуку зниклих дітей AMBER Alert за допомогою

соціальної мережі Facebook в Україні [2]. Фахівці ювенальної превенції Національної поліції України тривалий час вели переговори з Facebook App щодо цього. Зазначений проєкт було впроваджено 22 вересня 2021 року спільно з підрозділами ювенальної поліції, кіберполіції Національної поліції України, Міністерством цифрової трансформації України та Facebook [3].

Завдяки захищеному каналу комунікації Національної поліції України та команди безпеки Facebook здійснюється обмін інформацією про викрадення дитини з високим ризиком загрози життю та здоров'ю. Наприклад , інформація про те, де востаннє бачили дитину, фотографії, ім'я дитини, та інформація, яка допоможе ідентифікувати викрадача. Отриману інформацію від Національної поліції команда Facebook оперативно включає у повідомлення AMBER Alert. Facebook, використовуючи свої дані, свою технологічну здатність і механізми, визначає пул користувачів, які, найімовірніше, бачили або мають якусь інформацію про цю дитину. Також передається локація, де це сталося, і зона пошуку, яка цікава Національній поліції. Важливе значення має те, що зазначена інформація поширюється не по всій території країни, а саме визначаються локальні місця, таке повідомлення побачать люди (оповіщення конкретним людям-користувачам), які перебувають у зоні пошуку, де в останнє бачили дитину. У такий спосіб зібрати потрібну інформацію, яка допоможе знайти дитину, вдається за найкоротший час. Окрім того, Facebook має достатньо даних, щоб ефективно показувати повідомлення людям, у яких висока ймовірність, що вони щось знають про цей випадок. У зазначених повідомленнях будуть дані, куди потрібно звернутися. Наприклад, це може бути локальний офіс (територіальне віддлення поліції) підрозділу Національної поліції. В процесі пошуку дитини користувачі Facebook можуть робити у себе репости про зниклу дитину. Саме вони залишаються на сторінках. Після того, як дитину знайдуть, оповіщення про нього AMBER Alert в Facebook припиняють діяти. Треба зазначити, що загрози поширення неправдивих повідомлень про зниклих дітей виключена. Окрім того, підробити повідомлення, які були б схожі на AMBER Alert, практично неможливо [4].

Зазанчимо, що AMBER Alert є офіційною зворотною абревіатурою назви системи для America's Missing: Broadcast Emergency Response. Так вона була названа на честь 9-річної Ембер Хагерман (Amber Hagerman), яка була викрадена і вбита в Арлінгтоні, Техас у 1996 році. Колись використовувалися регіональні альтернативні назви сповіщень в деяких штатах: Levi's Call в Джорджії (на згадку про Леві Фреді (Levi Frady)), Maile Amber Alert на Гавайях (на згадку про Майлі Гілберт (Maile Gilbert)), Morgan Nick Amber Alert в Арканзасі (на згадку про Морган Нік (Morgan Nick)) і « Rachael Alert »в Юті (на згадку про Рейчел Райан (Rachael Runyan)). У США поширення сигналів AMBER Alert проводиться за допомогою комерційних радіостанцій, інтернет-радіо, супутникового радіо, телевізійних станцій, а також за допомогою систем кабельного телебачення за допомогою Системи

екстреного оповіщення і радіо Національного управління океанічних і атмосферних досліджень. Сповіщення також поширюються за допомогою електронної пошти, електронних дорожніх табло, електронних комерційних рекламних щитів і SMS-повідомлень. AMBER Alert так само об'єдналися з компаніями Google, Bing і Facebook для донесення інформації постійно зростаючому населенню: оповіщення AMBER Alert автоматично відображаються, якщо громадяни використовують пошук або функції карти в Google або Bing. За допомогою Google Child Alert (так само відому як Google Amber Alert в деяких країнах) люди бачать оповіщення Amber Alert, якщо шукають пов'язану інформацію в певних місцях розташування, де недавно була викрадена дитина, й ухвалено рішення про трансляцію оповіщення Amber Alert. Цей компонент системи AMBER Alert вже використовується в США (також ведуться розробки в Європі). Всі зацікавлені в отриманні SMS розсилки з оповіщенням AMBER Alert в їх окрузі можуть підписатися на неї, відвідавши сайт Wireless Amber Alerts, який безкоштовний відповідно до закону. У деяких штатах для показу сповіщень також використовуються табло лотерейних автоматів. Рішення щодо оголошення тривоги AMBER Alert ухвалюється будь-якою поліцейською структурою (переважно це поліція штату або дорожня поліція), яка розслідує будь-яке з викрадень. Публічна інформація AMBER Alert зазвичай становить ім'я, опис викраденого, опис підозрюваного у викраденні, а також опис і номерні знаки автомобіля викрадача, якщо такі є [5]. Повні або часткові аналоги системи були введені в деяких країнах. AMBER Alert діяла в 24 країнах світу. Україна стала двадцять п'ятою країною, яка частково використовує аналоги AMBER Alert за допомогою соціальної мережі «Facebook». Проте залишається проблема, яка полягає в тому, що зазначена інформація поширюється тільки серед користувачів Facebook. Facebook досі залишається соціальною мережею номер один у більшості областей нашої країни. Треба зазначити, що з початку 2021 року кількість користувачів Facebook скоротилася у всіх обласних центрах України. Про це йдеться в дослідженні соцмереж за перше півріччя 2021 року, проведеного комунікаційним агентством plusone social impact. Тобто зазначена інформація охоплює обмежене коло осіб, що негативно впливає на оперативний обмін інформацією. Facebook втратив аудиторію в усіх обласних центрах: найменше – в Києві (-3,17 %), найбільше – в Черкасах (-25,22 %). Проте в невеликих містах соцмережа продемонструвала невелике зростання – приблизно 2 %. Тільки в Дніпропетровській області падіння аудиторії становило 6 %. Загалом серед українців 18–35 років 80 % використовують Instagram, а 60 % – Facebook. Майже у всіх вікових групах за останні півроку Instagram збільшив кількість користувачів і за цим показником обійшов Facebook. Найбільше падіння в обох соціальних мережах спостерігається тільки серед 20-річних. Facebook випереджає Instagram за приростом старшої аудиторії (51–53, 55 і 58+ років) [6].

Отже, на підставі вищезначеного впровадження AMBER Alert за допомогою соціальної мережі Facebook в Україні має важливе значення для оперативного обміну інформацією та знаходження зниклої дитини. Важливим у цьому контексті є роль ЗМІ, які повинні здійснювати інформаційно-розяснювальну роботу серед населення. Проте для широкого охоплення аудиторії необхідно скористатися досвідом США й інших країн та розробити дієвий механізм сповіщення населення за допомогою інших інструментів.

Бібліографчні посилання

1. Клименко Ігор. Сервіс Amber Alert вже в Україні. URL: https://www.facebook.com/iklymenko.fb/posts/276996771095302
2. В фейсбуке украинцы помогают полиции искать детей: как работает AMBER Alert. URL: https://24tv.ua/ru/fejsbuke-ukraincy-pomogajut-policii-iskat-detej-rabotaet-amber_n1767076
3. AMBER Alert в Украине – как работает поиск похищенных детей. URL: https://biz.nv.ua › tech › amber-alert-v-ukraine-kak-rab.
4. Facebook и Нацполиция запускают систему оповещения о пропавших детях AMBER Alert. URL: https://ain.ua/2021/09/22/facebook-zapustil-opoveshheniya-o-propavshih-detyah/
5. AMBER Alert. URL: https://amberalert.ojp.gov/; First child saved by Amber Alert headed to college URL: https://www.ajc.com/news/national/first-child-saved-amber-alert-headed-college/gT6iGpYmeKvTHzPH8QaIkN/; Do Amber Alerts Put Drivers in Jeopardy? URL: https://www.latimes.com/archives/la-xpm-2002-oct-15-me-wheel15-story.html
6. Битва соцсетей, фоточки побеждают. Facebook теряет аудиторию в больших городах Украины. URL: https://biz.nv.ua/tech/facebook-protiv-instagram-kakaya-socset-populyarnee-v-ukraine-svezhie-dannye-infografika-50173080.html

Самойленко О. А.,
головний науковий співробітник,
доктор юридичних наук, доцент

Тітуніна К. В.,
головний науковий співробітник
відділу дослідження проблем
протидії кіберзлочинам та загрозам
інформаційній безпеці Міжвідомчого
науково-дослідного центру
з проблем боротьби з організованою
злочинністю при РНБО України,
кандидат юридичних наук

ДО ПИТАННЯ УЗАГАЛЬНЕННЯ СТАТИСТИЧНОЇ ІНФОРМАЦІЇ З МЕТОЮ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

Сьогодні офіційні статистичні відомості про кіберзлочини найбільш повно відображаються у звітності Національної поліції України, зокрема у Звіті про результати роботи підрозділів Національної поліції України, де,

крім кримінальних правопорушень, охоплених розд. XVI КК України, зазначається ще низка кримінальних правопорушень, що вчинені з використанням електронно-обчислювальної техніки, передбачених ст. 176, 185, 190 (ч. 3 і 4), 200, 229, 231, 301 (ч. 3, 4 і 5) КК України [1].

Цей перелік статей складно назвати повним щодо облікованої категорії злочинів, адже по-суті це тільки так звані «конвенційні злочини», тобто такі, що визнані кіберзлочинами у значенні Конвенції Ради Європи про кіберзлочинність. Диспозиція окремих статей КК України дозволяє виокремити й інші альтернативні Конвенції склади кіберзлочинів, як-от: порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163); розголошення комерційної або банківської таємниці (ст. 232); незаконне втручання в роботу автоматизованої системи документообігу суду (ст. 376) та багато інших злочинів, що можуть бути вчинені у сфері кіберпростору. Тож, зважаючи на вказану обставину, а також на високий рівень латентності кіберзлочинності загалом, наголосимо на проблемі наявності для цілей криміналістичного аналізу повної та достовірної інформації про стан та структуру кіберзлочинності.

Проте, аналізуючи наявні повні річні звіти за останні три роки (2018–2020 рр.), можна зробити окремі висновки щодо динаміки цього виду злочинності та її структури, що дозволять протидіяти кібрзлочинам та зрозуміти стан ситуації у цій сфері діяльності правоохоронних органів.

По-перше, питома вага обліковуваних Національною поліцією України кіберзлочинів порівняно із загально кримінальною злочинністю є невеликою, але прослідковується тенденція до її збільшення. Зокрема, в 2020 р. у провадженні органів НП України обліковано 23242 кримінальні правопорушення, що вчинені з використанням високих інформаційних технологій, для порівняння у 2018 р. – 22262 правопорушення. Це усього 0,5 % від усіх облікованих кримінальних правопорушень у 2018 р. та вже 1,5 % – у 2020 р.

По-друге, спостерігається неоднакова динаміка розвитку різних видів кіберзлочинів. У 2020 р. порівняно з 2018 р. кількість кримінальних правопорушень, зареєстрованих у звітному періоді, передбачених статтями лише розд. XVI КК України, збільшилась на 4 % (у 2020 р. – 2455, у 2018 р. – 2359); передбачених ст. 176, зменшилась на 13 % (у 2020 – 5240; у 2018 – 6001); передбачених ст. 185, зменшилась на 23 % (у 2020 – 45, у 2018 – 59); передбачених ст. 190 ч. 3, 4, зменшилась на 15 % (у 2018 – 1598, у 2020 – 1355); передбачених ст. 200 КК, збільшилась на 30 % (у 2018 – 364, у 2020 – 535); передбачених ст. 229, зменшилась на 16 % (у 2018 – 24, у 2020 – 20); передбачених ст. 301 ч. 3,4,5 зменшилась на 58 % (у 2018 – 597, у 2020 – 249). При цьому кількість осіб, яким повідомлено про підозру у вчиненні кримінальних правопорушень у сфері високих інформаційних технологій, загалом залишається стабільною (1606 у 2018 р. проти 1562 у 2020 р.),

аналогічно стабільним залишається показник щодо кількості осіб, яким пред'явлено обвинувальні акти (2018 р. – 1332; 2019 р. – 1062; 2020 р. – 1268).

По-третє, на 14 % зменшується кількість кримінальних правопорушень, за якими досудове розслідування закінчено. Якщо в 2018 р. таких проваджень було 8172, в 2019 р. – 6212, то в 2020 р. – 6956. Відносно стабільним залишається показник щодо кількості кримінальних проваджень, за якими на кінець звітного року розслідування не закінчено: в 2018 р. – 12070, в 2019 р. – 12174, в 2020 р. – 12666. Найбільшу частку правопорушень у зазначеній категорії становлять кримінальні правопорушення, передбачені ст. 176 КК України (за 2020 р. – це 50 %), ст. 190 ч. 3, 4 (за 2020 р. – 20 %), ст. 361 (за 2020 р. – 12 %).

По-четверте, не можна опускати такий показник якості розслідування, як встановлена сума матеріального збитку від злочину, що за три роки збільшився майже на 83 % (вимірюється у тис. грн): в 2018 р. – 77426; в 2019 р. – 96886, в 2020 р. – 483162.

По-п'яте, показники ефективності діяльності Департаменту кіберполіції Національної поліції України свідчать про значне збільшення навантаження на підрозділи кіберполіції. Зокрема, за 12 місяців 2018 р. безпосередньо підрозділами Департаменту розкрито 2674 кримінальні правопорушення та за їх участі – 2188; порівняно за 12 місяців 2020 р. безпосередньо підрозділами Департаменту розкрито 2572 кримінальні правопорушення та за їх участі – 3232.

На підставі наведених вище позицій можна констатувати, що збір, оброблення, узагальнення та аналіз інформації з метою протидії кіберзлочинності повинні відбуватися не тільки за умови дотримання високого рівня звітно-реєстраційної дисципліни, а також адекватного відображення структури кіберзлочинності. Систематизоване доведення до відома практичних працівників правоохоронних органів цих відомостей дозволить якісно та методично обґрунтовано ставитися останнім до процесу виявлення кіберзлочину, висування версій, організації та планування досудового розслідування.

Бібліографічні посилання

1. Офіційний матеріал звітності Департаменту організаційно-аналітичного забезпечення Національної поліції України.

Санакоєв Д. Б.,
завідувач кафедри фінансових
та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

СУЧАСНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ ПОЛІЦІЇ: СВІТОВИЙ ДОСВІД ТА ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ У ПРОТИДІЇ ОРГАНІЗОВАНИМ ФОРМАМ ЗЛОЧИННОСТІ

Використання новітніх інформаційних та комунікаційних технологій організованими злочинними групами, терористичними організаціями чи окремими злочинцями є головною проблемою для держав загалом та правоохоронних органів зокрема через складність явища, кількість задіяних факторів та учасників, а також значну сукупність злочинних технологічних засобів, що використовуються для фінансування та підтримки злочинних і терористичних дій.

Використання сучасних технологій цими угрупованнями зміцнює їхні можливості для підтримки своєї діяльності (фінансування, відмивання грошей, вербування, планування терористичних атак, шахрайство з використанням особистих даних) та анонімного вчинення злочинів. Ці злочинні групи та організації часто знаходяться в авангарді технологічних інновацій для планування, вчинення та приховування своєї злочинної діяльності та доходів від неї.

Які з найбільш ефективних інструментів вже використовують правоохоронці у світі для забезпечення публічної безпеки та які перспективи подальшого впровадження технічних пристроїв у діяльності поліції?

Виконаний нами аналіз фахових джерел з цього питання дозволив виокремити ***світові тенденції, що становлять підґрунтя сучасної поліцейської діяльності***, спрощують можливості забезпечення публічної безпеки і порядку, вивільняють ресурси, забезпечуючи проактивну роботу поліції та надають її діяльності більшої прозорості:

1. Соціальні мережі. Сьогодні активно й ефективно використовуються поліцією для збирання та поширення інформації, залучення спільнот. Зі зростанням потреби у прозорості соціальні мережі стали одним із найкращих способів зв’язку з широкою публікою. Платформи соціальних мереж, як-от: Facebook, Twitter, Reddit дозволяють отримувати оновлення у режимі реального часу. Крім того, створення широкої мережі в соціальних мережах може допомогти розкрити злочини, оскільки поліція може ділитися інформацією з ширшою аудиторією.

2. BodyCam, що забезпечують більшу прозорість та зменшують

кількість скарг, пов'язаних із застосуванням сили. Проте такі питання, як вартість, конфіденційність, зберігання даних, публічне розкриття та загальна ефективність, продовжують залишатися предметом дискусій.

3. Програмне забезпечення для розпізнавання обличчя (наприклад, NGI, Rekognition та NeoFace Reveal від NEC, FaceFirst) ідеально підходить для віддаленого спостереження, оскільки його точність і складність зростають. Однак були деякі розбіжності щодо розпізнавання осіб та потенційних расових упереджень [1]. Внаслідок цих проблем закони про біометричну конфіденційність стануть актуальною темою, оскільки цей тип технологій стає дедалі популярнішим.

4. Алгоритми прогнозування у поліцейській діяльності. Штучний інтелект (далі – ШІ) пропонує фундаментальний прорив у роботі поліції, переходячи від реактивного до проактивного (попереджувального) контролю. Це стало можливим завдяки розширеній аналітиці та моделям втручання, які, по суті, можуть «прогнозувати» злочинність – системи ШІ можуть проактивно сканувати масиви інформації, щоб забезпечити точне прогнозування злочинності за допомогою прогнозної аналітики, яка може допомогти поліції активно координувати свої дії на стадії до вчинення злочину.

5. Додатки GPS. Використовуються правоохоронними органами для швидшого відстеження та визначення місцезнаходження підозрюваних та умовно-достроково звільнених. Кулі GPS, наприклад, можуть бути випущені в транспортний засіб, щоб дистанційно відстежувати його рухи, а пристрої GPS-стеження можуть використовуватися для рецидивних правопорушень для відстеження їхнього розташування [2].

Водночас GPS дозволяє краще координувати та відстежувати місцезнаходження (у т.ч. фізіологічний стан) офіцерів та транспортних засобів. Це може допомогти ефективніше реагувати на інциденти, а також дозволяє отримувати більш точну інформацію про місцезнаходження для координації викликів та безпечніше і швидше скеровувати працівників поліції до цих інцидентів.

6. Використання **робототехніки** у роботі поліції продовжує розширюватися [3]. Наприклад, маленькі роботи у формі танків, оснащені датчиками, використовуються для проникнення у місця, куди небезпечно входити поліцейському, а потім надсилають аудіо- і відеопотік групі затримання, що відповідає за проведення заходу (операції). Дедалі досконаліші роботи зі знешкодження вибухових пристроїв також допомагають правоохоронцям, виконуючи небезпечні завдання, пов'язані з вибуховими речовинами.

7. Дрони. Допомагають у спостереженні, оскільки поліцейські підрозділи знаходять нові застосування для безпілотних літальних апаратів (БПЛА), оснащених оптичними, зумуючими та/або тепловізійними камерами [4]. Наприклад: пошукові та рятувальні операції, затримання зі стрілянинӧю, перестрілка між злочинцями, дорожньо-транспортні пригоди, огляд місця

події, візуальне спостереження та моніторинг натовпу.

8. Поліцейська діяльність, керована аналітикою [5], поєднує вирішення проблем, спостереження, обмін інформацією та підзвітність поліції з поліпшеними розвідувальними операціями та даними для інформування поліцейських зусиль, спрямованих на найбільш ймовірні сценарії та ситуації.

9. Система ShotSpotter, що впроваджується в США, яка використовує датчики для виявлення пострілів та залучає аналітиків для відстеження даних та миттєвої передачі їх у поліцію, що дозволяє їм прибути на місце події швидше, ніж будь-коли раніше [6].

10. Хмарні застосунки. Перехід до операцій із забезпечення безпеки у хмарному середовищі набув значного поширення: зокрема, Пентагон поставив 10 мільярдів доларів на свій гучний контракт на хмарну інфраструктуру спільного захисту підприємства (JEDI) [7]. У діяльності підрозділів поліції та ФБР США активно використовуються програмні продукти ApprissSafety та Fusus у так званих хмарних середовищах Центрів контролю злочинності в реальному часі у хмарах (RTC^3 – Real-Time Crime Center in the Cloud). Наприклад, технологія Fusus дозволяє будь-якому виду пристрою (БПЛА, камери контролю дорожнього руху, телефони або інші види пристроїв Інтернету речей та пристроїв, орієнтованих на публічну безпеку), перехоплювати і передавати дані про події в режимі реального часу. Інтегруючи всю цю інфраструктуру безпеки в безпечну хмару, Fusus змогла зробити RTC^3 доступним для більшості підрозділів, які можуть отримати доступ до цієї інформації з метою забезпечення публічної безпеки [8].

11. Програмне забезпечення для керування розслідуванням, кадрами (наприклад, Case Jacket, Forensics Capture, HooYu Investigate, Omnigo, Cerebral, SceneDoc, HR Acuity, програмні продукти InTime тощо). Дедалі очевиднішим є той факт, що використання електронної таблиці або олівця більше не допоможе. Це може призвести до негативних наслідків для підрозділів, зокрема високих понаднормових витрат, підвищеного ризику, високої плинності кадрів через низький моральний дух персоналу та неефективність. Крім того, ризик неукомплектованості або укомплектування співробітниками без достатньої мотивації може завдати шкоди безпеці працівників та громадськості. Забезпечити управління ризиками та економити на витратах агентств дозволяє впровадження спеціалізованого програмного забезпечення [9].

12. Використання негласних джерел та легендованих підприємств. Ми не випадково розмістили цей напрям діяльності поліції у нашому переліку останнім, оскільки переконані – людський фактор у поєднанні з негласними формами та методами роботи у протидії злочинності та, передусім, її організованим проявам, дозволить підняти ефективність такої протидії на якісно вищий рівень.

Яскравим прикладом вважаємо спеціальну операцію OTF Greenlight /

Trojan Shield (Зелене світло / Троянський щит), що проводилась з 2019 року Федеральним бюро розслідувань США (ФБР), Національною поліцією Нідерландів (Politie) та Управлінням поліції Швеції (Polisen) у співпраці з Управлінням боротьби з наркотиками США (DEA) та 16 іншими країнами за підтримки Європолу [10].

Сутність довготривалої операції полягала в тому, що ФБР у тісній співпраці з Федеральною поліцією Австралії стратегічно розробило та таємно керувало компанією з виробництва зашифрованих пристроїв під назвою ANOM, яка розвинулась та обслуговувала понад 12 000 зашифрованих пристроїв більше ніж 300 злочинних синдикатів у понад 100 країн, включно з італійською організованою злочинністю, злочинні банди мотоциклістів та міжнародні організації, що займаються незаконним обігом наркотиків.

Мета нової платформи полягала в тому, щоб спрямовуватись на глобальні організації, що займаються організованою злочинністю, незаконним обігом наркотиків та відмиванням коштів незалежно від того, де вони розташовані, і переконати злочинні організації звернутися до цього зашифрованого пристрою із функціями, що зацікавлять мережі організованої злочинності, такими як, наприклад, віддалене стирання та примусове видалення паролів.

ФБР та 16 інших країн міжнародної коаліції за підтримки Європолу та в координації з Управлінням боротьби з наркотиками США потім використали розвіддані з 27 мільйонів отриманих повідомлень і переглянули їх протягом 18 місяців, тоді як злочинці-користувачі ANOM обговорювали свою злочинну діяльність.

Протягом червня 2021 року було проведено понад 700 обшуків будинків, здійснено понад 800 арештів та вилучено понад 8 тонн кокаїну, 22 тонни канабісу та смоли канабісу, 2 тонни синтетичних наркотиків (амфетамін та метамфетамін), 6 тонн прекурсорів синтетичних наркотиків, 250 одиниць вогнепальної зброї, 55 автомобілів еліт-класу та понад 48 млн доларів США у різних валютах та криптовалютах. Ця операція дозволить Європолу ще більше поліпшити розвідувальну картину про організовану злочинність, що впливає на ЄС, завдяки якості інформації, що збирається. Ця поліпшена розвідувальна картина підтримуватиме постійні зусилля щодо виявлення чинних важливих злочинних цілей у глобальному масштабі.

Отже, виконаний нами аналіз сучасних інноваційних інформаційно-комунікаційних технологій, що використовуються повністю або частково правоохоронними органами розвинених країн світу (передусім США та Європи), свідчить про тенденцію до їх швидкого розвитку й постійного удосконалення. Зважаючи на сучасний стан розвитку та впровадження інноваційних технологій в діяльність підрозділів правоохоронних органів, зокрема й щодо протидії організованим формам злочинності, перспективними для України вважаємо такі напрями:

1) *розширення можливостей впровадження поліцейської діяльності,*

керованої аналітикою (Intelligence-Led Policing). Вбачаємо можливості реалізації цього напряму в контексті створення Центрів контролю злочинності в реальному часі у хмарних середовищах;

2) *оптимізація поліцейських технологій у хмарних середовищах*. Хмарні рішення не лише надзвичайно дешеві, порівняно зі старими локальними рішеннями, вони також пропонують можливість дефрагментувати свою технологічну інфраструктуру та оптимізувати свої операції. З огляду на те, що хмарні системи сьогодні мають переваги над локальними у сенсі захищеності та більш низькі показники втручань, згідно з політикою безпеки даних CJIS, ймовірне їх впровадження найближчим часом [11];

3) *використання можливостей БПЛА*, зокрема й у протидії організованим проявам злочинності (огляд місця події; огляд закритих об'єктів і територій; аеророзвідка; візуальне спостереження за особою, місцем або річчю; контроль за діяльністю ОГ у місцях позбавлення волі, контроль натовпу тощо);

4) *впровадження систем організації роботи підрозділу.* Стратегічними пріоритетними напрямами можуть стати скорочення кількості випадків із застосуванням сили, виявлення додаткових потреб у навчанні всередині підрозділів, тактика зниження шкоди, що підвищує безпеку співробітників та громад, а також стійке планування нагляду та підзвітності, що зміцнює зв'язки між поліцією та громадянським суспільством;

5) *впровадження у освітній процес* підготовки та підвищення кваліфікації поліцейських *систем і технологій VR*, що дозволить майбутнім та наявним працівникам поліції навчитись керувати кризовими ситуаціями та знижувати ескалацію небезпечних. Хоча може бути складно відтворити ці важливі ситуації у реальному житті, VR уможливлює відтворення будь-якого сценарію (наприклад, продукція компаній WRAP Reality, ApexOfficer, Axon, InVeris, та ін.), розробляючи та використовуючи під час підготовки поліцейських тренінги VR, що фокусуються на навчанні скорочення застосування сили тощо.

Бібліографічні посилання

7. https://www.brookings.edu/blog/techtank/2021/05/26/mandating-fairness-and-accuracy-assessments-for-law-enforcement-facial-recognition-systems/
8. https://www.starchase.com/
9. https://www.roboticstomorrow.com/story/2020/07/security-never-sleeps-robotics-in-law-enforcement/15449/
10. https://www.thedrive.com/article/15092/drones-in-law-enforcement-how-where-and-when-theyre-used
11. https://www.policechiefmagazine.org/changing-the-face-crime-prevention/
12. https://www.forbes.com/sites/elizabethmacbride/2018/10/30/the-scientist-the-investor-and-the-ceo-how-shotspotter-turned-a-profit-after-22-years/?sh=564739b0468c
13. https://www.businessinsider.com/jedi-jwcc-cloud-contract-legacy-pushing-multi-cloud-future-2021-8

14. https://www.fusus.com/rtc3-products/fusus-real-time-crime-center-in-the-cloud
15. https://www.capterra.com/investigation-management-software/s/free/
16. https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication
17. https://www.fusus.com/blog/infographic-why-cloud-based-solutions-are-the-future-of-law-enforcement

Сарахман О. М.,
доцент кафедри облікових
технологій та оподаткування,
кандидат економічних наук, доцент
Сідельник О. П.,
доцент кафедри фінансового
консалтингу та банківництва,
кандидат економічних наук, доцент
(Університет банківської справи)

ВПЛИВ ДІДЖИТАЛІЗАЦІЇ НА ОПЕРАЦІЙНІ РИЗИКИ БАНКІВ

З початку пандемії Covid-19 більшість банків України адаптувалися до віддаленого режиму роботи і обслуговування клієнтів у нових реаліях. Затрати на побудову нової сервісної моделі не закладалися повною мірою у бюджет витрат банків і стали відображенням збитків від однієї загальної події операційного ризику під назвою – Covid-19. Одним із фундаментальних елементів формування сучасної інформаційної економіки є цифрові платформи, які базуються на розвиненій IT- інфраструктурі [1].

Діджиталізація банківського сектора – довгостроковий процес, що має ознаки глобальної тенденції і позначається на розвитку банків у низці країн. Український банківський сектор активно долучається до цього процесу, намагаючись у такий спосіб утримувати клієнтів і підвищувати рівень своєї конкурентоспроможності на ринку фінансових послуг [2].

Зі свого боку, банки можуть оптимізовувати свої процеси, скорочувати бюрократичні процедури, впроваджувати сучасні послуги, підвищувати конкурентоспроможність. Важливою під час пандемії також є мінімізація соціальних контактів, яку забезпечує впровадження онлайн-послуг.

У банківській сфері ризик є цілком нормальним явищем, оскільки з метою отримання істотного прибутку необхідно ризикувати [3, 149–150].

Операційні ризики за типом наслідків і частотою прояву можна поділити на чотири категорії подій: що виникають із малою частотою і спричиняють невеликі збитки; що виникають часто та спричиняють невеликі

збитки; що характеризуються суттєвими збитками, але трапляються з малою ймовірністю; події, що трапляються часто і призводять до великих збитків.

Управління операційним ризиком має на меті мінімізацію ефекту від настання подій операційного ризику шляхом застосування належних заходів реагування, мінімізацію ймовірності виникнення подій операційного ризику шляхом запровадження системи внутрішніх контролів, передачу ризику через інструменти страхування і процеси аутсорсингу.

Національний банк України вже затвердив порядок визначення банками мінімального розміру операційного ризику та врахування його під час розрахунку нормативів достатності капіталу. Результати проведених банками тестових розрахунків свідчать, що врахування операційного ризику призведе до зростання ризикозважених активів на 25 %, що є співставним із даними інших країн [4].

В основі системи внутрішніх контролів банку лежить розподіл функцій підрозділів на першу лінію захисту, до якої належать всі бізнес-підрозділи та підрозділи підтримки, другу лінію захисту, тобто контролю, яку становлять підрозділи з управління ризиками та підрозділ комплаєнс, та третю лінію – внутрішній аудит.

Фокус системи внутрішніх контролів банку і розподіл ресурсів визначається, насамперед, процесом регулярного збору інформації щодо подій операційного ризику, аналізом причинно-наслідкових залежностей і запровадженням змін до продуктів та процесів установи для мінімізації ймовірності виникнення і масштабу втрат у майбутньому.

Проведений аналіз враховується під час встановлення показників толерантності до втрат у результаті реалізації подій операційного ризику, а саме під час розрахунку максимального розміру втрат, який приймається банком у межах функціонування ефективної системи внутрішніх контролів, за якої недотриманий дохід або операційні витрати на подальшу мінімізацію ризику будуть вищими, ніж розмір зменшення ризику. Іншими інструментами управління операційними ризиками є основні індикатори ризику і стрес-сценарії.

З іншого боку, стрес-тестування подій операційного ризику використовує накопичений досвід і процес моделювання для оцінки ймовірного впливу під час настання несприятливих сценаріїв, які відбуваються нечасто, проте ефект від настання яких дуже великий. Щорічно, відповідно до розширеного підходу вимірювання, банк розраховує розмір капіталу, необхідний для покриття втрат від настання подій операційного ризику [5].

Отже, останні тенденції формування банківських послуг та платежів і розвиток діджиталізації впливають на механізм управління банківськими процесами та ризиками. Операційний ризик має увійти до складу мінімальних вимог до капіталу банків, щоб убезпечити банки від можливих руйнівних наслідків несприятливих явищ у майбутньому.

Бібліографічні посилання

1. Заруцька О. П., Сосєдка О. В., Міняйло В. Ф. Сучасний стан електронного банкінгу та управління операційними ризиками. URL: http://scientificview.umsf.in.ua/archive/2020/1_67_2020/26.pdf
2. Холявко Н. І., Козлянченко О. М. Світові тенденції діджиталізації банківського сектора. URL: http://oaji.net/articles/2021/728-1628678985.pdf
3. Шурпенкова Р. К., Сарахман О. М. Управління кредитним ризиком банку: стратегічний аспект. *Стратегічний розвиток організації, міст та регіонів* : зб. матеріалів Міжнародної науково-практ. конф. (м. Ужгород, 26–27 жовтня 2017р.). Ужгород : Вид-во УжНУ «Говерла», 2017. С. 149–150.
4. НБУ запровадить нові вимоги до банків. URL: https://news.dtkt.ua/finance/bank-system/65386
5. Річний звіт за 2020 рік ОТП Банк. URL : https://ru.otpbank.com.ua/pdf/annual_reports/2021/otp-2020-22042021-final.pdf

Сеник В. В.,
завідувач кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат технічних наук, доцент

Кулешник Я. Ф.,
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, кандидат технічних наук, доцент

Ментинський С. М.,
старший викладач кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка»

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНОЛОГІЙ ЗАХИСТУ ХМАРНИХ СЕРВІСІВ

Упродовж тривалого часу нами проводились дослідження впливу пандемії, спричиненої вірусом COVID-19, на стан кіберзлочинності як в Україні,так і у світі. Окремі результати та висновки наведені у роботі [1].

Представленою публікацією ми прагнули доповнити уже опубліковані дослідження і зупинитися на питаннях забезпечення безпеки роботи з інформаційними ресурсами під час використання хмарних технологій.

Така необхідність виникла у зв'язку із тим, що пандемія COVID-19 поряд із іншими впливами на IT спонукала активізації перенесення інформаційних процесів у хмарне середовище. Звичайно, що активізації цих процесів сприяла не лише пандемія, а й розвиток IT-галузі. Такий стан призвів до того, що підприємства, установи та організацій отримали змогу знизити власні фінансові витрати на розвиток IT-інфраструктури, через використання потрібних IT-ресурсів хмарних сервісів. Крім цього такий вибір розглядається як ключовий перспективний, рентабельний та модернізаційний тренд, перехід на який забезпечує високу надійність, зручність у використанні, масштабованість і гнучкість, ніж розвиток власних робочих серверів. Згідно з даними Microsoft, у порівнянні з до карантинними показниками стався глобальний ріст кількості користувачів хмарних сервісів і за статистикою він склав 775% [2].

Поряд з цим, не зважаючи на усі переваги використання хмарних технологій, існують великі ризики з огляду кібернетичної безпеки. До таких ризиків, насамперед слід віднести: злом акаунтів, крадіжка та знищення інформації, проведення різного роду кібератак. Японська компанія Trend Micro, яка працює у сфері інформаційної безпеки, 8 грудня 2020 року опублікувала доповідь, у якій говориться, що віддалена робота стане одним з головних чинників зростання кіберзлочинності у 2021 році [3]. Основною причиною такого стану є те, що під час віддаленої роботи відбувається зв'язок домашніх комп'ютерів співробітників з корпоративною мережею. Як правило, корпоративні мережі у тій чи іншій мірі мають захист стосовно виявлення атак, а домашні комп'ютери часто такого захисту не мають. Таким чином, увійшовши до домашнього комп'ютера одного із співробітників зловмисники можуть отримати доступ до персональних комп'ютерів усієї установи через корпоративну мережу. На думку спеціалістів цієї ж компанії найближчим часом будуть виявлені нові уразливості програмного забезпечення та хмарних сервісів для віддаленої роботи, що пов'язано із збільшенням частки застосування таких технологій, а це неодмінно сприятиме активізації пошуку зловмисниками слабких місць у хмарних сервісах. Небезпекою стало також те, що зловмисники для здійснення зловживань стали використовувати технології штучного інтелекту під час підбору паролів, проведення автоматизованих атак на інформаційну систему, проведення аналізу великих масивів даних для отримання необхідної інформації.

При цьому за результатами опитування, проведеного KPMG і Harvey Nash серед IT-керівників країн Європи, Азії та США, лише п'ята частина компаній готова сьогодні протистояти кібератакам. Більшість керівників вважають вдосконалення систем кібербезпеки найвищим пріоритетом через

пікове збільшення рівня загрози з боку кіберзлочинності [4].

Чим же характерні кіберзлочини, які націлені на хмарні сервіси? Найчастіше атаки на хмарні сервіси зловмисниками проводять з локацій, які не визначалися попередньо як довірені і є аномальними для установ чи організацій. Після такого входу зловмисниками ініціюється доступ до тих чи інших даних, які в результаті опиняються у загальному доступі. Інший тип атак – це спроба входу до робочих акаунтів одночасно з різних географічних локацій, у тому числі з різних країн. Такі спроби в обов'язковому порядку слід відслідковувати та блокувати. І зрештою, зафіксовані випадки загрози безпеці внутрішніми порушниками, які полягають у витоку інформації, у випадку передавання користувачами документів через незахищені канали.

Підсумовуючи, можемо констатувати: у ситуації, яка нині склалася, пріоритетним стає не лише захист локальних інформаційних систем, а захист хмарних сервісів. Окрім розвитку технологій захисту хмарних сервісів, необхідно також проводити активні організаційні заходи із забезпечення безпеки інформаційних ресурсів, які передаються через різні канали зв'язку, посилити захист особистих комп'ютерів користувачів, які додаються до корпоративної мережі та розробити правила їх уведення у технологічні процеси. Через обмеженість публікації вважаємо у подальших дослідженнях розвинути дану тематику та дослідити нормативно-правову складову забезпечення захисту інформаційних ресурсів, які опрацьовуються засобами хмарних технологій.

Бібліографічні посилання

1. Шинкарук О. М., Сеник В. В., Зачек О. І., Магеровська Т. В. Стан та особливості протидії кіберзлочинності в Україні в умовах пандемії COVID-19. *Соціально-правові студії*. 2021. Вип. 3 (13). С. 68–76.
2. Дистанційна робота: складності і ризики для кібербезпеки. URL: https://softlist.ua/novyny/distantsijna-robota-skladnosti-i-riziki-dlya-kiberbezpeki
3. Надтока С. Ризики віддаленки. Головні кіберзагрози 2021 року. *Корреспондент.net*. 2020. URL: https://ua.korrespondent.net/business/web/4304611-ryzyky-viddalenky-holovni-kiberzahrozy-2021-roku
4. Три головні ризики від хмарних сервісів. Блог Максима Батуренко. URL: https://techno.nv.ua/ukr/technoblogs/tri-holovni-riziki-vid-khmarnikh-servisiv-bloh-maksima-baturenko-2477464.html

Синиціна Ю. П.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

АВТОМАТИЗОВАНІ ІНФОРМАЦІЙНІ СИСТЕМИ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

На сьогодні інформаційно-аналітичне забезпечення в діяльності Національної поліції України посідає дуже важливе місце, тому що саме такі засоби, як організаційні, правові та технологічні, забезпечують збирання, отримання, обробку інформації, які необхідні для виконання завдань в правоохоронній діяльності.

Прикладами ініціатив штучного інтелекту є [1]: штучний інтелект є правильним напрямком руху для водія за навігаційними картами; штучний інтелект є прийнятим рішенням щодо лікування захворювань онкології; штучний інтелект як система розпізнавання обличчя людини, мовних, текстових та відеоматеріалів; штучний інтелект є результатом розпізнавання тексту, прикладом якого є справи про банкрутство; виплати страхових відшкодувань; оскарження штрафів за паркування; штучний інтелект, як прояв у сфері музики, є емоційним навчанням роботів відчувати, розпізнавати та імітувати почуття.

Вагомі внески у досліджені фундаментальних теоретико-методологічних засад інформаціної безпеки в юридичній діяльності зробили І. В. Арістова, О. М. Бандурко, М. Я. Швець, В. С., Цимбалюк та інші. Однак за кожним стриманим кроком наукового пошуку відкриваються ще більші горизонти безмежного пізнання дійсності.

Співробітники поліції в процесі своєї роботи пов’язують її з внутрішнім законодавством та з самими організаціями. Також працівники Національної поліції під час діяльності складають бази даних оперативно-розшукового та оперативно-довідкового призначення. Ці бази даних містять у собі інформацію про реєстрацію всіх мешканців; кримінальні правопорушення в діях кримінальних правопорушників; конфіскування речей; господарів транспортних засобів; власників зброї, а також державну таємницю. Вся інформація потрібна для того, щоб робота підрозділів Національної поліції була успішною щодо боротьби з правопорушеннями.

До основних завдань правоохоронних органів щодо інформаційно-аналітичної діяльності можна віднести (рис. 1): утворення бази даних, які входять до системи Міністерства внутрішніх справ України; використання бази даних Міністерства внутрішніх справ України; виконання пошукової та аналітичної роботи; взаємодія з іншими різними органами державної влади.

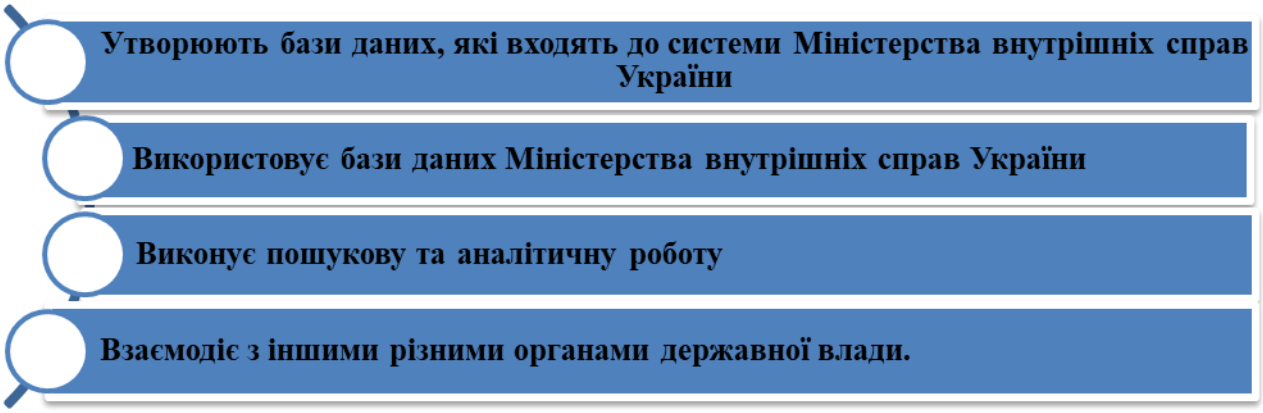


Рис. 1. Завдання правоохоронних органів
щодо інформаційно-аналітичної діяльності

Співробітники, які досягнули та використовують інформацію, мають зробити її організованою, бо потрібну інформацію чи якісні відомості знайти неможливо. Також є поняття Автоматизована інформаційна система, що означає організаційні системи, в яких обробка інформації використовує технічні і програмні методи.

Автоматизовані інформаційні системи в правоохоронній діяльності можна поділити на 6 систем (рис. 2): автоматизовані інформаційні системи, які пристосовані для збору і обробки інформації; автоматизовані інформаційні системи, які мають оперативні методи; автоматизовані інформаційні системи, які використовуються в слідчій системі; автоматизовані інформаційні системи, які мають криміналістичні нахили; автоматизовані інформаційні системи, які мають схильність до експертної діяльності; автоматизовані інформаційні системи управлінського методу.

Рис. 2. Класифікація АІС у правоохоронній діяльності

Підбиваючи підсумки, можна зазначити, що для виконання завданнь аналітичних підрозділів правоохоронних органів при здійсненні оперативно-розшукової діяльності необхідно розширювати використання інформаційних технологій в діяльності Національної поліції.

Бібліографічні посилання

1. Про затвердження Інструкції з організації функціонування Інтегрованої інформаційно-пошукової системи органів внутрішніх справ України : наказ МВС України від 10 березня 2010 року № 75.

2. Системна інформатизація законотворчої та правоохоронної діяльності : монографія / кер. авт. кол. М. Я. Швець; за ред. В. В. Дурдинця та ін. Київ : Навчальна книга, 2005. 639 с.

3. Хахановський В. Г., Підюков П. П., Смаглюк В. М. Інформатизація управління в органах внутрішніх справ : посібник. Київ : НАВСУ, 2003. 216 с.

4. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. *Відомості Верховної Ради*. 2015. № 40–41. Ст. 379.

5. Варенко В. М. Інформаційно-аналітична діяльність : навч. посіб. Київ : Університет «Україна», 2014. 417 с.

6. Радутний О. Е. Штучний інтелект, інформаційна безпека та законотворчий процес (кримінально-правовий аспект). *Інформація і право*. 2018. № 1(24). С. 149–158.

Станіна О. Д.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук

ПРО ВПЛИВ ПАНДЕМІЇ COVID-19 НА ЗМІНУ СТРУКТУРИ ЗЛОЧИННОСТІ В УКРАЇНІ ТА СВІТІ

В кінці 2019 року в китайському місті Ухань виникла нова хвороба – COVID-19, яка, як відомо, стала причиною подальшої глобальної пандемії, що поширилась на весь світ. Вже в березні 2020 року більшість країн світу були змушені ввести локальні, регіональні і, навіть, загальнонаціональні локдауни для забезпечення зниження темпів поширення коронавірусної хвороби. Такі дії мали позитивний ефект з погляду поширення вірусу та захисту життя людей [1], але в подальшому став все ясніше проявлятися негативний вплив соціального дистанціювання.

Як показав 2020 рік, введення локдауну досить суттєво вплинуло на різноманітні соціальні явища. Зміна звичного життя також відобразилася і на структурі злочинності як в Україні зокрема, так і у всьому світі загалом. Вулична злочинність та організована злочинність в умовах карантинних обмежень знижується, адже крадіжка відбувається з меншою вірогідністю за

умови різкого зниження кількості людей, які знаходяться на вулиці; інакше кажучи, неможливо пограбувати магазин, який постійно зачинено. Проте, як показує ціла низка досліджень, наприклад, соціальне дистанціювання призводить до підвищення рівня домашнього насильства [2].

Порівнюючи рівень злочинності у доковідному вересні 2019 р., під час локдауну 2020 р. та адаптивного карантину 2021 р. – на основі єдиного звіту про кримінальні правопорушення у Дніпропетровській області [3] – можна зробити припущення, що з введенням повного та адаптивного карантину в країні знизилася кількість кримінальних правопорушень, злочинів проти життя та здоров'я людини, але при цьому відслідковується тенденція підвищення кількості злочинів, пов'язаних з домашнім насильством. Зокрема, у 2019 році відбулося 35505 кримінальних правопорушень, з них: 2752 злочини – проти життя та здоров'я особи, 21714 – проти власності, 134 – пов'язані з насильством у сім'ї. У 2020 р. зафіксовано 27261 кримінальне правопорушення, з них: 2247 – проти життя та здоров'я особи, 11685 – проти власності, 236 – пов'язані з насильством у сім'ї. У 2021 р. відбулося 22339 кримінальних правопорушень, з них: 1869 – проти життя та здоров'я особи, 11893 – проти власності та 208 – пов'язані з насильством у сім'ї.

Згідно з наведеними даними єдиного звіту, видно, що у 2020 та 2021 рр. порівняно з доковідним 2019 р. загальна кількість правопорушень зменшилася на 23 % та 37 % відповідно; кількість злочинів проти власності зменшилася на 45 % та 46 % відповідно; тоді як рівень домашнього насильства виріс на 76 % та 55 % відповідно.

Зрозуміло, що подана статистика за три наведені роки не достатньою мірою є репрезентативною, але на її основі вже можна зробити припущення щодо зміни структури злочинності в Україні в бік зменшення кількості «вуличних» та збільшення «домашніх» правопорушень через зростання факторів, які спричиняють саме побутові конфлікти в місцях самоізоляції та відбування карантину.

Однак не треба забувати про інші фактори, що впливають на отримані результати. Наприклад, за останній рік, згідно з даними міжнародного проекту Numbeo, в Україні знизилася якість життя, що безумовно в подальшому буде мати негативний вплив на структуру злочинності в плані підвищення рівня злочинів проти власності.

До того ж варто взяти до уваги, з одного боку, можливе зниження звернень до правоохоронних органів через те, що люди уникають можливості проводити час поза своїм домом, а отже, можуть відкладати похід до поліцейського відділу чи взагалі відмовитися від ідеї звернутися до поліції. З іншого ж боку, маємо відмову у повідомленні про домашнє насильство через неможливість це зробити за допомогою телефону при постійній присутності правопорушника в одному житловому просторі з жертвою.

Зважаючи на вищезазначену інформацію, можна підбити деякі підсумки. Спиратися на одну тільки статистику в питаннях, що стосуються

життя та здоров'я людини, є не досить правильним рішенням, але її аналіз та правильна інтерпретація дозволяє прогнозувати важливі зміни у житті населення, що допомагає запобігти негативним чинникам та підсилити сприятливі фактори. Як показують дані за останні два роки, безумовно, соціальна ізоляція та дистанціювання мають вплив на всі рівні життя сучасної людини, що безпосередньо відображається у структурі злочинності. Зниження загального рівня правопорушень, імовірніше, не протримається досить довго, і, як показують дослідження аналогічних явищ в інших країнах, ймовірно, в подальшому ми станемо свідками зміни не кількісних показників, а якісних, а саме структури злочинності та ролі окремих її видів.

Бібліографічні посилання

1. Flaxman, S., Mishra, S., Gandy, A., Unwin, H. J. T., Mellan, T. A., Coupland, H., et al., (2020). Estimating the effects of non-pharmaceutical interventions on COVID-19 in Europe. Nature, 584 (7820), 257–261. URL: https://doi.org/10.1038/s41586-020-2405-7
2. Piquero, A. R., Riddell, J. R., Bishopp, S. A., Narvey, C., Reid, J. A., & Piquero, N. L. (2020). Staying home, staying safe? A Short-term analysis of COVID-19 on Dallas domestic violence. American Journal of Criminal Justice, 45(4), 601–635. URL: https://doi.org/10.1007/s12103-020-09531-7.
3. Єдиний звіт про кримінальні правопорушення : звітність Генеральної прокуратури України. Форма № 1 (місячна). URL: https://dnipr.gp.gov.ua/ua/documents.html?dir_id=111414

Сулейменов А. Д.,
старший преподаватель-методист
Центра по подготовке специалистов
по противодействию киберпреступности
Алматинской академии МВД
Республики Казахстан имени Макана
Есбулатова, подполковник полиции

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

В современном обществе невозможно двигаться вперед без использования информационных систем, обеспечивающих прием, обработку, хранение и представление информации. Современные информационные технологии не только порождают новые проблемы в обеспечении информационной безопасности, но и требуют рассмотрения новых направлений ее решения.

В Послании Главы государства Н. А. Назарбаева народу Казахстана от 17 января 2014 года «Казахстанский путь – 2050: единая цель, единые интересы, единое видение» говорится, что «государство должно стимулировать развитие транзитного потенциала в сфере информационных

технологий. К 2030 году через Казахстан мы должны пропускать не менее 2–3 % мировых информационных потоков. К 2050 году эта цифра должна быть как минимум удвоена» [1]. На уровне этого показателя очень важно обеспечить его безопасность для проведения мировых информационных потоков.

В целях определения интересов общества и государства в информационной сфере, совершенствования содержания государственной службы и нормативно-правовых актов по защите от внутренних и внешних угроз, анализа текущего состояния, связанного с информационной безопасностью, обеспечения единства принципов формирования и реализации методологической основы, регулирующей данную сферу, также в целях реализации Указа Президента Республики Казахстан от 15 февраля 2017 года № 422 «О мерах по реализации Послания Главы государства народу Казахстана от 31 января 2017 года “Третья модернизация Казахстана: глобальная конкурентоспособность”» Правительство Республики Казахстан постановило утвердить Концепцию кибербезопасности («Киберщит Казахстана») (далее – Концепция) от 30 июня 2017 года № 407. В концепции определены основные задачи и приоритеты, предъявляемые к личности в обеспечении информационной безопасности общества и государства. Также в данном документе рассмотрены технические и социально-политические аспекты информационной безопасности. Технический аспект предусматривает защиту национальных информационных ресурсов, информационных систем, информационно-телекоммуникационной инфраструктуры от авторского доступа, использования, раскрытия, взлома, изменения, чтения, проверки, записи или уничтожения для обеспечения целостности, анонимности и доступности информации. Социально-политические аспекты предусматривают пути предотвращения негативных действий для дестабилизации государства, таких как нанесение ущерба информационным системам, процессам и ресурсам, важнейшим структурам, повреждение политических, экономических и социальных систем, массовая психологическая агитация населения [2].

Когда речь идет об информационной безопасности, особое внимание уделяется трем, очень важным, обстоятельствам. Это: достижимость (оптимальность), целостность и анонимность (конфиденциальность).

Достижимость (оптимальность) – является параметром, характеризующим возможность беспрепятственного доступа пользователя к интересующей его информации в течение короткого времени.

Целостность – защита информации от взлома и неправомерного изменения. Под целостностью информации понимается способность автоматизированных систем защищать эту информацию от воздействия изменений при случайном или преднамеренном искажении.

Анонимность (конфиденциальность) – параметр, указывающий на необходимость ограничения доступа пользователя к информации, т. е. обеспечивающий защиту от неправомерного доступа или чтения.

Текущее состояние обеспечения информационной безопасности свидетельствует также о наличии следующих проблем:

- недостаток квалифицированных специалистов в области информационной безопасности, что, в свою очередь, ограничивает возможность в полной мере обеспечивать защиту информации на необходимом уровне от внешних воздействий;
- несовершенство системы обеспечения информационной безопасности особо важных объектов информатизации или частые нарушения работы системы;
- низкий уровень создания, внедрения и использования современных информационно-коммуникационных технологий, не отвечающий объективной потребности общества;
- зависимость страны от импорта информационных технологий, средств информатизации и защиты информации;
- ускорение информационного нападения между ведущими мировыми государствами, стремление государств к чрезмерному влиянию в информационном пространстве;
- недостоверная политика некоторых государств в области мирового информационного анализа;
- слабое развитие технологий информационного манипулирования;
- возможности воздействия провокационной информации на общественное сознание и государственные институты, наносящие ущерб национальным интересам страны;
- распространение недостоверной и умышленно искаженной информации в целях причинения вреда государственным интересам;
- открытость информационного пространства и др. [3].

Это говорит о необходимости придания особого значения обеспечению информационной безопасности не только структур государственного значения в стране, но и учреждений любой социально-экономической сферы.

Одним из основных вопросов, которые должны быть решены выше, является наличие достаточного количества специалистов по обеспечению информационной безопасности. Сегодня, в эпоху информационного общества, потребность специалиста в области информационных технологий в глубоком освоении криптологической науки, занимающегося вопросами защиты информации, с каждым днем становится все более очевидной. Одним из основных требований, предъявляемых к квалифицированному специалисту в этой области, занимающемуся изучением математических методов анализа информации и изучением возможности раскрытия кода информации без необходимости скрытого ключа, является овладение в совершенстве направлениями криптологии, особенно криптографии.

Знание симметричных криптосистем криптографии, таких как перемещение, размещение одного и более алфавитов, блочное шифрование, программирование, использующих только один ключ при шифровании и

обратном шифровании информации, и асимметричных криптосистем, таких как Эль-Гамаль, Ривест-Шамир-Эйдельман, Меркл-Хеллман и Хор-Ривест, использующих один ключ в шифровании информации, способствует повышению качества услуг специалистов отрасли в защите информации.

Криптографические методы защиты информации в автоматизированных системах необходимы не только для защиты информации, обрабатываемой на компьютере или хранящейся на различных запоминающих устройствах, но и для обеспечения полноты информации, передаваемой по сетевым каналам связи. То есть применение криптографических методов позволяет передавать скрытую информацию по каналам связи и обеспечивать достоверность информации путем ее хранения в зашифрованном виде на носителях информации.

Библиографические ссылки

1. Казахстанский путь – 2050: Единая цель, единые интересы, единое будущее : Послание первого Президента Республики Казахстан Н. А. Назарбаева народу Казахстана (Астана, 17 января 2014 года).

2. Об утверждении Концепции кибербезопасности «Киберщит Казахстана» : Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407.

3. Тулбасова Б. К., Омарова С. А., Унейбаева Р. К. Информационная безопасность и защита информации : учеб.-метод. комплекс. Алматы : Нур-Принт, 2012. 115 с.

Телійчук В. Г.,
доцент кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник, доцент

ЩОДО ПРОБЛЕМИ ОПЕРАТИВНО-РОЗШУКОВОЇ ПРОТИДІЇ НЕЗАКОННОМУ ОБІГУ ВОГНЕПАЛЬНОЇ ЗБРОЇ У МЕРЕЖІ «ІНТЕРНЕТ»

В Україні з усієї групи злочинів, пов’язаних із порушенням установлених правил поводження з загально небезпечними предметами, найбільш поширеним злочином є незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами. Неконтрольований обіг відповідних загально небезпечних предметів приховує в собі високий рівень небезпеки спричинення шкоди людям та довкіллю. Суспільна небезпека злочинів, пов’язаних із незаконним обігом зброї, зумовлена тенденцією розвитку насильницької озброєної злочинності, а ще незаконним збройним

підприємництвом [1].

Протидія незаконному обігу вогнепальної зброї у мережі «Інтернет» є складовою протидії злочинності. Протидія злочинності – це діяльність держави, яка спрямована на напрацювання стратегії реакції суспільства на злочинність (загально соціальний рівень) та профілактику злочинів, виявлення та запобігання (припинення) злочинним діям, реагування на вчинений злочин кримінально-правовими засобами (притягнення винних до кримінальної відповідальності) (спеціальний рівень). Однією зі складових спеціальної протидії незаконному обігу вогнепальної зброї у мережі «Інтернет» є оперативно-розшукова протидія. Протидія злочинності оперативно-розшуковими заходами містить у собі систему оперативно-розшукових та інших заходів і реалізується в окремих організаційно-тактичних формах.

Тенденції розвитку оперативно-розшукової діяльності у сфері використання інформаційних технологій спираються на застосування спеціальних технічних засобів контролю, фіксації та обробки інформації. Треба зазначити, що працівники органів Національної поліції (далі – НПУ) відстають від вимог часу, залишаючись технічно недостатньо озброєними в сучасному стані, від чого ефективність запобігання, виявлення та розслідування кримінальних правопорушень з використанням оперативно-розшукових заходів є низькими, і це важко приховати. Згідно із статистичними даними правоохоронних органів, приблизно 35–40 % традиційних злочинів щорічно вчиняється з використанням сучасних телекомунікаційних, комп’ютерних та інших технологій, а у майбутньому цей відсоток може суттєво збільшитись [2, с. 31]. Використання злочинцями в протиправній діяльності мережі «Інтернет», зокрема, під час незаконного розповсюдження вогнепальної зброї, бойових припасів і вибухових речовин, набуло сьогодні масштабних негативних тенденцій. Злочинцями відразу було позитивно оцінено технічні можливості використання в протиправній діяльності такого зв’язку, насамперед можливість у будь-якому місці країни та в будь-який час зв’язатися зі співучасником, при цьому зберігаючи анонімність абонентів-користувачів мережі «Інтернет». На відміну від стільникового телефонного зв’язку, комп’ютер (ноутбук) не завжди можна запеленгувати та визначити його місцезнаходження (відповідно, і користувача), оскільки для виходу в Інтернет можуть використовуватися портативні пристрої в різноманітних місцях, де є можливість підключення до мережі, що набагато спрощує вчинення протиправних діянь та впровадження в злочинну діяльність таких засобів зв’язку. Останнім часом усе частіше мережа «Інтернет» стала використовуватися злочинцями також як засіб платежу за вчинення різноманітних протиправних діянь, у тому числі для оплати під час придбання вогнепальної зброї, бойових припасів і вибухових речовин [3]. Мережа «Інтернет» являє собою просторову структуру, яка містить ієрархію різних учасників: установ реєстрації доменних імен і безлічі посередників, розподілених асиметричним способом (операторів системи та

інших). Усі вони забезпечують кінцевим користувачам можливість доступу до мережних протоколів і вебсерверів [4].

Характерною особливістю таких протиправних операцій є їх міжрегіональний характер: особа, яка замовляє вогнепальну зброю, бойові припаси й вибухові речовини, може перебувати в одному районі (міста чи регіону), особа, яка робить закладку вогнепальної зброї, бойових припасів і вибухових речовин – у другому районі (міста чи регіону), а процес легалізації отриманих від незаконного обігу цих засобів коштів – у третьому. Отже, злочинці розуміють, що, перебуваючи в різних регіонах країни, вони ускладнюють викриття своєї протиправної діяльності, оскільки в більшості випадків їх особа не відома покупцям вогнепальної зброї, бойових припасів і вибухових речовин. Зазначене унеможливлює фіксацію таких фактів злочинної діяльності оперативними підрозділами Національної поліції України.

До способів використання комп'ютерних технологій у сфері незаконного обігу вогнепальної зброї, бойових припасів і вибухових речовин належать такі: 1) приховування інформації щодо поставок партій вогнепальної зброї, бойових припасів і вибухових речовин шляхом криптографічного кодування електронних посилань; 2) шифрування інформації щодо номерів банківських рахунків, баз даних фінансових активів, способів зв'язку зі спільниками, даних обліку торговельних операцій; 3) шляхом використання неконтрольованих засобів електронного зв'язку для передачі інформації, безпосередньо пов'язаної з проведенням незаконних операцій, у тому числі за допомогою чат-кімнат в Інтернеті з обмеженим доступом; 4) «відмивання» доходів від незаконного обігу вогнепальної зброї, бойових припасів і вибухових речовин за допомогою електронних платежів [3].

Інтернет має три специфічні властивості, які можуть сприяти відмиванню грошей: вільний доступ, анонімність відносин між клієнтом та фінансовою установою, висока швидкість здійснення електронних угод.

Майже вся аудіо-, відео- та текстова інформація, яка є на сторінках сайтів в мережі «Інтернет», а так само й імена конкретних інтернет-сайтів розшукується його користувачами шляхом формування відповідних пошукових запитів у спеціальних пошукових сервісах. За своєю внутрішньою будовою пошукові сервіси можна поділити на такі складові частини: відкриту для користувача, та закриту від користувача.

Відкриту для користувача частину умовно можна поділити на такі, зокрема, складові частини:

– одне чи декілька доменних імен інтернет-сайту, через які здійснюється доступ до самого пошукового сервісу; графічна оболонка пошукового сервісу;

– інструменти для формування пошукових запитів та роботи з ними; блок відображення результатів пошуку інформації за сформованими пошуковими запитами.

Закриту від користувача частину можна умовно поділити на такі

складові частини:

– пошуковий індекс – перелік доменних імен інтернет-сайтів та конкретної інформації, яка розміщена в мережі «Інтернет», що може вивести пошуковий сервіс у блоці відображення результатів пошуку інформації за сформованими пошуковими запитами; пошукові роботи – це спеціальні програми, які сканують інформаційний простір мережі «Інтернет», та відносять чи виключають ту чи іншу інформацію до бази даних пошукового сервісу; внутрішні правила, за якими пошукові роботи відносять ту чи іншу інформацію до пошукового індексу пошукової системи; база даних, в якій зберігається аудіо-, відео- та текстова інформація, яку було включено до пошукового індексу пошукового сервісу.

Необхідно зазначити, що різні пошукові сервіси використовують різні внутрішні правила та різних пошукових роботів, через що їх пошукові індекси та бази даних можуть суттєво відрізнятись одна від одної. Саме тому під час пошуку інформації, що становить тактичний чи оперативний інтерес, необхідно користуватись різними пошуковими сервісами. Під час розробки оперативних заходів необхідно враховувати і технічні аспекти. Новітні технології дозволяють зловмисникам уникнути відстеження місця, де вони перебувають. Найбільш поширений спосіб уникнути інтернет-спостереження – використовувати комп'ютери із загальним доступом в інтернет-кафе, бібліотеках тощо. На сьогодні найбільш поширеним способом уникнути встановлення місцеперебування є використання анонімайзерів і TOR-мережі. У разі використання web-proxy через доступ провайдера до серверів, на яких знаходяться вебресурси, «сліди запитів» залишаються на ISP-сервері і дозволяють відстежити місцеперебування комп'ютера користувача.

У разі використання Інтернету в протиправній діяльності здебільшого затримати злочинців можна тільки за допомогою оперативних заходів. Під час використання TOR-мереж визначити місцеперебування кінцевого комп'ютера доволі складно, тому з метою профілактики можна розміщувати сайти-пастки для встановлення осіб, які цікавляться придбанням вогнепальної зброї, а також робити контрольні закупівлі [4].

Бібліографічні посилання

1. Шинкаренко І. І. Виявлення та встановлення зброї, бойових припасів або вибухових речовин, що перебувають у незаконному поводженні. *Право і Безпека*. 2014. № 3. С. 170–174. URL: http://nbuv.gov.ua/UJRN/Pib_2014_3_36
2. Максимус Д. О., Юхно О. О. Використання сучасних інформаційних технологій працівниками органів внутрішніх справ при проведенні негласних слідчих (розшукових) дій : навч. посіб. Харків : Ніка Нова, 2013. 102 с.
3. Кириченко О. В. Мережа Інтернет як засіб незаконного розповсюдження вогнепальної зброї, бойових припасів та речовин. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/6905/1/%D0%9C%D0%95%D0%A0%D0%95%D0%96%\
4. Телійчук В. Г. Оперативно-розшукова протидія наркозлочинності в мережі Інтернет як стратегія протидії наркозлочинності в Україні. *Вісник ДДУВС*. URL: http://visnik.dduvs.in.ua/wp-content/uploads/2019/02/NV_spec_1_2018.pdf

Трифонова О. В.,
декан факультету менеджменту,
професор кафедри менеджменту,
доктор економічних наук, професор
Іванова О. О.,
студентка 1-го курсу
факультету менеджменту

(Національний технічний університет «Дніпровська політехніка»)

ОЦІНЮВАННЯ ЯКОСТІ ЖИТТЯ НАСЕЛЕННЯ УКРАЇНИ ЯК СКЛАДОВА БЕЗПЕКИ ДЕРЖАВИ

Якість життя – це співвідношення умов і рівня життя з нормативами та /або стандартами, що є науково обґрунтованим. Якість життя до того ж характеризує задоволеність життям населенням з погляду на задоволення широкого набору потреб та інтересів.

Питання рівня життя повинні своєчасно вирішуватись з погляду їх прямого впливу на безпеку держави. Сучасні соціально-економічні та політичні чинники негативно впливають на якість життя та унеможливлюють своєчасне оцінювання рівня життя через слабку адаптацію традиційних наукових підходів до специфічних ситуації та можливих сценаріїв розвитку подій. Вважаємо недоцільним дослідження звужувати до статистичного аналізу матеріального становища. Розуміння рівня життя лише як матеріального добробуту не дає можливості повністю оцінити сучасні життєві стандарти, оскільки в цьому разі поза увагою залишаються важливі аспекти життєдіяльності людини, які мають соціальну спрямованість або відповідають цілям такого розвитку. Дослідження абсолютно всіх аспектів якості життя також є недоцільним, оскільки відбувається аналіз тих складових, які не суттєво впливають на формування сучасних закономірностей та/або не зазнали принципових змін протягом останніх років.

Поняття якості життя доволі широке і охоплює характеристики й індикатори рівня життя як економічної категорії, а також умови праці і відпочинку, житлові умови, соціальну забезпеченість і гарантії, охорону правопорядку і дотримання прав особистості, природнокліматичні умови, показники збереження навколишнього середовища, наявність вільного часу і можливості його доцільно використовувати, нарешті, відчуття спокою, комфортності і стабільності [1].

Зокрема, О. Богуцький пропонує розрізняти категорію у вузькому розумінні – для відбиття лише особистих потреб людей; у широкому – фактичного рівня споживання матеріальних, духовних та соціальних благ і послуг, ступінь задоволення раціональних потреб тощо. Особисті потреби є

однією з вихідних категорій у процесі аналізу життєвого рівня, які вирізняють особистість від інших у плані фізичному, інтелектуальному та соціальному. Джерелом їх задоволення є доходи населення [2]. В. О. Мандибура рівень життя у широкому розумінні вважає «…сукупністю відносин та умов, що визначають життя, працю, побут й інтелектуально-культурний розвиток людей, характеризує досягнутий у суспільстві за певний проміжок часу ступінь задоволення різноманітних потреб населення (не лише фізичних, а й соціальних, інтелектуальних, духовних), а також визначає та оцінює реальні економічні джерела та соціально-правові гарантії забезпечення життєдіяльності населення» [3]. На думку дослідника, ця категорія є відносною, оскільки залежить не тільки від рівня реальних доходів та споживання, а й ступеня розвиненості самих потреб. Тобто визнається динамічність рівня життя. Також зазначається, що рівень життя є багаторівневою категорією, має свою структуру, в якій виділяється три основні рівні: інтегрований, соціально-диференційований та особисто-персоніфікований (або сімейний).

Цими та іншими дослідниками було визначено безліч факторів, що впливають на якість життя населення. Серед них можна виділити такі фактори, як ВВП на душу населення, рівень безробіття, рівень бідності, сукупний дохід та сукупні витрати населення, рівень інфляції, прожитковий мінімум, індекс споживчих цін, кількість та середня тривалість життя населення та багато інших.

Визначимо найбільш вагомі показники, що впливають на рівень життя населення в Україні за допомогою методу узагальнення. Результати наведено у табл. 1.

Таблиця1

Показники, що впливають на рівень життя населення в Україні

Дослідник	Показники									
	Сукупний дохід	Сукупні витрати	ВВП	Рівень інфляції	Прожитковий мінімум	Рівень безробіття	Індекс споживчих цін	Кількість населення	Середня тривалість життя	Рівень бідності
Мандибура В.	1	1	1			1		1		
Горменін О.		1			1	1				1
Богуцький О.	1	1	1	1		1	1			
Геєць В.	1	1	1	1		1				
Горбатов В.	1	1						1	1	1
Колот А.	1	1		1	1		1	1	1	
Лук'яненко Н.	1		1	1	1		1	1	1	1
Чернявський Ю.	1	1	1		1	1	1			
Черенько Л.	1		1		1	1		1		
Шевченко Л.	1	1		1	1			1		1
Всього	9	7	6	5	6	6	4	6	3	4

Отже, з таблиці видно, що серед цих показників сукупний дохід населення виділяють 9 з 10 дослідників, сукупні витрати населення – 10 з 7, а такі показники, як ВВП на душу населення, прожитковий мінімум та кількість населення виділили 6 з 10 дослідників.

Бібліографічні посилання

1. Жеребин В. М., Романов А. Н. Уровень жизни населения. Москва : ЮНИТИ-ДАНА, 2002. 592 с.

2. Богуцький О. Аналіз соціально-економічної категорії рівня життя населення України. *Україна: аспекти праці*. 1998. № 2. С. 43–47.

3. Мандибура В. О. Рівень життя України та проблеми реформування механізмів його регулювання / відп. ред. Д. П. Богиня. Київ : Парламентське вид-во, 1998. 255 с.

Тютченко С. М.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ІННОВАЦІЙНА СКЛАДОВА В ЕКОНОМІЧНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

На функціонування і розвиток підприємства впливають безліч внутрішніх та зовнішніх факторів. У сучасних умовах трансформаційних змін в економіці проблема забезпечення економічної безпеки є дуже актуальною для кожного окремого підприємства та національної економічної системи загалом. Ця проблема вимагає від підприємств формування стратегії, здатної не тільки забезпечити, а й підвищити рівень власної економічної безпеки.

Є безліч трактувань вітчизняними та зарубіжними науковцями визначення поняття та методів щодо оцінки економічної безпеки підприємств. Для визначення рівня розроблено багато методик, заснованих на розрахунку різних наборів показників. Вчені пропонують механізми розрахунку складових економічної безпеки на усіх рівнях управління, приводять відповідні показники, що засвідчують рівень економічної безпеки країни, регіону, підприємства тощо. Крім того, обґрунтовують критичні значення показників, у разі перевищення яких стан безпеки за цією складовою визначають як загрозливий. Але на сьогодні немає єдиного загального методичного підходу до оцінки економічної безпеки підприємництва на макро- і мезорівнях управління [1].

На нашу думку, економічна безпека підприємства являє собою певну

систему складових елементів, важливе місце серед яких мають інновації, адже інновації є основою забезпечення конкурентоспроможності підприємства, сприяють підвищенню захисту від зовнішніх та внутрішніх загроз. Впровадження інновацій сприяє зростанню іміджу підприємства, його ділової репутації та впливає на розвиток економічних зв'язків. Поліпшення та розвиток зазначених напрямів приведуть до підвищення показників економічної безпеки підприємства.

Оцінка інноваційної безпеки має складатися з певних індикаторів, об'єднаних в шість блоків: людський потенціал, інноваційний потенціал, матеріально-технічна забезпеченість, здатність і можливість генерувати знання, адаптованість в інформаційному суспільстві і інноваційна конкурентоспроможність. Необхідно оцінювати вплив інноваційної складової на економічну безпеку.

Одним із основних напрямів забезпечення економічної безпеки підприємства є впровадження стратегії збільшення інноваційної активності та підвищення його інвестиційної привабливості. Ці інвестиційні стратегії повинні забезпечити вирішення таких питань:

- удосконалення відносин у сфері інновацій на різних рівнях;
- організації оцінки результативності та ефективності інноваційної політики на всіх рівнях;
- розробки системи інформаційного забезпечення інноваційної діяльності;
- розвитку інноваційної культури;
- удосконалення регіональної інноваційної інфраструктури;
- розвитку нанотехнологій.

Велике значення для розвитку інноваційної діяльності на підприємствах в інтересах забезпечення їх економічної безпеки має державна та регіональна інвестиційна політика на всіх рівнях управління. Ефективна інноваційна діяльність сприяє зміцненню економічних зв'язків і відносин, гарантує стабільність та стійкість у розвитку. Досвід розвинених країн свідчить, що однією з найважливіших складових економічної безпеки є інноваційна безпека, тобто здатність держави генерувати прогресивні зрушення в техніці, технології, робочої сили, інформації, товарах тощо.

Інноваційна діяльність не може здійснюватися без відповідного розвитку матеріально-технічної бази, кадрового та інвестиційного забезпечення. При цьому необхідно аналізувати і проводити оптимізацію державної інвестиційної політики по всіх галузях економіки [2].

У сучасних умовах кожна держава повинна захищати національну економіку від внутрішніх і зовнішніх загроз, здатних порушити процес суспільного відтворення, знизити досягнутий рівень життя населення і тим самим викликати загрозу безпеці [3]. Тож на рівні держави необхідно розробляти спеціальні програми та стратегії, які б сприяли інноваційному розвитку та підтримці підприємств.

Бібліографічні посилання

1. Тютченко С. М. Групування методів оцінки економічної безпеки підприємства. URL:https://visnik.dduvs.in.ua/wp-content/uploads/2019/06/6.pdf
2. The role of innovation in ensuring economic security of the enterprise. URL:http://www.sciencebsea.bgita.ru/2020/ekonom_2020_33/tipikin_rol.htm
3. Кукурудза И. И. Инновационная составляющая экономической безопасности Украины. URL : http://dspace.nbuv.gov.ua/bitstream/handle/123456789/8254/22Kukurudza.pdf?sequence=1

Тютченко С. М.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

Бут К. А.,
студентка 3-го курсу ФСПОУ
Дніпропетровського державного
університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА НА ПІДПРИЄМСТВІ

Сучасні підприємства використовують Інтернет як основний інструмент для розвитку ділової активності та охоплення ринку, що приводить до високих економічних результатів. Поряд з цими перевагами з'являються різні загрози безпеки для конфіденційної важливої корпоративної інформації.

У сучасному світі інформаційна безпека підприємства відіграє майже головну роль та вимагає розробки та впровадження заходів щодо її захисту та збереження. Раніше безпека розглядалася як державна або політична функція, але стрімкий розвиток сучасних інформаційних технологій вимагає впровадження нових законів, положень та програм щодо захисту інформації, персональних даних та активів у межах підприємства.

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, за якого забезпечено конфіденційність, доступність та цілісність інформації [1].

Найактуальнішою проблемою щодо безпеки для підприємства в сучасну епоху є хакерські атаки, які останнім часом надто почастішали. Мотиви для атаки можуть бути різними: від злому з метою наживи, що часто є основним, до помсти скривджених співробітників. В результаті порушується безпека управління підприємством чи установою або

відбувається крадіжка цінної корпоративної інформації [2].

Для стабільної роботи на кожному підприємстві повинна бути розроблена та затверджена політика безпеки, в тому числі й інформаційної, яка є складовою частиною загальної політики безпеки. Основами інформаційної безпеки є конфіденційність, цілісність і доступність. Конфіденційність повинна бути збережена, незалежно від того, в якому форматі зберігається інформація. Суворий контроль доступу, інформаційна підготовка користувача та шифрування даних є контрзаходами, які допомагають забезпечити безпеку корпоративної інформації від порушення конфіденційності.

Головними принципами забезпечення інформаційної безпеки є: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграція з міжнародними системами безпеки; економічна ефективність [1] .

Усі інфраструктури інформаційних систем повинні працювати спільно для забезпечення цілісності даних та інформації в корпоративному операційному середовищі. Жорсткий контроль доступу, системи виявлення вторгнень можуть пом’якшити ці загрози [3, с.75].

Відновлення системи після збоїв так само є важливим фактором, коли йдеться про цілісність і доступність інформації. Відновлення корпоративних даних має бути проведено таким чином, щоб не вплинути негативно на саму інформацію. Доступність гарантує, що доступ до даних здійснюється уповноваженими особами, що забезпечує надійність і ефективність роботи корпоративної інформаційної системи. Своєчасна установка виправлень для операційних і призначених для користувача систем, правильна конфігурація маршрутизаторів, застосування робочої станції управління конфігураціями та використання брандмауера – це тільки деякі зі способів запобігання атак, спрямованих на доступність системи [4].

Ефект від атаки може мати дуже руйнівні наслідки для бізнесу. Необхідно мати в штаті підприємства експертів, які є добре підготовленими у сфері інформаційної безпеки, зможуть уникнути ситуацій, що завдають шкоди підприємству. Персонал підприємства повинен бути навчений для підвищення рівня обізнаності та пильності.

Бібліографічні посилання

1. Тютченко С. М., Жила Т. В. Принципи функціонування системи інформаційної безпеки. URL: https://er.dduvs.in.ua/bitstream/123456789/5935/1/35.pdf

2. Інформаційна безпека 1С. URL: http://efsol.ru/articles/information-security-1c.html //

3. Ячменьов Є. Ф. Зовнішні чинники формування вимог щодо розробки інформаційно-аналітичної системи управління. URL:http://kafmen.ru/personal_pages/yachmenev_evgeniy/

4. Федорова Я. В., Попова Л. К. Методические подходы к анализу информационной безопасности. URL:http://studopedia.org/8-118391.html

Федчак І. А.,
доцент кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ,
кандидат юридичних наук, доцент

МОДЕЛЬ ЗАПОБІГАННЯ ЗЛОЧИННОСТІ «ПРЕВЕНЦІЯ ЗЛОЧИНІВ ЗА ДОПОМОГОЮ ЗМІНИ НАВКОЛИШНЬОЇ ІНФРАСТРУКТУРИ» (CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN – CPTED)

Попередження злочинності за допомогою екологічного проєктування (CPTED) – це модель запобігання злочинності через зміни у житловому середовищі для створення безпечніших районів. Модель виникла в Сполучених Штатах Америки, коли стало зрозуміло, що стратегії розбудови міст руйнують соціальні межі, необхідні для належного контролю. Термін CPTED увів в обіг К. Рей Джеффрі (C. Ray Jeffery). Джеффрі стверджував, що запобігання злочинності має зосереджуватись більше на чинниках, пов'язаних з природою злочинності, та на зменшення географічних можливостей для злочинності: «Злочинність можна контролювати за допомогою міського проєктування (дизайну), де безпека та охорона охоплює вулиці, будівлі та парки. Наші міста є небезпечні, оскільки вони відкривають можливості для здійснення злочинів». «Успішна модель боротьби зі злочинністю повинна мати справу… з екологічним дизайном, а не окремим правопорушником. Контроль навколишнього середовища, необхідний для боротьби зі злочинністю, може настати через містобудування, науку та технології та поведінкову терапію» [1, с. 224, 278].

У 1972 році (лише через рік) американський архітектор і проєктант Оскар Ньюман (Oscar Newman) опублікував книгу під назвою «Захищений простір». Ньюмен стверджував, що фізичний дизайн будівель і мікрорайонів може або посилити, або зменшити почуття контролю мешканців над своїм середовищем, в якому вони живуть [2].

З 1990 року у центрі уваги були не стільки ідеї та теорії, скільки набагато більше про практику CPTED. У 1991 році колишній поліцейський та тренер CPTED Тімоті Кроу (Timothy Crowe) публікує книгу «Попередження злочинності через екологічний дизайн», в якій автор визначає CPTED як: «... правильний дизайн та ефективне використання середовища можуть привести до зменшення страху перед злочинністю та частоти злочинів, і до поліпшення якості життя» [3].

Згідно з моделлю CPTED відповідна екологічна конструкція території також може збільшити розуміння злочинцем ймовірності виявлення та затримання, відомо, що це найбільший єдиний стримувач злочинності. CPTED пропонує широкі рекомендації архітекторам щодо проєктування

простору, наприклад, посадку дерев та усунення чагарників, правильне використання освітлення та заохочення пішохідного та велосипедного руху на вулицях [4].

Профілактика злочинності за допомогою екологічного проєктування (CPTED) спрямована на «виявлення умов фізичного та соціального середовища, що створюють можливості для скоєння кримінальних правопорушень або їх провокування ... і зміну цих умов, щоб уникнути злочинів ...».

Загалом CPTED «зосереджується на середовищі, де відбуваються злочини, і на методах зменшення вразливості». Центральна передумова CPTED полягає в тому, що на поширення злочинів можна впливати особливостями фізичного середовища. CPTED – це «специфічне управління, проєктування або маніпулювання безпосереднім середовищем, у якому злочини відбуваються систематично і постійно».

Модель превенції злочинів за допомогою зміни навколишньої інфраструктури (CPTED) зосереджено на управлінні фізичним плануванням і використанням рукотворного середовища для зменшення кількості злочинів. В основі логіки проєктування конкретного зовнішнього середовища з метою запобігання злочинності є те, що спроби запобігання злочинам, спрямовані на людей за допомогою таких методів, як загальне та індивідуальне стримування, менш ефективні, оскільки розміщення людей у фізичному середовищі є тимчасовим через властиву людям мобільність, тобто вони не є постійними елементами більшості середовищ протягом тривалого періоду часу. Такі речі, як будівлі та інші фізичні особливості навколишнього середовища, є «відносно постійними». Як наслідок, CPTED може мати вплив на злочинність через уявлення особистості про наявні ризики [5].

Відповідальність за зменшення злочинності та страху перед злочинністю повинні розподілятися між поліцією, органами місцевого самоврядування, місцевим бізнесом, активістами та місцевою громадою, тому навчання та інформація про принципи CPTED мають бути доведені до усіх, хто бере участь у процесі містобудування (забезпечити усвідомлення усіма учасниками своєї ролі та відповідальності щодо запобігання злочинам та посилення почуттів безпеки у суспільстві).

Отже, CPTED можна визначити так: це підхід до запобігання злочинності, а також антигромадської поведінки, страху перед злочинністю, та/або мінімізації завданих матеріальних та нематеріальних збитків, поліпшення якості життя та підвищення естетичної якості середовища через міжвідомчий процес планування, проєктування та підтримки певного фізичного середовища чи території (наприклад, місто, селище, село, мікрорайон чи сукупність будівель), включно із соціальним середовищем (із залученням людей, які є частиною цього середовища).

Підсумовуючи, треба зазначити, що запобігання злочинам є спільною відповідальністю, тому знання положень CPTED є вкрай важливими.

Бібліографічні посилання

1. Ray Jeffery C. Crime Prevention through Environmental Design. Beverly Hills: Sage Publications. 1971.
2. Newman O. Defensible space: Crime prevention through urban design. New York : Macmillan, 1972.
3. Crowe T. Crime prevention through environmental design. Woburn, MA: Butterworth-Heinemann, 1991.
4. Crime prevention through environmental design. URL: https://en.wikipedia.org/wiki/Crime_prevention_through_environmental_design.
5. Robinson Matthew B. The theoretical development of “CPTED” 25 years of responses to C. Ray Jeffery. URL: https://web.archive.org/web/20041109123322/http://www.acs.appstate.edu/dept/ps-cj/vitacpted2.html

Фещенко А. Ю.,
советник Управления ООН
по наркотикам и преступности (Вена),
подразделение по борьбе с отмыванием
средств и киберпреступностью

ПРОТИВОДЕЙСТВИЕ УГОЛОВНЫМ РИСКАМ КРИПТОВАЛЮТ

Имеет место постоянная гонка вооружений между правоохранителями и преступностью. Новые технологии постоянно появляются с одной и другой стороны. И это продолжается постоянно.

Но сейчас появились технологии, которые способны совершенно изменить концепцию организованной преступности. Это сочетание криптовалют, даркнета, почтовой доставки и появление смарт-контрактов. И первый пример этого – это полное изменение рынка киберпреступности, который работает как сервис «Cibercrime as Service» по криптовалютам. Уже тема популярная, известная, потому что рынок криминального использования растет. В прошлом году, по скромным оценкам, это порядка 4 миллиардов криминального использования. Оценка только рынка онлайн продаж наркотиков в Darknet при помощи криптовалют 1,7 миллиардов долларов. Это очень консервативная оценка. Одна гидра выдает от 1 миллиарда до 1,5 миллиардов долларов выручки в год и это только гидра darknet-маркет.

Преступный бизнес идет хорошо с использованием криптовалют. Изначально вопросы использования криптовалюты считались анонимными, псевдонимными. Сейчас есть инструменты, которые позволяют достаточно

неплохо расследовать, отслеживать криптовалюты от точки входа в виртуальный мир до точки выхода, когда они обмениваются на доллары, на евро и другие национальные валюты. Есть особенность, которая начинается с проблем нашего законодательства. Практически все страны мира ратифицировали конвенции Организации Объединенных Наций. Но они прекрасно написаны для ситуаций XIX века, более-менее XX века и работы с корреспонденцией, проникновением в помещения и т. д. Они худо-бедно позволяют работать с электронной почтой, компьютерами и Интернетом. С криптовалютами не работают совсем никак. Существует проблема: вся экономика, все наши гражданские кодексы основываются на праве собственности. Мы всегда можем сказать: если есть банковский счет – есть владелец этого счета. Есть наличные на руках – тот и их владелец. С криптовалютами ситуация абсолютно другая. Объект похож на нечто из квантовой физики. Пока криптовалюта, тот же bitcoin лежит без движения на счете, мы не можем сказать, кто является законным собственником, так как собственником может быть любой человек, у которого есть ключ. Таких людей может быть пять, десять, один, а может вообще никого не быть – ключ утерян и на этом все.

Законодательство почти всех стран мира не совсем переделано, чтобы отражать криптовалюту.

Следующий пример – DarkNet. Его появление привело к тому, что появились полностью анонимные рынки по продаже наркотиков, оружия, средств киберпреступления в онлайн. В результате нет физического контакта между заказчиком и организатором преступления. В результате получаем такую комбинацию: обмен информацией, реклама заключения сделки в DarkNet, доставка товара онлайн, почта или закладки и оплата в криптовалюте. Получаем практически идеальный рынок для сбора преступности, когда нет физического контакта между звеньями этого рынка и очень тяжело отслеживаются цепочки.

И это еще не все. Смарт-контракты, которые сейчас все больше и больше используются – это все тоже новый объект. Его нет практически ни в одном законодательстве стран мира.

Программа, которая работает себе спокойно в распределенной среде, живет в каком-то blockchaine. Смарт-контракт работает, распоряжается значительными суммами денег, отправляет, получает, реагирует на какие-то события. Но при этом смарт-контракт не является ни физическим, ни юридическим лицом. Он существует, проводит операции, а в правовом поле – его нет. Более того, он может существовать совершенно независимо от человека, который создал смарт-контракт, пользователь мог забыть пароль, запрограммировать смарт-контракт таким образом, чтобы он существовал без участия человека. Мы все смертны. Человек, который создал смарт-контракт, умер, а контракт продолжает работать сам по себе. В правовом поле почти ни в одной стране мира этой ситуации нет, но она есть, она существует и может

использоваться преступниками.

В результате мы получаем переход от классической модели организованной преступности до высокого уровня, что гарантирует исполнение преступных сделок, будь то договоры на поставку наркотиков, будь то заказные убийства, будь то поддержание высоких монопольных цен на каком-то рынке строительства, вывоза мусора… Но раньше классическая модель преступности была гарантом сделок за счет того, что все знали, кто распоряжается преступным миром, и преступность знала участников сделки за счет авторитета и других способов принуждения имела возможность устанавливать правила и гарантировать выполнение.

Сейчас произошло несколько шагов. Первый шаг был сделан Бен Ладеном при создании террористической платформы «Аль-Каида». Потому что она была построена по принципу рынка террористических актов. Одна часть физического контакта пропала.

Организатор «Аль-Каиды» продолжал, обязывал выполнение сделок. То есть когда деньги для финансирования терроризма использовались по назначению для совершения терактов, но при этом заказчики, спонсоры знали, кто их раб, кому они дают деньги. Гарант знал исполнителей, но исполнители совершенно не знали их заказчика и гаранта. Был создан рынок. Есть заказ на создание напряженности в определенном регионе. Есть оскал группировок, которые могут этот контракт выполнить. Кто делает лучше, эффективнее, тот и получает финансирование И в результате этого правоохранительные органы, спецслужбы могут устранить, арестовать одну ячейку. Они просто удаляют с рынка одну единицу и не могут двигаться дальше. Это уже был такой ассиметричный, односторонний преступный рынок.

Теперь при появлении смарт-контракта можно вообще убрать и вторую часть. В результате получается полностью симметричный рынок, когда есть рынок, который регулируется смарт-контрактом. Они гарантируют исполнение сделки, они выполняют производство оплаты преступных услуг преступников. Если ожидаемый результат достигнут, то есть если наркотики доставлены, если заказное убийство совершенно, если террористический акт произошел, то исполнитель получает свои деньги, которые ранее были запланированы заказчиком. Если событий не произошло в определенные сроки, то смарт-контракт возвращает деньги назад заказчику.

В результате мы получаем ужасную ситуацию для правоохранителей, когда преступный рынок работает. Мы можем заказать наркотики онлайн, мы можем заказать убийство, террористический акт, при этом ни заказчики, ни исполнители вообще не могут знать личности друг друга. Гарант точно также этой системы не знает, тем более этой системой может быть вообще компьютерный смарт-контракт.

Это новая реальность, к которой мы очень быстро движемся и это уже происходит. Это очень явно видно на рынке киберпреступности. Особенно

популярно то, что сейчас называется ransomware. Это взлом компаний с целью получения выкупа. Рынок стремительно развивается и сейчас, думаем через год, через два, он придет в очень интересную точку равновесия.

То есть, если ранее ransomware было, скажем так, точечным преступлением, которым заряжались компьютеры физических лиц, мелких пользователей и вымогался выкуп за расшифровку данных, то теперь этот бизнес переместился, и его жертвами являются более крупные компании и рынок работает по принципу Amazon, eBay. И для того чтобы стать выдающимся киберпреступником, нужно иметь только немного денег и доступ в Интернет, чтобы загрузить TOP браузер и знать несколько сайтов.

В результате имеем такую ситуацию. Первое, если я хочу участвовать в этом рынке, то я покупаю вредоносное программное обеспечение (готовый набор). Мне не нужно самому ничего писать. Мне даже не нужно быть специалистом по компьютерным технологиям – я его купил. Кого будем атаковать? Есть рынок услуг, когда мне уже за умеренную плату скажут: «В этой компании деньги есть, в этой компании денег нет. Во-первых, можешь атаковать. Во-вторых, ну, ты с них все равно ничего не возьмешь, потому что они на гране банкротства».

Хорошо, дальше мне нужно как-то заразить. Вирус должен проникнуть в сеть компании жертвы. Как мы знаем, самое уязвимое место компьютерной системы – это человек. Также есть рынок, в котором за умеренную плату есть люди, которые организуют сотрудника компании, который имеет доступ к их компьютерам. Он просто вставит флешку в их компьютер. Дальше все дело сделано. Ну и есть продажа информации про уязвимость этих компаний. Дальше все «прошло хорошо»: вирус сделал свое дело, компьютерная система компании заблокирована, нужно требовать выкуп. Снова есть специальный рынок, есть специально обученные люди, которые знают, как вести переговоры, которые имеют информацию о том, какой размер стартового покрытия террористов, которые за свой процент договорятся о сумме выкупа и организуют его передачу и получение. Естественно, выкуп будет перечислятся в криптовалюте. Полученную криптовалюту нужно обналичить, отмыть или что-то с ней сделать. Снова для этого есть сервисы, которые за умеренную плату мне отмоют мои доходы.

Итог. Мы имеем полностью сформировавшийся рынок, имеем новую экономику. Да, преступную. Но эта экономика, которая живет по своим законом рынка, развивается сейчас в очень интересном направлении. Это новая реальность.

Что делать? Опять же, в положительном смысле – гонка вооружений. Необходимо готовиться, знать, понимать, как это работает, иметь возможность проводить анализы риска. И если мы можем определить уязвимые точки преступного бизнеса, то придумать, разработать меры противодействия. Это могут быть технические инструменты, средства. Это может быть урегулирование по средствам законодательства, политики. Это

могут быть экономические инструменты. Ну и самое главное – это обучение специалистов. Как и во всех сферах деятельности, для того чтобы обеспечить порядок где-то, нужно достаточное количество сотрудников правоохранительных органов, которые понимают, присутствуют на этом рынке, на этой улице киберпространства. Которые понимают, что происходит, которые владеют информацией, ситуацией. Они могут делать какие-то действия, проводить расследования, изымать преступные крипто-активы.

Примеры – это хорошо изученный рынок криптовалют. Есть источники информации, есть профессиональный софт, есть законодательство с предписаниями про отмывание денег, которое дает инструменты, позволяющие проводить расследование.

Рынок развивается довольно таки неплохо. Если лет 5–6 тому назад практически мало кто знал, как расследовать, отслеживать биткоины, то сейчас, мы должны сказать, что правоохрана многих стран имеет инструменты для расследования этого и во многих случаях отслеживают биткоины, которые получены преступным путем, которые использованы для торговли наркотиками, которые используются в других преступлениях.

Одна из наших основных задач – обучение специалистов правоохранительных органов стран мира новым методам борьбы с преступностью, в том числе и с использованием криптовалют. То есть действительно за 3 дня по нашему опыту нормальный, адекватный офицер может научиться и будет способен проводить расследование криптовалют. Конечно, он не будет суперхакером, но он будет на достаточно хорошем уровне расследовать криптовалюты так же, как расследуют банковские операции, операции с наличными, другие финансовые операции.

Ну и конечно же, очень важно, чтобы законодательство соответствовало реальности. То есть если у нас есть смарт-контракт, есть у нас есть darknet, это должно быть регулировано и любая деятельность правоохраны в этой отрасли уже должна быть отрегулирована и чем-то аргументирована. Например, последнее достижение австралийского законодательства, которое наконец-то отрегулировало в стране порядок действий правоохраны в связи со взломом компьютеров злоумышленников. Это нужно делать в правовом поле во всех странах. Остается большой вопрос – это соблюдение прав человека при таких действиях в киберпространстве.

Фісуненко Н. О., доцент кафедри
аналітичної економіки та менеджменту
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ЦИФРОВІЗАЦІЯ ЕКОНОМІКИ ЯК СУСПІЛЬНЕ ЯВИЩЕ

На сьогодні весь світ входить у нову еру цифрової глобалізації, яка відзначається постійними потоками даних, що містять знання, ідеї, інформацію та інновації. Більшість європейських країн, завершивши індустріалізацію, вдало цифровізують економіки, удосконалюючи прискореними темпами інноваційні технології, де домінує автоматизація та цифрові платформи та штучний інтелект.

Розвиток вітчизняної економіки та суспільства, виробництво нових та модернізація наявних технологій зумовлюють необхідність змін у «звичній» діяльності всіх суб'єктів господарювання.

Як стверджує в своїх дослідженнях М. В. Руденко: «Реалізація інформаційно-комунікаційних можливостей та переваг новітніх технологій, необхідність набуття лідируючих позицій і зміцнення конкурентоспроможності секторів економіки у глобалізованому цифровому світі вимагають від уряду зваженої політики щодо цифровізації, лібералізації регулювання, адаптації нормативної бази, стимулювання інвестицій для просування цифрової економіки, враховуючи власні традиції і спираючись на наукове підґрунтя теорій і концепцій економічного розвитку» [1].

Сьогодні цифровізація є одним із головних чинників зростання світової економіки, оскільки завдяки їй не тільки підвищується продуктивність праці (пряма перевага), а й відбувається економія часу, створюються новий попит на нові товари і послуги, нова якість та цінність (непряма перевага) тощо. При цьому використання цифрових даних як ресурсу для виробництва зумовлює перехід від традиційної ринкової економіки до цифрової економіки, якою пронизуватимуться всі сектори: державний та приватний, реальний, невиробничий і фінансовий, видобувний, обробний та сектор послуг [2, с. 174].

Отже, суспільство спостерігає у цифровізації цілком нову модель власного розвитку, засновану на повсякденному застосовуванні цифрових технологій, що забезпечить оперативність обміну інформації та швидкість її доступу.

Переваги від цифровізації для суб'єктів господарювання та суспільства в цілому безсумнівні, адже користувачами цифрових продуктів та послуг є саме населення, яке має змогу одержувати швидкісний доступ до Інтернету, інформації і бази знань та інше, що на сьогодні є реаліями.

Позитивний ефект від цифровізації спостерігається на всіх рівнях. На рівні держави – це новий стимул для зростання ВВП, зниження рівня тіньової економіки, зміцнення довіри населення до державних органів влади завдяки прозорості та відкритості, наявність єдиної системи реєстрації як населення так і документів загального доступу.

На рівні підприємства: зростання продуктивності праці внаслідок цифровізації бізнес-процесів, можливості доступу до світових ринків, удосконалення товарів і послуг відповідно до потреб споживачів, поширення ринку збуту продукції, підвищення ефективності управління.

Для суспільства позитивним ефектом від цифровізації є оперативність обміну даними, швидкість доступу до інформації, знань, спілкування, полегшений доступ до послуг державних органів влади.

Отож, цифровізація надає багато переваг, але, крім позитивних моментів, цифровізація спричинює певні ризики.

Науковці Б. Я. Депутат, І. Б. Шевчук стверджують, що «варто розрізняти ризики цифрової трансформації та ризики цифровізації, зумовлені впровадженням цифрових технологій. Головний ризик цифрової трансформації економіки – можливе зростання рівня безробіття. По-перше, автоматизація процесів залишить без роботи частину населення. По-друге, виникатимуть нові потреби та запити з боку ринку на нові професії (герокінезіолог, естетист, спеціаліст із сонячних технологій, аналітик автотранспорту, ренатуралізатор, персональний вебменеджер, посол із культури компанії, міський фермер, аудитор екосистем, консультант із питань роботів. Іншим потужним ризиком є зростання кіберзлочинності (крадіжки персональних даних, коштів із рахунків, збирання безлічі конфіденційної та комерційної інформації, блокування діяльності тощо), боротьбу з якою потрібно проводити як на особистому, так і державному рівні [2 с. 175].

Отже, дійсно позитивний ефект від цифровізації економіки суттєво вплине на наше життя і його не доведеться чекати. Цифровізація суттєво прискорить розвиток інновацій, основ програмування, навчить всіх, хто бажає, впроваджувати цифрові технології в галузі економіки. А реалізація всіх умов дозволить підвищити продуктивність функціонування всієї економічної системи держави та одержати додаткові конкурентні переваги як суб’єктам господарювання, так і в глобалізованому цифровому світі загалом.

Бібліографічні посилання

1. Руденко М. В. Цифровізація економіки: нові можливості та перспективи. *Економіка та держава*. 2018. № 11. С. 61–65. DOI: 10.32702/2306-6806.2018.11.61
2. Депутат Б. Я., Шевчук І. Б. Цифровізація та її вплив на економіку України: переваги, виклики, загрози й ризи. *Причорноморські економічні студії*. 2019. Вип. 47-2. С. 173–177.

Хамініч С. Ю.,
професор кафедри аналітичної економіки та менеджменту Дніпропетровського державного університету внутрішніх справ, доктор економічних наук, професор

Коваленко-Марченкова Є. В.,
доцент кафедри аналітичної економіки та менеджменту Дніпропетровського державного університетувнутрішніх справ, кандидат економічних наук

ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ ЕКОНОМІЧНИХ ІНТЕРЕСІВ ДЕРЖАВИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Глобалізаційні процеси, інтеграція держави у світовий простір, інтернаціоналізація міжнародних зв'язків суттєво впливають на забезпечення як економічної, так і національної безпеки України. Саме демократизація суспільного життя вимагає сучасних підходів, прийомів та методів до впровадження ефективного інструментарію щодо управління в системі економічної безпеки.

Великий тлумачний словник сучасної української мови трактує категорію «безпека» як стан, коли кому- , чому-небудь ніщо не загрожує [1, с.70]. З погляду соціально-економічного важеля будь-якої країни, безпека – це захист життєвих інтересів кожної людини, суспільства загалом; захист держави від внутрішніх загроз та зовнішніх ворогів. Особливо ці питання актуальні для сьогодення – в період спалаху пандемії Covid-19 по всій планеті.

Стрімкий розвиток науково-технічної та технологічної складової національної економіки посилює необхідність стійкого та системного забезпечення економічної безпеки. До того ж відкритість міжнародної системи взаємозв'язків між країнами вимагає більш ретельного та усвідомленого захисту від впливу зовнішніх загроз та впровадження елементів глобалізаційних викликів як на міждержавному, так і на національному та регіональному рівнях.

У сучасному бізнес-середовищі все більш вагомо простежується збільшення та накопичення обсягів економічної та науково-технічної інформації, що сприяє розвитку та поширенню кібернебезпеки, інформаційної війни, конфліктів в інформаційному просторі тощо.

Інформація є знанням з усіма притаманними йому характеристиками: достовірністю, старінням, первинністю або вторинністю, відповідністю

досягнутого науково-технічного рівня тощо. Інформація – це дані про результати будь-яких дій або заходів, що попередньо не були відомі. Знання – це та частина інформації, яка циркулює у соціальному середовищі та має будь-який сенс тільки в її межах [2].

Важливим аргументом в запобіганні інформаційних негараздів у системі економічної безпеки суб'єкта господарювання й держави загалом (інформаційні війни, кібернебезпека, шахрайство в інформаційному просторі, крадіжки інформації тощо) є тісна співпраця з міжнародними та державними органами зберігання та розповсюдження інформації, її прозорості та конфіденційності, демократичності та публічності, з міжнародними органами інформаційної безпеки та іншими структурними ланками держав, які несуть відповідальність за національну безпеку тієї чи іншої країни.

Інший аспект захисту економічних інтересів держави – верховенство права. Визнання та дотримання всіх нормативно-правових аспектів та захист прав і свобод людини – одна з головних складових забезпечення національної безпеки держави.

Крім того, незалежність судової гілки в країні відіграє далеко не останню роль в забезпеченні гідного ставлення до людини та виконання своїх обов'язків з дотриманням відповідно професіоналізму, законності, якостей честі й гідності щодо особистості громадянина країни.

Ринкові переваги та лідерство дедалі більшою мірою стають результатом ефективного використання унікальних за своєю природою факторів нематеріального характеру, таких як знання і вміння працівників, професійна кваліфікація, освіта тощо, поєднуваних у категорію «інтелектуальний капітал» [3].

Важливою складовою забезпечення та обґрунтування економічних інтересів суспільства в системі національної безпеки є наука і освіта.

У макроекономічному аспекті інтелектуальний капітал у процесі економічної глобалізації став основним фактором, який визначає місце країни в сучасній економіці. У країнах – лідерах глобальної економіки окреслилися стала тенденція до заміщення товарно-матеріальних запасів інформацією, а основних фондів – знаннями. Дійсно, інтелектуальний капітал у сучасному конкурентному середовищі став основою для побудови інтелектуальної економіки [4].

Саме одними з показників якості життя визначено рівень освіти та впровадження науково-технічних інноваційних розробок. Парадигма сучасної цивілізації – гуманізація та гуманітаризація освіти. Гуманізація та гуманітаризація освіти формує особистість як нову сучасну генерацію людини XXI сторіччя.

Отже, економічні інтереси держави ґрунтуються на багатьох складових національної безпеки, що сприятиме реалізації та впровадженню практичних надбань вчених та спеціалістів-практиків в сучасних глобалізаційних умовах розвитку й демократизації суспільства.

Бібліографічні посилання

1. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. Київ; Ірпінь : ВТФ «Перун», 2009. 1736 с.

2. Косолапов В. В. Информационно-логический анализ научного исследования. Киев : УкрНИИНТИ, 1968. 352 С.

3. Кендюхов О. В. Гносеологія інтелектуального капіталу. *Економіка України*. 2003. № 4. С. 28–33.

4. Хамініч С. Ю. Управління підприємством на засадах освітнього потенціалу : монографія. Дніпропетровськ : Вид-во ДНУ, 2006. 288 с.

Ханькевич А. М.,
професор кафедри
оперативно-розшукової діяльності
та розкриття злочинів факультету № 2
Харківського національного
університету внутрішніх справ,
кандидат юридичних наук, професор

Третьяк О. С.,
старший юрисконсульт
юридичного департаменту
ПрАТ «Концерн АВЕК та Ко»,
здобувач PhD

ОПЕРАТИВНО-РОЗШУКОВЕ ПРОГНОЗУВАННЯ В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Прогнозування настання можливих наслідків у майбутньому закладено у самому процесі емпіричного пізнання життя будь-якою людиною розумною (Homo sapiens).

У сучасних умовах уміння у сфері діяльності оперативних підрозділів кримінальної поліції «зазирнути в майбутнє», попередити розвиток подій у небажаному для суспільства напрямі, передбачити розвиток кримінальної ситуації набуває особливо важливого значення, що зумовлено загрозою криміналізації суспільства, яка склалася у процесі реформування його соціально-політичного устрою, економічних відносин, й набула на цей момент особливої гостроти.

Сьогодні оперативно-розшукове прогнозування використовується для розробки правильної програми дій та ухвалення управлінських рішень, що забезпечують найкращі результати у виконанні завдань протидії протиправній діяльності організованих груп чи злочинних організацій. Як правильно зазначають деякі вчені, у цьому разі в подібних ситуаціях важливо

використовувати дуже продуктивний метод конструювання моделей поведінки раніше виявлених осіб, які становлять оперативний інтерес [1].

Під оперативно-розшуковим прогнозом треба розуміти висновок про передбачуваний на підставі детального кримінального аналізу оперативно-розшукових даних та іншої інформації розвиток подій, який будується на основі раніше відомих закономірностей діяльності учасників кримінального середовища, обізнаності про сучасний стан досліджуваного кримінального середовища, оцінки надійності інформаційних джерел та достовірності самої інформації про будь-які супутні й вихідні явища, що стосуються конкретної кримінальної ситуації.

Побудова оперативно-розшукового прогнозу, на відміну від побудови оперативно-розшукової версії, не має на меті пояснити вже відомий стан справ – прогноз створює проактивні цілі й установки для вирішення практичних завдань.

Експертна оцінка криміногенних факторів, які базуються на аналізі досвіду діяльності правоохоронних органів, є основою оперативно-розшукового прогнозування. Це може з успіхом застосовуватися підрозділами кримінальної поліції під час виконання оперативно-службових завдань у середовищі функціонування.

Достатньо часто методи прогнозування використовуються й у побудові традиційних оперативно-розшукових версій вчинення кримінальних правопорушень. Із практичного погляду висуванням версії мають мету пояснити емпірично встановлений або закономірно ймовірний стан справ. Функція прогнозу полягає в тому, щоб із точного знання фактів і закономірностей вивести нові відомості про невідомий ще розвиток подальших подій.

У результаті оперативно-розшукового прогнозування отримані висновки дозволяють вирахувати можливість виникнення абсолютно нових явищ, своєчасно змінювати розстановку оперативно-розшукових сил і вживати необхідних заходів. Прогноз являє собою не тільки виконання функції пізнання, але й інструмент практичного видозмінення реальності, він істотно впливає на дії і поведінку людей, які є суб’єктами протиправної діяльності [2].

Оперативно-розшукове прогнозування підвищує ефективність оперативно-розшукової діяльності, позитивно виявляючись в кожній з її форм: оперативному пошуку первинної оперативно-розшукової інформації, що проводиться підрозділами кримінальної поліції, оперативно-розшуковій превенції кримінальної протиправності та оперативно-розшукового забезпечення кримінальних проваджень.

Під час вирішення цільових завдань успіх оперативно-розшукової діяльності підрозділів кримінальної поліції залежить від попереднього глибокого вивчення джерел інформації, що дозволяє, наприклад, в окремих випадках, прогнозувати настання найбільш вдалого моменту для

встановлення довірчих контактів, проведення вербувальних бесід, обрання часу впровадження штатних негласних працівників у кримінальне середовище, своєчасного проведення затримань правопорушників, можливість й шляхи протидії діяльності правоохоронних органів з боку злочинних елементів тощо.

Ефективність використання оперативно-розшукового прогнозування сприяє значному підвищенню темпу проведення оперативно-розшукової діяльності, оскільки сприяє своєчасному ухваленню грамотних оперативно-тактичних рішень.

Висновок. Ускладнення соціальної та криміногенної обстановки, виникнення в українському суспільстві нових дестабілізуючих факторів вимагає ухвалення науково обґрунтованих, зважених рішень у сфері оперативно-розшукової протидії кримінальній протиправності, які на підставі аналізу можливих ризиків враховують результати прогнозування розвитку можливих ситуацій та їх наслідків. Сьогодні в діяльності підрозділів кримінальної поліції мало спланувати проведення тих чи інших оперативно-розшукових заходів чи негласних слідчих (розшукових) дій – важливо спрогнозувати ефективність результату від діяльності кримінальної поліції. У зв'язку з цим важливим завданням у сучасних умовах є подальше вдосконалення роботи у зазначеному напрямі.

Бібліографічні посилання

1. Khyzhniak Y., Khankevych A., Nazarenko I., Pleskach O., Tretiak O. Model of operational search prediction of intentional homicide by criminal police. Amazonia Investiga. 10(40). S. 37–44. URL: https://doi.org/10.34069/AI/2021.40.04.4 (дата звернення: 11.09.21).

2. Потапова Н. Н., Долгачева О. И. Прогнозирование и планирование в деятельности следователей и оперуполномоченных уголовного розыска при раскрытии и расследовании фактов дистанционных мошенничеств. *Вестник Казанского юридического института МВД России*. 2018. № 2 (32). URL : https://cyberleninka.ru/article/n/prognozirovanie-i-planirovanie-v-deyatelnosti-sledovateley-i-operupolnomochennyh-ugolovnogo-rozyska-pri-raskrytii-i-rassledovanii (дата звернення: 18.09.2021).

Худенко Д. М.,
т.в.о. начальника Департаменту
кримінального аналізу
Національної поліції України

ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНИХ ПРАЦІВНИКІВ ТА ІНСПЕКТОРІВ, ЯКІ ЗАЙМАЮТЬСЯ КРИМІНАЛЬНИМ АНАЛІЗОМ, ІНФОРМАЦІЄЮ ПРО ВІРТУАЛЬНІ АКТИВИ НА ОСНОВІ ПОЛІЦЕЙСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Верховною Радою України протягом останнього десятиліття зареєстровано більше 4 законопроєктів, пов'язаних із віртуальними активами або криптовалютами чи її похідними тощо. Було ухвалено закони, для цілей яких визначено поняття віртуальних активів [1], встановлено обов'язок декларування криптовалют [2] та ін. Як бачимо з попереднього твердження, законодавець допустив різні варіанти термінів щодо останніх сутностей або речей. Зауважимо, що з огляду на обсяг тез не будемо вдаватися у полеміку довкола термінології. Надалі будемо оперувати термінологією на основі чинного законодавства (п. 13 ч. 1 ст. 1 [1]) та наведемо факти й оціночні судження. І зосередимось на соціальному феномені цих речей в оперативно-розшуковій діяльності, кримінальному праві та процесі, суспільні відносини щодо яких склались та потребують подальшого правового врегулювання.

Відомо, що 11 червня 2020 року парламентом одержано черговий проєкт Закону України «Про віртуальні активи» № 3637. На думку авторів законопроєкту, його норми мають застосовуватися до правовідносин, що виникають у зв'язку з обігом віртуальних активів в Україні, визначати права та обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обігу віртуальних активів [3].

У м. Києві у торговому центрі «Globus», неподалік входу до станції метро «Майдан Незалежності», розташований один із перших криптоматів. Компанія TripleA повідомила, що за минулий рік Україна посіла 1-ше місце у світі за відсотком населення, яке володіє криптовалютами [4]. Chainalysis Inc. провело дослідження допустимого приросту Bitcoin за 2020 рік, за результатами рейтингу якого виявилось, що Україна посіла 10-те місце серед 25 країн [5].

З огляду на такий невичерпний перелік фактів та оцінок для нас стає очевидним, що суспільні відносини щодо віртуальних активів чи криптовалют та їх похідних виникли, існують та набувають поширеності. Однак використання віртуальних активів у злочинній діяльності, значна їх волатильність, яка приховує спокусу швидкого збагачення та високі ризики майнових втрат вимагає переосмислення не лише законодавчих підходів до правового регулювання, але й наявного арсеналу засобів та джерел

інформації.

Науковий інтерес до різних аспектів проблем, пов'язаних із віртуальними активами в оперативно-розшуковій діяльності, кримінальному праві та процесі виявили у своїх працях В. Білинський, Р. Благута, О. Карапетян, С. Леськів, А. Лисенко, В. Носов, О. Юхно та інші вчені.

На нашу думку, за умови ухвалення згаданого законопроєкту та узгодження нормативно-правових актів із цим Законом для кримінальної поліції особливої актуальності набуде потреба у подальшому вдосконаленні відповідних оперативно-розшукових засобів. Одним із таких засобів є обліки у вигляді інформаційних підсистем. На практиці міжнародні партнери вже допомогли українській поліції з придбанням спеціального програмного забезпечення із відслідковування руху засобів у вигляді віртуальних активів, але нами ще не використано власний потенціал засобів поліції. Зокрема, не вирішено питання щодо забезпечення оперативних працівників та інспекторів, які займаються кримінальним аналізом, інформацією про віртуальні активі на основі наявних інформаційних ресурсів.

Треба констатувати, що на сьогодні жоден із поліцейських інформаційних ресурсів не містить полів, які дозволяють систематизувати інформацію про віртуальні активи, що стали предметом або засобом злочину. Не систематизовану інформацію складно піддавати будь-якому аналізу, у тому числі кримінальному. Така ситуація в інформаційно-аналітичному забезпеченні оперативно-розшукової діяльності та кримінального провадження є не бажаною та змушує її вирішити. Нами з'ясовано, що є поліцейські інформаційні ресурси, які містять інформацію про віртуальні активи та адреси їх гаманців. Ми маємо на увазі інформаційну підсистему інформаційного порталу Національної поліції України (далі – ІП ІПНП) «Єдиний облік». Дана підсистема містить відомості стосовно повідомлень про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв'язку (п. 3 розд. ІІІ [6]). На жаль, у змісті її словників відсутні різновиди віртуальних активів. Це призводить до того, що надалі вибірка за певним критерієм є ускладненою, на неї доводиться витрачати зусилля декількох фахівців, а саме залучати представників підрозділу інформаційно-аналітичної підтримки. Особливо складно та довго робити вибірки, коли зустрічаються різні варіанти написання різновидів віртуальних актів, як-от: BTC або Bitcoin чи біткоїн, ETH, Ethereum або ефір чи ефірум тощо.

Зважаючи на вищевикладене, ми пропонуємо розглянути декілька варіантів часткового вирішення питання щодо забезпечення оперативних працівників та інспекторів, які займаються кримінальним аналізом, інформацією про віртуальні активі на основі власних інформаційних ресурсів. Вважаємо, що можливо проводити забезпечення на основі нової бази даних (інформаційної підсистеми) або ж через розбудову частини вже наявної підсистеми.

У першому випадку доведеться провести значно більший обсяг заходів впровадження. Наприклад, таким додатковим заходом є повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних.

У другому ж випадку таких заходів може бути менше, адже вбачається за можливе розбудувати частину вже наявної ІП ІПНП, що не потребує процедур повідомлення. Зокрема, такою базою даних (інформаційною підсистемою) поліції є «Єдиний облік» або «Річ».

Під час розробки проєкту технічного завдання або робочого проєкту треба передбачити створення таких полів з такими типами даних для засобу злочину: «дата та час транзакції» – дата та час; «адреса гаманця відправника» – текстовий; «вид віртуального активу (криптовалюти)» – словник; «сума транзакції віртуального активу» – число з комою із точністю до 10 знаків після коми; «тип гаманця» – словник; «виробник гаманця» – словник; «адреса гаманця отримувача» – текстовий та інші службові поля, які необхідні для ідентифікації введення, корегування та зв'язків даних.

Доцільно розглядати можливість формувати та підтримувати в актуальному стані словники на підставі відкритих джерел або за відомостями відповідного державного регулятора обігу віртуальних активів в Україні.

До того ж там, де це можна, буде раціональним виробити та застосувати відповідні правила перевірки правильності введення даних, що зменшить ризик помилок. Ще більш складними є питання оперативного внесення багатосимвольної і через це складної буквено-числової комбінації адреси та зазначення хешу транзакції. Вирішення цього аспекту розбудови може відбутись, наприклад, за допомогою сканування відповідного QR-коду адреси.

Звісно, виникнуть й інші додаткові питання, які потрібно буде вирішувати, але вищенаведене ілюструє одну з ідей забезпечення оперативних працівників та інспекторів, які займаються кримінальним аналізом, інформацією про віртуальні активі на основі власних інформаційних ресурсів.

Вважаємо, що у такий спосіб можливо не лише систематизувати та оптимізувати використання інформацією про віртуальні активі на основі власних інформаційних ресурсів, але й користати її у ролі відкритих даних для створення публічного інформаційного ресурсу або для розширення функціоналу програмного забезпечення, яке допомагає відслідковувати рух віртуальних активів.

Також разом з розглянутим напрямом забезпечення оперативних працівників та інспекторів, які займаються кримінальним аналізом, інформацією про віртуальні активи на основі власних інформаційних ресурсів, перспективною вважаємо роботу поліції над законодавчими ініціативами щодо інформаційно-аналітичного забезпечення оперативно-

розшукової діяльності та кримінального провадження внаслідок змін законопроєкту № 3637 у частині зберігання інформації, яка супроводжує переказ віртуальних активів, розширення її змісту та доступу до неї.

Бібліографічні посилання

1. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 р. № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20#n833
2. Про внесення змін до деяких законодавчих актів України щодо забезпечення ефективності інституційного механізму запобігання корупції : Закон України від 02.10.2019 р. № 140-IX. URL: https://zakon.rada.gov.ua/laws/show/140-20#n389
3. Про віртуальні активи : Проєкт Закону України № 3637. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=69110&pf35401=529256. Назва з екрану.
4. How many crypto owners in Ukraine? URL: https://triple-a.io/crypto-ownership-ukraine
5. Bitcoin Gains by Country: Who Benefited the Most from the 2020 Boom? URL: https://blog.chainalysis.com/reports/bitcoin-gains-by-country-2020.
6. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС від 03.08.2017 р. № 676. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text

Чобану Г.,
доктор экономических наук,
научный сотрудник Национального
научно-исследовательского института
труда и социальной защиты
Бухарестского университета
«ARTIFEX»

НЕОБХОДИМОСТЬ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ И РАСШИРЕНИЯ СПЕЦИАЛИЗАЦИИ В СОВРЕМЕННЫХ УСЛОВИЯХ КРИЗИСА ЭКОНОМИЧЕСКОГО И СОЦИАЛЬНОГО РАЗВИТИЯ

В нынешних условиях экономического развития, быстрой цифровизации всех отраслей общества и экономики, а также в условиях пандемического кризиса Covid-19 необходимость обеспечения информационной безопасности, кибербезопасности становится гораздо более необходимой и значительно более острой. Необходимо адаптироваться к требованиям кибербезопасности как государственных, так и частных организаций, которые в значительной степени выравнивают ее с экранами в связи с развитием информационных систем в последние десятилетия.

Остается важный вопрос – подготовка специалистов в этой области. Хотя в университетах есть специальные курсы в области информационной безопасности, кибербезопасности, проблем обучения и профессиональной подготовки все еще много. По этим причинам мы намерены затронуть в этой статье некоторые важные аспекты.

«Мы определяем навыки кибербезопасности как сочетание основных и передовых технических знаний и навыков, практикой стратегического управления, планирования, организации, дополнительных навыков, которые позволяют: понимать будущие киберриски, с которыми сталкиваются, создавать и распространять эффективно, повышать осведомленность о киберрисках, передовых методах и правилах, политиках, которые должны соблюдаться во всей организации; внедрять технические средства контроля и выполнять технические задачи, необходимые для защиты организации, на основе точного понимания уровня угрозы перед лицом; выполнения обязательств организации по кибербезопасности (юридические обязательства по защите данных); расследования и эффективное реагирование на будущие кибератаки в соответствии с требованиями организации)» [1]. Это набор знаний и навыков, которые организациям необходимо иметь как на рабочем месте, так и за пределами организации (например, если они передают свою кибербезопасность на аутсорсинг или нанимают внешних консультантов). Тем, кто работает в более широкой отрасли кибербезопасности – разрабатывая продукты или услуги кибербезопасности или проводя фундаментальные исследования, – могут потребоваться дополнительные навыки, технические знания и навыки, необходимые для исследования и разработки новых технологий, продуктов или услуг. Кибербезопасность – это чрезвычайно разнообразная область, требующая сильных технических навыков. Основываясь на существующей литературе и отраслевых мнениях экспертов, мы в общих чертах разделили – на технические навыки базового и высокого уровня. Базовые технические навыки кибербезопасности необходимы для реализации минимальных технических средств контроля, предусмотренных в утвержденной кибербезопасности. Они охватывают: безопасные интернет-соединения, защищенные устройства и программное обеспечение, контроль доступа пользователей к данным и устройствам, защиту от вирусов и других вредоносных программ, а также поддержание устройств и программного обеспечения в актуальном состоянии. Многим организациям требуется доступ к техническим навыкам высокого уровня, которые могут обеспечить кибербезопасность сверх минимального стандарта. Необходимые области технической экспертизы высокого уровня это: архитектура безопасности, тестирование на проникновение, информация об угрозах, криминалистический анализ, интерпретация вредоносного кода и мониторинг пользователей.

Еще один важный подход – оцифровка финансовых систем. По мнению Н. Р. Моштяну: «Финансирование цифровой трансформации стало самым

распространенным словом в последнее десятилетие. Повышение эффективности и выживаемости институтов связано с внедрением инноваций в области цифровых изменений. Редизайн организационной структуры любого учреждения начинается с сотрудников, их навыков и компетенций». В работе Н. Р. Моштяну указано, как процесс цифровизации финансовой системы и внедрение новых технологий изменили подход к рабочему месту, способ ведения бизнеса и изменили параметры предлагаемых финансовых продуктов и услуг. Также в исследовании представлены проблемы, с которыми сталкивается организационная структура в банковской сфере, и то, как меняется структура ее сотрудников. Начиная с примеров финансовых институтов и экстраполяции на рынок труда, в целом освещается движения на рынке труда и возможные решения для перенаправления учебных программ по специализации, чтобы вооружить людей квалификациями, навыками, которые сделают их пригодными для работы в текущих условиях[2].

По мнению авторов Д. Мэнсон и Р. Пайк: «Постоянные изменения в технологиях, потребности национальной безопасности требуют отличных профессионалов в области кибербезопасности, которые стремятся поставить цель для развития соответствующих практических навыков» [3]. Сегодняшняя система образования не готова к решению задачи подготовки достаточного количества профессионалов в области кибербезопасности, но программы, в которых используются соревнования и учебная среда, обеспечивающая углубленное обучение, заполняют этот пробел.

Информационная безопасность была областью исследований, преподавания в различных дисциплинах информатики в высшем образовании почти с момента появления современных компьютеров. В течение этого периода потребность в безопасности в учебной программе по информатике неуклонно возрастала. С возникновением глобального кризиса, из-за ограничений безопасности в развивающейся инфраструктуре информационных технологий, область кибербезопасности вызывает международный интерес и поддержку. Недавняя эволюция кибербезопасности показывает, что она начала формироваться как настоящая академическая перспектива, а не просто как область подготовки для определенных специализированных профессий. Этот отчет начинается с предпосылки, что кибербезопасность – это «метадисциплина». Таким образом, кибербезопасность следует формально интерпретировать как метадисциплину с множеством дисциплинарных вариантов, также характеризуемую общей моделью компетенций. Эта простая организационная концепция призвана повысить ясность развития области, что приведет к улучшению стандартов и целей для многих различных типов программ кибербезопасности [4].

Б. Блажич в своей статье «Дефицит рабочей силы в сфере кибербезопасности в Европе: переход к новой концепции образования и

обучения» отмечает: «Набор, поддержка и удержание достаточного количества профессионалов в области кибербезопасности на рабочем месте – это постоянная борьба не только за техническое направление кибербезопасности, но и за прошлые должности, связанные с менеджментом в киберсекторе» [5]. В работе рассматривается недостаток навыков в области кибербезопасности на европейском рынке труда и меры, принимаемые для улучшения образования в области кибербезопасности для удовлетворения выявленных потребностей. В статье исследуется, какие темы отсутствуют в деятельности по кибербезопасности в образовательных учреждениях высокого уровня в Европе и в курсах, предлагаемых инструкторами по кибербезопасности на рынке. Выводы основаны на данных опросов, проведенных Европейскими центрами кибербезопасности и Европейской организацией кибербезопасности. Эти результаты показывают, что в контексте программ кибербезопасности в высшем образовании и частных курсах, предлагаемых на рынке, не хватает тем. Обсуждаются и кратко обсуждаются общие вопросы аккредитации Европейских институтов высшего образования (IIS) и сертификации компетентности для различных профилей должностей в области кибербезопасности. Представлены действия, предпринятые для улучшения образования в этой области, в развивающемся образовательном секторе они предложены на основе сделанных выводов.

Заслуживает внимания статья К. Кабай, Д. Домингос, З. Котульского и А. Респисио «Образование в области кибербезопасности: эволюция дисциплины и анализ магистерских программ». По мере того, как объем информации критически важных сервисов, компьютеров и взаимосвязанных «вещей» в киберпространстве постоянно увеличивается, количество, изощренность и влияние кибератак становятся все более значительными. В последние десятилетия правительственные и неправительственные организации осознали эту проблему. Однако существующей рабочей силы в сфере кибербезопасности недостаточно для удовлетворения растущего спроса на квалифицированных специалистов по кибербезопасности, и в ближайшие годы дефицит будет увеличиваться. Между тем, чтобы удовлетворить растущий спрос на профессионалов в области кибербезопасности, академические учреждения создали программы кибербезопасности, в частности магистерские программы по кибербезопасности. Эта статья направлена на анализ того, какие темы кибербезопасности охватываются существующими магистерскими программами по кибербезопасности в ведущих университетах и как эти темы распределяются по курсам. Он начинается с обзора эволюции и созревания дисциплины кибербезопасности с упором на усилия JMA, которые включают раннее добавление информации и областей знаний о безопасности в учебную программу по ИТ и, в последнее время, разработку рекомендаций по учебной программе для поддержки определения программ кибербезопасности – послешкольная кибербезопасность [6].

Р. Вогель утверждает: «Текущий консенсус говорит нам о том, что существует глобальный разрыв в навыках, необходимых для компетентных сотрудников в области кибербезопасности. Нехватка этих навыков и обучения на местах имеет последствия для сектора национальной безопасности, для государственного и частного секторов. Считается, что для исправления этого, потребуются усилия, это дает возможность ИТ-специалистам, студентам университетов, соискателям работать в различных сферах государственной, административной, правоохранительной, национальной безопасности, в экономической деятельности, а также в военной» [7]. В этой статье исследуется контекст проблемы, природа нехватки навыков в области кибербезопасности и некоторые ключевые меры правительства по решению этой проблемы. Также рассматриваются новые тенденции в сфере занятости, проблемы занятости и их значение для практики. В статье утверждается, что настоятельно необходимо сократить разрыв в навыках киберпространства за счет использования окна возможностей, позволяющего заинтересованным сторонам перейти к кибербезопасности, чтобы сделать это посредством образования и обучения.

Автор Н. Р. Моштяну утверждает: «Финтехнологии и трансформация цифровых систем, наиболее часто используемые термины в последнее десятилетие, оказывают прямое влияние на любую организационную структуру и дизайн». Перестановка ценностей меняет бизнес-процесс. Он подчеркивает, что для сохранения конкурентоспособности и долговечности рынка организационные структуры должны идти в ногу с цифровой трансформацией и внедрением новых систем безопасности, чтобы противостоять кибератакам. Защита данных (финансовых и клиентских), повышение производительности, а также выживание организаций связаны с внедрением инноваций и принятием цифровых изменений в организационной культуре и реорганизацией ее структуры. Автор ставит вопрос, как новые технологии вместе с их требованиями могут улучшить организационную структуру для решения реальных задач (таких как кибер-атаки; и как цифровая трансформация и внедрение новых технологий изменили подход к требованиям к рабочим местам во всем мире)? Чтобы подчеркнуть необходимость изменений в бизнес-процессе, автор перестраивает организационную структуру с учетом вызовов новых технологий и реализации новых функций. Предлагаемое изменение для реорганизации организационной структуры основано на балансировании дифференциации и интеграции между специализированными отделами во избежание операционных рисков [8].

В заключение необходимо отметить, что подготовка специалистов в области кибербезопасности должна быть ориентирована на несколько приоритетных направлений:

1. Подготовка специалистов в области безопасности программного и аппаратного обеспечения на стороне компьютеров, сети и информационные

системы Повышенная безопасность Cyber Security для деятельности в области машиностроения, промышленности, драгоценного сельского хозяйства и технологий.

2. Подготовка специалистов по обеспечению кибербезопасности для экономической и финансово-банковской сферы, а также подготовка специалистов в области экономической безопасности со специализацией в области информационных технологий.

3. Подготовка специалистов в области информационных технологий и кибербезопасности для сферы государственного управления и государственного аппарата. Безусловно, особой отраслью является обеспечение кибербезопасности в военной деятельности и связанной с обеспечением национальной безопасности.

И последнее, но не менее важное – это медицина и обеспечение социальной защищенности населения, которая в ближайшее десятилетие будет активно развиваться. Не менее важно законодательное обеспечение этого сектора кибербезопасности с помощью как новых органических, так и обычных законов, дополняя и изменяя действующее законодательство в различных сферах деятельности.

Библиографические ссылки

1. Pedley D., McHenry D., Motha H., Shah J. Understanding the UK cyber security skills labour market. *United States Sentencing Commission, Sentencing Guidelines for United States Courts*. 2018. URL: http://www. ussc. gov/FEDREG/05_04_notice. Pdf
2. Mosteanu N. R. Finance digitalization and its impact on labour market. *Technium Soc. Sci.* 2020. № 8. S. 598.
3. Manson D., Pike R. The case for depth in cybersecurity education. *Acm Inroads*. 2014. № 5(1). S. 47–52.
4. Pedley D., Borges T., Bollen A., Shah J. N., Donaldson S., Furnell S., Crozier D. Cyber security skills in the UK labour market 2020.
5. Blažič B. J. The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society*. 2021. № 67.
6. Cabaj K., Domingos D., Kotulski Z., Respício A. Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*. 2018. Т. 75. S. 24–35.
7. Vogel R. Closing the cybersecurity skills gap. *Salus Journal*. 2016. № 4 (2). S. 32–46.
8. Moşteanu N. R. Challenges for Organizational Structure and design as a result of digitalization and cybersecurity. *The Business & Management Review*. 2020. № 11 (1). S. 278–286.

Чупілко Т. А.,
доцент кафедри комп'ютерних наук
та інженерії програмного забезпечення,
кандидат технічних наук Університету
митної справи та фінансів

КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ ПОКАЗНИКІВ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Економічна безпека відображає стійкість до внутрішніх та зовнішніх загроз національної економіки. Економічну безпеку зумовлюють такі фактори, як економічне зростання, і економіки в цілому, її окремих складових: зростання ВВП, показники покращення фінансових ресурсів, якості життя, інвестиції, витрати на інновації, зовнішній та внутрішній борг країни, фінансові та економічні ризики тощо. Для аналізу реального стану економічних показників є багато комп'ютерних технологій. Зупинимося на найбільш сучасних поширених трендах.

Великі дані – один з найважливіших технологічних трендів. Технології великих даних дозволяють зберігати величезні обсяги даних, управляти ними і обробляти їх так, щоб своєчасно отримувати інформацію, необхідну для ухвалення рішень. Управління даними враховує технологічні досягнення у сфері апаратних засобів і систем зберігання даних, мереж і обчислювальних моделей, таких як віртуалізація і хмарні обчислення. Велику роль відіграє аналітична обробка даних, яка асоціюється сьогодні з технологіями data mining, такими як штучний інтелект, регресійний аналіз, кластерний аналіз, факторний аналіз, визначення викидів.

Найбільш складним у роботі з великими обсягами інформації є обробка даних. Обробка даних – синонім таких термінів, як аналітика, дослідження операцій, аналіз, моделювання даних, прогнозування результатів. Методами математики і статистики дані перетворюються в робочі аналітичні висновки, рішення, продукти, що дозволяє ефективно управляти ними.

Найчастіше компанії використовують структуровані дані. Інформація зберігається у базах даних. Зараз популярними є реляційні бази структурованих даних MySQL, PostgresSQL, NoSQL. Окрім того, розвиток отримали нереляційні бази даних. Сервіси великих даних для організації сховищ пропонують відомі компанії: Amazon, Google, Microsoft, Yahoo.

Задачі обробки даних можна розв'язувати за допомогою великої кількості сучасних бібліотек популярних мов програмування, зокрема Python. Для аналізу даних використовують пакет статистичних методів та алгоритмів StatsModels, бібліотеку алгоритмів машинного навчання Scikit-learn. SciPy – бібліотека, що інтегрує фундаментальні пакети і найчастіше використовується в наукових дослідженнях. NumPy, Matplotlib, Pandas,

SymPy, NLTK – інструментарій *Python*, орієнтований на аналіз числових і текстових даних та візуалізацію [1].

У багатьох задачах аналізу економічних показників можна використати технології MS Office. Наприклад, Excel має широкі можливості і пакет аналізу, дещо обмежений за кількістю даних, але придатний для отримання результатів у першому наближенні для певних задач. За допомогою таблиць і вбудованого пакету аналізу можна проаналізувати характер даних, змоделювати і спрогнозувати результат [2]. Цей результат можна отримати на основі класичних підходів теорії ймовірностей та математичної статистики щодо нормування даних, кореляційного та регресійного аналізу, оцінювання прогнозних точкових та інтервальних значень економічних показників. Окрім того, в пакеті MS Office є потужний інструмент для імпорту і експорту даних та програмування, і в електронних таблицях, і в базах даних.

Популярним методом опрацювання даних є також машинне навчання (Machine Learning) – набір алгоритмів виявлення закономірності в даних. Машинне навчання на сьогодні є дуже популярною і перспективною технологією. Ринок машинного навчання швидко зростає. Серед завдань, які можуть вирішуватися засобами машинного навчання – прогнозування попиту, обсягу продажів, завантаження устаткування і інших ресурсів, виявлення тенденцій, прихованих взаємозв'язків, аномалій, повторюваних елементів; класифікація та аналіз показників та сегментація їх за різними параметрами; кластеризація та багато інших [3].

Треба надати увагу таким інструментам, як об'єктно-орієнтовані мови програмування, наприклад Python, що є відкритим для розробників, і має зручні можливості імпорту і перетворення даних різних форматів. Має більше 4000 бібліотек з готовими алгоритмами для абсолютно різних задач.

Однак для аналізу економічних показників необхідно мати достатньо глибоку математичну підготовку. Проблеми, що виникають під час вирішення завдань моделювання і прогнозування, регресійного, факторного і кластерного аналізу, пов'язані з розумінням самого процесу побудови і оцінювання моделі.

В основі сучасних програмних пакетів для моделювання і прогнозування лежать економетричні методи. Постають питання: чи пов'язані між собою досліджувані фактори і показник, чи є мультиколінеарність в системі даних, чи можна зменшити кількість змінних і тим самим спростити модель, яку форму залежності обрати для моделювання. Тільки після вказаних досліджень і перетворень даних можна скористатися бібліотекою. При цьому потрібно розуміти, які параметри потрібно задати для того чи іншого обраного методу: найменших квадратів, дерева рішень, абсолютних відхилень тощо. Оцінювання якості моделі відбувається за статистичними критеріями.

Тож сучасні комп'ютерні технології – невід'ємна частина забезпечення економічної безпеки.

Бібліографічні посилання

1. Чупілко Т., Ульяновська Ю., Мормуль М., Лагода А. Python для обробки даних і моделювання фінансово-економічних показників. *Інформаційні технології та комп'ютерна інженерія*. 2021. Т. 51. Вип. 2. С. 68–77. DOI: http://doi.org/10.31649/1999-9941-2021-51-2-68-77

2. Чупілко Т. А. Математичне моделювання кількісних показників ризику в моделі управління оборотним капіталом. *Ефективна економіка*. 2019. № 9. URL: http://www.ekonomy.nayka.com.ua.

3. Крис Элбон. Машинное обучение с использованием Python. Сборник рецептов: пер. с англ. Санкт-Петербург : БХВ-Петербург. 2019. 384 с.

Шаблиста О. О.,
ад'юнкт кафедри кримінального права та кримінології Дніпропетровського державного університету внутрішніх справ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ЗАХИСТУ ІНФОРМАЦІЇ НАЦІОНАЛЬНОЮ ПОЛІЦІЄЮ УКРАЇНИ

Сучасний розвиток суспільства неможливий без інформаційних технологій. У повсякденному житті використання інформації потребує захищеності від витоку, підробки та знищення її. У цьому нам може допомогти інформаційне право. Основними регулюючими правовими актами у галузі інформаційних ресурсів є Закони України «Про інформацію» та «Про державну таємницю». Водночас наявні більше ніж 150 нормативних правових актів різного рівня, що регламентують питання забезпечення збереження державної і службової таємниці. З огляду на те, що кримінально-правові норми, що діють у цій сфері, є бланкетними, то на практиці виникають певні труднощі щодо їх правильного розуміння та застосування.

Саму систему інформаційного права структурно поділяють на дві частини: загальна та особлива [1].

У загальній частині наводяться норми, які встановлюють основні поняття, загальні принципи, правові форми і методи правового регулювання діяльності в інформаційній сфері [2].

Особлива частина регулює суспільні відносини відкритої загальнодоступної інформації та інформації з обмеженим доступом (інститути державної таємниці).

Проблеми правового регулювання відносин в умовах інформаційного суспільства є актуальними і лише в деяких країнах створюється національна система законодавчого регулювання відносин у глобальному інформаційному просторі [1].

В Україні усі види інформаційних технологій, їх виробництво та засоби забезпечення цих технологій становлять спеціальну сферу діяльності, розвиток якої визначається державною інформаційною політикою та Національною програмою інформатизації [1].

Комплексна система захисту інформації з підтвердженою відповідністю – взаємопов'язана сукупність організаційних та інженерно-технологічних заходів, засобів і методів захисту інформації. Завданням комплексної системи захисту інформації є забезпечення конфіденційності (у разі обробки інформації з обмеженим доступом), цілісність, доступності інформації в системі «Інформаційний портал Національної поліції України» шляхом здійснення заходів, спрямованих на захист інформації від несанкціонованих дій (у тому числі з використання комп'ютерних вірусів), які можуть призвести до її випадкової або умисної модифікації чи знищення [3].

Провідна роль у створенні, впровадженні та використанні інформаційних систем як міжвідомчого, так і внутрішньовідомчого характеру належить центральним та регіональним підрозділам Національної поліції України. Усе це потребує від співробітників відповідних знань та навичок у галузі провідних інформаційних технологій [3].

Отже, потрібне подальше вдосконалення інформаційних технологій для захисту інформації у роботі співробітників Національної поліції України.

Бібліографічні посилання

1. Інформаційне забезпечення юридичної діяльності : підручник / кол. авт.; за заг. ред. д-ра техн. наук, проф. В. Б. Вишні. Дніпро : Дніпроперт. держ. ун-т внутр. справ, 2019. 228 с.
2. Державна інформаційна політика. URL: http: // merega. org.ua/law/projects/derzh polityka.
3. Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційне забезпечення професійної діяльності : навч. посіб. Дніпро : ДДУВС, 2018. 220 с.

Шелехов А. А.,
кандидат юридических наук, доцент,
ветеран Национальной полиции
Украины (Канада)

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕВОЗОК КОММЕРЧЕСКИХ ГРУЗОВ АВТОМОБИЛЬНЫМ ТРАНСПОРТОМ ОРГАНАМИ ПОЛИЦИИ КАНАДЫ И США

Экономическая безопасность государства многоаспектна. От транснациональных глобальных угроз до частных проблем отраслевого характера она проявляет себя, прямо завися от уровня экономического

развития общественных отношений. В любом случае, во всем этом многообразии уровень компетентности и профессионализма у правоохранителей должен быть надлежащим.

С 12 ноября 2021 г. патрульные полицейские Украины будут использовать специализированные автомобили – мобильные диагностические станции.

Мобильные диагностические станции полиции предназначены для того, чтобы контролировать соответствие технического состояния транспортных средств, подлежащих обязательному техническому контролю, установленным правилам, нормам и стандартам, касающимся безопасности дорожного движения. Мобильные диагностические станции оборудованы современными приборами, отвечающими государственным стандартам.

С помощью оборудования диагностической станции полицейские смогут:

– проводить замеры параметров света фар транспортных средств;
– измерять остаточную высоту рисунка протектора шин;
– осуществлять анализ выбросов выхлопных газов бензиновых и

газобензиновых двигателей;

– осуществлять замеры коэффициента дымности двигателей, работающих на дизельном топливе;

– производить замеры допустимого уровня внешнего шума транспортных средств;

– определять суммарный люфт рулевого управления транспортного средства;

– проверять другие элементы конструкции транспортных средств.

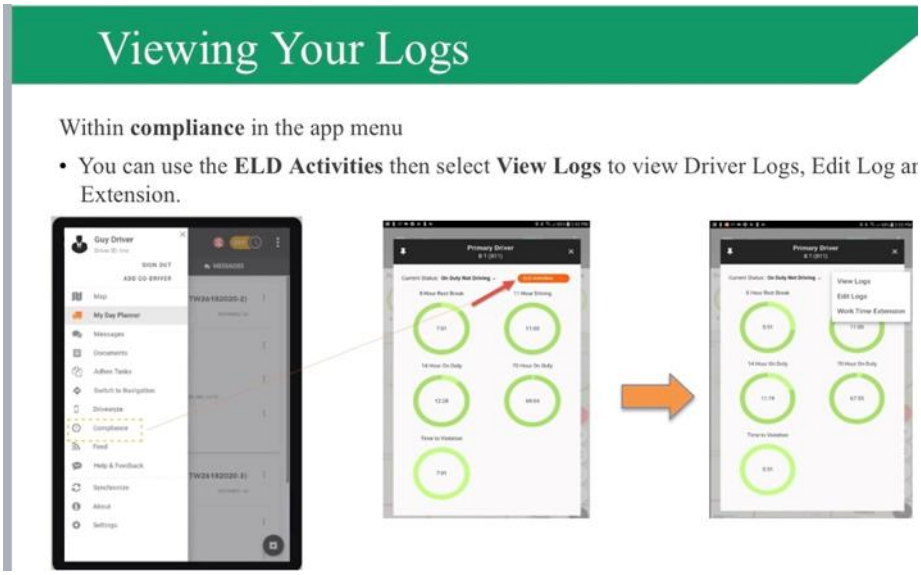
Такими станциями уже укомплектованы подразделения патрульной полиции в каждой области.

Транспорт, который будет проверяться: грузовые автомобили более 3,5 тонн и прицепы к ним, автобусы, автомобили такси, автомобили, перевозящие опасный груз, отдельные специализированные транспортные средства, легковые автомобили и прицепы к ним, используемые для перевозки пассажиров или грузов для получения прибыли.

Это лишь первые шаги в сторону обеспечения полицией безопасности коммерческих пассажирских и грузоперевозок в Украине.

Актуальным в свете выше изложенного стает вопрос использования опыта развитых стран, например, таких как США и Канада в обеспечении полицией безопасности коммерческих пассажирских и грузоперевозок.

Правоохранительные органы указанных стран весьма успешно справляются с решением указанной задачи и успели создать гибкую систему, позволяющую противодействовать вызовам реальности.



Итак первое, на что хотелось обратить внимание, это то, что все водители, которые получили водительское удостоверение на право управления коммерческим транспортом (CDL), обязаны создать персональный кабинет на сайте департамента транспорта (Drug and Alcohol Clearinghouse). Это означает, что каждый из них может быть проверен в течение рабочего времени на предмет употребления алкоголя и наркотиков. Как правило, система выбирает субъектов проверки случайным образом, сообщает об этом работодателю, и тот в течение короткого времени обязан обеспечить прохождение теста на алкоголь или наркотики (иногда оба) водителем, с последующим уведомлением департамента и самого водителя (все результаты проверок водители могут увидеть в персональном кабинете на сайте Департамента транспорта).

MALFUNCTIONS AND DIAGNOSTICS

If you receive any of the following malfunctions or errors on your ELD device, you must review your records of duty status for accuracy as soon as safely possible. You will be required to maintain paper logs if the malfunction hinders the accurate recording of hours-of-service data (which includes a location at each change of duty status). The Omnitracs ELD device immediately notifies the motor carrier of the malfunction without driver intervention.

Power - An ELD must be powered and function within one minute of the vehicle's engine receiving power and remain powered for as long as the vehicle's engine stays powered.

Engine Synchronization - An ELD is required to establish a link to the engine ECM and monitor its connectivity to the engine ECM and its ability to retrieve the vehicle parameters.

Timing - The ELD must cross-check its compliance with the external UTC source and must record any timing compliance malfunction.

Data Recording - An ELD must monitor its storage capacity and integrity and must detect a data recording compliance malfunction if it can no longer record or retain required events.

Data Transfer - An ELD must implement in-service monitoring functions to verify that the data transfer mechanism(s) are continuing to function properly.

Positioning - An ELD must monitor the availability of position measurements meeting the listed accuracy requirements and track the distance and time from the last valid measured point.

Other - Any other ELD-detected malfunction such as Bluetooth, device, etc.

Make the Call, Save Lives. www.truckersagainsttrafficking.org
1-888-3737-888 (US) • 1-800-222-TIPS (Canada) • 01800-5533-000 (Mexico)
Text INFO or HELP to BeFree (233733)

Truckers are the eyes and the ears of our nation's highways. If you see evidence of human trafficking, call the National Hotline and report your tip.

For law enforcement to open an investigation on your tip, they need "actionable information." This would include:
- Descriptions of cars (make, model, color, license plate number, etc.) and people (height, weight, hair color, eye color, age, etc.). Take a picture if you can.
- Specific times and dates (When did you see the event in question take place? What day was it?)
- Addresses and locations where suspicious activity took place

Questions to Ask:
- Do you keep your own money? If not, who does?
- Do your parents/siblings/relatives know where you are? If not, why not?
- When was the last time you saw your family?
- Are you physically or sexually abused? Are you or your family threatened?
- What is the nature of the threats?

Trafficking Red Flags to Look For:
- Lack of knowledge of their whereabouts; not in control of ID/passport
- Restricted or controlled communication — not allowed to speak for self
- CB chatter about "commercial company" or flashing lights signaling "buyer" location
- Acknowledgement of a pimp and making a quota
- Signs of branding or tattooing of trafficker's name (often on the neck)
- A van or RV that seems out of place out by trucks; a vehicle dropping someone off at a truck and picking them up 15-20 minutes later

Warning:
If you're watching a crime in progress, call 911 and then call the hotline. If you're at a truck stop/travel plaza or any other place of business, notify the manager-on-duty. Please do not approach traffickers. Allow law enforcement to deal with traffickers and recover victims. Approaching traffickers is not only dangerous for you and their victims but could lead to problems in the eventual prosecution of traffickers.

Omnitracs, LLC
717 N. Harwood Street, Suite 1300
Dallas, TX 75201 U.S.A

80-JA402-1 Rev. G
November 2019

FMCSA Registration ID: WTMD ELD ID: MCP200

omnitracs

OMNITRACS HOS DOT ELD DRIVER CAB CARD

For use with Omnitracs Mobile Computing Platform 200 (MCP200).

FMCSA Registration ID: WTMD ELD ID: MCP200

VIEW ELD DRIVER LOG

1. From the main screen, tap the Hours of Service icon.
2. Tap the **Day Log** tab (A).
3. Tap the **Inspector** button (B).

The device is in inspector mode and the DOT officer can see more details in the Day Log tab for the selected period.

- Scroll through the available days by using the arrows in the top right (C).
- Use the scrollbar (D) to reveal more records for that particular day.
- If asked, tap the **Header** button (E) to show that information to the officer.

4. When prompted, tap the **Graph** tab (F) to show your day log.
- Scroll through the available days by using the arrows in the top right (C).
- Tap the **Next** and **Previous** buttons (G) to cycle through the status events.
- Tapping the **Info** button (H) will show you the carrier information for the driver for the selected day.

ERODS TRANSFER

1. Tap the **Day Log** tab. (A)
2. If you are still in "Inspector mode" tap on the **Driver** button. (B)
3. Tap the **ERODS** button. (C)
4. Select Web Services or Email. (D)
5. Enter a comment if requested then tap **Send**. (E) Comments can be added to allow DOT officers to easily find the ERODS file on the FMCSA website.

A confirmation screen appears. If the transfer is unsuccessful, the display is considered a compliant secondary record of duty status.

More help information and step-by-step instructions can be found on the MCP200 by tapping on the training icon on the home screen. You can also watch training videos on the web at https://customer.omnitracs.com/training

 80-JA402-1 Rev. G

Таким образом, осуществляется внезапный контроль со стороны департамента (государства) за обеспечением безопасности коммерческих перевозок с точки зрения недопущения управления коммерческими транспортными средствами в состоянии наркотического или алкогольного опьянения. Данное обстоятельство не отменяет дополнительных проверок полицейскими при остановке транспортного средства.

Следующим аспектом, на который хотелось бы обратить внимание, является проверка сотрудниками полиции веса и технического состояния транспортных средств, осуществляющих коммерческие перевозки.

Для решения этой задачи на дорогах создана сеть весовых станций, на которых осуществляется не только взвешивание транспортного средства, а при необходимости его проверка (существует три уровня проверки) от проверки документов на груз, разрешений на перевозки, регистрации транспортных средств, уплаты налогов и сборов, соблюдения водителем рабочего времени (электронных логбуков ELD) до тщательной проверки технического состояния транспортного средства с использованием специального оборудования.

В данном контексте интересен вопрос обеспечения контроля за рабочим временем водителя. Все коммерческие транспортные средства в США и большинство в Канаде (хотя в Канаде возможно использование бумажного вида логбука) оборудованы специальными электронными девайсами для контроля за временем водителя. Они связаны со спутниками и фиксируют любую активность, от включения двигателя до времени езды и отдыха водителя. В США рабочая смена водителя коммерческого транспорта составляет 14 часов, из которых он может ехать только 11 часов, в Канаде соответственно 16 и 13. Отдых должен составлять 10 и 8 часов

соответственно.

Таким образом, с использованием логбука при проверке коммерческого транспортного средства полицейские получают доступ к рабочему времени водителя в Канаде на 2 недели, в США – на 1 неделю. Выявление нарушения рабочего времени наказывается очень строго, к примеру, за 3 нарушения водителя лишают лицензии на управление коммерческим транспортом, а одновременные штрафы для водителя составляют 1500–2000 тысячи долларов, для компании 10000–30000 тысяч долларов.

Таким образом, кроме решения проблемы контроля транспортировки грузов с перевесом, управления транспортными средствами в состоянии алкогольного и наркотического опьянения, технического состояния транспортных средств, решается проблема полноценного отдыха водителя, чем существенно повышается безопасность коммерческих пассажиров и грузоперевозок.

Указанные инструменты призваны существенно дополнить систему безопасности перевозок коммерческих грузов автомобильным транспортом органами полиции. Ключевая роль при этом, кроме нормативно-правового регулирования и организационных мероприятий, отводится специализированной технике и программному обеспечению.

Передовой опыт США и Канады в этой области может быть полезен полицейским Национальной полиции Украины и других страх при решении аналогичных задач.

Шеломенцев В. П.,
головний спеціаліст відділу
запровадження інновацій та проєктного
менеджменту МВС України,
кандидат юридичних наук,
заслужений юрист України

Шаповалова О. В.,
вчитель математики та інформатики
Херсонської загальноосвітньої школи
І-ІІІ ступенів № 53

ЗАКОНОДАВСТВО ПРО ЗАГРОЗИ ДИТИНІ У КІБЕРПРОСТОРІ

Проблеми безпеки дітей у кіберпросторі набувають особливого значення у період пандемії COVID-19, переходу на дистанційне навчання.

Приблизно 1,5 мільярда дітей у всьому світі на період карантину не відвідують школу. Через необхідність дотримання заходів соціального

дистанціювання освіта та соціалізація перемістилися у кіберпростір. Мало того, що багато дітей вперше приєднуються до онлайн-світу, вони також проводять в мережі на 50 % більше часу, ніж будь-коли раніше [1].

Діти, через свій вік, слабкий вольовий та емоційний контроль, імпульсивність поведінки належать до найбільш уразливих груп населення. Водночас чинне законодавство не визначає окремо ті загрози, що є найбільш актуальними з погляду безпеки дітей у кіберпросторі.

Зокрема, Стратегія кібербезпеки України щодо розроблення концептуальних підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі лише особливо відмічає дітей (досягнення цілі С.3). Кіберзагрози дітям не визначено [2].

Закон України «Про основні засади забезпечення кібербезпеки України» як об'єкти кібербезпеки розглядає лише конституційні права і свободи людини і громадянина (стаття 4) [3].

У поточному році широкому колу громадськості для обговорення було представлено проєкти Концепції з розвитку цифрових прав дітей, підготовлену Міністерством цифрової трансформації України, та Концепції виховання дітей та молоді в цифровому просторі, підготовлену Національною академією педагогічних наук України.

Метою Концепції з розвитку цифрових прав дітей визначено забезпечення прав і свобод дитини, розвиток цифрових прав дитини у контексті визначених ризиків для здоров'я, розвитку фізичного та психічного здоров'я, а також експлуатації та зловживань у цифровому середовищі. Проєкт Концепції містить розгорнутий перелік ризиків для фізичного та психічного здоров'я і розвитку дитини, на які вона може наразитися під час перебування у цифровому середовищі. Проте він містить лише з восьми позицій [4].

Треба відмітити, що визначені загрози кібербезпеці дитині мають переважно не технологічний характер – вони знаходяться у свідомості у формі недостатньої обізнаності щодо функціонування кіберпростору, ігнорування норм та правил безпечної поведінки у кіберпросторі тощо.

Метою Концепції виховання дітей та молоді в цифровому просторі є визначення провідних ідей і принципів виховання дітей і молоді в цифровому просторі. Водночас як основна загроза для дітей у цифровому середовищі розглядається лише кібербулінг (п. 2.6 Концепції). Відмічається, що він має досить великий спектр форм і рівнів інтенсивності: від невинного сперечання в чатах і жартівливого тролінгу в месенджерах до жорстких емоційних руйнівних нападів, терору й переслідування офлайн тих жертв, які знайдені у віртуальному світі, аж до грубого шантажу та примусу до самоушкоджень [5].

Зважаючи на зазначене, треба відмітити, що перелік кіберзагроз дітям є неповним і тому вбачається за доцільне:

– сформувати реєстр кіберзагроз дитині, що забезпечить збір та

фіксацію інформації про виявлені загрози кібербезпеці дитині;

– розробити класифікатор кіберзагроз дитині.

Реєстр та класифікатор доцільно розглядати як елементи Концепції з розвитку цифрових прав дітей [4].

Безпеку у кіберпросторі треба розглядати з погляду процесу взаємодії у відкритій системі «дитина-кіберпростір». Безпека такої системи розглядається як стан підконтрольності їй певного комплексу зовнішніх та внутрішніх параметрів її буття. Наявність загрози або небезпеки хоча б для одного з основних елементів системи призводить до виникнення небезпеки для всіх інших елементів. Тому треба виходити з необхідності забезпечення безпеки кожного з елементів системи «дитина-кіберпростір».

Під загрозами дитині у кіберпросторі (кіберзагрозами) розуміються наявні та потенційно можливі явища і чинники кіберпростору, що спричиняють негативний вплив на дитину, утворюють небезпеку для її життя, здоров'я, фізичного, соціального та психічного розвитку.

Для кожного запису в реєстрі кібербезагроз дитині доцільно відображати:

– категорію кіберзагрози – тип загрози з урахуванням обраних категорій (наприклад: здоров'я, майно, права);

– опис кіберзагрози з погляду причини, події та наслідку (впливу);

– ймовірність реалізації (ризик);

– вплив на об'єкт захисту та очікуване значення (оцінюються попередні значення (перед вжиттям заходів) та залишкові значення (після вжиття заходів);

– заходи реагування на кіберзагрозу – заходи, які треба вживати для мінімізації ризику її реалізації.

Реєстр кібербзагроз дитині дозволить здійснювати їх глибокий аналіз, тобто системне оброблення наявної інформації про загрози кібербезпеці дитини з метою ухвалення ефективного управлінського рішення щодо мінімізації ризиків їх реалізації.

Ризики кібербезпеці дитини розглядаються як імовірність виникнення небезпеки, пов'язаної з діяльністю дитини у кіберпросторі протягом певного періоду часу та можливі масштаби заподіяної шкоди. Кіберпростір можна розглядати як певну зону ризику, тобто місце, де діяльність дитини пов'язана з можливою небезпекою та спричиненням негативних наслідків.

Оцінювання загроз кібербезпеці дитини можна визначити як науково обґрунтований процес, який містить ідентифікацію небезпеки дитині у кіберпросторі, характеристику такої небезпеки, оцінку її впливу, характеристики ризиків та можливих наслідків для дитини.

Класифікатор кіберзагроз дитині доцільно формувати на таких ознаках, як: загрози забезпечення безпечного середовища для дитини у кіберпросторі; загрози формуванню стійкості дитини у кіберпросторі.

Метою класифікатора кіберзагроз є ідентифікація та визначення, на

основі структурованого підходу, певних класів загроз безпеці дитині у кіберпросторі, а також розроблення загальних описів для кожного класу загроз.

Реєстр та класифікатор кіберзагроз є динамічними структурами, що дозволяє її своєчасно розширювати (змінювати). Впровадження реєстру та класифікатора кіберзагроз дозволить створити ефективну систему управління ризиками та загрозами безпеці дітей у кіберпросторі.

Під такою системою розуміється комплекс процедур та правил, спрямованих на виявлення, оцінювання, моніторинг та мінімізацію ризиків кібербезпеки дитини. Під управлінням ризиками кібербезпеки дитини можна розуміти процес ідентифікації та оцінювання ризиків кібербезпеки дитини, розроблення та здійснення належних заходів, спрямованих на їх мінімізацію.

Бібліографічні посилання

1. COVID-19: 7 key ways to keep children safe online. URL: https://news.itu.int/covid-19-7-key-ways-to-keep-children-safe-online/

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

3. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

4. Проєкт Концепції з розвитку цифрових прав дітей. URL: https://thedigital.gov.ua/storage/uploads/files/Проєкт акта.pdf.

5. Проєкт Концепції виховання дітей та молоді в цифровому просторі. URL: https://naps.gov.ua/ua/press/releases/2384/.

Шурпенкова Р. К.,
доцент кафедри облікових технологій
та оподаткування Університету
банківської справи (м. Львів),
кандидат економічних наук, доцент

ОЦІНКА СТАНУ ТА ПРОБЛЕМ СОЦІАЛЬНОЇ БЕЗПЕКИ У КОНТЕКСТІ ВЗАЄМОЗВ'ЯЗКУ З ЕКОНОМІЧНОЮ БЕЗПЕКОЮ

Якісно оцінити стан і проблеми соціальної безпеки держави в сучасних умовах складно, але надзвичайно актуально. Протягом останніх років в Україні відбулися зміни в політичній, економічній та соціальній сферах, що мають значні системні наслідки. Щоб попередити їхнє перетворення на катастрофічний стан, необхідно оперативно ухвалювати державно-управлінські рішення, що визначають пріоритети розвитку в нестабільних умовах, подолання негативних наслідків прояву соціальних ризиків та

небезпек, а також встановлення рівноваги в соціальній системі. Для забезпечення соціальної стабільності в суспільстві ці процеси мають бути керованими з боку органів публічної влади. Об'єктом управлінських впливів є зміна умов і факторів, які певною мірою впливають на забезпечення соціальної стабільності та прискорення виходу з кризи [1, с. 158–162].

У сучасних умовах господарювання протидіяти загрозам можна володіючи достовірною та точною інформацією, спираючись на яку суб'єкт господарської діяльності обирає партнерів, встановлює взаємовідносини та визначає форму розрахунків з клієнтами та постачальниками, вирішує питання про інвестування своїх коштів [2, с. 262– 265].

Проблемам соціальної безпеки та її забезпечення присвячені наукові праці багатьох вітчизняних та зарубіжних вчених, серед яких: Л. А. Весельська, М. М. Єрмошенко, Д. В. Зеркалов, О. І. Іляш, М. І. Купира , Е. М. Лібанова, В. О. Онищенко, Т. В. Поснова, Б. І. Сташків, А. М. Штангрет, Б. О. Язлюк, І. І. Яремко.

Науковці справедливо звертають увагу на те, що соціальна безпека є метою, засобом і результатом діяльності людини стосовно захисту людини від чинників, явищ, подій та процесів, що становлять їй загрозу [3, с. 12]. На думку О. Скрипнюк і В. Тихого, соціальна безпека – це позитивно врегульований правовими нормами і реалізований на практиці стан, коли держава забезпечує наявними в її розпорядженні демократичними методами підтримання гідного рівня життя громадян та гарантує можливість задоволення основних потреб їх розвитку [4, с. 45].

Саме економічна безпека головним чином визначає стан і рівень соціальної безпеки. Серед різноманітних чинників, які ускладнюють або навіть унеможливлюють реалізацію національних інтересів у соціальній сфері, є економічні чинники. Економічні чинники та умови, які створюють небезпеку для безпечної життєдіяльності людини і суспільства, реалізації національних економічних інтересів, здійснюють дестабілізувальний вплив на функціонування і динамічний розвиток соціально-економічної системи суспільства загалом, є загрозами економічній безпеці держави.

Найбільш вагомими загрозами, що зумовлюють загрози національним інтересам у соціальній сфері в Україні через призму економічної безпеки, є: недостатні темпи відтворювальних процесів та подолання структурної деформації в економіці; критична залежність національної економіки від кон'юнктури зовнішніх ринків, низькі темпи розширення внутрішнього ринку; нераціональна структура експорту з переважно сировинним характером; небезпечне для економічної незалежності України зростання частки іноземного капіталу у стратегічних галузях економіки; велика боргова залежність держави, критичні обсяги державних зовнішнього і внутрішнього боргів; «тінізація» національної економіки; переважання в діяльності управлінських структур особистих, корпоративних, регіональних інтересів над загальнонаціональними [5, с. 126–130].

Отже, у сучасних умовах соціальна безпека стає одним з найважливіших видів національної безпеки, оскільки вона фокусує всі основні проблеми національної економіки. Сучасні соціально-економічні процеси у суспільстві все більше залежать від соціальної безпеки і рівня розвитку соціальної сфери. Водночас під впливом соціальної безпеки розвиваються і формуються всі сфери життя, у тому числі й економічна складова.

Потреба безпеки є важливою потребою людини і конкретним мотивом її діяльності, а система забезпечення безпеки є важливим атрибутом складних соціально-економічних систем.

Бібліографічні посилання

1. Давидюк О. О. Соціальна безпека: проблеми теоретичного аналізу та побудови системи показників. Київ : Абрис, 2002. С.158–162.
2. Демко І. І. , Шурпенкова Р. К. Обліково-аналітичне забезпечення безпеки підприємства. *Розвиток банківських систем світу в умовах глобалізації фінансових ринків* : матеріали XI Міжнародної науково-практ. конф. 27 жовтня 2017 р. Черкаси : ЧНІ ДВНЗ «Університет банківської справи», 2017. С. 262–265.
3. Попов М., Тихий В. Безпека як фундаментальна категорія в методології правознавства (до постановки проблеми). *Вісник Академії правових наук України.* 2000. № 3. С. 10–16.
4. Скрипнюк О., Тихий В. Соціальна держава і проблеми забезпечення соціальної безпеки. *Вісник Конституційного Суду України*. 2002. № 2. С. 44–49.
5. Кальницька М. А. Соціальна безпека: поняття та загрози в контексті взаємозв'язку з економічною безпекою. *Причорноморські економічні студії*. 2017. Вип. 16. С. 126–130.

Якименко Ю. М.,
доцент кафедри управління
інформаційною та кібернетичною
безпекою Державного університету
телекомунікацій,
кандидат військових наук

ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ІННОВАЦІЙНОГО РОЗВИТКУ

У сучасних умовах проблема економічної безпеки є актуальною, оскільки підприємства працюють в умовах різних зовнішніх і внутрішніх ризиків, а конкурентне економічне середовище приховує численні погрози. Ця обставина вимагає від суб'єктів управління підприємством побудови комплексної системи, спрямованої на підвищення рівня економічної безпеки.

У забезпеченні економічної безпеки істотне значення має інноваційна

активність як цілеспрямована діяльність зі створення, освоєння у виробництві і просуванню на ринок продуктових, технологічних та організаційно-управлінських нововведень. Інноваційна активність знаходиться в центрі інноваційної політики держави, оскільки є передумовою економічного зростання, підвищення рівня і якості життя населення й кожного робітника підприємства.

Сутність сучасних інновацій у сфері економічної безпеки організацій розкривається в різноманітті чинників, від яких вона залежить. Ці чинники можуть бути визначені системою критеріїв і показників.

Інноваційний шлях розвитку підприємства відіграє істотну роль у підвищенні рівня його ділової репутації (іміджу), що забезпечить йому переваги в більшій доступності до кредитних ресурсів і до інвестиційних проєктів, а також більшою ймовірністю укладення вигідних довгострокових контрактів. Це однозначно підвищить і рівень економічної безпеки підприємства.

Водночас такі сучасні проблеми, як нестабільна політична, і як наслідок, нестабільна економічна ситуація в державі, низький рівень фінансування наукових розробок, високий рівень корупції в управлінських структурах, слабке впровадження і освоєння нових технологій і видів техніки, призводять до зниження інноваційної активності підприємства. Тим самим це зумовлює появу і розвиток ризиків і загроз у забезпеченні їх економічної й інформаційної безпеки.

Тому проблема забезпечення економічної безпеки підприємства знаходиться в площині вирішення сучасних проблем шляхом інноваційного розвитку і характеризується підвищеною увагою вітчизняних і зарубіжних вчених. Проблемні питання забезпечення економічної безпеки досліджували В. І. Фостяк [1], І. О. Корчинський, В. К. Сенчагов, Ю. І. Ільків, Е. І. Данилова, Я. І. Чмир та ін.

Як видно з результатів аналізу міжнародних рейтингів Doing Business – сприятливості ведення бізнесу в країнах, що проводиться Групою Світового банку, позиція України за 12 напрямами ділової діяльності є не дуже вдалою. Україна в 2020 році посіла 64-те місце серед 190 країн [2]. Результати досліджень банку за поточний рік завжди інформують про дії політиків, допомагають країнам ухвалювати обґрунтовані рішення і дозволяють зацікавленим сторонам більш точно оцінювати економічні і соціальні поліпшення, тим самим бути цінним інструментом для приватного сектора, громадянського суспільства, наукових кіл, журналістів і розширення розуміння глобальних проблем. За результатами аналізу більше 30 законодавчих змін, які були впроваджені в Україні в 2021 році і демонстрації істотного прогресу по 10 компонентах, Україна може піднятися в рейтингу Doing Business, щонайменше, до 20 позицій. Більшість країн, які займають лідируючі позиції в рейтингу, обрали напрямом свого пріоритетного розвитку інноваційні перетворення. Тому для визначення впливу інновацій

на економічну безпеку підприємств необхідно додатково виконувати аналіз їх інноваційної активності.

Стимулюючим фактором для інноваційної активності підприємств були створені з 2008 року мережі регіональних центрів інноваційного розвитку, метою яких є забезпечення інформаційно-аналітичної, методичної, організаційної та іншої підтримки інноваційного розвитку регіонів України [3, с. 237]. Отже, концентрація ресурсів підприємств на основних напрямах зростання своєї інноваційної активності дозволить підвищити конкурентоспроможність вітчизняної продукції, освоїти нові ринки і прискорити темпи економічного зростання, зміцнивши тим самим економічну безпеку.

Інноваційна активність характеризується інтенсивністю інноваційної діяльності. Оцінка інноваційної діяльності передбачає вивчення технологічних, маркетингових і організаційних ініціатив, які і є основою аналізу інноваційної активності підприємства (рис. 1).

Рис.1. Компоненти інноваційної активності підприємства

Важливими індикаторами, що характеризують інноваційну діяльність, є витрати на інновації та їх питома вага в загальній величині витрат підприємства [4].

Технологічна інноваційна активність спрямована на одержання і застосування нових знань для вирішення технологічних і інженерних завдань, на забезпечення виробництва і роботу його як єдиного ефективного комплексу. До неї відносять зміни, засновані на застосуванні досягнень науково-технічного прогресу, новітніх технологій і засобів управління.

Продуктова інноваційна активність передбачає випуск продукції або надання послуг, що є новими або мають нові властивості або способи їх застосування.

Процесна інноваційна активність спрямована на впровадження нових технологій, поліпшення способу виробництва або доставки продукту. Вона містить зміни в технології, виробничому обладнанні, застосування нових матеріалів, програмного забезпечення.

Маркетингова інноваційна активність містить впровадження нових

методів дослідження ринку, участь у виставках, ярмарках, презентаціях, охоплює істотну зміну дизайну, паковання продукту, його просування на ринок.

Організаційна інноваційна активність передбачає використання нових управлінських прийомів в діяльності підприємства, створення робочих місць, розширення і зміцнення зовнішніх зв'язків, скорочення витрат на управління. Оцінити рівень організаційної результативності роботи організацій можна на основі індикаторів інноваційної активності.

Отже, розглянутий підхід до забезпечення економічної безпеки підприємства в умовах інноваційного розвитку завдяки індикаторам інноваційної активності підприємства дозволить виконати оцінку його інноваційної діяльності, що є предметом подальших досліджень.

Бібліографічні посилання

1. Фостяк В. І. Управління безпековою діяльністю промислових підприємств. URL: http://dspace.lvduvs.edu.ua/bitstream/1234567890/3507/1/fostyak_d.pdf.
2. Кузякив О. Украина и Doing business: плюс 7 позиций – победа или поражение? URL: https://biz.liga.net/ekonomika/all/opinion/ukraina-i-doing-business-plyus-7-pozitsiy---pobeda-ili-porajenie
3. Киба О. В. Роль инноваций в обеспечении экономической безопасности промышленного предприятия. *Теоретичні і практичні аспекти економіки та інтелектуальної власності*. 2014. Вип. 1(10). Т. 1. С. 234–238.
4. Разработка инновационного проекта с целью повышения уровня экономической безопасности предприятия. Белгород, 2018. 119 с. URL: https://core.ac.uk/download/pdf/333603666.pdf.

Ящук В. І.,
доцент кафедри управління
інформаційною безпекою
Львівського державного університету
безпеки життєдіяльності,
кандидат економічних наук, доцент

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ВИЗНАЧЕННЯ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ РИТЕЙЛУ

Зважаючи на специфіку діяльності підприємств ритейлу, для визначення рівня їх економічної безпеки доцільно використати методичний підхід, відповідно до якого визначається перелік показників, а також методи розрахунку рівнів функціональних складових та інтегрального індикатора економічної безпеки підприємств ритейлу. Цей методичний підхід передбачає такі етапи конструювання інтегральної оцінки економічної

безпеки підприємств ритейлу: формування множини показників; розрахунок їх значень; нормалізація показників; визначення вагових коефіцієнтів для показників та рангів функціональних складових; розрахунок інтегрального індикатора. Визначення рівня кожної функціональної складової економічної безпеки підприємств ритейлу здійснюється за формулою:

$$R_i = \sum_{j=1}^{m} w_{ij} z_{ij}, \qquad (1)$$

де w_{ij} – вагові коефіцієнти, що визначають ступінь внеску j-го показника у зведений індикатор рівня i-ї функціональної складової; z_{ij} – нормалізовані значення вхідних показників x_{ij}.

Відбір множини показників за кожною складовою економічної безпеки здійснюється з урахуванням специфіки діяльності підприємств ритейлу. З метою забезпечення інформаційної односпрямованості з множини показників x_{ij} виділено стимулятори (зв'язок між інтегральним індикатором I та показником прямий) та дестимулятори (зв'язок обернений), які нормалізуються з метою зіставлення.

Для визначення вагових коефіцієнтів показників функціональних складових економічної безпеки пропонується модель головних компонент факторного аналізу за допомогою пакета Statistica для: 1) виокремлення головних компонент і розрахунку факторних навантажень; 2) ідентифікації головних компонент. За формулою (1) розраховують значення індикаторів рівня кожної функціональної складової економічної безпеки підприємств ритейлу.

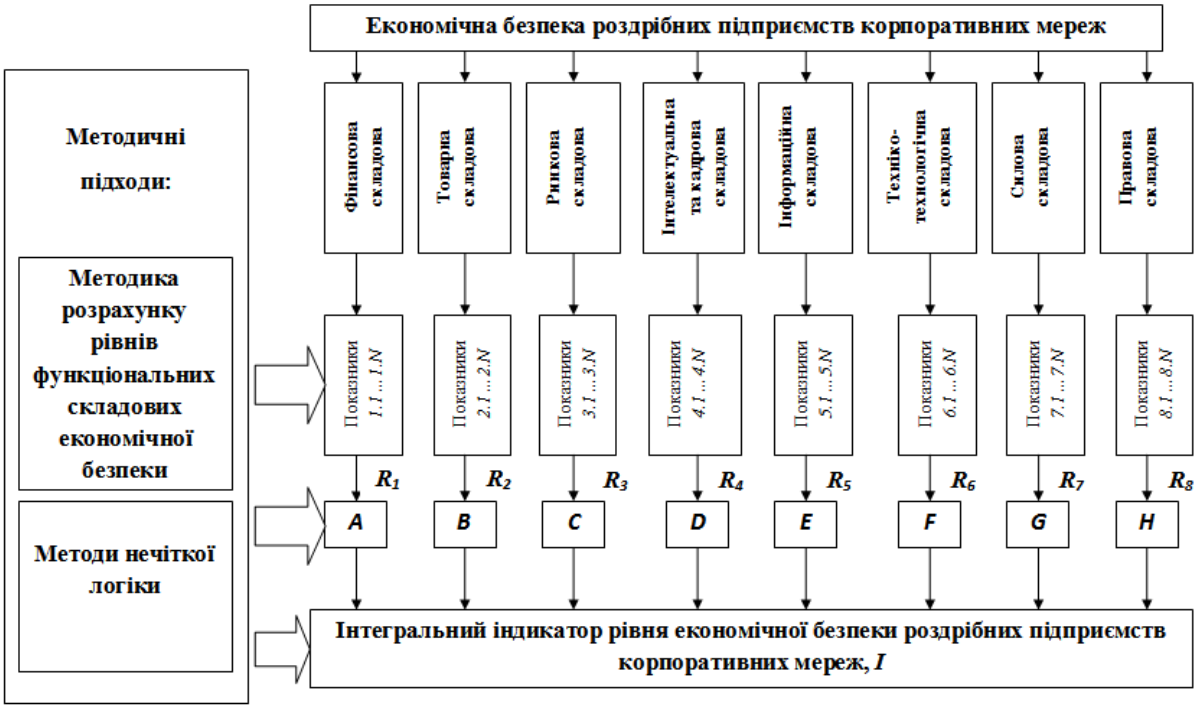


Рис. 1. Структурно-функціональна модель оцінювання рівня економічної безпеки підприємств ритейлу *(розроблено автором)*

У зв'язку з «нечіткістю даних» інтерпретація отриманих результатів є ускладненою, оскільки немає визначених меж рівнів функціональних складових та інтегрального індикатора [2]. З огляду на це наступним етапом запропонованого методичного підходу визначення інтегрального індикатора є застосування методів нечіткої логіки відповідно до розробленої структурно-функціональної моделі (рис. 1). На рисунку наведено взаємозв'язок вхідних (показників функціональних складових) і вихідних даних (індикаторів економічної безпеки як за кожною складовою, так і загалом) та їх структуру.

Для реалізації нечіткого логічного виведення інтегральні значення рівнів функціональних складових (R_1, R_2 ... R_8) подаються у вигляді таких лінгвістичних змінних: «рівень фінансової безпеки» (A), «рівень товарної безпеки» (B), «рівень ринкової безпеки» (C), «рівень інтелектуальної та кадрової безпеки» (D), «рівень інформаційної безпеки» (E), «рівень техніко-технологічної безпеки» (F), «рівень силової безпеки» (G), «рівень правової безпеки» (H) [1].

Для знаходження інтегрального індикатора у вигляді лінгвістичної змінної «рівень економічної безпеки підприємств ритейлу» визначено співвідношення між вхідними та вихідною змінними:

$$I = f_I(A, B, C, D, E, F, G, H), \qquad (2)$$

де I – позначення лінгвістичної змінної рівня економічної безпеки підприємств ритейлу; A, B, C, D, E, F, G, H – позначення лінгвістичних змінних рівнів функціональних складових економічної безпеки підприємств ритейлу.

Отже, інтегральний індикатор економічної безпеки підприємств ритейлу визначається ієрархічно згідно з деревом логічного виведення, що потребує визначення термінів лінгвістичних змінних, розроблення матриці співвідношень між лінгвістичними змінними, правил нечіткого логічного виведення та врахування рангу кожної функціональної складової, визначеної експертним шляхом.

Бібліографічні посилання

1. Ящук В. І. Методи оцінювання економічної безпеки підприємства рітейлу. *Вісник Львівської комерційної академії*. Серія : Економічна. Львів : Вид-во Львівської комерційної академії, 2010. Вип. 33. С. 126–130.
2. Ящук В. І. Методичні підходи до забезпечення економічної безпеки підприємства рітейлу. *Вісник Національного університету «Львівська політехніка»*. Проблеми економіки та управління. Львів : Вид-во Національного університету «Львівська політехніка», 2010. № 668. С. 218–223.

КУРСАНТИ ТА СТУДЕНТИ

Janine Al-Shargabi,
student of the Law Faculty
of Sofia University (Bulgaria)

LINE 102 – REVIEW FROM ZHANIN

Line 102 is a truly innovative educational method implemented at the Dnipropetrovski State University of Internal Affair. It combines theoretical knowledge and practical experience that helps turn students into young professionals. This methodology, if applied in other universities and educational institutions, will have a very positive effect on the level of retained knowledge and expertise of the students.

The first very important aspect of line 102 is the theoretical information it presents to students. This is done in a very effective way due to a number of factors:

- The lectures are renowned professionals that are able to talk in depth about their experiences and the newest developments in their respective field.
- There is a strong connection between students and lecturers, students are encouraged to be proactive and to ask questions, participate in tasks and develop their skills as much as possible.
- Lectures include multimedia: presentations, videos, etc, all of this makes the information easy to digest and keeps students engaged.
- Students are encouraged to participate in discussions and academic writing, this helps them form their own opinions and develop a deeper understanding of the topics.

This engaging approach is very effective in turning theoretical and abstract knowledge into information that manages to engage the students. When the students feel as if they are actively participating in the educative process, they are more likely to remember the topics they learned and the interesting insights their lecturers shared.

The innovative approach of Line 102 is the practical aspect of the project. Students are able to engage in real life simulations of emergencies and to act as victims, perpetrators, police officers and dispatchers. This is very beneficial for them on a number of levels:

- First, they can gain practical insight into what their line of work looks like. By acting out different situations they have to face unexpected events, interact with others in realistic simulations, this way they can see face to face what can happen when on duty. This helps them develop a work method in the future. When

they finally go into their professional careers they will know how to keep calm, what to expect, how to react when an issue arises, etc.

- There are many instances of abuse and police brutality carried out by policemen and law enforcement. This is an ever growing problem for many societies in the world, this includes Ukraine, Bulgaria, the US and many others. It is important that we acknowledge this issue and look for ways to fix it. It is very beneficial that the students can be managed and supervised during their first experiences in Line 102. This can limit the instances of mistakes or malpractice. When acting out different scenarios, they are under the supervision of their teachers, who can give them advice on what to do, show them the correct ways to follow different protocols and to penalise them for any misuse of power or faulty procedures that may have been very detrimental if carried out during their actual time at work.
- The students can play out every role during their time in Line 102. They can be a police officer as well as a dispatcher, a criminal or a victim. They see how the process plays out from every angle. This is very beneficial for them because it gives them a deeper understanding. One day when they have to help a victim they will know what that person may have experienced and how they may have felt. When they have to chase a criminal they will know what is going on in their mind and may find it easier to track them down. When they have to cooperate with dispatchers, they will know how to do that more effectively, having a grasp of what their line of work looks like.
- Line 102 is also very important for cultivating social bonds between students. It mixes groups and encourages teamwork and bonding. These connections are important for creating a tight knit student body. These students will grow up to be professionals willing to cooperate with each other in the name of the public.

A very impressive aspect of Line 102 is the technology that the university has in order to facilitate the project. There is a computer room where students have lectures and a special booth for the dispatchers during the simulations. It is very admirable that the university is investing in technology and media in the highly technological era we live in.

Lastly, another positive development is the fact that Line 102 tries to include all types of situations during simulations. This again shows that the university updates its curriculum and activities in line with the times we live in. The university specifically focuses on Domestic Violence in a time where such instances of abuse sadly are on the rise. This is a very important topic that needs to be discussed and explored in depth. In order for the police to be perceived as a respectable and trustworthy institution, it must understand the actual problems of the people and to know how to effectively react. If students learn how to act in all sorts of situations and act with integrity and respect for protocols and the rights of people, they will grow into great professionals.

Байрак К. С., курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник – Рижков Е. В.,
завідувач кафедри економічної та
інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ДО ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

«Хто володіє інформацією, той володіє світом», – відомий вислів Натана Ротшильда, який дуже влучно описує, чому людям так важливо знати будь-яку інформацію, у тому числі інформацію, яка є таємною. Вислів було сказано ще у XVIII столітті, з того часу багато чого змінилося, зокрема обсяг отримуваної інформації. Щодня з різних джерел: книги, газети, журнали, Інтернет, телебачення, радіо сучасна людина отримує у сотні разів більше інформації, ніж люди у XVII-XVIII століттях.

І звісно ж розвиток інформаційного забезпечення є одним із актуальних питань, оскільки у демократичному суспільстві, яке є однією з головних ознак громадянського суспільства, вільний доступ до інформації має першочергове значення. Для розвитку концепцій, до яких прагне Україна, – громадянського суспільства та правової держави – пріоритетним є розвиток нормативно-правового регулювання різних сфер життя людини. І одна з найважливіших сфер – це інформаційне забезпечення, оскільки кожна людина має право на вільне розповсюдження, пошук та одержання інформації [1].

Через вільний доступ до великих обсягів інформації суспільство стало більш вразливим, саме тому створено принцип інформаційної безпеки, який описаний в Законі України «Про основні засади розвитку інформаційного суспільства на 2007- 2015 роки» [2].

Під інформаційною безпекою розуміється стан захищеності життєво важливих інтересів людини, суспільства, держави, за якого запобігається завдання шкоди через: неповноту, невчасність та невірогідність використовування інформації; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації.

Законодавець забезпечив не тільки достовірність інформації, а й доступ для кожного громадянина бути почутим, завдяки Закону України «Про

Суспільне телебачення і радіомовлення України» від 17.04.2014 року № 1227–VII, створюється суспільне телебачення та радіомовлення, де громадяни можуть бути залучені до обговорення та висловлення власної думки щодо актуальних питань держави [3].

Крім того, важливим кроком є створення спеціального профільного органу – Міністерство інформаційної політики України, основними завданнями якого є забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів; забезпечення здійснення реформ ЗМІ щодо поширення суспільно важливої інформації, що визначено постановою КМУ від 14.01.2015 року № 2 «Питання діяльності Міністерства інформаційної політики України» [4].

І звісно ж найголовніше процесуальне забезпечення інформаційної безпеки – це створення кіберполіції, яка є частиною кримінальної поліції Національної поліції України. Головним завданням кіберполіції є не тільки захист інформаційного простору, а й протидія кіберзлочинцям, які порушують вищеперераховані нормативно-правові акти.

Звісно ж нормативно-правове регулювання інформаційної безпеки в Україні створюється і розвивається, оскільки щодня комп'ютерні технології змінюються та вдосконалюються.

Бібліографічні посилання

1. Загальна декларація прав людини від 10 грудня 1948 року. *Верховна Рада України*: *офіційний вебпортал*. URL: http://zakon4.rada.gov.ua/laws/show/995_015
2. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України. *Верховна Рада України*: *офіційний вебпортал*. URL: http://zakon4.rada.gov.ua/laws/ show/537-16
3. Про Суспільне телебачення і радіомовлення України : Закон України від 17.04.2014 року № 1227–VII. *Верховна Рада України*: *офіційний вебпортал*. URL: http://zakon4.rada.gov.ua/laws/ show/1227-18
4. Питання діяльності Міністерства інформаційної політики України : Постанова КМУ від 14.01.2015 року № 2. *Верховна Рада України*: *офіційний вебпортал*. URL: http://zakon4.rada.gov.ua/laws/ show/2-2015-%D0%BF

Барановська О. В., Михайлов Д. Є.,
здобувачі вищої освіти
спеціальності 051 «Економіка»
Науковий керівник – Кононова І. В.,
професор кафедри
аналітичної економіки та менеджменту
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, доцент

ПРИНЦИПИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

На сучасному етапі підприємства України вимушені функціонувати в складних та непередбачуваних умовах нестабільності, які є генераторами проблем, що перешкоджають гармонійному та динамічному їх розвитку. Саме наявність проблем, що формують множину загроз розвитку вітчизняним підприємствам, підтверджує необхідність приділення підвищеної уваги принципам забезпечення їх економічної безпеки.

Перш ніж переходити до безпосереднього вивчення принципів забезпечення економічної безпеки підприємств, треба, насамперед, зупинити свою увагу на дослідженні понять «безпека» та «безпечне функціонування» та розмаїття поглядів та думок науковців щодо їх змісту.

З філософського погляду безпечне функціонування є проявом однієї з характеристик стану руху матеріальної субстанції, серед форм руху якої реалізуються лише стійкі форми, а нестійкі швидко руйнуються внаслідок внутрішніх і зовнішніх впливів.

У тлумачному словнику української мови поняття «безпека» визначається як стан, коли кому або чому-небудь ніщо не загрожує [1]. За визначенням В. Даля, поняття «безпека» має трактуватися як стан, властивість за прикметником «безпечний» і одночасно – дію. Безпечний – означає незагрозливий, той, що не може заподіяти зла чи шкоди, нешкідливий, збережений, вірний, надійний. Безпека – це відсутність небезпеки, збереженість, надійність. Небезпека – стан, властивість за прикметником «небезпечний». Небезпечний – означає ненадійний, загрозливий, той, що завдає шкоду, біду, хворобу, нещастя. «Небезпека» і «безпека» характеризують якість, властивість або стан [2]. Енциклопедичний словник І. Брокгауза та І. Ефрона містить характеристики понять «небезпека» і «безпека», в якому стверджується, що безпека досягається усуненням небезпеки, тобто стан із повною відсутністю небезпеки [3]. Юридична енциклопедія поняття «безпека» визначає як стан захищеності життєво важливих інтересів особи, суспільства і держави від зовнішньої і внутрішньої

загрози [4].

Зважаючи на розглянуті визначення, можна запропонувати принципи забезпечення економічної безпеки, які б узгоджувалися зі змістом безпеки та безпечного функціонування підприємства.

На нашу думку, можна виокремити три групи основних принципів забезпечення економічної безпеки підприємства:

1. Загальні (пов'язані з усіма характеристиками економічної безпеки): комплексність (повнота аналізу стану підприємства та загроз його функціонуванню для підвищення здатності долати загрози, забезпечуючи стійкість до них, та захищати власні інтереси, сприяючи розвитку); системність (забезпечення економічної безпеки потребує побудови механізму, що являє собою систему взаємопов'язаних елементів, спрямованих на формування захисних реакцій підприємства щодо впливу загроз та сприяє отриманню потрібних результатів); компетентність (забезпечення економічної безпеки потребує певних знань та уміння їх застосовувати).

2. Функціональні (пов'язані з функціональними характеристиками економічної безпеки): альтернативність (розгляд різних варіантів дій, спрямованих на захист інтересів, подолання загроз та забезпечення стійкості до них); законність (дії, спрямовані на захист інтересів, подолання загроз та забезпечення стійкості до них мають розроблятися з врахуванням обмежень, продиктованих законодавством); прийнятність ризику (виявлення і реалізація доступних заходів щодо нівелювання негативного впливу загроз); своєчасність (заходи щодо забезпечення економічної безпеки мають розроблятися та реалізовуватися вчасно); адекватність (заходи щодо забезпечення економічної безпеки мають відповідати ситуації, що склалась); превентивність (в процесі забезпечення економічної безпеки має надаватися перевага попередженню впливу загроз).

3. Результативні (пов'язані з результативними характеристиками економічної безпеки); оптимальність (досягнення під час забезпечення економічної безпеки найкращих результатів з врахуванням умов, що склалися); інтегрованість (підпорядкованість мети забезпечення економічної безпеки головній меті функціонування підприємства); збалансованість (досягнення результатів, які забезпечують баланс інтересів суб'єктів, що функціонують в економіці).

Отже, дотримання цих принципів дасть змогу підвищити результативність забезпечення економічної безпеки підприємства.

Бібліографічні посилання

1. Великий тлумачний словник сучасної української мови / керівники проекту: П. М. Мовчан, В. В. Німчук, В. Й. Клічак ; Ін-т укр. мови НАН України, Ін-т мовознавства НАН України, Всеукр. т-во «Просвіта» ім. Т. Шевченка. Київ : Дніпро, 2009. 1332 с.
2. Економічна безпека в умовах глобалізації світової економіки. Дніпропетровськ :

«ФОП Дробязко С. І.», 2014. Т. 2. 349 с. URL: http://ecofin.at.ua/monografy/monografija_ehb_t2.pdf
3. Качала Т. М. Сутність економічної безпеки як основи сталого розвитку економічної системи. *Сучасні перспективи розвитку системи економічної безпеки держави та суб'єктів господарювання* : монографія за ред. проф. Мігус І. П. Черкаси : ТОВ «Макалут». Черкаси, 2012. С. 27–39.
4. Велика українська юридична енциклопедія. Харків: Право, 2018. С. 52-53.

Братішко Н. А.,
студентка 3-го курсу юридичного
факультету Дніпропетровського
державного університету
внутрішніх справ
Науковий керівник – Тютченко С. М.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

На сьогодні в усіх розвинених країнах велика увага приділяється інформатизації суспільства. Держави, які будуть володіти потужними інформаційними ресурсами та ефективною системою їх реалізації, опиняться на вершині науково-технічного прогресу.

Можна побачити, що зараз стає все більш нових технологій та засобів інформатизації. Не відстає від цих процесів і Україна, в якій також відбувається впровадження сучасних технологій майже в усі сфери життєдіяльності, зокрема в правоохоронні органи. Створюються та використовуються різні інформаційно-пошукові системи, бази та банки даних. За допомогою цих інформаційних ресурсів правоохоронні органи мають змогу одержати багатоцільову, довідкову та статистичну інформацію, адже це сприяє ефективному виконанню ними різноманітних оперативно-службових завдань.

Отже, інформаційне забезпечення органів Національної поліції – це комплекс методів, заходів та засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення завдань. Інформаційні підсистеми як складові інформаційного забезпечення призначені для збирання, накопичення, зберігання та обробки інформації з певних напрямів обліків і

орієнтовані на використання в діяльності більшості правоохоронних структур [1, с. 396].

Застосування інформаційних технологій є головним чинником зміцнення законності, забезпечення стабільності та розвитку демократичних засад в управлінні державою. Органи поліції у своїй роботі використовують інформацію, пов'язану з відомостями про стан публічного порядку і рівня злочинності на певній території. Службовці внаслідок своєї діяльності накопичують величезні бази даних оперативно-довідкового й оперативно-розшукового призначення. Відповідно в цих базах містяться відомості, які стосуються обліково-реєстраційних даних громадян, правопорушень і кримінальних подій, викрадених і вилучених речей, а також предметів антикваріату, власників транспортних засобів тощо.

Інформація, яка здобувається і використовується Національною поліцією, повинна бути упорядкована, і тому впровадили автоматизовану інформаційну систему. За допомогою цієї системи співробітники інформаційних служб мають змогу упорядкувати обсяг інформації, з якою доведеться працювати органам внутрішніх справ, і змогу постійно поповнювати її новою та видаляти застарілі відомості [2, с. 50].

Головним органом, на якого покладено функції з формування інформаційних ресурсів Національної поліції, є Департамент інформаційно-аналітичного забезпечення МВС. Цей підрозділ є структурним підрозділом апарату МВС, і тому головне призначення полягає у розробці та впровадженні інформаційних технологій в діяльність органів внутрішніх справ.

Наказом Національної поліції України від 30 грудня 2015 р. № 228 створено Департамент інформаційної підтримки та координації поліції (ДІПКП) «102» Національної поліції України, який організовує та здійснює передбачені законодавством України заходи, спрямовані на інформаційно-аналітичне та інформаційно-пошукове забезпечення правоохоронної діяльності й захист персональних даних під час їх обробки у структурних підрозділах апарату Національної поліції України. ДІПКП визначає основні напрями діяльності поліції у сфері інформатизації, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, бере участь у розроблені проєктів нормативно-правових актів МВС з питань, що належать до компетенції поліції та стосуються інформаційно-аналітичного забезпечення, а також обробки персональних даних в органах і підрозділах поліції [3].

Також треба зазначити, що правоохоронні органи мають вже чималі навики з використання різних інформаційних та інформаційно-телекомунікаційних систем. Департаментом інформаційно-аналітичного забезпечення створюються та постійно удосконалюються системи інформаційного забезпечення [4, с. 204].

Отже, підсумовуючи вищевикладене, можна сказати, що в Національній поліції активно ведеться діяльність стосовно розвитку

інформаційного забезпечення, впроваджуються нові підсистеми та здійснюється поповнення автоматизованих банків даних, за допомогою яких забезпечується належне функціонування всієї системи.

Бібліографічні посилання

1. Варенко В. М. Інформаційно-аналітична діяльність : навч. посіб. К.Університет «Україна», 2014. 417 с. URL: https://divovo.in.ua/pars_docs/refs/5/4448/4448.pdf
2. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі : зб. наукових статей за матеріалами доповідей Всеукр. науково-практ. конф. 23 грудня 2016 р. Львів : ЛьвДУВС, 2017. 313 с. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/konf_23.12.16_zbirnuk.pdf
3. Департамент інформаційної підтримки та координації поліції «102» Національної поліції України. URL: http://www.npu.gov.ua/ uk/publish/article/1820541.
4. Хахановський В. Г., Тебякін О. М. Інформаційне забезпечення правоохоронних органів : навч.-метод. комплекс (слідча спеціалізація). Київ : НАВСУ, 2004. 640 с.

Булдакова А. Є.,
курсант 2-го курсу факультету
підготовки фахівців для органів
досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРОБЛЕМИ ВИКОРИСТАННЯ ТЕХНІЧНИХ ЗАСОБІВ ПРАЦІВНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Одним з основних завдань Національної поліції є забезпечення публічної безпеки та порядку і для його виконання поліція уповноважена застосовувати превентивні заходи. Згідно зі ст. 31 Закону України «Про Національну поліцію» одним з таких заходів є застосування технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису. Застосування нагрудної камери (відеореєстратора) поліцейського або автомобільного відеореєстратора вкорінилося в наше життя і не є незвичайним. Та попри те, що нашому часу властивий науково-технічний прогрес, в Україні застосування сучасних технічних засобів не актуальним і є нагальною проблемою сьогодення.

Застосування органами, підрозділами поліції технічних приладів і технічних засобів, що мають функції автоматичної фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису, регулює «Інструкція із

застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису». Там передбачені такі технічні засоби, як автомобільна система технічних приладів, портативного відеореєстратора, стаціонарна система технічних приладів і технічних засобів фото- і кінозйомки, відеозапису, а також безпілотний літальний апарат [1]. Проте, якщо провести соціальне опитування, навряд хоч одна людина відповість, що колись бачила застосування поліцейського дрона.

Водночас у 2020 році регулярне використання поліцейських дронів стало нормою в багатьох містах США. Офіцери можуть зосередитися на забезпеченні безпеки спільноти за допомогою технології дронів, а інтеграція забезпечує легкий збір даних і автоматичне звітування. Федеральне дотримання вимог, звітність, сповіщення про технічне обслуговування та реєстрація – це трудомісткі завдання, і AirData керує цими завданнями у фоновому режимі, дозволяючи відділам поліції зосередитися на безпеці громади [2].

В Японії дрони настільки поширене явище, що виникла потреба регулювати їх. Центральний поліцейський департамент Токіо ухвалив рішення використовувати безпілотники, оснащені сітками, для перехоплення дронів, які літають над режимними об'єктами без відповідного дозволу [3].

А Китай є світовим лідером у технологіях й розробляє такі технічні засоби, застосування яких в діяльності Національної поліції українцям складно уявити. Китайська поліція почала використовувати сонцезахисні окуляри, оснащені спеціальною технологією розпізнавання облич, для ідентифікації підозрюваних. Окуляри підключені до внутрішньої бази даних, а це означає, що поліція може швидко сканувати натовп під час пошуку втікачів. Ця технологія дозволяє поліції фотографувати підозрюваних, а потім порівнювати їх із фотографіями, що зберігаються у внутрішній базі даних. Якщо воно збігається, то посадовій особі буде надіслано інформацію про ім'я та адресу особи [4].

В 2021 році в службу управління авіації та поліції на воді було поставлено понад 30 нових БпЛА. Завдяки цьому в Національній поліції виникла змога більш ефективно проводити спеціальні операції під час супроводження шляхом проведення повітряної рекогносцировки, а також більш продуктивно здійснювати пошук зниклих осіб. Зараз з фахівцями безпілотних літальних апаратів проводяться навчально-тренувальні збори. Перший крок було зроблено, проте цього замало для значного поліпшення рівня виконання поліцейськими їх професійних обов'язків [5].

Ми можемо зробити висновок, що впровадження новітніх технологій мультиспектрального аналізу та 3D-моделювання суттєво поліпшить виявлення, документування, попередження та фіксацію кримінальних правопорушень, охорону громадської безпеки та власності, а також слугуватиме джерелом інформації під час здійснення досудового

розслідування. Тому використання технічних засобів є необхідним для належного виконання покладених на поліцію повноважень, ефективного забезпечення публічної безпеки та порядку та протидії злочинності.

Бібліографічні посилання

1. Інструкція із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису. URL: https://zakon.rada.gov.ua/laws/show/z0028-19#Text (дата звернення: 23.10.2021).
2. Chula Vista PD Drone Program Uses AirData to Provide Full Transparency to Community. URL: https://www.google.com/amp/s/dronelife.com/2021/10/07/chula-vista-pd-drone-program-uses-airdata-to-provide-full-transparency-to-community/amp/ (дата звернення: 23.10.2021).
3. У Японії з'являться дрони-поліцейські. URL: https://ishop.if.ua/novyny/u-yaponiyi-zyavlyatsya-drony-policeyski (дата звернення: 23.10.2021).
4. Китайська поліція знаходить підозрюваних через окуляри. URL: https://www.google.com/amp/s/www.bbc.com/ukrainian/news-42979942.amp (дата звернення: 23.10.2021).
5. Національна поліція отримала понад 30 нових БПЛА. URL: https://defence-ua.com/news/natsionalna_politsija_otrimala_ponad_30_novih_bpla_foto-2537.html (дата звернення: 23.10.2021).

Волкова А. В., курсант 2-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ФІШИНГ – ОСНОВА КІБЕРАТАК

Проблема фішингу з кожним роком стає все більш поширеною. Фішинг – це атака, заснована на соціальній інженерії, яка проводиться через недоліки кібербезпеки для обману користувачів з метою крадіжки їх логінів, паролів і грошей [1].

Основною метою фішингу є отримання цінних даних, які можуть бути продані або використані зловмисником для здійснення заборонених дій проти майна людини, таких як вимагання, викрадення грошей або особистих даних. Фішинг існує впродовж багатьох років, за цей проміжок часу кіберзлочинці розробили достатній спектр методів інфікування жертв. Зловмисники, які займаються фішингом, найчастіше представляються

працівниками банків чи інших фінансових установ для того, аби змусити жертву фішингу заповнити фальшиву форму та отримати дані її облікових записів. Крадіжка інформації, тобто фішинг – поширена проблема, яка здійснюється шляхом розсилки спаму або підроблених електронних листів. Цей тип атаки припускає отримання користувачем шахрайського листа, що містить посилання на шкідливий вебсайт, який призначений для збору інформації та особистих даних користувача.

Відповідно до статистики в Україні протягом червня 2021 року на інформаційні ресурси державних органів було скоєно понад 50 тисяч кібератак, які своєчасно та успішно були усунені. Система захищеного доступу державних органів до мережі «Інтернет» заблокувала 50 571 атаку різних видів, що на 17 % більше, ніж попередні рази. У системі реагування на кіберінциденти та кібератаки на об'єктах моніторингу зафіксовано 1 177 118 підозрілих подій, а саме: отримання прав користувача – 49 %; спроби отримання прав адміністратора – 22 %; підозріле застосування кодів та нестандартних протоколів – 8 %. А основна кількість інцидентів стосується саме поширення шкідливого програмного забезпечення – 74 %, а також фішингу – 25 %.

В останні роки фішингові сайти стали великою проблемою. Є безліч методів розпізнавання фішингових сайтів, але внаслідок постійного розвитку виду цього шахрайства, зробити це буває складно. Для того щоб не зіткнутися з фішингом, важливо дотримуватися певних правил: користуватися лише перевіреними та захищеними офіційними сайтами, платіжними сервісами; увійшовши на невідомий сайт, з незнайомим іменем – не вводити конфіденційну інформацію в наведені поля; перебуваючи на банківських сайтах, важливо стежити, щоб було встановлено захищене з'єднання HTTPS, для того аби була можливість перевірити відповідність сертифікату HTTPS та захищеність сайту від кібератак.

Отже, дуже часто бувають ситуації, коли на пошту або в особисте повідомлення надходять дивні посилання, які складно ідентифікувати, важливо ніколи не переходити за посиланнями, тому що саме такі повідомлення надсилають злочинці під час використання методів поширення вірусів, фішингових сайтів. Якщо таке посилання надійшло від друга, варто переконатися у тому, що воно не становить загрози вашим персональним даним, бо у наш час є багато схем зламування облікових записів і надсилання шахрайських розсилок, про які ніхто і не здогадується. Боротися з фішингом дуже легко, якщо підвищувати власну грамотність: приділяти увагу деталям та намагатися зберегти приватні дані, паролі та іншу важливу інформацію від посягань кіберзлочинців.

Бібліографічні посилання

1. Кіберзлочинність в Україні: вебсайт. URL:
2. https://www.science-community.org/ru/node/%2016132
3. Здійснення кібератак на державні інформаційні ресурси: вебсайт. URL: https://www.google.com/amp/s/ua.interfax.com.ua/news/telecom/750914-amp.html

Волчок Є. В.,
здобувач 2-го курсу магістратури
Одеського державного
університету внутрішніх справ,
співробітник відділу security analyst
ТОВ «Група інформаційної безпеки
«ФС ГРУП», м. Одеса

Науковий керівник – Ісмайлов К. Ю.,
старший науковий співробітник НДЛ
з проблемних питань кримінального
аналізу Одеського державного
університету внутрішніх справ,
начальник 5-го відділу 3-го управління
ДКП НПУ, кандидат юридичних наук,
доцент, підполковник поліції

ЕКСПЛУАТАЦІЯ ВРАЗЛИВОСТЕЙ В МОБІЛЬНІЙ КРИМІНАЛІСТИЦІ IOS-ПРИСТРОЇВ

Внаслідок розвитку інформаційних технологій та різноманітної електронно-обчислювальної техніки, таких як комп'ютери, ноутбуки, мобільні телекомунікаційні пристрої, з'являються нові методи та заходи захисту інформації від несанкціонованої передачі та витоку її.

В багатьох пристроях як первинний захист використовується метод шифрування накопичувача різними засобами: як запроваджений розробником операційної системи (Google або Apple, якщо ми говоримо про мобільні пристрої), так і безпосередньо виробниками пристроїв.

В нашому випадку мова буде йти безпосередньо про витяг і подальший криміналістичний аналіз отриманої інформації з Apple пристроїв на основі операційної системи iOS (iPhone, iPod) та iPadOS (iPad), їх методи захисту Secure Enclave Protection (TouchID, FaceID), DAP та їх можливі вразливості як апаратного, так і програмного характеру. Оскільки пристрої виробництва Apple досить поширені серед населення (приблизно 30–40 % від загальної кількості смартфонів на території України), тому має сенс звернути увагу саме на цей прошарок, адже на сьогодні є багато методів щодо отримання інформації з пристроїв на операційній системі Android (як апаратними методами, так і за допомогою програмних властивостей безпосередньо від розробників цих самих пристроїв або операційної системи). Наприклад, компанія Samsung розробила власну систему захисту даних Knox, але навіть вона беззахисна в деяких випадках. Нижче наведені порівняльні таблиці 1 і 2 з кількістю знайдених вразливостей на Android та iOS за весь час [1, 2]:

Таблиця 1

Кількість знайдених вразливостей в Android

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Bypass something	Gain Information	Gain Privileges	# of exploits
2009	5	3							1			
2010	1	1	1									
2011	9	1	1		1		1		4	1	3	
2012	7	5	3	2						1		1
2013	4		1	1	1				1	1	1	
2014	12	2	4	1		1			1	2	1	1
2015	95	46	49	50	37				13	14	17	
2016	500	104	72	91	38				47	96	236	
2017	840	86	206	170	32			1	30	113	36	
2018	609	32	84	143	12	2	1	2	17	63	3	
2019	491	37	107	41	24	3		1	39	22	1	
2020	859	46	97	104	27	9		5	148	97	3	
2021	394	17	44	35	33	2		3	40	10	6	
Total	3826	380	669	638	205	17	2	12	341	420	307	2
% of all		9.9	17.5	16.7	5.4	0.4	0.1	0.3	8.9	11.0	8.0	

Отже, метою нашого дослідження є використання різноманітних програмних та апаратно-програмних методів і способів для можливості отримання інформації з пристроїв Apple для проведення оперативно-розшукових заходів та проведення криміналістичного аналізу отриманої інформації. А саме приклад буде наведений на основі застосування мініатюрного комп'ютера Raspberry Pi 4 [2].

Цей пристрій завдяки розміру, форм-фактору та автономності дозволяє зручно переносити буквально в кишені і використовувати його під час проведення слідчих дій, виїзду до місця скоєння правопорушення, або під час затримання підозрюваного суб'єкта без застосування ПК, ноутбука або іншого типу ЕОМ.

Таблиця 2

Кількість знайдених вразливостей в iOS

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Bypass something	Gain Information	Gain Privileges	# of exploits
2007	1		1	1								
2008	1	1	1									
2009	10	2	3	2	2				2	3		
2010	20	11	9	5	3				4	2	1	
2011	83	52	7	6	6		5		7	13	1	
2012	155	114	70	67	60		8		15	9	1	
2013	95	57	50	42	46		4		17	9	1	
2014	120	50	51	35	33			1	20	24	4	
2015	386	232	211	184	191			5	44	63	13	1
2016	168	113	79	81	81		3		8	42	11	
2017	388	241	222	210	194		14		39	63	5	
2018	125	63	63	55	50		1		19	19	2	
2019	354	9	101	101	167	2	14			26	5	
2020	305	17	141	57	60		8	2	6	13	5	
2021	244	14	118	22	26		5	3	7	6	7	
Total	2455	976	1127	868	919	2	62	11	188	292	56	1
% of all		39.8	45.9	35.4	37.4	0.1	2.5	0.4	7.7	11.9	2.3	0.0

На сьогодні для експлуатації цього методу підтримуються пристрої, які мають апаратну вразливість checkm8, виявлену у вересні 2019 року [3], а саме від моделі Apple iPhone 5S до iPhone X з декількома застереженнями. Етапи отримання інформації з досліджуваного пристрою:

1. Для початку роботи необхідно на пристрій Raspberry Pi встановити та налаштовати операційну систему зі скриптами, підключити зовнішнє джерело живлення або power bank (підзарядник) та Lightning-кабель для підключення Apple пристроїв.
2. Досліджуваний пристрій попередньо необхідно перевести у режим DFU (Device Firmware Upgrade).
3. І залишається тільки підключити до пристрою Raspberry Pi, після

чого буде запущений автоматизований процес експлуатації вразливості checkm8 та збір усієї можливо доступної інформації з пристрою.

Оскільки більша частина інформації знаходиться у зашифрованій області пам'яті та оберігається в тому числі засобами SEP (Secure Enclave Protection), а сам засіб на цей час в стадії PoC (Proof of Concept), можна отримати лише не зашифровану інформацію, яка доступна в стані BFU (Before First Unlock).

Отже, за допомогою цього методу можна автоматизовано отримати таку інформацію:

– дані про Wi-Fi мережі, до яких підключався пристрій + геопозиція по BSSID точок доступу;

– облікові записи на пристрої (iCloud, Apple ID, поштові скриньки, тощо);

– дані ОС (версія, номер збирання, інша технічна інформація);

– дані про встановлені раніше SIM (номер, ICCID);

– дані статусу функції «Екранного часу»;

– заблоковані (додані в чорний список) мобільні номери;

– облікові дані, які використовуються для входу в FaceTime, iMessage;

– дата та спосіб створення (хмара або локально на ПК) останнього бекапу, підключення до ПК (назва самого ПК і версія iOS пристрою).

Вся отримана інформація зберігається у вигляді архіву безпосередньо на накопичувачі MicroSD, з якої і виконується загрузка ОС, або на зовнішній USB накопичувач для більш зручного подальшого дослідження.

Надалі планується багато нововведень та доопрацювань для більшої автоматизації, структуризації і впровадження роботи з тимчасовими даними, додатків з динамічними GUID і, найголовніше, зі зв'язкою ключів (keychain-2.db).

Бібліографічні посилання

1. CVE Details. URL: https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224.
2. CVE Details. URL: https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49.
3. Шах и мат! Как устроен нашумевший эксплоит checkm8 и как им воспользоваться. URL: https://xakep.ru/2019/11/21/checkra1n.
4. Raspberry Pi 4 URL: https://www.raspberrypi.com/products/raspberry-pi-4-model-b.

Гнатко А. Р.,
слухач магістратури
Навчально-наукового інституту права
та кібербезпеки Одеського державного
університету внутрішніх справ

ПОДОЛАННЯ ОПОРУ ДО ПРОГРАМ АНАЛІЗУ ЗЛОЧИННОСТІ (огляд спеціальної літератури США)

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України та його реалізація буде здійснюватися шляхом посилення можливостей національної системи кібербезпеки з метою протидії кіберзагрозам у сучасному середовищі безпеки [1]. Відповідно до Закону України «Про національну безпеку» визначено об'єкти національної безпеки та основні завдання її забезпечення [3]. Тому будь-яка суспільна діяльність може досягнути поставленої мети, якщо вона належним чином доктринально визначена, скерована, організована та оптимально ресурсно забезпечена. Ці вимоги повною мірою стосуються діяльності щодо протидії та запобігання злочинності, яка є різновидом суспільної діяльності. Яскравим прикладом для України у цьому напрямі є досвід правоохоронних органів США [2].

Програми аналізу злочинності дають змогу керівникам поліції США об'єктивно визначити характер злочинної діяльності відповідно до своєї юрисдикції та розробити відповідні патрульні та тактичні плани дій для ефективної боротьби з нею. Водночас підрозділи аналізу злочинності можуть надавати інформацію, необхідну для того, щоб використовувати обмежені ресурси з їх найкращою вигодою. Отже, інформації для ознайомлення співробітників правоохоронних органів з роботою підрозділу аналізу злочинності мало. Мало хто з аналітиків злочинності може реалізувати програму аналізу злочинності, не зустрівши певного опору. Поліцейські розповідають людям, що їм робити цілий день, і, зазвичай, домагаються свого. Якщо поліцейські визначать, що когось збираються затримати або заарештувати, тоді вони це здійснюють. Офіцери не так довго звикають контролювати інших, що й самі стають стійкими до контролю. Вони приймуть контроль з боку керівників відомств та керівників (зазвичай), але рідко від когось іншого. Те, що це створює проблеми у їхніх міжособистісних стосунках, розуміють поліцейські психологи по всій країні США. Офіцери можуть бачити аналітика як ще одну людину, яка намагається контролювати їхні дії та вивести їх із зони комфорту. Спочатку програму можна сприймати як інструменти, які департамент використовуватиме для «виправлення того, що не зламалося». Заради власної самооцінки усвідомте, що ця взаємодія особистої динаміки створює опір програмам. Чекайте цього,

готуйтесь до цього і не сприймайте це особисто. Будьте собою. Навчіться у офіцерів, надайте їм те, що вони хочуть і потребують, і з часом ви отримаєте бажане прийняття. Можна було б подумати, що будь-яка програма, яка могла б надати правоохоронцям підозрілу інформацію, точне знання про те, коли і де відбуваються злочини, а також підвищену здатність ідентифікувати, затримувати та успішно притягати до відповідальності злочинців, була б позитивно сприйнята. Чому люди можуть бути стійкими до цього? Через помилкові уявлення, які вони можуть мати щодо програми. Ці хибні уявлення, разом із стратегіями, які можуть бути використані для подолання опору, який вони викликають, зазначаються нижче, а саме:

Комп'ютери замінять нас усіх. Сьогодні комп'ютери впроваджуються в різноманітні галузі людської діяльності. Усі найважливіші функції сучасного суспільства, так чи інакше, пов'язані з комп'ютерами, комп'ютерними мережами і комп'ютерною інформацією. Більшість державних органів отримали значні переваги від автоматизації. Впровадження програми аналізу злочинності часто служить поштовхом до комп'ютеризації правоохоронних органів; як наслідок, деякі люди бояться втратити роботу. Як правило, єдине, що сталося, це те, що люди були звільнені для виконання інших завдань. Автоматизація служить для створення робочих місць у багатьох агентствах. Занепокоєння виявляється таким чином: «Ви чули, що департамент збирається придбати один із цих чудових нових комп'ютерів? Я маю на увазі, ви ніколи не бачили такого великого комп'ютера. Він замінить нас усіх! Бюро документації буде справою минулого. Навіть друкарки та діловоди втратять роботу! Нічого цього не було б, якби ми не долучилися до цієї нової програми аналізу злочинності».

Стратегії подолання опору: 1. Підготуйте оцінку потреб, щоб визначити, чи обґрунтовано придбання автоматизованої системи обробки даних. Якщо так, зверніться до наступної стратегії. 2. Визначте, скільки людей необхідно і скільки часу зараз витрачається на обробку даних. Визначте персонал та економію часу завдяки автоматизації. 3. Автоматизована система допоможе людям, надаючи їм швидший доступ до інформації. Поясніть, що люди, які більше не потрібні для обробки даних, будуть надавати цінні послуги відділу, виконуючи інші обов'язки. 4. Визнайте та прийміть, що деяких людей лякають комп'ютери. Запропонуйте їм показати, як працює комп'ютер і що він робить для них. Дайте людям зрозуміти, що їм надається можливість розширити свої знання та навички, працюючи в середовищі, керованому комп'ютером. 5. Допомагайте персоналу розробляти комп'ютерні додатки для надання їм конкретної допомоги; покажіть їм, як використовувати різні пакети програмного забезпечення для створення власних файлів та програм [2].

Отже, досвід поліції США щодо подолання опору до програм аналізу злочинності є актуальним та своєчасним для підрозділів Національної поліції

України в процесі запровадження Стратегії кібербезпеки України.

Бібліографічні посилання

1. Президент утвердил новую Стратегию кибербезопасности Украины. URL: https://www.ukrinform.ru/rubric-polytics/3304776-prezident-utverdil-novuu-strategiu-kiberbezopasnosti-ukrainy.html
2. Steven Gottlieb and Shel Arenberg (1992).Crime Analysis: From Concept to Reality. Retrieved from: URL: https://www.ojp.gov/pdffiles1/Digitization/137374NCJRS.pdf
3. Дороганов Е. А., Рудой К. М. Система безопасной передачи информации транспортными каналами связи мобильных станций. *Кібербезпека в сучасному світі: актуальні виклики* : Всеукр. науково-практ. конф. (29 листопада 2019 р., НУ «Одеська юридична академія»). Одеса, 2019. С. 119–121.

Голубєва Д. В.,
курсантка 2-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
(Дніпропетровський державний університет внутрішніх справ)

«ГРУПИ СМЕРТІ»: ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЇЇ ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНИМИ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Під впливом глобалізації інтернет і активний розвиток інформаційних технологій сьогодні є невід'ємною складовою сучасного суспільства, зокрема покоління Z. Життя юнаків та підлітків у XXI столітті постійно супроводжується використанням мережі «Інтернет» під час навчання чи на дозвіллі. Незважаючи на позитивну результативність, у технологічному прогресі також наявні й негативні наслідки. Новостворені проблеми, викликані інформатизацією суспільства, потребують їх глибокого вивчення та дослідження, пошуку шляхів їх усунення і правового регулювання.

Останнім часом в Україні доволі актуальною і гострою поставала проблема розвитку та діяльності так званих «груп смерті» – спільнот в соціальних мережах, що мають на меті під видом гри вплинути на психіку малолітньої дитини чи підлітка та довести її до вчинення самогубства. Найвідомішими є такі «смертельні ігри», як: «Синій кит» (різновиди його назв – «Тихий дім», «Море китів», «F57»), «Червона сова», «Біжи або помри» та інші. Пік їхньої популярності припав на кінець 2016 – початок 2017 років,

що в той час утворило моду на «кіберсуїцид». Як можна дізнатися зі ЗМІ, «групи смерті» беруть свій початок із Росії, а тому головним середовищем діяльності цих груп була соціальна мережа «Вконтакте», де також навіть створювались пабліки, тематика яких була сторінки померлих людей, зокрема тих, які покінчили з життям самостійно (від «смертельних ігор» у тому числі).

У лютому 2018 року було ухвалено Закон України «Про внесення зміни до статті 120 Кримінального кодексу України щодо встановлення кримінальної відповідальності за сприяння вчиненню самогубства»: у диспозиції статті йдеться про встановлення відповідальності не лише за доведення особи до самогубства або до замаху на нього, а й за схиляння та сприяння його вчинення [1].

Станом на 25 квітня 2017 року українська кіберполіція виявила 926 «груп смерті», 600 з яких – піддалися блокуванню. Крім того, органами поліції було відкрито приблизно 35 кримінальних проваджень і попереджено більше 10 випадків суїциду серед неповнолітніх, з яких встановлено 4 факти самогубства, що були безпосередньо пов'язані з квестами «смертельних ігор». За статистичними даними, кількість «записів», що ідентифікувалися як зареєстровані на території України, становила 34 970 [2].

Певною мірою діяльність таких груп є формою кіберзлочину. Більша кількість постраждалих від кіберзлочинців не повідомляє про це правоохоронним органам, залишаючи такі злочини латентними. Причинами цього постають необізнаність громадян щодо механізму повідомлення такої інформації, люди ніби соромляться того, що вони стали жертвами кіберзлочинців, корпорації переймаються про свою репутацію. Але найголовнішою причиною замовчування таких випадків є сумніви щодо можливостей правоохоронних органів, що, насправді, є виправданим, адже традиційні методи розслідування злочинів у технологічній сфері швидко застарівають у зв'язку з її стрімким розвитком [3].

Кіберзлочини належать до злочинів високого інтелектуального рівня, а тому для ефективності стратегії боротьби з ними необхідна методологічна та науково-технічна підготовленість фахівців [3]. Зараз в оперативних підрозділах кіберполіції Національної поліції України відбуваються численні дослідження вищезгаданих явищ, впроваджуються новітні методики викриття таких злочинів та заходи щодо їх застереженню, а також створюється і активно доповнюється і по цей час відповідна законодавча база у вигляді Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року.

Бібліографічні посилання

1. Лубенець І. Г., Толочко Г. В. Особливості вітчизняного та іноземного законодавства щодо відповідальності за доведення до самогубства. URL : http://elar.naiau.kiev.ua/bitstream/123456789/15220/1/%D0%97%D0%91I%D0%A0%D0%9D%D0%98%D0%9A_2019_p107-109.pdf.

2. Лугіна Н. А., Ошийко М. А. «Групи смерті» в Україні: їх сутність та перспективи запобігання. *Журнал східноєвропейського права*. 2020. № 73. С. 85–90. URL: http://ir.nusta.edu.ua/bitstream/123456789/4757/1/4510_IR.pdf.
3. Неня О. В. Проблеми та перспективи розслідування кіберзлочинів. URL: https://web.mvs.gov.ua/files/pdf/Zbirka_Den_Nauky_2018.pdf#page=121.
4. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Добош В. В., курсант 3-го курсу
факультету підготовки фахівців
для підрозділів стратегічних розслідувань
Науковий керівник –Неклеса О. В.,
викладач кафедри фінансових
та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ

ЗНАЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

У сучасному світі фінансовій безпеці повинна приділятися особлива увага, оскільки її значенням для економіки держави не треба нехтувати. Необхідно зазначити, що будь-які проблеми, що тим чи іншим шляхом торкаються фінансової безпеки, безпосередньо впливають й на економічну безпеку держави загалом.

Необхідно розуміти, що всі аспекти національної безпеки так чи інакше однаково пов’язані з її фінансовою безпекою. Яскравим підтвердженням цього висловлювання може стати так звана ланцюгова реакція. У разі відсутності фінансів це призведе до нестачі коштів на різні сфери життя – економічну, соціальну та інші, що зі свого боку призведе до загрози національній безпеці [1].

Тож розуміємо, що на сьогодні ми повинні використовувати такі шляхи вдосконалення фінансової безпеки України, як: встановлення меж іноземної участі в капіталі вітчизняних організацій; галузеві обмеження; заходи щодо компаній, що здійснюють обмежувальну ділову політику, що спотворює умови конкуренції; вимоги у сфері виробництва, використання місцевих компонентів, передачі технологій тощо; розробка дієвих систем контролю залучення і використання коштів іноземних запозичень [2].

Своєрідним відображенням безпеки фінансової системи країни як сукупності видів фінансових відносин є індекс фінансового стресу в країні, динаміку змін якого варто відстежувати, намагаючись прогнозувати

фінансові перспективи розвитку як країни, так і підприємств. Наприклад, Україна протягом останніх дванадцяти років не один раз перебувала у стані достатньо гострого фінансового стресу, що безумовно негативно впливало на фінансову стійкість та фінансове забезпечення у процесі ведення господарської діяльності багатьох українських підприємств.

Проаналізувавши цю динаміку, ми можемо стверджувати, що на сьогодні Україна повинна укріплювати свою фінансову безпеку, саме тому вона повинна здійснити такі дії, а саме:

1. Реформувати підхід до бюджетного процесу на місцевому, державному, а також на рівні міжбюджетних відносин.
2. Створити стратегію скорочення бюджетного дефіциту, а також стратегію накопичення власного капіталу.
3. Погасити довгострокові запозичення сектора економіки, а також зменшення кількості зовнішнього боргу держави.
4. Розробити та запровадити зростання державної економіки за допомогою виваженої грошово-кредитної політики.
5. Стабілізувати національну грошову одиницю, а також розробити стратегію зниження рівня інфляції.
6. Зменшити кількість капіталу, що вивозиться за кордон за допомогою створення сприятливих умов для репатріації вивезеного капіталу.

Виконавши запропоновані вище вимоги, наша країна не лише поліпшить своє економічне становище, також вона зможе стабілізувати економіку, що зменшить ризики економічної кризи в державі. Ці вимоги щодо стабілізації економіки нашої держави також будуть відігравати вагомий внесок на розвиток в цілому. Як ми вже зазначали вище, будь-яка структура держави прямо залежить від фінансової безпеки, а отже, поліпшивши цей показник, ми допоможемо нашій державі зробити крок на шляху до розвитку.

Зважаючи на це, ми розуміємо, що фінансова безпека України є важливим компонентом загальнодержавної безпеки й її вплив на економіку просто колосальний. Отже, ми повинні реформувати сучасний підхід до фінансової безпеки нашої держави, що у подальшому допоможе нам впевненіше себе почувати на міжнародній арені, а також зменшить ризики фінансових криз.

Бібліографічні посилання

1. Смоквіна Г. А. Фінансова безпека як стратегічна складова економічної безпеки України. *Економіка: реалії часу*. 2014. Вип. 3. С. 30–36. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=econrch_2014_3_6/

2. Вашай Ю. В. Шляхи підвищення рівня фінансової безпеки України на сучасному етапі. *Галицький економічний вісник*. 2012. Вип. 6. С. 137–144. URL : http://elartu.tntu.edu.ua/handle/123456789/2287/

Дроговоз С. Є.,
курсант 2-го курсу
факультету підготовки
фахівців для підрозділів
превентивної діяльності
Науковий керівник – Рижков Е. В.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ
кандидат юридичних наук, професор

ПОЗИТИВНІ ТА НЕГАТИВНІ АСПЕКТИ ВИКОРИСТАННЯ В ДІЯЛЬНОСТІ ПАТРУЛЬНОЇ ПОЛІЦІЇ СИСТЕМИ «ЦУНАМІ»

На сучасному етапі розвитку людства найбільшу цінність становлять цінність людини як особистості, її життя та здоров'я, однією з таких важливих цінностей є інформація, в тому числі особисті дані та відомості про людей. У XXI столітті, крім великої ваги та значення інформації в житті суспільства, є її захист від загроз, витоку тощо, що належить до однієї з найголовніших функцій держави, адже без кругообігу інформації неможлива робота майже всіх як державних, органів так і юридичних осіб. Взагалі захистом інформації є сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [1].

Важливим суб'єктом, який безпосередньо працює з інформацією, відомостями, даними громадян та який бере участь у запобіганні її загальному поширенню та неправомірному витоку, є Національна поліція України. Крім того, інформація є одним з найважливіших засобів, який використовують поліцейські для забезпечення прав та свобод людини, запобіганню та припиненню правопорушень, підтриманню громадського порядку. Для більш ефективної реалізації повноважень, покладених на поліцейських, відповідно до ст. 23 Закону України «Про Національну поліцію України» [2], а також для оптимізації роботи поліцейських в діяльність патрульної поліції, яка безпосередньо стикається з правопорушеннями та першою прибуває на місця події, було запроваджено так звану систему централізованого управління нарядами патрульної поліції «ЦУНАМІ».

Для початку необхідно з'ясувати поняття зазначеної системи. Отже, «ЦУНАМІ» – це система, так званий комплекс апаратних та програмних засобів, а також особового складу, який призначений для управління та

розподілення сил Національної поліції України. Основне призначення цієї системи полягає у скороченні часу на реагування повідомлень та звернень громадян про різноманітні правопорушення, також для зручності та підвищення швидкості роботи поліцейських, підвищення швидкості передачі відомостей про своєчасність та результати реагування патрулю на правопорушення під час безпосереднього виконання службових обов'язків. Загалом можемо зробити висновок, що основний задум, мета реалізації цієї системи була досягнута. Адже навантаження на гарячу лінію «102» на добу є просто неймовірним – 3000 викликів та повідомлень на добу, а загальний потік інформації на один пульт оператора лінії «102» становить 280 звернень на добу. При цьому час на прийом звернення набагато скоротився, зараз оператори приймають виклик та з'ясовують подробиці про події адміністративних, кримінальних та інших правопорушень лише протягом 2 хвилин! Як бачимо, виконано неймовірно великий обсяг роботи щодо удосконалення роботи патрульних поліцейських, це стосується як навчання особового складу, так і встановлення відповідного технічного забезпечення поліцейських, а саме кожен екіпаж патруля оснащений так званим мобільною логістичною підсистемою LIS-N (Logistic Information System – M) на планшеті. Ця підсистема надає можливість дистанційно здійснювати обмін необхідною інформацією між диспетчером та патрулем, забезпечує доступ до баз даних відомчої інформаційної системи, патруль може складати електронні протоколи та друкувати квитанції на місці події.

Крім вже багатьох зазначених позитивних аспектів системи «ЦУНАМІ», існують деякі недоліки під час роботи з нею. Одним з таких є те, що операторами лінії «102» є звичайні цивільні особи, а не особовий склад Національної поліції України. Через те, що оператори цієї лінії проходять лише так звані курси тривалістю 2 місяці, не всі, але деякі з них, приходячи на роботу, не розуміють деяку специфіку в роботі поліцейського, оператори зазвичай виконують функцію психолога, основне завдання полягає в заспокоєнні заявника, переконанні залишитися на місці події та очікувати на приїзд патрульних поліцейських. Для того щоб точніше визначати характер обставин події й тактику поведінки поліцейських, почали впроваджувати так званих помічників диспетчерів, такими помічниками є найбільш підготовлені патрульні поліцейські, які допомагають диспетчерам правильно та точно надавати завдання патрулям.

Другим недоліком у функціонуванні «ЦУНАМІ» є встановлення зв'язку між оператором та екіпажем патрульної поліції, адже він забезпечується лише за допомогою звичайних SIM-карток мобільного оператора «Київстар». На перший погляд може здатися, що це не є недоліком, а навіть позитивною якістю, адже мобільні оператори зазвичай забезпечують так званий «найшвидший інтернет», легкість у передачі інформації. Однак ці плюси є доволі сумнівними, адже через перенавантаженість під час роботи мобільних операторів, особливо на великі

свята, інформація може передаватися набагато повільніше або не передаватися взагалі, а без вчасної передачі інформації між диспетчером та патрулем неможливе вчасне реагування на правопорушення. Зниження швидкості обміну інформацією відбувається через те, що звичайні мобільні оператори надають послуги в цьому разі як поліцейським, так і звичайним пересічним громадянам.

Наступним недоліком користування звичайними SIM-картками патрульними є те, що ці картки не мають високого рівня захищеності від витоку інформації, що дозволяє правопорушникам безперешкодно потрапляти до інформаційних баз даних Національної поліції України [3, с. 14–36].

Для вирішення цієї проблеми, на нашу думку, необхідно замість звичайної SIM-картки створити спеціальну SIM-картку з багатоступеневим рівнем захисту, яка б при цьому використовувалась лише в діяльності поліцейських.

Крім того, ще одним кроком до удосконалення користування системою «ЦУНАМІ» може стати використання принципу «My pole» – мобільного додатка, який кожен може встановити у своєму смартфоні та за допомогою одного натискання на екран (кнопки «SOS») викликати наряд поліції на місце події. Такий принцип виклику поліції застосовується з 2017 року у Дніпропетровській, Вінницькій, Закарпатській, Рівненській, Черкаській, Івано-Франківській областях [4, с. 165–168]. У аспекті розгляду нашої теми, можливо, доцільно було б створити подібний мобільний додаток зі спеціальним доступом. Тобто додаток, який би використовувався лише в діяльності поліції.

Підсумовуючи викладене, можемо запропонувати такий шлях вирішення проблем, які виникають у поліцейських під час роботи з системою «ЦУНАМІ»: здійснити оснащення патрулів поліції мобільними пристроями (службові планшети, смартфони) з особистим кодом для реєстрації кожного поліцейського, встановити спеціальний для службового користування мобільний додаток «My pole». При цьому під час передачі оперативної інформації необхідно використовувати SIM-картку з декількома рівнями захисту та яка передбачена для користування лише підрозділами Національної поліції України.

Отже, можемо зробити висновок, що за час функціонування Національної поліції України введено багато інновацій в роботу поліцейських, основним є те, що відбувається все швидший перехід від паперових носіїв інформації до цифрових, електронних, що значно полегшують та пришвидшують організацію роботи поліцейських. Однак в гонитві за сучасністю необхідно враховувати навіть найменші дрібниці, особливо у сфері захисту прав і свобод громадян та протидії злочинності.

Бібліографічні посилання

1. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII. *Відомості Верховної Ради України (ВВР*). 1992. № 48. Ст. 650.
2. Про Національну поліцію : Закон України від 2 липня 2015 року № 580-VIII. *Відомості Верховної Ради (ВВР)*. 2015. № 40–41. Ст. 379.
3. Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційне забезпечення професійної діяльності : навч. посіб. Дніпро : ДДУВС, 2018. 220 с.
4. Економічна та інформаційна безпека: проблеми та перспективи : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 27 квіт. 2018 р.). Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2018. 276 с.

Еркенов Б. Д., магистрант 2-го курса
Научный руководитель – Жемпиисов Н. Ш.,
заведующий кафедрой
специальных юридических дисциплин,
кандидат юридических наук,
старший советник юстиции
(Академия правоохранительных органов при Генеральной Прокуратуре Республики Казахстан)

НЕКОТОРЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН

В Послании Президента страны народу Казахстана 1997 года – «Казахстан – 2030. Процветание, безопасность и улучшение благосостояния всех казахстанцев» в качестве долгосрочного приоритета определена национальная безопасность, одним из элементов которой является экономическая безопасность [1, с. 27].

Важная роль информационных технологий в социально-экономической и культурной жизни общества и государства предъявляет повышенные требования к решению вопросов экономической безопасности.

Экономическая безопасность Республики Казахстан (далее – РК) это состояние защищенности национальной экономики от внутренних и внешних условий, процессов и факторов, ставящих под угрозу ее устойчивое развитие и экономическую независимость, готовность и способность институтов власти создавать механизмы реализации национальных интересов развития национальной экономики как внутри, так за пределами страны [2, с. 4].

Обеспечение экономической безопасности государства требует использования комплексного подхода, включающего организационные, технические, программные, социальные механизмы, способные реализовать

конституционные права и свободы человека и гражданина в области получения информации, пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности РК, политической, экономической и социальной стабильности, законности и правопорядка, развитии взаимовыгодного международного сотрудничества.

За 30 лет независимости РК термин «экономическая безопасность» прочно вошел в отдельные пункты нормативно-правовых актов страны. К важнейшим из таких нормативных документов последних лет относятся: Закон Республики Казахстан от 28 августа 2009 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Указ Президента РК 20.02.2021 года «О некоторых вопросах Агентства Республики Казахстан по финансовому мониторингу» (далее – АФМ), а также Указ Президента РК от 15.10.2021 года «О концепции правовой политике до 2030 года» (далее – Концепция).

Следует отметить, что Концепция обращает внимание на противодействие экономической преступности и требует дальнейшего продолжения наращивание способов и методов, в том числе с использованием инновационных и цифровых технологий борьбы с любыми формами правонарушений и их профилактик, обеспечение законности и общественной безопасности, защиты прав и свобод граждан, неотвратимости наказаний за любые правонарушения, неукоснительное следование принципу «нулевой терпимости (толерантности)» к правонарушениям» [3, с. 32].

За последние годы реальную угрозу экономической безопасности РК представляет такое явление, как «отмывание денег и финансирование терроризма», которое также охватывает и вывод капитала за пределы РК.

По нашему мнению, одним из важнейших шагов в противодействии отмыванию денег и финансированию терроризма, а также защите экономической безопасности стало создание 6 октября 2004 года, поддержанной ФАТФ (Группа разработки финансовых мер борьбы с отмыванием денег, далее – ФАТФ), Международным валютным фондом, Всемирным банком, региональной группы по типу ФАТФ Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма (далее – ЕАГ).

Уполномоченным органом в противодействии экономическим правонарушениям – АФМ РК планируется создание следующих инновационно-информационных систем по обеспечению экономической безопасности:

- единой базы данных для всех субъектов финансового мониторинга (далее – СФМ) с аккумуляцией сведений о лицах и компаниях с рисковыми признаками (в т. ч. отказ в проведении операции, установлении и прекращении деловых отношений);
- модернизация Информационной системы «Электронная счет-фактура» (далее – ЭСФ) в части выявления и запрета выставления ЭСФ,

расширить список товаров, приобретение и реализация которых должна отражаться в модуле «Виртуальный склад»;

- изучение возможности дополнительной идентификации, наряду с электронной цифровой подписью, через Face ID, при сдаче налоговых отчетов и выписке ЭСФ [4].

В настоящем АФМ РК подготовлен пакет поправок в законодательство, которые направлены на совершенствование мер противодействия правонарушениям с использованием криптовалюты [5].

Правовая реформа должна создать необходимые условия для развития новых общественных отношений, обеспечивающих эффективную защиту экономической безопасности страны.

Исходя из вышеизложенного, Республика Казахстан и впредь будет наращивать усилия по обеспечению экономической безопасности в целях гарантированного соблюдения одного из основополагающих конституционных принципов деятельности Республики Казахстан – экономического развития на благо всего народа.

Библиографические ссылки

1. Казахстан – 2030. Процветание, безопасность и улучшение благосостояния всех казахстанцев : Послание Президента страны народу Казахстана 1997 года.
2. Социально-экономические приоритеты в системе финансовых координат / под общей ред. А. А. Рогачева. Алматы : Ғылым, 1999.
3. Об утверждении Концепции правовой политики до 2030 : Указ Президента РК от 15.10.2021г.
4. https://www.gov.kz/memleket/entities/afm/documents/details/209651?lang=ru (дата обращения: 26.10.2021г.).
5. https://www.gov.kz/memleket/entities/afm/press/news/details/274363?lang=ru (дата обращения: 26.10.2021г.).

Задорожня І. І.,
курсант 2-го курсу факультету
підготовки фахівців для органів
досудового розслідування
Науковий керівник – Гребенюк А. М.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

КРИМІНАЛЬНИЙ АНАЛІЗ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

З року в рік інформаційні технології все більше і більше поширюються в житті людей як в особистому, так і в суспільному. Вони стали для всіх буденним явищем, яке полегшило спілкування між собою, дало можливість здійснювати покупки через Інтернет, відразу оплачувати їх, підтримувати зв'язок з іншими та надавати допомогу дистанційно тощо.

Поява інформаційних технологій значно відобразилася на роботі суспільства та державних органів. Це призвело до змін, які відбулися не лише у державних органах управління, але й у виконавчих. Як ми знаємо, одним із органів виконавчої влади України є Національна поліція. На неї покладено чимало завдань та обов'язків, які вона повинна виконувати. В цьому їй допомагає інформаційне забезпечення професійної діяльності, яке з року в рік розширюється та надає можливість якісніше виконувати поставлені завдання.

У сучасному світі злочинність бере вищий рівень та вимагає застосування у боротьбі проти неї найбільш актуальних та ефективних засобів. На сьогодні одним із таких засобів є кримінальний аналіз, який являє собою комплекс методів, які використовуються для зберігання, оцінки, аналізу та реалізації інформації під час розслідування кримінальних правопорушень. Це дозволяє правоохоронним органам опрацьовувати велику кількість даних та надає змогу зробити висновок щодо структури злочинної організації.

Загалом аналізи поділяють на:

- оперативний;
- тактичний;
- стратегічний.

Всі ці види відіграють важливу роль у виконанні службових дій та повноважень правоохоронців, а саме підрозділів аналітики Національної поліції.

Оперативний аналіз необхідний для збирання та обробки даних про кримінальні правопорушення, щоб полегшити та скоординувати роботу слідчо-оперативної групи. Тобто це роботи за кримінальним провадженням щодо осіб чи злочинних угрупувань, які причетні до правопорушення. Метою цього аналізу є перевірка гіпотез щодо можливої злочинної діяльності підозрюваних осіб. Під час проведення оперативного аналізу встановлюються зв'язки, структури злочинних груп, ролі їх окремих учасників за допомогою використання трансакцій, потоків та маршрутів переміщення об'єктів, за аналізом телефонних трафіків тощо. Внаслідок процесу кримінального аналізу створюються такі аналітичні продукти:

a) схеми та графіки;

b) карти;

c) інформаційні замітки, що утворюють та поєднують аналітичні результати і рекомендації;

d) робочі книги Excel, в яких використовувалися аналітичні техніки.

Існують й інструменти, які використовує поліція для обробки та опрацювання інформації, яка їм надходить [2, 3]:

1. Ms Excel.
2. IBM i2 Analyst`s Notebook.
3. iBase.
4. GIS.

Тактичний аналіз дає змогу оцінити обстановку, що склалася через нанесення інформації на карти, тобто самостійно визначає райони з підвищеним ризиком скоєння злочинів. Його метою є ідентифікація ризиків та зон, де більш поширена злочинність, за короткий та середній строк.

Тактичний аналіз має аналітичні техніки, такі як: аналіз проблеми, часовий аналіз, статичний аналіз, геопросторовий аналіз, аналіз шаблонів злочинів, порівняльний аналіз, аналіз ризиків та аналіз місць концентрації злочинів [4].

Стратегічний аналіз спрямований на розгляд діяльності організованих злочинних груп та перспективу в роботі по боротьбі з ними. Він застосовується для більш масштабних довгострокових проблем і цілей, тобто для прогнозування зростання інших видів кримінальних правопорушень. Цей вид доволі часто використовується в інших сферах. Головною особливістю стратегічного аналізу є те, що загалом він допомагає вищому керівництву організації чи навіть керівництву середньої значущості.

До порядку проведення стратегічного кримінального аналізу входять такі елементи:

- аналіз середовища (обстановки);
- аналіз ресурсів відомства;
- формування місії та варіантів стратегії;
- аналіз варіантів стратегій з урахуванням обраних критеріїв прийняття управлінського рішення;

- вибір (формування) загальної стратегії.

Отже, з появою інформаційних технологій змінюється не тільки буденне життя громадян, а й життя та діяльність державних органів влади, як наслідок, істотні зміни та нові явища, які полегшують та організовують їх діяльність, спрямовуючи на правильний шлях для вирішення поставлених завдань.

Бібліографічні посилання

1. Про Національну поліцію : Закон України від 2 липня 2015 року № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

2. Тактичний кримінальний аналіз: теорія та практика : навч. посіб. / за заг. ред. Користіна О. Є.; МВС України, ДНДІ МВС України, ОДУВС. Київ, 2020 р. 212 с.

3. Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційне забезпечення професійної діяльності : навч. посіб. Дніпро : ДДУВС, 2018. 220 с. URL: http://er.dduvs.in.ua/handle/123456789/3718

4. Шинкаренко І. Р. Кримінальний аналіз як напрямок діяльності підрозділів кримінальної поліції: Історичні витоки : наукова робота. URL: https://er.dduvs.in.ua/bitstream/123456789/1682/1/16.pdf .

Зеленський А. В.,
курсант 2-го курсу факультету
підготовки фахівців для органів
досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У КІБЕРПРОСТОРІ

Метою дослідження цієї проблеми стала актуальність питання в сучасному світі, де захист інформації в кіберпросторі стоїть вкрай гостро.

Актуальність теми полягає в наявній проблемі фішингу особистих даних користувачів операційної системи Android, які у подальшому можуть бути використані на просторах Даркнету для завдання шкоди відповідним користувачам, а у деяких випадках навіть прямого шантажу щодо розповсюдження особистих даних особи.

Наприклад, незважаючи на створену віртуальну «залізну завісу», влада Китаю фактично визнала повну залежність і незахищеність внаслідок повсюдного використання програмної платформи для мобільних облаштувань Android (частка платформи на ринку Китаю за підсумками 2020 року – 75,4 %), ґрунтовану на «відкритому» коді [1].

Це явище позитивно впливає на розвиток електронної промисловості і реального сектора, що використовують «відкрите» програмне забезпечення для виробництва мобільних пристроїв, але при цьому створює реальну загрозу для особистих даних користувачів вищевказаної операційної системи.

Китайська влада вже угледіла загрозу в платформі Android. Свої висновки влада КНР обґрунтувала підсумками дослідження Китайської академії телекомунікаційних досліджень (China Academy of Telecommunications Research), проведеного на замовлення Міністерства промисловості і інформатизації. За їх даними, ринкова частка платформ iOS, Windows, iPhone, Tizen і Firefox OS, навіть в сумарному порядку, істотно поступаються на китайському ринку платформі Android [2].

Розглянемо наявні загрози для кібербезпеки України з урахуванням актуальних тенденцій розвитку IT-технологій у світі. За даними Hi-tech.UA, частка пристроїв з операційною системою Android в Україні становить 74,43 %, найпершим конкурентом Andoid на ринку є операційна система, яка становить 24,99 % користувачів по всій країні і тільки 0,58 % становлять інші оперативні системи. Не може не тішити те, що майже чверть користувачів смартфонів в Україні надали перевагу операційній системі IOS, що є більш перспективною і захищеною [3].

Зараз зловмисники практично повністю сконцентрувалися на створенні і поширенні «фішингових вірусів» для операційної системи Android. 2019 рік охарактеризувався вибуховим зростанням кількості шкідливих програм для ОС, якщо за увесь 2018 рік було виявлено майже 5300 нових шкідливих програм для всіх мобільних платформ, то в деякі місяці 2019 року кількість виявлених Android зловмисників перевищило цю кількість майже вдвічі.

Отже, розглядаючи актуальні проблеми кібербезпеки, з якими стикаються громадяни України щодня, стає очевидною небезпека використання операційної системи Android з погляду забезпечення безпеки персональних даних. Проте є більш надійна операційна система, яка користується меншим попитом в межах України, аніж Android, але є набагато надійнішою для її користувачів – операційна система IOS.

Зараз особисті дані користувачів системи Android знаходяться під можливою загрозою фішингу, що сприяє зростанню правопорушень з боку хакерів. Для забезпечення безпеки персональних даних користувачів, рекомендуємо користуватись більш захищеними операційними системи, як IOS та інші. Були інциденти з участю власників та розробників операційної системи IOS щодо відмови надавати особисті дані користувачів працівникам ФБР, що потягнуло за собою накладання штрафу на компанію.

Внаслідок дослідження та опрацювання даних ми вирішили, що ОС IOS не є ідеалом можливої захищеності персональних даних користувачів, але за результатами аналізу ринку ОС в Україні є фаворитом серед них щодо безпеки особистих даних користувачів.

Бібліографічні посилання

1. Internet Society – всесвітня громадська організація під управлінням широкої опікунської ради. URL: http://www. internetsociety.org/sites/default/files/bpdeconstructing-cybersecurity-16nov-update. doc.doc_RU_121712.pdf «Погляди на кібербезпеку: 2012г.»
2. CNews|безпека Сергей Попсулин. URL: http:// safe.cnews.ru/news/top/index. shtml?2013/08/02/537614&utm_ source=twitterfeed&utm_medium=twitter «ФБР здатна дистанційно включати мікрофони в смартфонах Android»
3. Hi-tech.UA. Доля iOS втрое ниже чем Android, но денег на приложения в ней тратят в 2 раза больше. URL: https://hi-tech.ua/dolya-ios-vtroe-nizhe-chem-android-no-deneg-na-prilozheniya-v-nej-tratyat-v-2-raza-bolshe/#:~:text=%D0%94%D0%BE%D0%BB%D1%8F%20iOS%20%D0%BD%D0%B0%20%D1%80%D1%8B%D0%BD%D0%BA%D0%B5%20%D0%BC%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D1%8B%D1%85,Android%20%D0%B2%20Google%20Play%20Store.

Калашнік Є. О.,
курсант 2-го курсу факультету
підготовки фахівців для органів
досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ПІДҐРУНТЯ ВІЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ В УКРАЇНІ

Забезпечення інформаційної безпеки в наш час стає одним із безперечно нагальних питань не тільки для діяльності фахівців з ІТ-сфери й науковців, що здійснюють фахові дослідження з суміжних інформаційних питань, а й для виокремлення такого необхідного, чітко регламентованого нормативного підґрунтя. Доля інформаційного простору, із врахуванням сучасних тенденцій до інформатизації, поставлена під питання, відповіді на які багато в чому залежать від стану і тенденцій розвитку економіки та інформаційної безпеки загалом. Необхідність в дослідженні публічно-правових міжгалузевих та міжсистемних механізмів регулювання й стабільного функціонування інформаційної безпеки є беззаперечною й однією з найбільш актуальних.

Аналізуючи раніше згадану необхідність, варто зазначити один з найбільш показових прикладів зовнішнього інформаційного впливу на

Україну, а саме безпосередні дії Російської Федерації щодо інформаційного забезпечення анексії Автономної Республіки Крим та організації сепаратистських заворушень у південно-східних регіонах нашої держави. Тобто ще від початку 2014 року з боку Росії здійснювався надпотужний інформаційно-психологічний тиск на суб'єкти інформаційного простору України й населення загалом, нарощувалася інформаційна експансія в національний інформаційний простір, захоплювались стратегічні об'єкти вітчизняної телекомунікаційної інфраструктури.

Зазначені події знайшли відображення в реальності на тлі, насамперед, відсутності узгодженої, а також заздалегідь зваженої державної політики України у сфері саме інформаційної безпеки, що характеризувалася низькою ефективністю як системи державного регулювання національним інформаційним простором, так і прогалинами й фрагментарністю вітчизняного нормативно-правового поля у зазначеній сфері.

Опрацьовуючи чинну нормативну базу, досить легко помітити, що поняття «інформаційної безпеки України» досить широко застосовується як в Конституції України, так і в низці інших нормативно-правових актів, що підготовлені та затверджені органами і законодавчої, і виконавчої влади.

Однак, наприклад, в Законі України «Про національну безпеку України», що є безперечно основним орієнтиром забезпечення безпеки нашої держави, сутність «інформаційної безпеки» подано як невід'ємний складник національної безпеки України без точного визначення цього поняття [1].

Справді, істотним зрушенням у нормативно-правовому регулюванні національної безпеки в інформаційному просторі стало розроблення та введення в дію Доктрини інформаційної безпеки України (далі – Доктрина), яка була підготовлена відповідно до статті 107 Конституції України, частини другої статті 2 Закону України «Про основи національної безпеки України» та постановляла «Увести в дію рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України» (додається), затвердити Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України (додається), а також Кабінету Міністрів України забезпечити реалізацію Концепції реформування Державної служби спеціального зв'язку та захисту інформації України [2].

Варто зазначити, що ця Доктрина стала першим вітчизняним нормативно-правовим документом, у якому проголошується особливе місце інформаційної безпеки в системі забезпечення національної безпеки, по-перше, як невід'ємного складника кожної зі сфер забезпечення національної безпеки, а по-друге, як важливої самостійної сфери забезпечення національної безпеки [3]. До того ж вагомою новацією зазначеної Доктрини стало чітке виокремлення трьох головних напрямів «національних інтересів» державної політики у забезпеченні інформаційної безпеки України: технологічного розвитку, захисту інформації та «інформаційно-

психологічного, зокрема щодо «створення сприятливого психологічного клімату в національному інформаційному просторі» [4].

Проте для продуктивного забезпечення всебічного становлення зазначеної Доктрини необхідно мати документи, які б послідовно деталізували її в аспектах, наприклад, концепції інформаційної безпеки України, створенні чітких схем чи форм стратегії інформаційної безпеки України, формуванні програми та плану імплементації положень попереднього документа. Однак такі документи й досі не розроблені і не введені в дію. Вже декілька років серед актуальних є низка нових законопроєктів стосовно інформаційної безпеки держави, а саме «Про засади інформаційної безпеки України», «Про кібернетичну безпеку України», «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України». Саме в цих законопроєктах встановлено та зазначено спроби до вирішення наявних недоліків чинного законодавства.

Підсумовуючи, зазначимо: забезпечення суверенітету інформаційного простору та гарантування інформаційної безпеки України з нормативно-правового погляду має бути комплексним і містити:

– уніфікацію та чітке тлумачення загальних положень законодавства;

– конструктивно обмірковане забезпечення державою стратегічно важливих напрямів розвитку і захисту національного інформаційного простору;

– визначення та врегулювання засад і меж діяльності як вітчизняних, так і закордонних суб’єктів інформаційних відносин у національному інформаційному просторі України;

– зосередження принципів, засад та методів щодо захисту національних інтересів України як у міжнародних, так і в національних, визначених законом, інформаційних відносинах.

Визначаючи ж позитивні зрушення в зазначеній тематиці інформаційної безпеки, їх доцільно зазначити не лише завдяки затвердженню рекомендацій Комітету цифрової трансформації України від 31 березня 2021 року «Електронна демократія в Україні – дорожня мапа для цілі – Україна в ТОП-20 країн за розвитком електронної демократії» для Кабінету Міністрів України та відповідним органам влади щодо прискорення процесу розробки законопроєктів, що дозволять ефективно протидіяти наявним кіберзагрозам, здійсненню перевірки та вжиття невідкладних заходів щодо припинення можливих витоків інформації та здійсненню заходів щодо перевірки наявності комплексних систем захисту інформації в кожній із зазначених у ЗУ «Про основні засади забезпечення кібербезпеки України» установах, а й завдяки здійсненим владними ешелонами загалом крокам, що полягають як у затвердженні офіційного курсу країни на вдосконалення наявного стану безпеки інформаційного простору, так і в поступовому й раціональному прокладанні шляху до створення повноцінної об’єктивно комплексної системи захисту інформації.

Бібліографічні посилання

1. Про національну безпеку України : Закон України. Документ 2469-VIII, чинний, поточна редакція. Редакція від 01.08.2021, підстава – 1702-IX.

2. Рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року «Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України» : Указ Президента України від 22 жовтня 2021 року № 544/2021.

3. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки. *Стратегічні пріоритети*. 2012. № 3 (24). С. 152–157.

4. У Комітеті з питань цифрової трансформації відбулися слухання на тему: «Електронна демократія в Україні – дорожня карта для цілі – Україна в ТОП-20». URL: https://thedigital.gov.ua/news/komitet-rozglyanuv-4-zakonoproekti-ta-obgovoriv-praktiku-vikonannya-zakonodavstva-pro-kiberbezpeku-z-derzhavnimi-organami

Калюжна А. О., слухачка
магістратури юридичного факультету
Науковий керівник – Косиченко О. О.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

РИЗИКИ ВИКОРИСТАННЯ СИСТЕМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Біометрія все частіше використовується для ідентифікації громадян у різних сферах життя: для отримання банківських послуг, для складання он-лайн іспитів, оплати проїзду на транспорті тощо [1–3]. Біометричні дані вважаються «надчутливими». При цьому виникають питання довіри до штучного інтелекту стосовно ухвалення остаточних рішень. І збереження паперових копій документів у багатьох випадках має сенс. Тобто є певні ризики використання біометричних даних.

Біометричні дані, на відміну будь-яких інших, що використовуються для ідентифікації, є невід'ємною частиною кожної людини. На відміну від пароля, номера телефону та прізвища, що використовуються зараз, не можна в разі витоку або компрометації даних, змінити своє обличчя, сітківку, фігуру, відбитки пальців тощо. Це надчутливі, але при цьому незмінні дані, які, в принципі, можна вкрасти.

Біометрична інформація та інші, персональні або платіжні дані, що зберігаються в конкретних базах даних, схильні до банальних витоків, кількість яких у всіх сферах життя неухильно зростає. Це відбувається

переважно не через технологічні проблеми, а через людський фактор.

Прихильники біометрії запевняють, що бази даних якось особливо захищені, що впроваджені відповідні криптографічні системи. Насправді немає ніяких особливих способів убезпечити біометричні дані – це звичайні дані, які зберігаються у звичайних базах даних. І працюють з ними ті ж люди, звичайні системні адміністратори, які отримують не звичайні зарплати, при цьому вони самі призначають права доступу – тобто можуть налаштувати собі доступ, куди завгодно та будь-якого рівня. Тут діє старий закон: якщо є можливість для зловживань – то треба вважати, що вони вже є.

Справді, нелегальні послуги «пробивки» людей за особистими даними існують уже давно, чорний ринок інформації бурхливо розвивається. Шахраї дуже винахідливі, тому щойно з'являється новий вид цифрового контенту, вони відразу вигадують, як із цього можна отримати прибуток. Будуть бази біометричних даних – і з них будуть витоки, крадіжки, продаж даних.

Зараз набирає обертів технологія так званої глибокої підробки – Deepfake. В Інтернеті ви можете знайти масу відео із заміною осіб зірок, політиків, відомих людей. Звичайна людина щодня проходить під сотнями камер, її обличчя, хода, голос потрапляють у десятки баз даних різного рівня та різних видів власності, а з баз вони витікають будь-куди. Тести у цій сфері показують гнітючі результати: наприклад, у дослідженні південнокорейських вчених системи біометричної аутентифікації MS Azure та Amazon у 68 % та 78 % випадків відповідно розпізнавали фальшиві особи, з дуже високим ступенем впевненості.

Аудіофейки взагалі зараз виконуються просто ідеально, а авторизацію за голосом зараз уже використовують у реальних банківських додатках. На цей час немає надійних технологій розпізнавання таких фейків.

Тому під час впровадження біометрії головна небезпека полягає в тому, що поки що неясно, як захистити і верифікувати ці дані. Громадяни здають відбитки пальців та фото обличчя, їхні обличчя знімають без їхнього відома та згоди на вулицях, на транспорті, в офісах та торгових центрах. Потім таку інформацію може хтось «злити», вкрасти, перехопити та використати, наприклад, у великих угодах з нерухомістю, пі час управління рахунком у банку, під час проходу на закриті об'єкти тощо.

Висновок: якнайменше здавати біометричні дані, не вестися на «зручність» і уявний виграш. Ці дані гарантовано вкрадуть та продадуть. При цьому той, хто збирає ваші біометричні дані, не вважає за потрібне пояснити, як ці дані планується захищати, у тому числі від своїх співробітників.

Існує думка, що біометрія має спростити ідентифікацію користувачів. Проте ще ніхто з прихильників біометрії не обґрунтував, яку ціну буде сплачено за уявне спрощення ідентифікації. При цьому змінюється рівень інформаційної безпеки на ілюзорний виграш від спрощення ідентифікації користувачів.

Крім того, треба розуміти, що система біометричної ідентифікації – це

система штучного інтелекту, яка не має 100 % якості. Їй завжди властиві помилки першого та другого роду: тобто вона може розпізнати «неправильний» об'єкт як правильний чи не пропустити правильний об'єкт. Тобто завжди залишається ймовірність, що система вас не розпізнає чи розпізнає вас як когось іншого, на кого ви схожі.

Сфера біометричної автентифікації перспективна та швидко розвивається, з кожним роком зростає кількість досліджень та розробок у цій сфері. Однак ці методи недосконалі, і завжди є ймовірність помилок. Варто уважно зважити всі «за і проти», перш ніж ухвалити рішення використати біометрію для захисту своїх конфіденційних даних та коштів. Якщо вкрадений пароль або банківську картку можна замінити, то як замінити вкрадене «обличчя» чи «палець»? Втрачений чи вкрадений біометричний ідентифікатор стає скомпрометованим уже назавжди. Про це слід пам'ятати, погоджуючись використовувати метод біометричної автентифікації. У людей має бути вибір – здавати чи не здавати свої біометричні дані, адже ризики їхнього несанкціонованого використання, як і раніше, залишаються високими.

Бібліографічні посилання

1. Биометрическая идентификация: удобство и риски. URL: https://plus-one.rbc.ru/society/biometricheskaya-identifikaciya-udobstvo-i-riski

2. Биометрия и информационная безопасность. URL: https://safe-surf.ru/users-of/article/659637/

3. Суомалайнен А. Биометрическая защита: обзор технологии. Изд-во ДМК-Пресс, 2019. 99 с.

Касич Є. Ю.,
здобувач 2-го курсу вищої освіти
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПОШИРЕННЯ КІБЕРЗЛОЧИННОСТІ В СУЧАСНІЙ УКРАЇНІ, ПРОБЛЕМАТИКА ТА ШЛЯХИ ВИРІШЕННЯ

На сьогодні глобальною проблемою не тільки України, але й усього світу є поширення кіберзлочинів, спроби подолання та звісно статистика даних правопорушень, що значно зросла з періодом усесвітньої пандемії. Кіберзлочини мають різні напрями, що реалізуються у зовсім не схожих

сферах життя: від шахрайських схем за допомогою смартфону до розповсюдження дитячої порнографії, але ж структура з кожним роком стає все ширше та посягає на значні соціальні блага та цінності.

Як ми вже сказали, що через введення карантину статистика кіберзлочинів зросла. Це пов'язано з тим, що суспільство почало віддавати перевагу глобальній мережі «Інтернет» та ставити на задній план спілкування в соціальних мережах, згідно з цим шахраям простіше розповсюджувати павутиння шахрайства, адже закриті магазини, банки, кінотеатри тощо штовхають користуватися онлайн-послугами, які не завжди у сучасному світі є легалізовані та законні. Якщо порівняти статистику 2021 року з іншими роками, ми бачимо значну різницю. Про це розповів глава Департаменту кіберполіції Олександр Гринчак в інтерв'ю в РБК-Україна: «На сьогодні в нас дійсно зросла статистика по кіберзлочинах. За чотири місяці цього року, порівняно з минулим, ми бачимо приріст на 25 %. На цей час ми зафіксували 1157 таких інцидентів. По них ми вже оголосили 263 підозри» [1]. Статистика інших років вказує: «Стрибок кількості всіх кіберзлочинів відбувся в 2017 році. Після цього кількість злочинів має тенденцію зростати. Так в 2017 було зафіксовано 1795 справ, в 2018 році – 1023, за останні півроку – 1005» [2].

Найбільш актуальною проблемою є кримінальні правопорушення з участю неповнолітніх. На нашу думку, саме цей вид є найбільш поширеним, адже діти або неповнолітні – особи, які мають великий рівень довіри, вважають, що сварки з друзями, погані оцінки, матеріальне неблагополуччя – це дилема, яка немає виходу, саме тому звертаються до Інтернету або поглиблюються до онлайн-життя за порадою та розумінням, потрапляючи на челенджі, летальні ігри та депресивний контент, що штовхає дитину до вчинення суїциду та інших наслідків. Щодо цього під час інтерв'ю Олександру Гринчаку поставили таке запитання, на яке він дав обґрунтовану відповідь: «Через соцмережі вже кілька років відбуваються злочини за участю неповнолітніх. Це і «групи смерті» так звані «сині кити», зараз це ще й челенджі в Tik-Tok на кшталт «напийся таблеток». У нас вже є жертви і постраждалі від цього. Як цьому можна протидіяти?

– Щодо дітей, то ми щодня відстежуємо статистику незалежно від того, стався суїцид або вдалося врятувати дитину. Ми виїжджаємо на кожен такий випадок і оглядаємо девайси, щоб зрозуміти, в чому причина. Стосовно нещодавніх інцидентів, то ми не фіксували їх зв'язок із суїцидальними групами. Як правило, причина – це любов, непорозуміння з друзями в школі, проблеми з навчанням або батьками або просто неблагополучна сім'я. Звісно, коли є проблеми, дитина замикається. Вона заходить в Інтернет, а там маса деструктивних каналів, інформаційних джерел і підозрілих людей, які можуть «підкинути» депресивну музику або скинути в особисті пост із закликом, що «нічого робити в цьому світі» і краще просто померти…» [1]. Отже, кіберполіція запроваджує нові кроки подолання саме цього летального

виду злочинності у онлайн-існуванні підлітків.

Також нині «В Україні кожна четверта дитина за останній рік стикалася з проявами сексуального насильства в Інтернеті» [3]. Ми звернулись до офіційних джерел щодо інцидентів проявів сексизму над дитиною «Кожних 5 хвилин Internet Watch Foundation знаходить у мережі фото чи відео сексуального насильства над дитиною. 46 000 000 зображень із дитячою порнографією зберігається у базі Європолу. Третина цих матеріалів припадає на селфі, тобто дітей змушують робити інтимні фото чи відео самостійно. Щоб досягти своєї мети, злочинці вдаються до особливих практик: секстингу, онлайн-грумінгу та сексторшену» [4] .

Крім того, правоохоронці вже розробили шляхи припинення вчинення правопорушень. По-перше, для того щоб мати більш розвинуту систему, ми звертаємось до європейських або американських партнерів для обміну інформацією та досвідом. По-друге, «Кіберполіція весь час вказує на необхідність ратифікації парламентом додаткових положень Конвенції про кіберзлочинність від 23 листопада 2001 року. Йдеться про удосконалення збору цифрових доказів, що дасть правоохоронцям якісно документувати та оперативно розслідувати кримінальні кіберпорушення. Ми повинні узгодити кримінальне законодавство у сфері інфотехнологій до європейських стандартів та підвищити кримінальну відповідальність за вчинення кіберзлочинів» [5].

Зважаючи на вищенаведене, можна зробити висновок, що ця проблема посягає глобального масштабу та для її подолання треба звертатись до європейських партнерів. Також впровадження програм роботи із неповнолітніми та малолітніми особами щодо небезпеки інтернету та кіберзлочинів. Створювати відповідні гуртки у школах, проводити тренінги для поширення необхідної інформації, спрямованої на захист та певною мірою на протидію проявів кіберзлочинів.

Бібліографічні посилання

1. Глава Департаменту кіберполіції Олександр Гринчак про злочинні схеми через месенджери, шахрайство по телефону і з банківськими картами, «групи смерті» в соцмережах, легалізацію криптовалют і «піратство» – в інтерв'ю РБК-Україна. URL: https://www.cyberpolice.gov.ua/news/glava-kiberpolicziyi-oleksandr-grynchak-cherez-kryptovalyutu-proxodyt-bilshist-zlochynnyx-operaczij-395/ (дата звернення: 19.10.2021).
2. За п'ять років кіберзлочинність в Україні зросла вдвічі. URL: https://www.epravda.com.ua/rus/news/2019/10/21/652782/ (дата звернення: 19.10.2021).
3. Кількість кіберзлочинів в Україні в 2021 році зросла на 25 %. URL: https://www.rbc.ua/ukr/news/kolichestvo-kiberprestupleniy-ukraine-2021-1622012394.html (дата звернення: 18.10.2021).
4. Сексуальне насильство онлайн: як захистити дитину в інтернеті. URL: https://kyivstar.ua/uk/cybersecurity/seksualne-nasylstvo-onlayn-yak-zahystyty-dytynu-v-interneti (дата звернення: 19.10.2021).
5. Міжнародні хакерські угруповання: як працюють і що робить Кіберполіція. URL: https://biz.nv.ua/ukr/experts/hakeri-ta-kiberpoliciya-chi-vdastsya-zahistiti-ukrajinciv-novini-ukrajini-50165630.html (дата звернення: 19.10.2021).

Ковбаса М. В., слухач 2-го курсу магістратури факультету соціально-психологічної освіти та управління
Науковий керівник –Верхоглядова Н. І.,
завідувач кафедри аналітичної економіки та менеджменту Дніпропетровського державного університету внутрішніх справ, доктор економічних наук, професор

ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВА: СУТНІСТЬ ТА ОЗНАКИ

На сьогодні, в умовах дестабілізації усіх сфер економіки, економічна безпека підприємства є однією з основоположних передумов дієвого розвитку підприємства. Оцінка рівня економічної безпеки підприємства дає можливість здійснити аналіз ефективності організації, виявити загрози для бізнесу, проблемні аспекти, що можуть виникнути у майбутньому.

Актуальність цієї тематики зумовлена невизначеністю та непередбачуваністю функціонування ринкової економіки, що призводить до небезпечних явищ у підприємстві, та зі свого боку вимагає на належному рівні сформувати систему економічної безпеки підприємств.

Дослідженню проблем, пов'язаних з економічною безпекою окремих суб'єктів господарювання, присвятили свої наукові доробки як вітчизняні, так і зарубіжні вчені, серед яких можна виділити, зокрема: А. Гальчинського, Т. Г. Васильціва, С. Мочерного, К. Горячева, В. Мунтіяна, Г. Козаченко, Г. Андрощука, О. Ляшенко, С. Довбня, Р. Реверчука, В. Франчука та багато інших. Незважаючи на велику кількість праць вчених, є невирішені проблемні питання щодо сутності економічної безпеки окремих видів суб'єктів господарювання.

Варто почати з того, що з посиленням інтеграції національної економіки в міжнародні об'єднання, а також у зв'язку з глобалізацією світового господарства, перед кожним підприємством постає необхідність значного посилення рівня економічної безпеки.

За наявності повної економічної самостійності підприємства здатні самостійно визначати економічну політику, організовувати процес виробництва та відповідно нести відповідальність за результати своєї діяльності у сфері господарювання. Все це вимагає від керівників та/або власників окремих суб'єктів господарювання вжиття заходів, що забезпечуватимуть економічну безпеку бізнесу та створюватимуть комплексну систему безпеки.

На думку М. І. Камлика, економічна безпека підприємства – це такий стан розвитку суб'єкта господарювання, який характеризується стабільністю

економічного та фінансового розвитку, ефективністю нейтралізації негативних факторів і протидії їх впливу на всіх стадіях його діяльності [1, с. 9].

Зі свого боку, С. І. Ніколаюк, Д. Й. Никифорчук економічну безпеку підприємства визначають як стан юридичних, виробничих відносин і організаційних зв'язків, матеріальних і інтелектуальних ресурсів, щодо яких гарантується стабільність функціонування, фінансовокомерційний успіх, прогресивний науковотехнічний і соціальний розвиток [2, с. 15].

Проте, зважаючи на багатогранність та багатофакторність цього поняття, найбільш повним та ємним, на думку автора, є визначення Т. Васильцева, який пропонує під економічною безпекою підприємства розглядати такий стан функціонування, за якого підприємство та його продукція є конкурентоспроможними на ринку, а також одночасно гарантується: найбільш ефективне використання ресурсів, інтелектуального та кадрового потенціалу; стабільність функціонування та прогресивність розвитку; можливість протистояти негативним впливам зовнішнього та внутрішнього середовища його функціонування [3, с. 18].

Варто наголосити на тому, що є розбіжність щодо розуміння сутності поняття «економічна безпека підприємства», проте можна виділити три підходи для визначення останньої. Вчені виділяють такі основні підходи, як системний, ресурсний і функціональний.

Беручи до уваги системний підхід, вчені вбачають у ньому сукупність підсистем, відповідно до яких і відокремлюють складові економічної безпеки. Зі свого боку, прихильники ресурсного підходу зосереджені на тому, що певний суб'єкт господарювання у своїй діяльності може використовувати частку корпоративних ресурсів, а тому, на їх думку, економічна безпека формується з ймовірних загроз кожній з часток корпоративних ресурсів підприємництва. При цьому функціональний підхід є найбільш поширеним та полягає у виокремленні зі складу економічної безпеки відповідних елементів, спираючись на їх функціональну спрямованість.

Отже, економічна безпека підприємства є універсальною категорією, що полягає у захисті суб'єкта господарювання на всіх рівнях економічних відносин: як на рівні кожного громадянина, так і на рівні держави. Проте зараз відсутнє єдине визначення досліджуваного поняття, адже вчені мають особисте бачення щодо сутності поняття «економічної безпеки підприємництва».

Бібліографічні посилання

1. Камлик М. І. Економічна безпека підприємницької діяльності. Економікоправовий аспект : навч. посіб. Київ : Атіка, 2010. 432 с.

2. Ніколаюк С. І., Никифорчук Д. Й. Безпека суб'єктів підприємницької діяльності : курс лекцій. Київ : КНТ, 2005. 320с.

3. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізм зміцнення : монографія. Львів : Вид-во ТзОВ «Ліга Прес», 2008. 385 с.

Коляда Д. В.,
курсант 2-го курсу факультету
підготовки фахівців для підрозділів
стратегічних розслідувань

Науковий керівник – Паршин Ю. І.,
професор кафедри фінансових
та стратегічних розслідувань,
доктор економічних наук, професор
*(Дніпропетровський державний
університет внутрішніх справ)*

ПОДОЛАННЯ ЕКОНОМІЧНОЇ КРИЗИ В УКРАЇНІ ПІД ЧАС ПАНДЕМІЇ COVID-19

На цей час економіка держави та об'єктів господарювання доволі мало захищенна. Це зумовлено тим, що їм доводиться пристосовуватись до змін в умовах карантину. Всесвітній карантин утворив цілу низку різнопланових загроз для розвитку української економіки, через те, що ці загрози нові, їх адекватна оцінка доволі складна [1, с. 55].

Весь світ намагається побороти проблеми, викликані SARS-CoV-2. Звичайно, Україна не виняток. З певною часткою умовності такі заходи можна поділити на такі категорії: технічні та організаційні, фінансово-економічні, соціально-політичні та інформаційно-психологічні. Це умовний поділ. Це відбивається в тому, що вони пов'язані за походженням і функціями. Також вони будуть відображені в найближчому майбутньому.

Однак з огляду на практику різних етапів протидії поширенню вірусу SARS-CoV-2 і проявів пандемії COVID-19 в Україні значущість цих категорій може бути різною. Тож на початку поширення вірусу насамперед були технічні та організаційні аспекти. Тобто евакуація громадян України з-за кордону, контроль їх стану (самоізоляція), організація карантину. Інформаційні та психологічні загрози також важливі.

Також на початковому етапі протидії поширенню коронавірусу в Україні стали проявлятися соціальні та фінансово-економічні аспекти цієї боротьби. Зокрема, загострюється проблема пошуку додаткових джерел фінансових ресурсів для боротьби з поширенням коронавірусу SARS-CoV-2. Це питання допомогли вирішити в основному за рахунок коштів резервних фондів і місцевої влади, спонсорства. Але потім стало ясно, що це тільки перший прояв фінансово-економічних проблем.

Для того щоб ця проблема не була за «італійським сценарієм» першочерговим завданням є подолання технічно-організаційних та інформаційно-психолгічних загроз. Технічно-організаційна сфера боротьби з поширенням пандемії COVID-19 на територію України потребує значного

залучення фінансових ресурсів [1, с. 57].

За оцінкою ризиків Міністерства економіки України одним з найсильніших загроз не лише України, а й світу виявиться в «новій світовій кризі» [2]. Важлива особливість цієї короновірусної кризи в тому, що вона за досить короткий час захопила практично всі країни світу, чим зумовила соціально-економічне падіння. Це ускладнило співпрацю різних країн світу. Внаслідок чого питання напрямів економічної політики доволі важливе. Оскільки криза охопила майже всі країни, ця політика повинна бути побудована на міжнародному рівні. Зрозуміло, що і власні напрями подолання поширення короновірусної інфекції в кожній країні окремо також мають бути. Ще більша складність виникає внаслідок можливого загострення політичних суперечностей. Для прискорення економічного відновлення можна використати зменшення тарифів і оподаткування операцій з міжнародної торгівлі, насамперед тих, які безпосередньо стосуються експорту-імпорту медичного обладнання та устаткувань, виробів, призначених для захисту особи (першочергово лікарів) від заражень, лікарських та профілактичних препаратів тощо [3].

Для України виникнення чергової кризи не стало надзвичайною подією, а було цілком очікувано. В нашій державі, як і в інших, прослідковується послідовне послаблення економіки. Та входження країни до короновірусної кризи не було катастрофічним.

Наслідками України від цієї кризи виявилися в зменшенні ділової активності, погіршенні кон’юнктури на світових ринках промислових товарів (важливих для України), послабленні інвестиційної активності. Вторинні наслідки будуть виявлятися в поглибленні глобальної економічної депресії.

Отже, подоланням наслідків короновірусної кризи є раціональні кроки влади, які враховують соціально-економічне, суспільно-політичне та гуманітарне середовища та користуються довірою громадянського суспільства до владних дій.

Бібліографічні посилання

1. Кулицький С. Проблеми розвитку економіки України, обумовлені пандемією коронавірусу COVID-19 у світі, і пошук шляхів їх розв’язання. *Україна: події, факти, коментарі*. 2020. № 8. С. 53–63. URL: http://nbuviap.gov.ua/images/ukraine/2020/ukr8.pdf. (дата звернення: 15.10.2021).

2. Вплив COVID-19 на економіку і суспільство країни: підсумки 2020 року та виклики і загрози ост пандемічного розвитку. Департамент стратегічного планування та макроекономічного прогнозування. *Консенсус-прогноз*. 2021. № 53. URL: https://me.gov.ua (дата звернення: 05.10.2021).

3. Чинники, складові і результати запровадження і реалізації антикризової політики в окремих країнах світу та Україні. Прогноз соціально-економічного розвитку України у 2021 р. / наук. ред. В. Юрчишин. Київ : Заповіт, 2021. 200 с. URL: https://razumkov.org.ua/uploads/article/2021_ukraine_economic_forecast.pdf (дата звернення 15.10.2021).

Коптєв О. С., здобувач 2-го курсу вищої освіти факультету підготовки фахівців для підрозділів кримінальної поліції
Науковий керівник – Прокопов С. О.,
старший викладач кафедри економічної та інформаційної безпеки
(Дніпропетровський державний університет внутрішніх справ)

ТАКТИЧНИЙ КРИМІНАЛЬНИЙ АНАЛІЗ

Тактичний аналіз ідентифікує підозрілі ознаки, підозрілих осіб та групи осіб, підозрілі зв'язки між кількома фактами (факторами), сферами чи територіями, території з високим потенціалом злочинної діяльності (гарячі точки), типи людей, схильних стати жертвами злочинів, та сприятливі періоди часу для злочинних проявів [1].

Тактичний аналіз дає особам картину постійних або нових моделей злочинності в межах їхньої юрисдикції: динаміка злочинності; аналіз часу; просторовий аналіз, географічний аналіз, аналіз місць концентрації злочинів; спосіб вчинення злочину; профіль жертви та підозрюваного; породжують чи викликають чинники (соціальні, демографічні, економічні тощо).

Тактичний аналіз забезпечує підтримку поліції та є підходом до поліпшення її роботи. Одержувачами результатів тактичного аналізу є замовники тактичного аналізу, а також інші працівники поліції, які можуть використовувати результати аналізу у своїй діяльності.

Бенефіціаром тактичного аналізу є концепція, яка включає як клієнта, який подав запит на тактичний аналіз, так і інших членів організації, які використовують результати аналізу. З огляду на те, що для тактичного аналізу використовуються важливі ресурси, важливо, щоб було якомога більше бенефіціарів. Результати тактичного аналізу корисні для всієї правоохоронної системи на всіх рівнях організації, оскільки дозволяють знизити вартість діяльності та підвищити ефективність [3].

Основною метою аналізу є виявлення тактичних закономірностей, ознак і специфічних елементів у серії злочинів з метою вироблення ефективних тактичних рішень та правильного застосування наявних сил і засобів для досягнення максимального результату. Мета аналітичної діяльності – отримати максимальну користь від інформації, яка є у нашому розпорядженні для того, щоб правильно зрозуміти та оцінити ситуацію, побачити її у перспективі та, зрештою, успішно діяти [2].

На тактичному рівні аналіз інформації проводиться відразу після отримання даних, відомостей про походження подій або про ті події, які можуть відбутися в найближчому майбутньому, а також у складних

кримінальних провадженнях. Роль такого аналізу полягає в спрямуванні та підтримці інформаційних знань з метою виявлення злочинних об'єктів (осіб, груп, організацій), відносин між ними, тактики дій, а також їх статусу [3].

Результати аналізу на тактичному рівні (залежно від їх масштабу і можливості реалізації) використовуються в приватних і оперативних рішеннях, під час проведення різних складних, стандартних і разових операцій. Як правило, інформація, яка використовується на цьому рівні, має низький рівень сумісності («байки» про інформаційні повідомлення, заяви потерпілого чи свідків, допит підозрюваних). Ця інформація допомагає визначити місце та роль підозрюваних у злочинних групах та організаціях, зв'язок між ними.

Велика цінність тактичного кримінального аналізу полягає в тому, що він є специфічною системою зворотного зв'язку. Тобто отримана інформація знову дає підстави судити про те, наскільки глибоко вивчені злочинні прояви, адекватно зроблені висновки, оптимально сплановані заходи боротьби зі злочинністю та наскільки ці заходи були ефективними.

Різні методи кримінального аналізу можна застосовувати без будь-яких комп'ютерів. Однак аналіз без використання комп'ютерів займає набагато більше часу, обмежує кількість даних, які аналітик здатний обробити, а виконані вручну звіти і діаграми створюють зовнішнє враження менш професійних.

Найкраще використовувати електронні таблиці та бази даних. Багато організацій використовують спеціально розроблені бази даних. Електронні таблиці дозволяють розміщувати дані в колонки і рядки. Цифрова інформація може зберігатися в табличному форматі, а необхідні обчислення виконуються автоматично (визначення суми, середніх величин, відсотків тощо).

Аналізуючи необроблені дані, корисно мати можливість сортувати їх в певному порядку або ж фільтрувати їх так, щоб показувати тільки ті з них, які становлять інтерес. Це особливо важливо під час аналізу великої кількості звітів одночасно. Комп'ютер дозволяє робити це.

Бібліографічні посилання

1. Криминалистика : в 5 т. / под общей редакцией И. В. Александрова. *Т. 2. Методология криминалистики и криминалистический анализ: учебник для бакалавриата, специалитета и магистратуры*. Москва : Из-во Юрайт, 2019. 167 с.
2. Цільмак О. М., Користін О. Є., Шаптала О. С., Талалай Д. В. Криміналістичні засоби та методи розкриття та розслідування правопорушень : підручник. Одеса : РВВ ОДУВС, 2016. 302 с.
3. Шинкаренко І. Р. Проблеми запровадження кримінального аналізу в діяльність підрозділів кримінальної поліції: теоретико-історичне підґрунтя. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2017. № 1. С. 56.

Корінь Д. К., курсант 2-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
*(Дніпропетровський державний
університет внутрішніх справ)*

ПРОБЛЕМИ ІНФОРМАЦІЙНОГО ЗАХИСТУ ПІДПРИЄМСТВ ТА УСТАНОВ

Вже досить довго багато компаній аналізують безпеку різних підприємств. Встановлюють різні структурні моделі комерційних підприємств, фінансових установ, банків, державних установ, навчальних закладів та слабозахищених, але важливих підприємств, державного значення. Фахівці з різних країн почали моделювати та організовувати хакерські напади на важливі об'єкти для подальшого аналізу збитків та системи безпеки. Протягом тривалого часу, приблизно 10 років, різні організації вивчали вплив багатьох факторів на розвиток загроз у кіберпросторі. Всі ці спроби фінансувалися окремими компаніями, які розробляють первісну частину захисту мережі, та державами, які використовують багато ресурсів для створення систем моніторингу, контролю та перевірки безпеки на державному рівні на основі певних стандартів. Найбільшу роль у розвитку таких систем відіграли США та Китай. Згідно з Вікіпедією, Департамент національної кібербезпеки (NCSD) є підрозділом управління кібербезпеки та комунікацій Директорату національної безпеки і програм, МВС США. Він був створений 6 червня 2003 року на базі Національного центру захисту інфраструктури, Федерального центру комп'ютерних інцидентів та Національної системи зв'язку. Місія NCSD полягає у співпраці з приватним сектором, урядом, військовими та розвідувальними органами для оцінки ризиків і зниження можливостей атакувати та загрожувати сфері інформаційних технологій та пристроїв, що мають безпосередній вплив на функціонування важливих IT-структур уряду США та приватного сектора. NCSD також надає аналіз системи внутрішньої та зовнішньої інформаційної безпеки, здійснює раннє попередження та допомогу, у разі надзвичайних ситуацій для державного та приватного секторів. Як частина всеосяжного національного плану для забезпечення кібербезпеки держави NCSD виконує більшість завдань міністерства. Бюджет NCSD на 2011 фінансовий рік становить 378 мільйонів доларів США. В Китаї інформація щодо державних технологій та розробок у межах кіберпростору є таємною та не оприлюднюється владою,

але в інтернеті можно знайти деяку інформацію щодо цього. За словами американського аналітика Джеймса Малвенона, організація військових кібероперацій Китаю прихована і децентралізована, а операції реалізуються за допомогою постійного мінливого складу офіційних, громадських та напівцивільних груп [1].

Принаймні з 2004 року у Народно-визвольній армії Китаю є підрозділ «61398», призначений для взлому та хакерських атак на комп'ютерні мережі противника. Окрім спеціальних сил Народно-визвольної армії, керівництво Китаю також використовує хакерські групи для проведення кібершпигунства та кібератак, наймасштабнішою з яких є «Альянс Червоних Хакерів» (Red Hacker Alliance), який, за деякими оцінками, налічує приблизно 80 тисяч осіб. За словами російських експертів з інформаційної безпеки В. С. Овчинського та Е. Ларіни, «Альянс Червоних Хакерів» – це неформальна, але контрольована урядом мережа, до складу якої входять не лише хакери з самого Китаю, а й громадяни Китаю з усього світу, які тісно співдіють з 3 та 4 управліннями Генерального штабу армії КНР [2].

Ці дані тривалий час зберігалися в таємниці і не розкривалися, не використовувалися в країні або щодо об'єктів, які становили чи могли становити загрозу. У кіберпросторі набагато складніше знайти об'єкти загрози, техніки та способи маскування, а також інструменти та засоби для влаштування хакерських атак. Саме це було причиною того, що багато підприємств та організацій не знали, що їх ресурси використовувалися для реалізації загроз: «рекламних вірусів», «хробаків», «вірусів-маскувальників». З роками хакери стали більш винахідливим та почали створювати віруси, які дуже швидко потрапляють у систему, ігноруючи будь-які перешкоди. Наприклад, зловмисники почали використовувати «віруси-маскувальтники» у вигляді важливого листа від родичів, керівництва на роботі або важливих повідомлень від постачальників програмного забезпечення. З аналізу вірусів, що становлять загрозу, 94 % з них використовуються для операційних систем Windows, приблизно 5 % – для операційних систем: MacOs, Unix, Linux та операційних систем приладів для комунікації та лише 1 % для авторських програмних забезпечень, які створені за власними розробками, де не враховані досвід та способи захисту від можливих загроз.

Сьогодні існує багато дискусій щодо питання побудови системи безпеки, але для вирішення цього питання, насамперед, треба розуміти, що для цього потрібен досвід та знання різних систем безпеки та протидії. Треба зазначити, що саме працівники, адміністратори та менеджери створюють систему безпеки на підприємстві або проводять комплексний аудит компанії, встановлюють заходи безпеки, організовують та встановлюють нагляд за інформативним середовищем компанії, але на їх шляху є багато проблем, які важко пояснити керівництву. Візьмемо, наприклад, попередні масштабні організації різних

форм власності. Коли віртуальне середовище та комп'ютерна інфраструктура не були розвинені, вони організували секретні підрозділи для контролю за витоком інформації та співпрацювали з СБУ, МВС та Міжнародною організацією кримінальної поліції.

В Україні політика кібербезпеки та інформаційного захисту покладена на численні державні органи, а саме: Державне агентство спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство внутрішніх справ України, Генеральний штаб України, Збройні сили України та навіть Національний банк України. Кожна з цих служб має свою галузь у сфері кібербезпеки, за якою встановлює контроль та несе відповідальність. За даними департаменту кіберполіції, кількість кіберзлочинів в Україні зросла в середньому на 2500 на рік. Згідно з доповіддю, опублікованою на вебсайті правоохоронних органів, співробітники кіберполіції брали участь у розслідуванні понад 10 тисяч встановлених кримінальних справ щодо високих технологій та IT-сфери. Загалом цього вистачало протягом довгого часу, але сьогодні кордони відкриті, і багато держав створили органи контролю за небезпечною діяльністю у кіберпросторі. У багатьох країнах ці агентства призначені для виявлення негативних активностей трафіку (спаму), обмеження доступу населенню до небезпечних секторів у мережі, встановлення засобів захисту державної та особистої інформації населення, а також заборони використання небезпечних чи заборонених урядом ресурсів.

Через високу вартість підтримки локальних серверів, модернізації, забезпечення баз даних, утримування IT-фахівців відповідного рівня, приватні компанії рідко використовують локальні сервери, замість цього підприємства можуть використовувати хмарні технології та підтримувати правильну організацію потоків інформації – це б дозволяло зекономити купу грошей та безпечно ресурс компанії. Важливим організаційним фактором захисту клієнтів є обізнаність працівників та дотримання ними основних правил використання робочого майна. На нашу думку, було б правильно заборонити працівникам компанії користуватися корпоративною поштою для приватного листування, зберігати та проводити обмін інформації за допомогою флеш-накопичувачів, по-перше, флеш-накопичувачі дуже уразливі для вірусів, по-друге, робоча інформація або інші ресурси – це власність компанії, а не інформація для розповсюдження, а за допомогою флеш-накопичувачів дуже легко її викрасти або копіювати стороннім особам. Також ми б рекомендували користуватися тільки ліцензованим антивірусом, який пройшов перевірку часом та організація, яка його створила, довела його ефективність. Вважаємо, що важливу роль також відіграє підготовленість та постійне підвищення професійного рівня працівників, саме тому рекомендуємо надати змогу фахівцям IT-сфери, юристам та бухгалтерам користуватися новими технологіями та проходити навчальні курси для отримання практичних навичок, підвищення кваліфікації.

Бібліографічні посилання

1. Національне управління кібербезпеки США. URL: uk.wikipedia.org/wiki/ Національне_управління_кібербезпеки_США.
2. Альянс червоних хакерів. URL: uk.wikipedia.org/wiki/Альянс_червоних_хакерів.

Костюк Ю. А., курсант 3-го курсу факультету підготовки фахівців для підрозділів стратегічних розслідувань ***Науковий керівник – Неклеса О. В.,*** викладач кафедри фінансових та стратегічних розслідувань *(Дніпропетровський державний університет внутрішніх справ)*

СТРУКТУРА Й ОСОБЛИВОСТІ ЕКОНОМІЧНОЇ ЗЛОЧИННОСТІ НА СПОЖИВЧОМУ РИНКУ

На сьогодні Україна – одна з провідних держав з потужним зовнішньоекономічним потенціалом. Але з погляду найважливішого завдання – забезпечення якості життя і добробуту людей – до необхідного рівня ще далеко. Фундаментальним чинником, що зумовлює необхідність прийняття відповідних заходів, є падіння попиту домашніх господарств. На цей час це основний драйвер уповільнення виходу країни з кризи. У нинішній кризі два основних чинники: населення і торгова галузь.

Розвинути внутрішній ринок можна шляхом стимулювання попиту домашніх господарств через зростання доходів працюючих громадян і пенсіонерів, а попит з боку держави – через пом'якшення контрольно-наглядової діяльності і зростання кількості держзамовлень для малого і середнього бізнесу. Наявність такого феномена «працюючих бідних» не тільки обмежує купівельну спроможність великої частини населення, без якої розвиток внутрішнього ринку неможливий, але й підвищує соціальну напруженість. Крім того, це відбивається на продуктивності і якості праці, призводить до дефіциту кадрів у виробничій сфері.

Споживчий ринок є одним з найважливіших ланок всього ринкового механізму. Специфіка кожного елемента споживчого ринку визначається конкретними характеристиками і динамікою взаємодії між собою з метою забезпечення потреб населення і успішного функціонування економіки. Водночас споживчий ринок схильний не тільки до соціальних, економічних і політичних потрясінь, але також стикається з неринковим впливом кримінальних структур і тіньових економічних явищ. Поєднання цих чинників призводить до зростання частки «Живуть за межею бідності», до

чергового падіння середнього класу і нового стрибка рівня соціальної нерівності. За всього різноманіття способів протиправної поведінки у сфері економіки саме організована злочинна діяльність здатна завдати нищівного удару по базису держави, звести нанівець результати всіх зусиль, спрямованих суспільством та інститутами влади на остаточний вихід із системної кризи, в якій перебуває економіка України. Небезпечно також і те, що проникнення криміналу в економіку руйнує надії та очікування населення щодо сильної та соціально орієнтованої держави [1].

До перспективних методів боротьби з корупцією треба віднести: максимальне посилення покарання на законодавчому рівні; забезпечення відповідного легітимного доходу посадових осіб; створення конкурентного середовища; забезпечення прозорості діяльності посадових осіб; ротація кадрів, що перешкоджає формуванню корупційних зв'язків; вдосконалення механізмів взаємодії чиновників з рядовими громадянами; формування механізмів моніторингу з боку громадянського суспільства. Боротьба з незаконним підприємництвом вимагає значних зусиль від уповноважених органів, але відповідна робота необхідна з огляду на значну шкоду, що завдається державі, суспільству і легальному підприємництву. Внаслідок ухилення від оподаткування суб'єктами незаконного підприємництва (тіньовим бізнесом), державний бюджет недоотримує значні фінансові ресурси [2].

Боротьба з шахрайством, як з традиційним видом злочину, відрізняється підвищеною складністю з огляду на незвичайний динамізм форм його прояву. Це вимагає від усіх суб'єктів постійного моніторингу нових форм і швидкої реакції, яка передбачає відповідні зміни економічних, політичних, правових, інформаційних та організаційних форм протидії. Статистика злочинів, пов'язаних з шахрайством, підтверджує значущість цього напряму державного регулювання споживчого ринку.

Сучасні методи боротьби з шахрайством на споживчому ринку повинні вдосконалюватися на основі пріоритету ринкових (економічних, інформаційних, політичних, цивільно-правових) методів боротьби над силовими і містити в собі: вдосконалення нормативно-правового забезпечення боротьби з шахрайством, організаційно-структурне забезпечення боротьби з шахрайством з урахуванням накопиченого досвіду, вдосконалення системи підготовки кадрів для правоохоронних органів, розвиток міжвідомчого і міжнародного співробітництва у сфері боротьби з шахрайством [3].

Контроль за обігом алкогольної продукції є невід'ємною частиною загальної політики забезпечення національної безпеки і пов'язаний, насамперед, з обмеженням вільної торгівлі алкогольною продукцією, а також її споживанням на території країни.

На сьогодні необхідне державне регулювання виробництва і збуту алкогольної продукції з урахуванням соціально-демографічних і економічних

показників, що показують ступінь задоволеності потреб суспільства. Незважаючи на певні досягнення, що виражаються в зниженні споживання алкоголю, все ще є необхідність у проведенні заходів щодо збереження здоров'я нації в обмеженні споживання спиртного не стільки внаслідок заходів державного контролю над виробництвом і збутом алкогольної продукції, а внаслідок підвищення рівня життя і вдосконалення соціальних механізмів.

Отже, якісний моніторинг та аналіз економічної злочинності на споживчому ринку дозволить виробити своєчасні заходи протидії та забезпечити стале функціонування кожного з елементів споживчого ринку. Наближення до стійкої рівноваги за допомогою збалансованості між обсягом і структурою попиту населення та пропозиції матеріальних благ і послуг, між оборотом грошових і товарних ресурсів стане якісним результатом підтримки економічної безпеки.

Бібліографічні посилання

1. Сандул В. А. Злочини у сфері інтелектуальної власності – основний чинник економічної загрози споживчому ринкові України. Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна. 2012. Вип. 1. С. 128–138. URL: http://nbuv.gov.ua/UJRN/Nvldu_e_2012_1_16
2. Ніпіаліді О. Б. Профілактика економічної злочинності як важливий напрямок діяльності правоохоронних органів: стан, тенденції, проблеми. *Актуальні проблеми правознавства*. 2020. Вип. 4. С. 61–67. URL: http://nbuv.gov.ua/UJRN/aprpr_2020_4_11
3. Денисов С. Ф., Філей Ю. В. Причини та умови злочинності у сфері економіки. *Криміналістика і судова експертиза*. 2021. Вип. 66. С. 272–283. URL: http://nbuv.gov.ua/UJRN/krise_2021_66_30

Кочкіна Д. А., курсант 2-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
*(Дніпропетровський державний
університет внутрішніх справ)*

ВИТІК ДАНИХ ЯК ОДИН З ОСНОВНИХ РІЗНОВИДІВ КІБЕРАТАК

Україна в XXI сторіччі стала частиною всесвітньої науково-технічної революції, яка спричинила утворення нового інформаційного суспільства, що бере участь в економічному та соціальному розвитку країн всього світу. Проте з часом позитивним аспектам такої глобальної субстанції стала

загрожувати низка проблем, зумовлених високою вразливістю інфосфери щодо стороннього кібернетичного впливу. Інформаційний та кібернетичний простори піддаються таким кібератакам, як фішинг, атаки програм-вимагачів, шкідливі програмні забезпечення, витік даних, DDoS-атаки, атаки «людина посередника» (MitM), SQL-ін'єкції, експлойти нульового дня, атаки методом повного перебору (брутфорс) тощо. Наприклад, декілька років тому стався витік 2,5 мільйона облікових даних компанії Drizly, починаючи з 2013 року було розкрито номери кредитних карт більше ніж 10 млн клієнтів Prestige Software, і це вже не кажучи про витік даних із соціальних мереж. Отже, виникла потреба у створенні надійної системи кібернетичної безпеки для належного контролю над відповідними відносинами, що відіграє велику роль у геополітичній конкуренції більшості країн світу [1, с. 4].

Основними суб'єктами національної системи кібербезпеки України, що відповідають за становлення, розвиток і захист кіберпростору, є Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національний банк України, Міністерство інфраструктури України, Міністерство оборони України, Збройні сили України. Вони здійснюють свою діяльність на основі таких нормативно-правових актів, як: Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що ухвалюються на виконання законів України.

Зараз більшість організацій користуються багаторівневими системами обробки інформації (хмарні сховища, корпоративні мережі тощо) з метою передачі даних, які надалі перетворюються на можливий осередок їх витоку. Витік даних можна тлумачити як процес неконтрольованого розголошення (поширення) важливої приватної інформації.

Залишивши десь якусь інформацію, вам тут же надходить комерційна пропозиція, заснована на них; купивши автомобіль, на наступний день вам починають надходити дзвінки від компаній з пропозицією оформити страховку – це все є сигналами про те, що ваші особисті дані потрапили у відкритий доступ [4].

Для того щоб запобігти поширення через мережу ваших особистих даних, необхідно: по-перше, встановлювати складні багатоструктурні паролі, різні для кожного сайту; по-друге, уважно ознайомлюватись з умовами обробки персональних даних; по-третє, не встановлювати маловідомі додатки, що потребують доступу до даних стаціонарних, портативно персональних комп'ютерів чи смартфонів; по-четверте, не вводити логіни й паролі, перебуваючи в незнайомій Wi-Fi мережі (власник відповідної мережі

бачить ці дані, що може призвести до можливого їх витоку).

Для запобігання витоку комерційних даних є декілька дієвих методів, по-перше, це шифрування даних. Переваги цього способу полягають у простоті застосування (реалізація шифрування проводиться спеціальним ПЗ), у разі потреби передачі важливих електронних документів за межі комерційної мережі вони будуть зберігатися на флеш-носії, хмарному носії або в клієнтській пошті тільки в зашифрованому вигляді, високий ступінь надійності. По-друге, це контроль персоналу за допомогою систем обліку робочого часу, що характеризується як комплексне апаратне та програмне забезпечення, яке документує точний час прибуття на роботу, час виходу, діяльність персоналу за комп'ютером, записує листування корпоративної пошти, здійснює відеоспостереження і передає всі ці дані керівництву фірми або людині з відділу безпеки. Далі вся отримана інформація аналізується і виявляється кількість працівників, які могли поширювати комерційну таємницю [5].

Отже, в цій науковій роботі було зазначено поняття «витоку даних», яке можна визначити як один із видів кібератак, що відбувається, коли конфіденційна інформація користувача стає вразливою; перелічена низка методів, які слугують превентивними заходами щодо запобігання стороннього кібернетичного впливу. Також було надано перелік нормативно-правових актів, що регулюють цю сферу діяльності в Україні й допомагають накопичувати важливий досвід у захисті власної ІТ-інфраструктури, та органи, через які відбувається механізм їх реалізації.

Бібліографічні посилання

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект. Київ : Державний університет телекомунікацій, 2015. 4 с.

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 10.10.2021).

3. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.10.2021).

4. Самые популярные виды кибератак в 2021. URL: https://10guards.com/ru/articles/the-most-common-types-of-cyber-attacks-in-2021/ (дата звернення: 10.10.2021).

5. Витік даних: як виявити та виправити? URL: https://indevlab.com/uk/blog-ua/vitik-danih-br-yak-viyaviti-ta-vipraviti/ (дата звернення: 10.10.2021).

Криса О. Ю., курсант 3-го курсу
факультету підготовки фахівців для
підрозділів стратегічних розслідувань
Науковий керівник – Паршин Ю.І.,
професор кафедри фінансових та
стратегічних розслідувань, доктор
економічних наук, професор
*(Дніпропетровський державний
університет внутрішніх справ)*

ТІНЬОВА ЕКОНОМІКА: ПРИЧИНИ ВИНИКНЕННЯ

Тіньова економіка є суттєвою перешкодою для розвитку сталої економіки України, зростання соціальних стандартів життя населення країни та входження її на світовий ринок. Вона негативно впливає на економічні процеси та активізує криміналізацію економічних процесів, корумпованість органів державної влади та низьку правову і податкову культуру юридичних та фізичних осіб [1].

Перш ніж розпочати дослідження на цю тематику, треба визначити поняття тіньової економіки. Під тіньовою економікою в Україні розуміють сукупність видів економічної діяльності, заборонених законодавством України, або тих, які з різних причин не враховані у офіційній статистиці [2]. Тіньова економіка наявна в усіх сферах економічної діяльності. Вона виявляється в таких аспектах: виплата неофіційної заробітної плати (заробітна плата «в конвертах»); корупція; «відкати» та відмивання коштів; незаконна підпільна діяльність; шахрайство; приховування доходів; проведення готівкових операцій без обліку.

Міністерство економіки України виділяє такі чинники, що стримують процеси детінізації економіки в Україні:

– низький рівень захисту прав власності;

– недосконаліть судової системи країни, і як наслідок, низький рівень довіри суспільства та інвесторів до неї;

– високий рівень корупції в країні;

– недостатній рівень захисту інтелектуальної власності;

– низький рівень ліквідності фондового ринку, захисту прав інвесторів поряд із недостатньою спроможністю регулятора протидіяти зловживанням на ринку;

– наявність територій, непідконтрольних уряду, утворених під час збройного конфлікту на території країни, та, як наслідок, зростання «потенційних можливостей» для застосування схем контрабанди товарами [3].

Треба зауважити, що Мінекономіки зазначає, що сприятливі умови та

належне інституційне середовище неможливо створити доти, доки не будуть подолані системні чинники, що стримують процеси детінізації економіки в Україні [3]. А також зазначимо, що карантині обмеження, що призвели до тимчасового припинення діяльності певних організацій, призвели до зменшення рівня тіньової економіки. Але це зменшення рівня є слабковираженим, оскільки карантинні обмеження дозволили не лише призупинити роботу організацій, а й дозволили розширити можливості тіньових операцій.

Отже, треба зазначити, що в Україні найбільш поширеною причиною виникнення тіньової економіки є високий рівень корупції та рівень злочинності в економічній сфері. Протидія тінізації економіки України можлива лише після проведення певних реформ, впровадження чіткої державної програми боротьби з організованою злочинністю, в тому числі і в економічній сфері та корупції, розробки комплексної стратегії протидії у співпраці із зарубіжними партнерами, насамперед з метою використання їх позитивного досвіду у боротьбі з цим загрозливим для національної безпеки явищем.

Бібліографічні посилання

1. Бочі А., Поворозник В. Тіньова економіка в Україні: причини та шляхи подолання. *Приховані тригери економічного зростання в країнах Вишеградської четвірки та в Україні*. 2014. URL: http://icps.com.ua/assets/uploads/files/t_novaekonom_kaukra_ni.pdf (дата звернення: 15.10.2021).

2. Літвінцев Р. Причини тіньової економіки України. URL: https://www.klubok.net/article2533.html (дата звернення: 15.10.2021).

3. Тенденції Тіньової Економіки. *Міністерство економіки України*. URL: https://me.gov.ua/Documents/List?lang=uk-UA&id=e384c5a7-6533-4ab6-b56f50e5243eb15a&tag=TendentsiiTinovoiEkonomiki (дата звернення: 15.10.2021).

Кричун А. Ю., слухач магістратури
юридичного факультету
Науковий керівник – Косиченко О. О.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЮРИДИЧНІЙ ДІЯЛЬНОСТІ

Не дарма наш вік носить назву «інформаційний», адже він характеризується тим, що життя людини дуже тісно пов'язане з сучасними технологіями, які глибоко інтегрувались в усі можливі сфери життя суспільства. Можна навіть сказати, що люди потрапили в своєрідну залежність від своїх ґаджетів: не знайдеться людини, яка в повсякденній діяльності не користувалася б планшетом, комп'ютером або мобільним телефоном. Всі ці технології допомагають оптимізувати діяльність, зекономити час та отримати нові знання. Комп'ютеризація юридичної діяльності – один з напрямів підвищення її ефективності.

Людина – неодмінний суб'єкт юридичної діяльності. Слідчий і суддя, судовий експерт та адвокат, працівники карного розшуку та співробітники інформаційних центрів можуть розглядатися як головні компоненти складно організованих правозастосовних систем (прокуратури, органів юстиції, МВС тощо). Поширення комп'ютерів, як свідчать останні десятиліття, справді «... стимулювало безліч нових ідей про людину як взаємодіючої частини більших систем, про її психологію, про те, як вона навчається, запам'ятовує, приймає рішення...» [1]. Те, що відбувається, являє собою двоєдиний процес: людина вдосконалює комп'ютерні системи, які удосконалюють людину. Удосконалення відносин у людино-машинних системах у сфері юриспруденції – одне з найважливіших завдань сучасної юридичної діяльності.

Юридична професійна діяльність в сучасних умовах життя тісно пов'язана з пошуком, обробкою та використанням правової інформації. Правова інформація на друкованих носіях, юридична література наукового та практичного значення, як і раніше, залишаються у використанні юристів в ролі початкового інформаційного матеріалу для ухвалення правових рішень. Однак життя потребує від юристів знань у сфері інформаційної техніки та технологій пошуку та використання юридичних текстів в електронному вигляді, а також практичних умінь та навичок (компетенцій) їх використання. Персональні комп'ютери та раціональні способи зміни стану інформації

(інформаційні технології) дозволяють юристу швидко знайти та обробити юридичні тексти, передати їх по мережі «Інтернет», отримати відповідь на свої запити, здійснити вибірку даних з деякої сукупності інформації тощо. Крім того, вони дають змогу вирішувати швидко та правильно, а отже найбільш ефективно, правові завдання, що виникають [2].

Для інформаційних технологій загалом є цілком природним те, що вони застарівають і заміняються новими. На сьогодні є декілька технологій, які широко використовуються в сучасній юридичній діяльності.

Першим, і мабуть найбільш значущим, досягненням в ІТ-технологіях в юридичній діяльності, яке беззаперечно змінило життя юристів, є *довідково-правова система* (ДПС).

В 60-70-х роках ХХ століття на Заході у вигляді паперових носіїв накопився величезний слабко структурований інформаційний масив законодавчої інформації (документи внутрішнього, міжнародного права, парламентські матеріали тощо). Приблизно тоді ж у суспільне життя стали проникати комп'ютерні технології. Щораз більший масив правової інформації, яким ставало дедалі складніше керувати та систематизувати, а також щораз більші можливості комп'ютерних технологій спонукали західних юристів звернутись до спеціалістів у сфері ІТ-технологій [3].

На сьогодні, починаючи з 2011 року, почали з'являтись так звані мобільні ДПС. Це ті ДПС, які доступні для роботи з мобільних пристроїв: телефони, планшети тощо. Також на сайтах відповідних ДПС з'являються мобільні версії сайтів із законодавчою базою для більш зручного користування.

Іншим, не менш важливим, досягненням можна вважати впровадження майже у всі види юридичної діяльності *автоматизованих інформаційних систем* (АІС). АІС успішно впроваджуються в процеси інформатизації різних сфер державного та муніципального управління, систем судочинства, правоохоронної ті експертної діяльності тощо [3].

Відповідно, третім та четвертим досягненням ІТ-технологій, що змінили життя юридичної спільноти, стали *електронний документ* (ЕД), *електронний документообіг* (ЕДО) та *електронний підпис* (ЕП).

ЕД, ЕДО та ЕП можуть бути в процесуальному провадженні у вигляді двох форм: 1) форма електронних доказів; 2) форма електронної системи оцінки доказів. В першому випадку електронні докази (відео-, аудіозаписи, SMS-повідомлення тощо) являють собою традиційні докази, які мають сліди правопорушення. У другому випадку ЕДО та ЕП спільно являють собою елементи інформаційної безпеки під час захисту персональних даних, що містять в собі комерційну або іншу таємниці [3].

Окрім вищевказаних, є також інші ІТ-технології, що можуть використовуватись в юридичній діяльності, серед яких: деякі технічні прилади (засоби аудіо- та відеозапису, мультимедійні смартфони, планшетні ПК тощо), правові портали, електронне правосуддя, доступ до інших

інтегрованих баз даних офіційної правової інформації, можливість використання як докази цифрової інформації, отриманої реєструючими приладами, працюючими в автоматичному режимі.

Одним із нововведень сьогодення, у зв'язку з епідеміологічною ситуацією у світі, вважають проведення допитів, судових засідань тощо в режимі відеоконференції. Цей вид ІТ-технологій застосовують не лише за умови хвороби будь-якого з учасників справи або під час розгляду справ, де фізична зустріч підозрюваного та потерпілого є небажаною, але й також в міжнародних судах під час вирішення питань між громадянами різних країн.

Однак, на жаль, жодна з вищевказаних технологій ні на крок не наближає юристів до автоматизації творчої та експертної юриспруденції. Вони, безумовно, полегшують роботу юриста, але лише у питаннях пошуку інформації, а не в її інтелектуальній обробці з погляду юридичної логіки.

Протягом багатьох років вивчається питання полегшення роботи юриста завдяки штучному інтелекту, який буде вирішувати більшість стандартних питань автоматично. Один із напрямів використання штучного інтелекту в юриспруденції – це оцінка ймовірності результатів справи. Для цього роботизованій техніці необхідно ознайомитися з фабулою справи, вивчити відповідне законодавство, проаналізувати попередню судову практику. Нова технологія, розроблена вченими Університетського коледжу Лондона, чітко передбачила 79 % рішень Європейського суду з прав людини [4].

Резюмуючи, можна сказати, що інформаційні технології відіграють величезну роль сучасної юридичної діяльності. Завдяки інформаційним технологіям вдалося домогтися прискорення ухвалення юридичних рішень, удосконалено процес пошуку та систематизації доказів, а юристи отримали можливість у будь-який момент знайти всі необхідні відомості щодо актуальних законів та правових актів.

Звичайно, нові технології змінюють світ на краще, можуть оптимізувати роботу юриста, дають простір професійного розвитку. Проте штучний інтелект ніколи не зможе замінити професії, де необхідний творчий підхід та певні моральні аспекти, притаманні лише людині.

Бібліографічні посилання

1. Бирюков Б. В. Кибернетика и методология науки. Москва, 2004. С. 243.
2. Комп'ютерні технології «мультимедіа» в юриспруденції. URL: https://studbooks.net/1152435/pravo/kompyuternye_tehnologii_multimedia_v_yurisprudentsii (дата звернення: 01.11.2021).
3. Драпезо Р. Г., Сергеев О. Д., Жариков Е. В., Лященко И. В., Быданцев Н. А. Краткий обзор ИТ-технологий, используемых в юридической деятельности. *Весник Кемеровского государственного университета.* 2013. № 1 (53). С. 306–312.
4. Жаркынбеков М. Искусственный интеллект в юриспруденции. URL: https://online.zakon.kz/Document/?doc_id=36647699&pos=3;-52#pos=3;-52 (дата звернення: 01.11.2021).

Кріпак А. Ю., курсант 2-го курсу
факультету підготовки фахівців
для підрозділів кримінальної поліції
Науковий керівник– Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
*(Дніпропетровський державний
університет внутрішніх справ)*

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Розвиток інформаційних систем в Україні на сучасному етапі науковці характеризують як низький і роблять висновок, що впроваджені інформаційні системи на сьогодні не здатні в повному обсязі реалізувати своє призначення у процесі діяльності правоохоронних органів. Тому питання вдосконалення інформаційного забезпечення правоохоронних набуває особливої актуальності.

Діяльність Національної поліції загалом та Департаменту патрульної поліції як її структурного підрозділу спрямована також і на забезпечення дорожнього руху, що є досить комплексним поняттям, та містить у собі все, що стосується трафіку на дорозі: від дотримання правил, здійснення перевірки транспортних засобів, встановлення умов та правил на перевезення небезпечних вантажів до ухвалення конкретних адміністративних рішень стосовно осіб, що їх порушують. Інформаційно-аналітичне забезпечення діяльності поліції в сучасному інформаційному світі відіграє надзвичайно важливу роль у розкритті та попередженні вчинення злочинів загалом та у сфері безпеки дорожнього руху зокрема [2]. Як вказують вчені, що є, на нашу думку, найбільш об'єктивним аргументом: інформаційна діяльність поліції перебуває у тісному та безперервному зв'язку з аналітичною, оскільки будь-яка отримана важлива інформація стає предметом аналітичних процесів, завдяки яким остання доповнюється, трансформується та об'єктивується [3].

Прикладом інформаційно-аналітичної поліцейської діяльності є такі відомі інформаційні системи (банки чи бази даних), як: «Інтелектуальна система кримінального аналізу у режимі реального часу» (R.I.C.A.S.), система «ОРІОН», яка містить всю інформацію з обмеженим доступом (грифом) з агентурних повідомлень та оперативно-розшукових справ, система «АРМОР» містить всі дані та інформацію, зібрану всіма підсистемами департаментів: звіти про правопорушення, стислі результати огляду місця події, інформацію про осіб, що перебувають у розшуку, незначні інциденти, дорожньо-транспортні пригоди тощо, а також допоміжна

інформаційно-аналітична система «ЦУНАМІ» яка дозволяє відстежити місце перебування всіх патрульних екіпажів, швидкість пересування, а також скоординувати їх дії.

Для вирішення окресленого питання у структурі МВС України та у структурі Національної поліції створені відповідні підрозділи [1]. У структурі МВС України – Департамент інформаційних технологій, який у 2017 році реорганізовано у Департамент інформатизації та Департамент аналітичної роботи й організації управління; у структурі Національної поліції – Департамент організаційно-аналітичного забезпечення та оперативного реагування.

На цей час триває розроблення і впровадження нормативно-правового забезпечення щодо взаємодії цих підрозділів у сфері інформаційно-аналітичної діяльності, розподілу інформаційних ресурсів між МВС України та Національною поліцією, функцій щодо забезпечення правоохоронної діяльності.

Отже, дослідивши історичні, політичні, економічні аспекти генезису правоохоронної сфери на території сучасної України, а також врахувавши стан інформаційно-технічного прогресу, пропонуємо виокремити п’ять етапів становлення інформаційно-аналітичної діяльності органів правопорядку: дореволюційний (початок XVIII століття – 1917 рік); ранній Радянський (1917 – початок 1970-х років); автоматизації інформаційної діяльності (початок 1970-х – початок 1990-х років); інформатизації ОВС України (початок 1990–2015 роки); інформаційного забезпечення Національної поліції України (2015 – дотепер) [4].

На основі аналізу характерних особливостей формування, накопичення, зберігання та використання інформаційних ресурсів для кожного з етапів встановлено підґрунтя щодо подальшого розроблення нових правових та організаційних засад інформаційно-аналітичної діяльності, що дасть змогу задовольнити не лише теоретичні, а й практичні потреби щодо проведення реформ як у Міністерстві внутрішніх справ, так і в його складі – Національній поліції України.

Бібліографічні посилання

1. Статистичні дані по галузі автомобільного транспорту. *Міністерство інфраструктури України*. URL: https://mtu.gov.ua/content/statistichni-dani-po-galuzi-avtomobilnogo-transportu.html?PrintVersion
2. Єсімов С. С. Юридична природа інформаційно-аналітичної діяльності Національної поліції. *IT право: проблеми і перспективи розвитку в Україні*. URL: http://aphd.ua/publication-151/
3. Положення про Департамент патрульної поліції. URL:http://patrol.police.gov.ua/wp-content/uploads/2016/03/n594-polozhennya-pro-dpp_compressed.pdf
4. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. *Відомості Верховної Ради*. 2015. № 40–41.

Лагода М. В., курсант
Науковий керівник – Паршин Ю. І.,
професор кафедри фінансових
та стратегічних розслідувань,
доктор економічних наук, професор
*(Дніпропетровський державний
університет внутрішніх справ)*

ЕКОНОМІЧНА БЕЗПЕКА ДЕРЖАВИ ТА ПІДПРИЄМСТВА В УМОВАХ ІННОВАЦІЙНОГО РОЗВИТКУ

Економічна безпека – стан економіки, під час якого показники економічного зростання мають позитивну динаміку, ефективно задовольняються потреби, правильно використовуються ресурси держави, відбувається захист економічних інтересів країни. Також до економічної безпеки належать: природні багатства, виробничі і невиробничі фонди, нерухомість, фінансові ресурси, людські ресурси, господарські структури, сім'я, особа.

Досі майже не викликає суперечок твердження, що головною складовою економічної безпеки підприємства є саме фінансова.

Безпека підприємств має такі складові:

- фінансова;
- політико-правова;
- інтелектуальна і кадрова;
- техніко-технологічна;
- інформаційна;
- силова.

Свідчення економічної безпеки дуже важливі, бо завдяки цим даним ми маємо конкретні показники стійкості, мобільності та, загалом, уявлення про стан економічної безпеки: зростання ВВП, рівень і якість життя більшості населення, темпи інфляції, рівень безробіття, структура економіки, майнове розшарування населення, криміналізація економіки, стан технічної бази господарства, витрати на науково-дослідні роботи, конкурентоспроможність, імпортна залежність, відкритість економіки, внутрішній і зовнішній борг держави.

Інноваційний розвиток базується на привнесенні нових прогресивних технологій, передових рішень та змін в управлінській організаційній діяльності, які мають стосунок до мікро-, та макроекономічних процесів розвитку – створення технопарків, технополісів, проведення політики ресурсозбереження, інтелектуалізації всієї виробничої діяльності, софтизації та сервізації економіки.

Важливу роль для суспільства мають галузі, що належать до «високих

технологій», а також ті, що задовольняють прямо потреби людей.

Ринок інновацій базується і орієнтується на окремих індивідах та їх потребах. Зростає кількість середніх та малих підприємств, які швидко пристосовуються до умов зовнішнього середовища. Інноваційний розвиток підприємства – це позитивні якісні зміни стану підприємства внаслідок здійснення інноваційної діяльності, формування та ефективного використання інноваційного потенціалу, також це процес розвитку внаслідок формування та використання інноваційного потенціалу, спрямований на якісні зміни стану підприємства. Завдяки темпам модернізації зростає потреба до найкращої якості послуг та їх різноманітності. Тобто суспільство прагне до різноманіття, тому стає більш відкритим до інновацій. Виникає потреба творчих кадрів – людей, які можуть привнести нововведення в організаційну, науково-технічну та екологічну культуру. Ця нова модель передбачає зміну понять науково-технічного прогресу і науково-технічного розвитку. Також виникають нові пріоритети у суспільства: добробут, інтелектуалізація виробничої діяльності, використання високих та інформаційних технологій, екологічність. Також вона потребує нової фінансової-кредитної політики, кращого стимулювання інновацій, активного залучення до виробництва малого та середнього приватного бізнесу – на мікрорівні тощо.

Висновок: економічна безпека є певним віддзеркаленням потенціалу інноваційного розвитку, що особливо притаманне фінансовій складовій обох явищ. З іншого боку, економічна безпека підприємства може бути метою та наслідком інноваційного розвитку, який може стати джерелом додаткових загроз, які не дотримуються стану безпеки. Такий зв’язок між двома явищами потребує комплексного підходу до них, заснованого на їх розгляді як двох нерозривно пов’язаних та взаємно впливаючих один на одного важелях ефективності управління.

Бібліографічні посилання

1. Інноваційний тип економіки. URL: https://uk.wikipedia.org/wiki/Інноваційний_тип_р
2. Економічна безпека. URL: https://uk.wikipedia.org/wiki/Економічна_безпека
3. Економічна безпека України: стан, проблеми та перспективи : тези доп. Учасників Всеукр. науково-практ. конф. (22 квіт. 2016 р.). Львів : Львів. ун-т внутр. справ, 2016. С. 25–30. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/konf_22_04_2016.pdf

Лукомська А. А., курсант
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Мирошниченко В. О.,
професор кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

КІБЕРБЕЗПЕКА ВІДДАЛЕНОЇ РОБОТИ У СФЕРІ БІЗНЕСУ ПІД ЧАС ПАНДЕМІЇ COVID-19

Декілька років тому віддалена робота була рідкісним явищем на ринку праці. Зараз в умовах пандемії COVID-19 це практично єдина можливість зберегти працездатність бізнесу.

Захист інформації в комп'ютерних мережах являє собою комплексну систему, що містить апаратно-програмні засоби і методи, а також організаційно-правові заходи, які дозволяють запобігти або максимально ускладнити можливість реалізації загроз інформації. Для оцінки ефективності такої системи необхідно мати інструмент її формального подання, в ролі якого є модель захисту інформації [1, 2].

Для оперативної організації віддаленої роботи співробітників недостатньо одного рішення керівництва: потрібна підготовлена інфраструктура, яка є не у всіх компаній. Тому настає час інформаційно-технічних відділів та служб інформаційної безпеки, які покликані забезпечити безперервність і, що важливо, безпеку бізнес-процесів компанії. Цим службам необхідно швидко розробляти захисні заходи для технологій віддаленого доступу для співробітників своїх компаній та організацій.

Як показує практика, не всі сервіси організації безпечні, витоки інформації з бізнес-систем найбільших корпорацій трапляються із завидною регулярністю, і навіть VPN може виявитися ненадійним інструментом і бути зламаний. Через відсутність часу на аналіз і підбір додаткових засобів захисту ті компанії, які раніше фокусувалися переважно на обороні периметра, виявляться найбільш уразливими, оскільки тепер жодного периметра не існує.

Потребує вирішення і проблема забезпечення безпеки під час використання особистих пристроїв, якими користуються співробітники для організації віддаленого доступу. Не всі компанії можуть собі дозволити забезпечити співробітників робочими своїми технічними засобами. Непідконтрольні службі інформаційної безпеки пристрої з домашніх мереж Wi-Fi будуть масово підключатися до внутрішніх корпоративних ресурсів. Зобов'язати всіх співробітників ставити прийняті в компанії засоби захисту на

особисті комп'ютери, поширити туди прийняту в організації політику безпеки – теоретично можливо, але не в режимі переведення всього персоналу на віддалений формат роботи. Крім того, це спричинюватиме не тільки технічні, а й юридичні та організаційні складнощі. Тому ризики з найбільшою ймовірністю зростуть у компаній, які активно захищають лише кінцеві робочі станції, залишаючи без уваги корпоративну інфраструктуру загалом.

У цій ситуації службам безпеки компанії варто звернути увагу на такі рекомендації:

Необхідно скласти політику безпеки під час віддаленої роботи. Політика повинна бути короткою, зрозумілою, описувати основні ризики, заходи захисту та обмеження, що можуть виникнути під час віддаленої роботи.

Провести позапланове експрес-навчання і підготувати коротку пам'ятку, яка містить основи кіберграмотності. Це допоможе співробітникам не розслаблятися і не допускати помилок, вбереже від специфічних для віддаленої роботи неприємностей.

У разі термінового впровадження захисних рішень треба віддавати перевагу відомим на ринку компаніям зі сфери кібербезпеки. Довіра до таких постачальників знизить ймовірність зробити помилку, ціна якої для реального бізнесу зараз зросла в кілька разів. Якщо немає упевненості відповісти на питання про те, які процеси відбуваються в інформаційній інфраструктурі компанії, то для наведення порядку і встановлення контролю, в тому числі для інформаційно-технічних відділів, це зараз – головне завдання. Підключення до ресурсів через неврахований VPN, масове використання одного облікового запису, перебір паролів, дивні сплески певних типів внутрішнього трафіку за відсутності користувачів в мережі – далеко не повний список загроз безпеки, які особливо часто виникають під час віддаленої роботи співробітників компанії. Використання систем внутрішнього моніторингу в додаток до периметрового захисту набуває актуальності саме зараз.

Важливо сфокусуватися на захисті від тих видів атак, які стають актуальними в нових умовах, навіть якщо раніше їх не було в моделі загроз компанії. Зараз службі безпеки необхідно оперативно переглянути модель загроз, не забуваючи про засоби протидії DDoS-атакам і зовнішнім вторгненням, оскільки кількість точок проникнення і способів порушення конфіденційності, цілісності та доступності інформації стало більше. Це створює нові можливості для кіберзлочинців щодо навіть найконсервативніших в плані IT-інфраструктури компаній.

Захист і контроль особистих пристроїв – непросте завдання, тому необхідно сфокусуватися на забезпеченні безпеки на стороні важливих бізнес-систем і сервісів. Це дозволить не тільки контролювати легітімність роботи власних користувачів в них, але і більш ефективно виявляти вторгнення зовнішніх зловмисників.

Впровадження концепції Zero Trust (нульової довіри до користувачів і пристроїв), або хоча б її окремих елементів, стане хорошим рішенням саме

зараз. Незважаючи на те, що на старті процесу можливі деякі незручності для користувачів, комфортом доведеться пожертвувати. Допускати людей в корпоративну інфраструктуру ззовні, не впевнившись у застосуванні всіх необхідних процедур з погляду безпеки – рішення, яке може обійтися дорожче. Корисним рішенням може бути впровадження контролю внутрішнього трафіку (клас NTA – Network. Traffic Analysis). При цьому інциденти виявлятимуться автоматично, не потребуючи навіть перенастроювання наявної політики безпеки, не кажучи вже про додаткову покупку ще будь-яких безпекових рішень.

Як видно, вимушена дистанційна робота ставить перед співробітниками і організаціями нові проблеми щодо забезпечення безпеки інформації. Наведений вище список рекомендацій можна продовжувати довго, і він все одно може виявитися неповним. Його складання для конкретної компанії залежить від особливостей сфери бізнесу і прийнятої стратегії захисту інформації. Віддалений доступ співробітників до інфраструктури компанії – це завжди питання якісної настройки системи забезпечення інформаційної безпеки та застосування інструментів, здатних контролювати роботу співробітників з будь-якого місця, з метою максимально нівелювати ризики витоку конфіденційної інформації та порушення роботи корпоративних ресурсів.

Бібліографічні посилання

1. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : затв. наказом ДСТСЗІ СБ України від 28.04.1999 р. № 22.

2. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методи та засоби захисту інформації : в 2 т. *Т. 2. Інформаційна безпека*. Київ : Арий, 2008. 344 с.

Масоха В. О., курсант 2-го курсу
факультету підготовки фахівців для
підрозділів стратегічних розслідувань
Науковий керівник – Паршин Ю. І.,
професор кафедри фінансових
та стратегічних розслідувань,
доктор економічних наук, професор
*(Дніпропетровський державний
університет внутрішніх справ)*

СТРАХОВІ РЕЗЕРВИ ТА ЇХ ЗБЕРЕЖЕННЯ

Будь-які підприємства, торгівельні чи промислові, створюють певну систему економічних показників, щоб бачити реальний фінансовий результат своєї діяльності. Там містяться лише дані про сукупність доходів та витрат страховика. На відміну від підприємств, страхові компанії з метою забезпечення майбутніх виплат страхових сум створюють ще й страхові

резерви. Саме вони визначають галузеву специфіку страхових компаній [1].

Послідовність цієї процедури містить у собі, на початку, внесення страхової премії, а лише з часом – надання страхової послуги у вигляді страхового відшкодування. Сума виплат не повинна збігатись із внесеною премією, тому що страховику потрібно мати резерв, який повинен бути достатнім для виконання договору страхування у разі потреби.

Нормативно-правова база страхових резервів базується на Законі України «Про страхування», де передбачене зобов'язання дотримання страховиками умов забезпечення платоспроможності. Саме тому були створені страхові резерви. Вони поділяються на: резерви зі страхування життя та технічні резерви. Це розмежування створене через неоднаковий розподіл коштів на певну категорію ризикових ситуацій [3].

Також є певний перелік технічних резервів, які зобов'язані вести страховики. Наприклад, облік незароблених премій (це лише ті премії, які були отримані безпосередньо під час дії укладеного договору), вони ж містять частки від сум надходжень страхових платежів. І, безперечно, облік самих збитків. Тому що вони містять у собі зарезервовані несплачені страхові суми та інші дані. Найбільш широко використовуються резерви незаробленої премії та збитків. Переважно страховики ухвалюють рішення про ведення таких обліків з нового календарного року. Для цього їм необхідно лише повідомити письмово орган, який має повноваження у цій галузі [2].

Не рідко можна спостерігати як страховик буває не впевнений, з будь-яких причин, у правильності розрахованого ним же тарифу. Для захисту обох сторін, створюється додатковий резерв ризиків, які ще не минули. Як показує практика, такі збитки сплачуються не відразу, а через значний проміжок часу. Це зумовлено тим, що потрібен певний час, за який можна встановити точну суму збитку.

Проблеми страхових резервів показані більше у країнах з розвиненою ринковою економікою [4]. Ми можемо спостерігати існуючий там загальноприйнятий розподіл галузей страхування залежно від термінів виникнення зобов'язань страховика. Цей розподіл містить два пункти. Під час першого претензії погашаються протягом терміну страхування або відразу по закінченню, а в іншому – тривалий період урегулювання справи.

Тож зазначимо, що страхові резерви є обов'язковими грошовими фондами страхових компаній. Дії страховика повинні бути такими, щоб він ураховував безпечність та прибутковість.

Бібліографічні посилання

1. Базилевич В. Д. Страхова справа. Київ : Знання, 2012. 203 с.
2. Борисова В. А. Страхові послуги. Суми : Довкілля, 2014. 216 с.
3. Про страхування : Закон України від 7.03.1996 р. № 85/96-ВР. URL : https://zakon.rada.gov.ua/laws/main/85/96-%D0%B2%D1%80#Text
4. Навроцький С. А. Соціально-економічні аспекти страхування АПК. Суми : Довкілля, 2012. 316 с.

Миршака В. С.,
здобувач магістратури
Перетятько К. О.,
здобувач бакалаврату
Науковий керівник –Фісуненко Н. О.,
доцент кафедри
аналітичної економіки та менеджменту,
кандидат економічних наук, доцент
(Дніпропетровський державний університет внутрішніх справ)

СУТЬ ТА СТРУКТУРА ФАКТОРІВ, ЩО ВПЛИВАЮТЬ НА ФОРМУВАННЯ КОНКУРЕНТОСПРОМОЖНОСТІ ПІДПРИЄМСТВА

Конкурентоспроможність є найважливішим чинником забезпечення безпеки фірми, тобто її виживання у «суворих умовах дійсності» і її подальшого ефективного розвитку. Висока конкурентоспроможність фірми є гарантом отримання високого прибутку в ринкових умовах. При цьому фірма має на меті досягти такого рівня конкурентоспроможності, який допомагав би їй виживати на досить довгостроковому проміжку часу.

Зацікавленість підприємств у результатах своєї діяльності підсилює необхідність підвищення конкурентоспроможності продукції, яка випускається, що потребує вдосконалення роботи всіх служб та підрозділів суб'єкта господарювання. У зв'язку з цим у сучасній економіці головним напрямом фінансово-економічної і виробничо-збутової стратегії кожного підприємства стає підвищення конкурентоспроможності для закріплення його позицій на ринку з метою отримання максимального прибутку.

Конкурентоспроможність залежить від різних факторів, як-от: конкурентоспроможність товарів підприємства на зовнішньому і внутрішньому ринках; вид виробленого товару; місткість ринку (кількість щорічних продажів); легкість доступу на ринок; однорідність ринку; конкурентні позиції підприємств, що вже працюють на цьому ринку; конкурентоспроможність галузі; можливість технічних нововведень у галузі; конкурентоспроможність регіону і країни.

Як показує світова практика ринкових відносин, взаємозалежне вирішення цих проблем гарантує підвищення конкурентоспроможності підприємства.

Отже, конкурентоспроможність підприємства – це комплексна характеристика підприємства, що характеризує його можливість у будь-який момент часу забезпечувати свої конкурентні переваги і прибутковість, а також адаптуватися до постійно змінюваних умов зовнішнього середовища.

Під факторами, що впливають на конкурентоспроможність фірми, розуміють стани характеристики та властивості систем, в межах яких позиціонує фірма. В економічній літературі поняття «фактор» трактується так: «фактор – один з основних ресурсів виробничої діяльності підприємства та економіки в цілому; рушійна сила економічних виробничих процесів, що впливають на результат виробничої економічної діяльності» [1].

Отже, до домінуючих факторів зовнішнього середовища підприємства, що впливають на конкурентні переваги, доцільно віднести: 1. Фактори, опосередковані соціально-економічними умовами. 2. Фактори, опосередковані економіко-правовою базою. 3. Науково-технічні фактори.

Домінуючі фактори внутрішнього середовища, що визначають конкурентні переваги, доцільніше розглядати з позицій аналізу: економічного потенціалу підприємства – виробництво, просування і збут продукції, організаційна структура та менеджмент, маркетинг, фінанси і фінансовий стан підприємства; невиробничого оточення – постачальники, клієнти, маркетингові посередники, контактна аудиторія.

Отже, фактори, опосередковані станом внутрішнього середовища фірми: виробництво традиційного асортименту товарів / послуг; просування збуту товарів / послуг; організаційна структура та менеджмент; комплекс маркетингу; фінанси.

Суб’єктивні фактори, що впливають на конкурентні переваги організації, розглядаються як фактори, опосередковані рівнем професійної мобільності та компетентності фахівців підприємства.

Оцінка можливостей підприємства за цими вісьма факторами дозволяє побудувати гіпотетичний «радар конкурентоспроможності» (рис. 1).

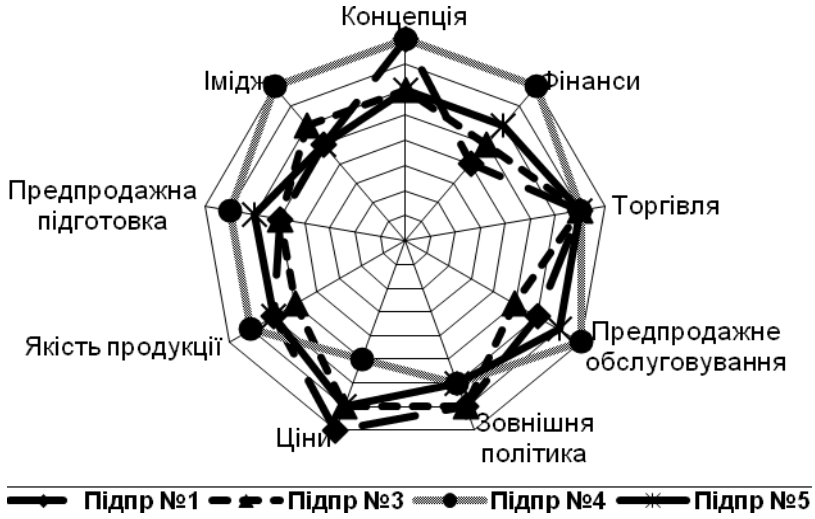


Рис. 1. Радар конкурентоспроможності

Якщо підійти однаково до оцінки конкурентних можливостей низки фірм, накладаючи схеми одна на одну, то, на думку авторів, можна побачити слабкі і сильні сторони одного підприємства щодо іншого.

Зокрема, У. Зулькарнаєв всю сукупність факторів, що впливають на конкурентоспроможність організації, пропонує розділити на 3 групи: цілі, які ставить перед собою організація; ресурси, якими володіє організація, і вміння продуктивно їх використовувати; фактори зовнішнього середовища [2].

Отже, не претендуючи на всю повноту, проведений аналіз факторів, що впливають на конкурентоспроможність фірми, показує, наскільки складна проблема підвищення конкурентоспроможності й утримання позицій підприємства на ринку.

Бібліографічні посилання

1. Бугас Н. В., Босецька О. В. Управління конкурентоспроможністю підприємства в нестабільному ринковому середовищі. *Ефективна економіка*. 2015. № 11. URL: http://nbuv.gov.ua/UJRN/efek_2015_11_31.

2. Zhosan G. The substantiation of the strategy of social responsibility of the enterprise with the aim of providing efficiency of its activities. *Marketing and Management of Innovations*. 2017. № 3. S. 267–279 doi: 10.21272/mmi.2017.3–25 Available from: http://mmi.fem.sumdu.edu.ua/journals/2017/3/267-279.

Моргалюк К. Р.,
слухачка магістратури
юридичного факультету
Науковий керівник – Рибальченко Л. В.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат економічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ПРОБЛЕМИ ШАХРАЙСТВА НА ПІДПРИЄМСТВІ

Згідно з Кримінальним кодексом України шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою. Найчастіше шахрайство класифікують як зовнішнє, як таке, яке здійснюється на підприємстві контрагентами або третіми особами, і внутрішнє шахрайство, яке відбувається працівниками цього ж підприємства.

Ці проблеми виникають через те, що шахраї створюють свої схеми та впроваджують їх у реальне життя для заволодіння чужими грошима через шахрайські дії.

Внутрішнє шахрайство впливає на репутацію не лише самого

підприємства, а й на його клієнтів, що може призвести до їх втрати. Хіба будуть клієнти чи постачальники працювати з підприємством, де відбуваються крадіжки інформації? Звісно, що ні. Тому це питання є актуальним не лише в нашій державі, а й в усьому світі.

Є різні причини шахрайства працівників на підприємстві. Одна з найчастіших – низька фінансова мотивація працівників. Наступною є шахрайські дії управлінського складу та заступників керівників підприємства. Ще важливою причиною шахрайства є схильність працівників, які мають доступ до матеріальних та фінансових звітів і ресурсів, до вчинення злочинних дій.

Якщо розглядати соціологічну теорію злочинності, то для вчинення злочину необхідні такі умови, як:

– бажання вчинити злочин, що залежить від самої особистості та її моральної складової;

– створення сприятливих умов для вживання злочинної діяльності;

– можливість використовувати сприятливі умови на свою користь та задоволення своїх потреб.

Саме збіг цих умов є ймовірністю вчинення службового злочину, які за останні роки мають тенденцію до зростання.

Важливим є й те, що роботодавець має вчасно звернути увагу на працівника, який проявляє такі дії, для зупинення можливих шахрайських вчинків:

– зміна даних у фінансових звітах;

– неправильні відрахування та відхилення показників від нормалізованих значень;

– викривлені показники доходів працівника;

– повідомлення від колег та контрагентів на працівника про його діяльність та інше.

Найпоширенішими схемами шахрайства є придбання товарів та послуг за надвисокими цінами, або таких товарів, яких не існує, створення благодійної допомоги, яка не відбувалася, фальсифіковані виплати, реалізація інвестиційних проєктів, яких немає, та інше.

Від таких шахрайських дій страждає підприємство і його працівники, галузі, державні та комерційні установи, а також держава.

Такими вчинками шахраїв можуть скористатися конкуренти і використовувати певні заходи щодо втручання в діяльність інших підприємств для створення шкідливих шахрайській дій із корисними для себе наслідками.

Частими також є махінації щодо шахрайських дій зі створення економічних злочинів, що призводять до значних збитків на підприємстві. Такі злочини не завжди можна швидко розкрити, для цього на підприємстві створюються служби безпеки, обов’язками яких є відстеження злочинних дій та їх викриття.

Для викриття шахрая витрачається багато часу, можливо, місяць, два, півроку чи більше. За цей час шахрай може завдати суттєвих збитків підприємству. Тому необхідно вживати дієві заходи захисту інформації на підприємстві щодо виявлення шахраїв, у тому числі і через комунікації між співробітниками. Проведення внутрішнього аудиту та професійна діяльність служби безпеки приведе до зростання обсягів розкритих порушень та зміцнення економічної безпеки усього підприємства.

Виявлення причин і умов корпоративного шахрайства на вітчизняних підприємствах показало, що ризик створених шахрайських дій є великий. Відповідно, витрати на створення служб безпеки також можуть бути великими, але зважаючи на створення небезпеки на підприємстві, вказує на його надійний економічної захист, що є важливим напрямом діяльності підприємства та стратегій його функціонування.

Важливим є викриття злочинних шахрайських дій, щоб припинити породження іншими подібного, припинити нових шахраїв, створення нових схем та витоку корпоративної інформації про активи компанії та інше.

Непокарані шахраї є підґрунтям для появи нових. Якщо шахрайство створюють керівники вищої ланки, це призводить до значних проблем в усій корпорації чи установі. Виявити економічні злочини дуже тяжко, особливо якщо вони сталися на високому рівні, серед керівників. Таке може призвести до руйнування корпорації та виробничих потужностей. Ризик шахрайства може перетворитися на стратегічний виклик бізнесу, який потребує активного підходу до управління на найвищому керівному рівні компанії.

Бібліографічні посилання

1. Rubalchenko L., Ryzhkov E. Ensuring enterprise economic security. Scientific Bulletin of the Dnipropetrovsk State University of inteRnal Affairs. 2019. Special Issue № 1. S. 268–271.
2. Рибальченко Л. В., Косиченко О. О. Латентність економічних злочинів як загроза безпеці підприємництва в Україні. *Регіональна економіка та управління*. 2019. № 3 (25). С. 68–73.

Морохіна К. Д., курсант 2-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Гребенюк А. М.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ОСНОВНІ ПОЛОЖЕННЯ ПРО КРИМІНАЛЬНИЙ АНАЛІЗ

У нашому сучасному світі стан справ у сфері протидії поширенню злочинності серйозно перешкоджає проведенню демократичних реформ та порушує соціальну рівновагу в суспільстві, тому дослідження кримінальної аналітичної діяльності набуває вагомої значущості. Через що найважливішим завданням Національної поліції є перебудова моделі її діяльності. Як приклад можна брати країни ЄС, що успішно впровадили у правоохоронну діяльність тактики та стратегії, в яких удосконалили процеси аналітичного пошуку й аналітичної діяльності на підставі реструктуризації та оптимізації потоків інформації.

Розглядаючи термін «кримінальний аналіз», потрібно розібрати окремі поняття (а саме «кримінальний» та «аналіз»), які становлять зміст цього терміна. Під словом «кримінальний» ми розуміємо це як той, що стосується вивчення кримінальних правопорушень, боротьби та профілактики правопорушень. Аналіз – це метод дослідження, який вивчає предмет, уявно чи реально розчленовуючи його на складові елементи, як-от частини об'єкта, його ознаки, властивості, відношення, отже, розглядає кожен з виділених елементів окремо в межах єдиного цілого [1].

Кримінальний аналіз – специфічний вид інформаційно-аналітичної діяльності, спрямований на встановлення та передбачення взаємозв'язків між даними про злочинну діяльність та іншими даними, потенційно з ними пов'язаними, їх оцінювання, інтерпретацію та прогнозування розвитку досліджуваних подій з метою їх використання під час досудового розслідування та здійснення оперативно-розшукової діяльності, а також для розроблення тактичних і стратегічних заходів щодо протидії злочинності [2].

Як показала статистика, впровадження системи кримінального аналізу в діяльність Національної поліції дало змогу підвищити аналітичний супровід органу досудового розслідування у сфері протидії злочинності, а також створило передумови для створення міжнародного співробітництва.

Кримінальний аналіз є специфічним видом інформаційно-аналітичної діяльності, яка полягає в ідентифікації та щонайточнішому визначенні

внутрішніх зв'язків між різними видами інформації (відомостями, даними), що стосуються злочину, і будь-якими іншими даними, отриманими з різних джерел, їх використанні в інтересах ведення оперативно-розшукової та слідчої діяльності. Також треба зазначити, що сутність кримінального аналізу полягає в тому, що він допомагає керівництву правоохоронного органу ухвалювати правильні рішення у сфері боротьби з організованою злочинністю, а також надає підтримку слідчому, оперативному працівникові в здійсненні слідчо-оперативної роботи шляхом узагальнення здобутої інформації про організоване злочинне угруповання та надання рекомендації з проведення конкретних слідчих (розшукових) або негласних (слідчих) розшукових дій, оперативно-розшукових заходів з урахуванням особистості конкретного правопорушника, особливостей та структури організованого злочинного угруповання [2].

Кримінальний аналіз спрямований на підтримку діяльності із правозастосування. Продукти кримінального аналізу формують платформу для організації діяльності поліції, керованої аналітикою (продукти кримінального аналізу слугують основою побудови організації і тактики діяльності поліції за новою філософією – переходу від реактивних методів діяльності поліції – реакції на кримінальну подію – до проактивних (вжиття заходів щодо проблеми чи ситуації з наміром усунути або пом'якшити її наслідки), коли діяльність поліції керується продуктами аналізу закономірностей і тенденцій, які ідентифікуються у кримінальному середовищі).

З вищесказаного можна зрозуміти, що кримінальний аналіз передбачає визначення шляху щодо «мінімізації ризику» для суспільства у злочинному світі. На нашу думку, кримінальний аналіз часто застосовується для проведення дій з розкриття правопорушень, він допомагає встановити взаємозв'язки між накопиченими фактами, які, зі свого боку, дають змогу перевірити або виключити слідчі версії.

Бібліографічні посилання

1. Аналіз. URL: https://uk.wikipedia.org/w/index.php?curid=52953
2. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львів. держав. ун-т внутр. справ, 2021. 288 с. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/3723

Нагорна Д. А., курсант 2-го курсу
факультету підготовки фахівців для
підрозділів стратегічних розслідувань
Науковий керівник – Паршин Ю. І.,
професор кафедри фінансових
та стратегічних розслідувань,
доктор економічних наук, професор
*(Дніпропетровський державний
університет внутрішніх справ)*

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ЯК ОДИН ІЗ ГОЛОВНИХ НАПРЯМІВ БЕЗПЕКИ ПІДПРИЄМСТВА

Зародження поняття загрози інформаційної безпеки почалось саме тоді, коли і поява інформаційного середовища. Її проявами тоді стали незаконне використання, пошкодження, крадіжки інформації з комп'ютерів. Пізніше це проявлялось у перекачуванні по мережі неправдивої інформації, вірусів.

В умовах ринкових відносин, коли держава вже не несе відповідальності за результати фінансово-господарської діяльності підприємства, забезпечення безпеки стає однією з найбільш важливих і актуальних проблем його життєдіяльності [1].

Безпека підприємства – це стан стійкої життєдіяльності, за якого забезпечується реалізація основних інтересів і пріоритетних цілей підприємства, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов функціонування [4, с. 6].

У процесі ведення бізнесу підприємці наштовхуються на необхідність певних дій з інформацією, а саме: отримання, обробки, зберігання, перетворення передачі та ліквідації. Важливу інформацію треба ще ретельніше охороняти від зловмисників. Цінність визначає такий ряд параметрів, як корисність, достовірність, своєчасність, релевантність. Під час захисту інформації треба перекрити всі канали її можливого витоку та забезпечити безпеку зберігання на усіх носіях, що є на підприємстві. Особливо важливим є інформування співробітників щодо актуальних загроз та способів захисту даних.

Є дві форми загрози інформаційної безпеки – зовнішні та внутрішні. До перших належить копіювання цінних документів або викрадення файлів; викрадення флеш-карт; викрадення інформації у процесі її передавання по мережі «Інтернет»; пошкодження носіїв з інформацією; донесення інформації до фірм-конкурентів або взагалі до інших країн; викрадення інформації за допомого інсайдерів; переманювання персоналу на іншу фірму.

Внутрішніми загрозами є:

– крадіжка, зараження інформації вірусами або пошкодження файлів

службовцями компанії;

– причини психологічного характеру у зв'язку з відносинами між співробітниками підприємства;

– незадоволення рівнем заробітної плати;

– недобрі відносини між співробітниками та керівництвом підприємства.

Підвищенні вимоги до інформаційної безпеки припускають відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Забезпечення інформаційної безпеки підприємництва може здійснюватися за окремими напрямами.

Правовий напрям, зміст якого полягає у виробленні ефективної державної політики у сфері забезпечення інформаційної безпеки підприємства.

Організаційний напрям полягає у забезпеченні збереження конфіденційної інформації підприємства шляхом формування корпоративної системи захисту; формуванні специфічних правил та рекомендаційних норм [3]; запровадження єдиних правил ведення, зберігання, аналізу, обробки інформації; побудові та обладнанні інформаційних систем, організації пропускного режиму, протипожежного захисту, застосуванні охоронного телебачення, зберіганні документів [4].

Програмно-технічний напрям, у межах якого здійснюється використання сертифікованих, легальних засобів програмного та апаратного забезпечення [3].

Отже, в умовах глобалізації забезпечення інформаційної безпеки на підприємстві полягає у постійному контролі за джерелами виникнення потенційних загроз (антропогенні, технологічні та стихійні джерела) та необхідності здійснювати захист інформації різними способами (захист програм від читання та копіювання, захист авторських прав на інформацію, захист від несанкціонованого доступу і запуску програм, самотестування).

Бібліографічні посилання

1. Бандуляк М. Поняття та система безпеки підприємства. URL: http://banduliak.blogspot.com/2013/03/blog-post_21.html (дата звернення: 10.10.2021)

2. Качан О.І. Інформаційна безпека підприємства в умовах глобалізації. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/09/234.pdf (дата звернення: 10.10.2021)

3. Герасименко О.В., Козак А.В. Інформаційна безпека підприємства: поняття та методи її забезпечення. URL: http://intkonf.org/ken-gerasimenko-ov-kozak-av-informatsiyna-bezpeka-pidpriemstva-ponyattya-ta-metodi-yiyi-zabezpechennya/ (дата звернення: 17.10.2021)

4. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. *Науковий вісник НЛТУ України*. 2008. Вип. 18.9. С. 270–273.

Недєлков К. Ю., здобувач 2-го курсу магістратури Одеського державного університету внутрішніх справ, співробітник відділу research and forensic ТОВ «Група інформаційної безпеки «ФС ГРУП», м. Одеса
Науковий керівник – Ісмайлов К. Ю., старший науковий співробітник НДЛ з проблемних питань кримінального аналізу Одеського державного університету внутрішніх справ, начальник 5-го відділу 3-го управління ДКП НПУ, кандидат юридичних наук, доцент, підполковник поліції

АВТОМАТИЗОВАНИЙ АНАЛІЗ ОБРАЗІВ ФАЙЛОВОЇ СИСТЕМИ ТА ЗБІР ЦИФРОВИХ ДОКАЗІВ КРИМІНАЛЬНОГО ХАРАКТЕРУ ЯК СПОСІБ ЗАПОБІГАННЯ КІБЕРАТАК

Витонченість хакерських інструментів зростає мало не щодня. Якщо кілька років тому шкідливе програмне забезпечення (ПЗ) найчастіше купувалося у самого розробника, який міг зникнути відразу після продажу, не гарантуючи працездатності продукту, то сьогодні практично будь-яка людина з мінімальними теоретичними і практичними навичками в комп'ютерній вірусології та кібербезпеці може придбати malware-as-a-service [1] з повною технічною підтримкою, включно з розробкою ботнету під ключ, купівлею доменного імені, орендою сервера, розгортанням контрольної панелі на сервері (далі C&C-сервер) [2], послугою шифрування шкідливого ПЗ або обфускації коду, тестуванням на детектування великою кількістю антивірусних рішень тощо.

За даними міжнародної некомерційної організації «The Spamhaus Project», яка, у тому числі, досліджує активність ботнетів [3] та географічне розташування їхніх C&C серверів, у своєму звіті [4] за 2-й квартал 2021-го року помістило Україну на 8-ме місце у світі за кількістю розміщених C&C серверів зловмисників (рис. 1).

Порівняно з першим кварталом цього ж року – у другому кварталі кількість зафіксованих серверів зловмисників збільшилась вдвічі. Крім того, один з українських хостинг-провайдерів посів п'яту сходинку (рис. 2) у рейтингу найпопулярніших у зловмисників «майданчиків» для розміщення контрольних панелей ботнетів.

Rank	Country	Q1 2021	Q2 2021	% Change Q on Q
#1	United States	338	281	-17%
#2	Russia	195	233	19%
#3	Netherlands	207	168	-19%
#4	Germany	99	117	18%
#5	France	71	92	30%
#6	Latvia	31	84	171%
#7	United Kingdom	49	57	16%
#8	Ukraine	22	44	100%
#9	Switzerland	59	41	-31%
#10	Seychelles	29	38	31%

Rank	Country	Q1 2021	Q2 2021	% Change Q on Q
#11	Czech Republic	-	31	New entry
#12	Moldova	29	29	0%
#13	Panama	-	16	New entry
#13	Canada	26	16	-38%
#15	Malaysia	-	15	New entry
#15	Poland	-	15	New entry
#17	Finland	-	14	New entry
#18	Vietnam	-	13	New entry
#18	Turkey	25	13	-48%
#20	Brazil	20	12	-40%

Рис. 1. Рейтинг країн, в яких були розміщені C&C сервери
у 2-му кварталі 2021-го року

Через що ще більше актуалізується питання потенційної загрози та превентивних методів виявлення контрольних серверів зловмисників.

Рис.2. Рейтинг хостинг-провайдерів, на яких зафіксовано розміщення C&C серверів у 2-му кварталі 2021-го року

Метою дослідження є розробка алгоритму виявлення та дослідження контрольних серверів ботнетів завдяки автоматизованому аналізу файлової системи цих та збір криміналістичних цифрових доказів.

Rank	Q1 2021	Q2 2021	% Change	Network	Country
#1	35	82	134%	pq.hosting	Russia
#2	53	74	40%	google.com	United States
#3	21	68	224%	serverion.com	Netherlands
#4	51	56	10%	ovh.com	France
#5	23	53	130%	itldc.com	Ukraine
#6	-	49	New Entry	nano.lv	Latvia
#7	131	48	-63%	privacyfirst.sh	Germany
#8	-	47	New Entry	mgnhost.ru	Russia
#9	19	46	142%	hetzner.de	Germany
#10	-	40	New Entry	baxet.ru	Russia
#11	-	35	New Entry	ipjetable.net	France
#12	45	29	-36%	cloudflare.com	United States
#12	-	29	New Entry	digitalocean.com	United States
#14	-	28	New Entry	Internet.it	Russia
#15	26	26	0%	alibaba-inc.com	China
#16	-	25	New Entry	hostsailor.com	U. Arab Emirates
#17	-	22	New Entry	microsoft.com	United States
#18	-	21	New Entry	m247.ro	Romania
#19	-	16	New Entry	offshoreracks.com	Panama
#19	-	16	New Entry	mivocloud.com	Moldova

Зловмисники нерідко вдаються до розгортання своїх послуг і сервісів на «білих» чи «сірих» хостингах, що спричиняє фінансові та репутаційні втрати як жертвам шкідливих кампаній, так і самим хостинг-провайдерам.

Найчастіше для розгортання C&C-панелей використовується VPS (Virtual Private Server) або VDS (Virtual Dedicated Server) з т. з. LAMP

конфігурацією (Linux (ОС), Apache (WEB-сервер), MySQL (СУБД – система управління базами даних), phpMyAdmin (вебінтерфейс для адміністрування СУБД)). Ця конфігурація цілком схильна до автоматизації отримання необхідної інформації для проведення аналізу і збору криміналістичних доказів.

Більш детально зупинимось на розробленій нами концепції автоматизованого рішення для аналізу файлових систем підозрілих орендарів VPS/VDS з отриманням цифрових доказів зловмисників, що дозволить як припинити підготовку шкідливої кампанії, так і потенційно встановити наміри і самого зловмисника. Алгоритм ПЗ, який дозволить отримати з C&C-сервера зловмисника таку інформацію (у разі вилучення дампа ОС у хостинг-провайдера з боку правоохоронних органів у межах кримінального провадження або розслідування):

- SQL дамп бази даних та їх структуру;
- лог-файли підключень SSH/RDP протоколів;
- отримання даних про жертви вірусних кампаній;
- отримання даних про зловмисників.

Щодо одержуваної структури бази даних, то за інформацією з відкритих джерел (наприклад, збірника вихідних кодів C&C-панелей деяких троянів-стілерів внаслідок витоку інформації або припинення розробки і підтримки шкідливого програмного забезпечення (далі ШПЗ) хакером (надається для дослідницьких цілей – https://github.com/threatland/TL-TROJAN)), зустрічаються порожні «шаблони» баз даних того чи іншого ШПЗ, в якому присутня структура та назва таблиць бази даних. За цими даними можна визначити унікальні особливості і з високою точністю визначати приналежність бази даних до того чи іншого виду ШПЗ безпосередньо за структурою бази даних, тобто створення певних сигнатур.

Отже, проаналізувавши усю згадану вище інформацію, робимо висновок, що для розробки алгоритму виявлення, дослідження C&C серверів та збору цифрових доказів необхідно:

- мінімізація часу обробки дампу до ~10 хвилин (залежності від кількості та обсягу інформації, що знаходиться в дампі ФС та потужності дослідного ПК);
- уніфікування процесу обробки дампів файлових систем (далі ФС) з різними версіями і родинами ОС (Ubuntu, Debian, Centos, Windows та інші);
- підвищення відмовостійкості для того, щоб на процес і подальшу обробку дампів не впливали вихід з ладу локального серверу бази даних MySQL завдяки інтеграції можливості діагностики та відновлення БД в разі виникнення помилок;
- створення сигнатур баз даних найчастіших шкідників, які дозволяють категоризувати бази даних і відразу ж виокремлювати потрібну інформацію з потрібних таблиць БД;
- ведення статистики отриманої інформації з кожного дампа і

сумарну кількість отриманої інформації після всього циклу обробки дампів ОС;

- автоматизація роботи за планувальником завдань без участі «ззовні»;
- додавання повного журналювання процесу роботи скрипта і збирати налагоджувальну інформацію в разі якихось несправностей для максимально оперативного вжиття заходів і локалізації проблеми.

Цей проєкт призначений для спрощення і прискорення процедур ідентифікації призначення деяких серверів, на які можуть надходити скарги, а також ті сервери, які можуть використовуватися у вірусних кампаніях зловмисниками.

Бібліографічні посилання

1. Malware-as-a-Service: Who Can Put an End to It? URL: https://clario.co/blog/malware-as-a-service.
2. Command and Control [C&C] Server. URL : https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server.
3. Ботнет. URL : https://ru.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82.
4. Spamhaus Botnet Threat Update: Q2-2021. URL : https://www.spamhaus.org/news/article/813/spamhaus-botnet-threat-update-q2-2021

Одоєвцев А. В., здобувач вищої освіти спеціальності 051 «Економіка»
Жигуліна Я. О., здобувач вищої освіти спеціальності 051 «Економіка»
Науковий керівник – Кононова І. В.,
професор кафедри аналітичної економіки та менеджменту,
доктор економічних наук, доцент
(Дніпропетровський державний університет внутрішніх справ)

ЗАСТОСУВАННЯ МАРКЕТИНГОВИХ ІНСТРУМЕНТІВ ДЛЯ ОЦІНЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Сучасні підприємства України вимушені функціонувати в досить складних соціально-економічних умовах, що характеризуються великою кількістю наддинамічних та практично не прогнозованих чинників макро- і мікросередовища, негативний вплив яких призводить до глибокої структурної деформації вітчизняного підприємництва.

Аналіз наявних напрацювань щодо аналітичного оцінювання економічної безпеки підприємства дає змогу залучити маркетинговий інструментарій для вирішення проблеми її забезпечення. Результати досліджень, опубліковані в наукових працях різних вчених, як-от: О. Антипін, О. Бурдяк, В. Бутов, О. Вівчар, О. Головко, О. Губарев, В. Ігнатов, Г. Козаченко, О. Патрухін, В. Ткачук, І. Отенко, С. Філиппова доводять наявність переваг використання маркетингових методів для оцінювання економічної безпеки підприємства з метою підвищення її рівня [1–4].

Проблема діагностики економічної безпеки підприємства визначається тим, що підприємство є відкритою соціально-економічною системою зі складною структурою. Всі елементи економічної системи підкоряються цілому. Будь-який процес у складній системі відбувається під впливом величезної кількості зовнішніх і внутрішніх факторів, що мають імовірнісний характер, а траєкторія розвитку системи являє собою результат взаємодії безлічі процесів (соціальних, економічних, виробничих, природних тощо) [3].

Для оцінки економічної безпеки підприємства можна використовувати різні види маркетингових інструментів, як-от SWOT, PEST та SNW-аналіз. Такі інструменти маркетингу дають змогу створити фундамент для вдалого поєднання маркетингових інструментів з іншими методиками оцінки економічної безпеки підприємства, є перспективним напрямом досліджень і мають низку переваг над традиційними кількісними та якісними методами. Саме маркетингові методи оцінювання дозволяють вивчати такі динамічні процеси та їх вплив на економічну безпеку. Вони, на відміну від численних статистичних методик з різними критеріями оцінювання, є наочними і краще пристосованими до практичної діяльності управлінця. Також вітчизняними науковцями розроблено різні матриці для вибору стратегії економічної безпеки залежно від репутації підприємства [1], залежно від рівня загроз [2], або від якості корпоративного управління [4]. Кожна з розроблених матриць відображає певну частину внутрішнього чи зовнішнього середовища підприємства (як частку ринку, обсяги продажів, темпи зростання фірми, стадію життєвого циклу товару тощо), і в сукупності дозволяє проводити комплексний аналіз рівня економічної безпеки підприємства.

Будь-якому підприємству з метою його успішного функціонування, необхідно зберегти себе як ціле, а також свої складові (персонал, інформацію, матеріальні і нематеріальні активи, фінанси, клієнтуру) і, крім того, зберегти перспективи розвитку. Складна ситуація вимагає від працівників економічних служб підприємства оперативної розробки конкретних рекомендацій щодо забезпечення економічної безпеки. Організація дослідження зазначених та інших проблем, пов’язаних із процесами, що відбуваються на підприємствах, формують наукову основу для розробки концепцій перспективного соціально-економічного розвитку підприємства в умовах оптимального використання наявних економічних ресурсів, що зрештою забезпечить повноцінне, стабільне й життєздатне на

глобальному рівні зростання національної економіки в цілому.

Треба зазначити, що саме за умови поєднання SWOT, PEST та SNW в єдиний комплекс оцінки ми отримаємо потужний, різносторонній, дієвий механізм для виявлення впливу як зовнішніх, так і внутрішніх факторів з метою попередження виникнення загроз та забезпечення економічної безпеки підприємства в цілому.

Використання SWOT, PEST та SNW аналізу як єдиного комплексу оцінки економічної безпеки підприємства демонструє всебічне та глибоке охоплення всіх проблем та перешкод, що стоять на шляху до забезпечення економічної безпеки. Використання такого потужного комплексу маркетингового інструментарію дає змогу робити прогнози не тільки в короткостроковій перспективі, а й будувати стратегію підприємства на довгостроковий період розвитку.

Бібліографічні посилання

1. Денисов В. Т. Матричный инструментарий принятия управленческих решений стратегического характера. URL: http://vestnik.osu.ru/2010_8/22.pdf (дата звернення: 01.10.2021).
2. Дмитрук Є. В. Визначення стратегії фірми в залежності від сили та напряму впливу репутації підприємства на рівень його економічної безпеки. *Вісник Східноукраїнського національного університету імені Володимира Даля.* 2010. № 8 (150). С. 358–364.
3. Фролова Л. В. Методичні підходи до оцінювання економічної безпеки підприємства. *Актуальні проблеми економіки.* 2016. № 3 (177). С. 199–209.
4. Вахлакова В. В. Оцінювання фінансової та ринкової складових економічної безпеки підприємства. *Бізнес Інформ*. 2017. № 8. С. 212–218. URL: http://business-inform.net/export_pdf/business-inform-2017-8_0-pages-212_218.pdf (дата звернення: 01.10.2021).

Полоз А. М., слухач магістратури
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник –Мирошниченко В. О.,
професор кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ДОКТРИНА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ЯК ЗАСІБ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ З БОКУ ЗОВНІШНЬОПОЛІТИЧНИХ СУБ'ЄКТІВ

Гострі зовнішньополітичні події поставили перед Україною нові виклики у сфері інформаційної безпеки. Зокрема, це стосується гібридної війни, в межах якої до інших форм агресії додалася інформаційна агресія із різноманітними засобами маніпуляції. Інформаційні фактори загрози інформаційній безпеці України з боку агресора – Російської Федерації набули глобального характеру і отримують дедалі більше поширення не тільки на території України, але й усього світового співтовариства.

Зважаючи на це, Україна дещо реформувала суб'єктний склад забезпечення інформаційної безпеки, спираючись на безпекову концепцію і відповідну доктрину. Наприкінці червня 2014 р. у Нацгвардії з'явилося управління інформаційної безпеки, головною метою якого є пошук і викриття імовірних та реальних загроз, а також створення превентивних механізмів для захисту інформаційного простору держави. Крім того, у грудні 2014 р. створено Міністерство інформаційної політики (МІП), яке взяло на себе повноваження з фільтрації інформації, яка надходить ззовні, а також реагування на агресивні інформаційні атаки з боку агресора шляхом формування патріотичного порядку денного в засобах масової інформації [1].

У Постанові Кабінету Міністрів України «Питання діяльності Міністерства інформаційної політики України» № 2 від 14.01.2015 р. серед переліку завдань зазначено «… забезпечення формування та реалізації державної політики у сферах інформаційного суверенітету України та інформаційної безпеки, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами… ». Тобто базовим завданням державного органу є забезпечення інформаційної безпеки. Із цього випливає, що поняття «інформаційна безпека» має не тільки правоохоронне значення. Це поняття як елемент національної безпеки стосується всіх сфер життєдіяльності суспільства: економіки, мистецтва, освіти або громадського життя тощо. Тож українська концепція забезпечення інформаційної безпеки

шляхом реорганізації та створення нових державних органів, до повноважень яких належить захист інформаційної складової національної безпеки, значно розширила галузі, у яких необхідно вживати заходів для інформаційної протекції. Аналогічно розширено повноваження Національної ради з питань телебачення і радіомовлення та Державного агентства з питань кіно протягом 2014–2016 рр. [2].

Доктрина інформаційної безпеки, ухвалена Радою національної безпеки та оборони від грудня 2016 р. та імплементована Указом Президента України від 25.02.2017 р., на сьогодні є концептуальним документом у сфері забезпечення інформаційної безпеки [3]. Текст базового документа почали розробляти ще з 2014 р. фахівці Міністерства інформаційної політики та Комітету Верховної Ради з питань свободи слова та інформаційної політики. Крім того, до роботи над цим нормативно-правовим актом залучалися вітчизняні експерти, журналісти, медіаюристи, представники громадських організацій, іноземні партнери та представники сфери ІТ тощо. Загалом, Доктрина – результат інтелектуальної діяльності значної кількості фахівців, який у перспективі повинен стати надійною правовою основою для протидії інформаційним загрозам з боку зовнішньополітичних суб'єктів та надавати можливість в правовому полі відповідати на агресивні напади з боку агресорів. Доктрина ґрунтується на нормах Конституції України, законах України, Стратегії національної безпеки України, затвердженої Указом Президента від 26 травня 2015 р. № 287, а також положеннях міжнародних договорів, згоду на обов'язковість яких надано Верховною Радою України тощо [4, 5]. Тобто Доктрина є правовим, спеціалізованим та важливим документом у сфері забезпечення інформаційної безпеки України, тому що її положення містять норми багатьох інших нормативно-правових актів, а також рекомендації значної кількості фахівців, що робить її фундаментом інформаційної безпеки.

У Доктрині визначено пріоритети державної політики в інформаційній сфері, до яких віднесено створення та розвиток структур, до повноважень яких входитиме інформаційно-психологічна безпека. Ці структури, насамперед, повинні бути започатковані в Збройних силах України, і доречно при цьому звернути увагу на міжнародну практику у цьому аспекті, зокрема держав-членів НАТО та інших суб'єктів міжнародної безпеки та оборони тощо. Крім того, відповідно до положень Доктрини державна політика повинна бути спрямована на розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України, а також забезпечення повного покриття території України цифровим мовленням із першочерговим акцентом на прикордонні і тимчасово окуповані території. На нашу думку, вищеперелічені глобальні пріоритети в інформаційній політиці та безпеці є виваженими стратегічними кроками для забезпечення інформаційної стабільності в державі. Вони базуються на досвіді європейських держав у сфері інформаційної безпеки і є принципово нові, спрямовані на досягнення

цілей Доктрини [3].

Безперечно, можна повністю погодитись із доцільністю встановлення більш суворого контролю за інформацією, яку поширюють засоби масової інформації та ресурси Інтернет. Це висвітлено у Доктрині як один із базових пунктів, що в умовах існування значної кількості загроз для інформаційної безпеки України є пріоритетним. Інформаційну складову національної безпеки держави не можна недооцінювати, адже вона є підґрунтям для формування окремих елементів світогляду, ідеології, суспільної моралі тощо, а панування екстремістських, хибних або руйнівних для суспільної думки позицій негативно впливає не тільки на стан суспільних відносин, але й авторитет державної влади, її цінність та взаємодію з населенням, збереження порядку і безпеки тощо. Доктрина передбачає, що встановлення більш суворого контролю за інформацією, яка надходить від засобів масової інформації, потребує розширення повноважень державних регуляторних органів, які регламентують функціонування інформаційного простору держави та наділені законодавчою ініціативою щодо формування механізму виявлення фіксації, блокування та видалення загрозливих елементів з інформаційного сегмента держави [2, 3, 6].

Розбалансованість та розпорошеність діяльності, а також інституційна невизначеність є детермінантою зниження ефективності заходів у протидії загрозам інформаційній безпеці України. Суттєвою проблемою у цьому разі є відсутність єдиної координації діяльності у сфері інформаційної безпеки. Наприклад, у Доктрині визначено необхідність централізації діяльності та створення ефективних алгоритмів координації та контролю всередині механізму забезпечення інформаційної безпеки. Однак ці положення є, ймовірніше, декларативними, адже виникають ризики відсутності належного реагування в разі виникнення суттєвих загроз інформаційній безпеці в умовах відсутності належних механізмів [2, 3, 7, 8, с. 50–58].

Доцільним було б також звернути увагу на розширення повноважень Міністерства з окупованих територій, повноваження якого необхідно розширити в аспекті вирішення інформаційних загроз, та розширити таким чином положення Доктрини. На це у власних дослідженнях з даного приводу вказує і медіаексперт Д. Дудик [2, 3, 9, с. 34–37].

Отже, інформаційна безпека є важливою складовою національної безпеки держави і саме від її захисту державними і недержавними структурами залежить стабільність суспільних відносин та ідеології, пануючої в суспільстві. В Україні сьогодні наявні загрози інформаційній безпеці з боку зовнішньополітичних суб’єктів, що зумовлено складними подіями на тимчасово окупованих територіях. Доктрина інформаційної безпеки укладена широким колом фахівців для здійснення заходів, спрямованих на попередження численних інформаційних загроз, однак і вона має певні неточності, які необхідно усунути для ефективної діяльності механізму забезпечення інформаційної безпеки.

Бібліографічні посилання

1. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. *Центр досліджень соціальних комунікацій НБУВ СІАЗ НЮБ ФПУ*. *Резонанс.* 2017. № 18. URL : http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2760:doktrina-informatsijnoji-bezpeki-yak-zasib-protidiji-informatsijnim-zagrozam-2&catid=63&Itemid=393 (дата звернення: 08.10.2021).

2. Питання діяльності Міністерства інформаційної політики України : Постанова Кабінету Міністрів України від 14.01.2015 р. № 2. URL : https://zakon.rada.gov.ua/laws/show/2-2015-%D0%BF#Text (дата звернення: 08.10.2021).

3. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 08.10.2021).

4. Конституція України : Закон України в редакції від 01.01.2020 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 08.10.2021).

5. Про Стратегію національної безпеки України : Рішення Ради національної безпеки і оборони України від 06.05.2015 р. № n0008525-15. URL: https://zakon.rada.gov.ua/laws/show/n0008525-15#Text (дата звернення: 08.10.2021).

6. В Україні розроблена і прийнята Доктрина інформаційної безпеки. URL: https://ua.korrespondent.net/ukraine/3820536- vsikh-pereviriat-vlada-prydumala-novyi-zakhyst-vid-rf (дата звернення: 08.10.2021).

7. Державна інформаційна політика формування інформаційного суспільства: зарубіжний досвід. URL : http://www.nbuviap.gov.ua/index.php?option =com_content&view=article&id=3 244:derzhavna-informatsijna-politika-formuvannya-informatsijnogo-suspilstvazarubizhnij-dosvid&catid=81&Itemid=415 (дата звернення: 08.10.2021).

8. Конах В. К. Сучасні тенденції в захисті національних медіапросторів від російської пропаганди. Стратегічні пріоритети. Національний інститут стратегічних досліджень, 2016. 132 с.

9. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Видавничий дім «Гельветика», 2017. 168 с.

Попко С. В., курсант 3-го курсу
факультету підготовки фахівців для
підрозділів стратегічних розслідувань
Науковий керівник – Неклеса О. В.,
викладач кафедри фінансових
та стратегічних розслідувань
*(Дніпропетровський державний
університет внутрішніх справ)*

ТЕОРЕТИЧНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Для ефективного управління сучасними українськими підприємствами, залученими в процеси сучасної нестабільної економіки, важлива наявність актуальних науково-методологічних підходів до забезпечення стійкої та надійної економічної безпеки. Поточний стан економіки сприяє регулярному виникненню економічних криз, це свідчить про те, що розробка прийомів оцінки загроз і механізмів підвищення економічної безпеки бізнесу та підприємницької діяльності набуває особливої актуальності. Вивчення публікацій, присвячених забезпеченню економічної безпеки підприємств, дає можливість стверджувати, що більшість матеріалів відображає відсутність єдиного підходу до визначення сутності та важливості економічної безпеки.

Активізація досліджень проблем економічної безпеки визначила розвиток декількох підходів, серед яких можна виділити: системний, нормативно-правовий, функціональний та синергетичний.

Системний підхід до дослідження економічної безпеки пов’язаний з вивченням всіх господарських процесів підприємства з позиції теорії динамічних систем. У цій теорії безпека розглядається як властивість, стан підприємства, зумовлений взаємодією системи і мікро-, макросередовища функціонування.

Нормативно-правовий підхід спирається на законодавчі акти у сфері економічної безпеки. Основу правової бази під часи розробки системи економічної безпеки підприємства становлять: Закон України «Про Бюро економічної безпеки» від 28 січня 2021 року, наказ Міністерства економічного розвитку і торгівлі України «Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України» від 29 жовтня 2013 року, а також інші нормативно-правові акти, спрямовані на захист підприємств, їх економічну безпеку. Ці документи містять концептуальні ідеї безпеки, основні терміни та їх визначення.

Функціональний підхід до економічної безпеки передбачає наявність прямої залежності між ступенем впливу будь-якого фактора на діяльність підприємства і наслідком від цього впливу, що виявляється як зміна

становища підприємства.

Проблема економічної безпеки підприємств знайшла відображення і в синергетиці, де безпека суб'єкта господарювання визначається як динамічно стійкий стан щодо несприятливих впливів, діяльність щодо захисту від внутрішніх і зовнішніх загроз, а також забезпечення дієвих зовнішніх і внутрішніх умов його існування, які гарантують його стабільний розвиток. Згідно з таким трактуванням економічну безпеку підприємства визначає вплив зовнішнього середовища, яка в умовах ринку постійно змінюється, ніколи не залишається стабільною, до того ж у сучасних умовах національної економіки.

Цей підхід поширений у публікаціях вітчизняних вчених-економістів, які розглядають зміст категорії економічної безпеки підприємства з позицій істотного впливу зовнішнього середовища і способів захисту від його ж негативного впливу.

Наявність загроз стабільному функціонуванню підприємства зумовлює необхідність застосування відповідних методологічних прийомів дослідження економічної безпеки підприємства [1].

У своєму дослідженні ми дотримуємося першого підходу, спрямованого на ідентифікацію, оцінку та управління ризиками і загрозами економічної безпеки підприємства, оскільки, на нашу думку, тільки своєчасне і навіть випереджаюче управління ризиками дозволить підприємству мінімізувати їх вплив на економічну безпеку.

В теорії економічної безпеки розглядаються такі загрози і їх класифікації:

– за сферами виникнення (внутрішні та зовнішні);

– за об'єктом посягання (майно, інформація, технології);

– за природою виникнення (правові, економічні, природні, екологічні);

– за величиною втрат або збитку (помірні, значні і катастрофічні);

– за віддаленістю в часі (близькі, далекі).

Результатом проведення моніторингу та оцінки економічної безпеки підприємства є вибір відповідного умовам, що склалися, напряму нейтралізації загроз [2, с. 213].

Отже, економічна безпека підприємства має специфічні особливості. Її забезпечення та постійна підтримка є досить складним процесом в управлінні підприємством. Проте, незважаючи на складність забезпечення економічної безпеки, а також на відносну новизну цього фактора для багатьох підприємств, вона є актуальним елементом менеджменту підприємств, без реалізації якого не можна забезпечити їх стійкий розвиток.

Бібліографічні посилання

1. Денисов С. Ф., Філей Ю. В. Причини та умови злочинності у сфері економіки. *Криміналістика і судова експертиза*. 2021. Вип. 66. С. 272–283. URL: http://nbuv.gov.ua/UJRN/krise_2021_66_30
2. Мішеніна Н. В., Мішеніна Г. А., Ярова І. Є. Економічний аналіз : навч. посіб. Суми : СумДУ, 2014. 306 с.

Рец В. В., слухач магістратури
факультету підготовки фахівців
для органів досудового розслідування
Науковий керівник – Мирошниченко В. О.,
професор кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СТРАТЕГІЧНЕ ЗАВДАННЯ СВІТОВОЇ СПІЛЬНОТИ: ПРОБЛЕМАТИКА

У сфері забезпечення інформаційної безпеки на міжнародному рівні важливе значення має міжнародне співробітництво усіх суб'єктів міжнародного права, які диференційовано між собою взаємодіють. Інформаційна безпека є запорукою стабільності у світі. Саме тому держави, зокрема Україна, повинні здійснювати пошук спільних рішень в межах міжнародних організацій або в межах переговорів укладанням договорів або меморандумів, які стосуються напрямів протидії інформаційним та кіберзагрозам, кібервійнам, інформаційному тероризму та інформаційної злочинності. Треба зауважити, що світові проблеми, пов'язані з інформаційними загрозами, стосуються безпосередньо окремої держави, впливаючи на її суспільно-політичну, економічну, ідеологічну та багато інших сфер діяльності [1].

Міжнародне співтовариство створило нормативно-правову базу для реагування на кіберзлочини та кібертероризм і закликає держави до активної боротьби зі злочинними загрозами інформаційній безпеці. Однак проблематика полягає у відсутності ефективних механізмів, які б могли реалізувати матеріальні норми та рекомендації щодо попередження кіберзлочинів або притягнення осіб, що їх вчинили, до певного виду юридичної відповідальності. Боротьба з такими серйозними проблемами, як кіберзлочини та кібертероризм здійснюється державами через механізми міжнародного співробітництва в галузі права та безпеки. Державами контролюється використання технологій, комунікацій та ресурсів з тим, щоб вони не були використані для вчинення міжнародних злочинів та злочинів міжнародного характеру. Інформаційно-телекомунікаційні мережі – це платформа, на якій зібрано значний моноліт інформації, саме тому вони є інструментом поширення екстремістських позицій, а також відомостей, які становлять загрозу для національної безпеки окремої держави. Міжнародне співтовариство, базуючись на існуючій та функціонуючій нормативно-правовій базі, робить кроки до формування дієвих та ефективних механізмів попередження інформаційних загроз із диференційованих джерел. На сьогодні досягнуто певного успіху в цій царині, адже у розробці норм

двостороннього і багатостороннього співробітництва для запобігання вчинення правопорушень у сфері користування Інтернетом та іншими інформаційними та телекомунікаційними базами даних або банками інформації досягнуто неабиякого прогресу [2].

Необхідно наголосити, що світова спільнота має чимало напрацювань у сфері забезпечення інформаційної безпеки, значна кількість яких робить акцент на необхідності чіткого розуміння і виокремлення факторів, що зумовлюють загострення загроз інформаційній безпеці. Детермінанти загроз інформаційної безпеки є системними та створюють перешкоди для реалізації прав і свобод людини та громадянина кожної окремої держави. М. Т. Гаврильців зазначає, що аналіз викликів – це завжди суб'єктивний процес сприйняття суб'єктом певних факторів через призму власних інтересів і професійності [3, с. 201].

У теорії інформаційної безпеки розглядається механізм загрози безпековому компоненту в межах гібридної війни. Зокрема, посягання на інформаційну безпеку держави під час гібридної війни здійснюється за такою моделлю: агресор втручається в інформаційно-комунікаційний простір країни з метою придушення опору та формування ідеологічної позиції і переконань, які відповідають інтересам агресора. Це здійснюється з використанням різноманітних інструментів маніпулювання, починаючи від впливу і маніпуляції громадською думкою через засоби масової інформації і аж до вчинення кіберзлочинів [4, с. 18]. Саме тому на сьогодні світова спільнота вважає, що запобігання загрозам інформаційній безпеці як важливому елементу національної безпеки є одним із стратегічних завдань і формує низку відповідних концепцій.

Отже, міжнародна інформаційна безпека сьогодні є стратегічним завданням всього світового співтовариства, зусиллями якого створено значну нормативно-правову базу із запобігання кіберзагрозам. Однак проблематика полягає у відсутності ефективних механізмів, які б могли реалізувати матеріальні норми та рекомендації щодо попередження кіберзлочинців або притягнення їх до певного виду юридичної відповідальності. Боротьба із такими серйозними проблемами, як кіберзлочини та кібертероризм здійснюється державами через механізми міжнародного співробітництва в галузі права та безпеки.

Бібліографічні посилання

1. Макаренко Є. А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. Актуальні проблеми міжнародних відносин. 2011. Вип. 102 (Ч. І).

2. Report on World Internet Development 2016 of World Internet Conference «Innovation-driven Internet Development for the Benefit of All – Building a Community of Common Future in Cyberspace». URL: http://www.wuzhenwic.org/2016-11/18/c_61834.htm (дата звернення: 08.10.2021).

3. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал.* 2020. № 2. С. 200–203.

4. Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 4. С. 16–26.

Рожков Е. Є., студент групи Б-ПД-932
Науковий керівник –Рибальченко Л. В.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат економічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ШАХРАЙСТВО В ІНТЕРНЕТІ

Сьогодні в Україні та у світі поширюється шахрайство в інтернеті, оскільки багато людей працюють, здійснюють покупки у ньому, тому шахраї використовують інтернет для заволодіння чужим майном, бо на цей час це актуально.

Необхідно зазначити, що відбувається різке збільшення злочинів проти власності у зв'язку з економічними, політичними та соціальними перетвореннями. Це стосується, зокрема, і шахрайства, особливо через мережу «Інтернет». Велика інформаційна система стала благодатним середовищем для здійснення шахрайства в мережі «Інтернет». Використання Інтернету для здійснення шахрайства, мабуть, є одним із поширених видів кіберзлочинності.

Спочатку необхідно визначитись з поняттям шахрайства. Регулювання шахрайства в цілому передбачене Кримінальним кодексом України (ст. 190). Згідно з цією статтею під шахрайством треба розуміти заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою [1].

Обманом є повідомлення неправдивих відомостей або приховування, умовчування певних обставин, повідомлення про які було обов'язковим за цих обставин. А зловживання довірою полягає у тому, що злочинець для заволодіння майном потерпілого використовує близькі, довірчі стосунки з ним. Внаслідок шахрайських дій потерпілий – власник, володілець, особа, у віданні або під охороною якої є майно, добровільно передає майно або право на майно винній особі. Безпосередня участь потерпілого у передачі майнових благ і добровільність його дій є обов'язковими ознаками шахрайства, які відрізняють його від викрадення майна та інших злочинів проти власності.

Поняттям та особливостями шахрайства займались такі вчені зі сфер психології, педагогіки, політології, соціології та історії, зокрема Ю. А. Єрмакова, Т. С. Кабаченко, Ц. Р. Кара-мурзи, Г. А. Ковальова, І. К. Мірошник, Є. В. Сидоренко, Ю. М. Дмитрієнко, Н. В. Гребіня, К. Л. Попова, У. Альбрехт, Дж. Венц, Т. Уільям та ін.

Під Інтернетом треба розуміти велику базу інформації. Інтернет став невід'ємною частиною для людей. Але розвиток інформаційних технологій не

тільки приносить позитив та легкість, а й призводить до негативних наслідків, а саме розвитку нових злочинів, до яких належить шахрайство в мережі «Інтернет». У нашому сьогоденні інформація стала предметом злочинної діяльності. Для шахраїв це досконалий інструмент, завдяки якому вони можуть залишатися анонімними під час вчинення злочинів. З кожним кроком цей вид шахрайства все більше удосконалюється, шахраями використовуються більш актуальні продумані способи та маніпуляції людьми [2, с. 30].

Цей вид шахрайства має свої особливості, до яких належать:

– контакт між потерпілим і правопорушником відбувається через Інтернет;

– жертва не бачить і майже ніколи не знає зловмисника особисто;

– передача грошей або майна здійснюється дистанційно.

Розслідуванням цього виду шахрайства займається кіберполіція. До видів шахрайства в мережі «Інтернет» належить фішинг, шахрайство з кредитними картами, фіктивні інтернет-магазини, пропозиції допомоги в погашенні боргу, пропозиції швидкого заробітку. Щодо фішингу, то можна вважти його найстарішим видом шахрайства в Інтернеті. Його мета – отримання логіна та пароля користувача з метою подальшого використання його особистих даних. Прикладами фішингу є розсилка з електронної пошти, схожої на адресу відомого бренду, з проханням авторизуватися на сторонньому ресурсі; використання сайтів, майже ідентичних популярним інтернет-магазинам, фінансовим організаціям і соцмережам. Стосовно шахрайства з кредитними картками, то шахраї можуть отримати кредит на картку користувача у разі, якщо останній не заблокував її у випадку втрати або коли користувач повідомив особисті дані, які містяться на картці (номер картки, термін дії та CVV-код).

Отже, сутність шахрайства полягає у психологічному впливі шахрая на жертву, а саме досягнення матеріальної вигоди шляхом обману або шантажу. До основних прийомів злочинного маніпулювання і психологічного впливу на свідомість та поведінку жертви в мережі «Інтернет» можна віднести:

– маніпулювання змістом та формою надання інформації;

– створення штучного дефіциту часу для ухвалення рішення (вимагання сплатити неіснуючу послугу або товар у найкоротші терміни).

Дослідивши літературу, зазначимо, що шахраї гарні психологи та знають, на які слабкі сторони треба надавити для отримання результату, а саме, щоб люди добровільно розлучалися зі своїми грішми (жадібність, віра «в щасливий випадок», спрага «халяви» тощо). На практиці притягнути до відповідальності таких шахраїв вкрай важко, оскільки вони в Інтернеті є анонімними. Тому, для того щоб не стати жертвою шахраїв, необхідно:

– не надавати особисті дані на незнайомих сайтах. Паспортні і платіжні дані, телефон, логін і пароль в Інтернеті надавати тільки в разі 100 % впевненості, що перебуваєте на офіційних сайтах;

– уточнювати інформацію та ставити додаткові запитання, що

стосуються ситуації;

– не робити великих передплат під час покупки в інтернет-магазині;

– не користуватися підозрілими сервісами або пропозиціями інших громадян.

Зазвичай, люди або сервіси, які пропонують швидкий заробіток, на практиці і є шахраями.

Тож, підсумовуючи вищевикладене, потрібно правоохоронним органам та іншим органам проводити масові інформування населення щодо діяльності шахраїв, їх методів та прийомів, щоб люди не стали жертвою шахраїв. Наприклад, як це зробили у Вільногірському бюро правової допомоги, де провели бесіду з населенням про найпоширеніші нині види шахрайства, в тому числі і про «телефонних» злочинців та про наслідки таких SMS-повідомлень [3].

Бібліографічні посилання

1. Кримінальний кодекс України : Кодекс від 05.04.2001р. № 2341-III в редакції від 04.10.2021р. *Відомості Верховної Ради України (ВВР)*. 2001. № 25–26. Ст.131.

2. Прудка Л. М. Психологічні особливості шахрайства в мережі Інтернет. *Південноукраїнський правничий часопис*. 2018. № 2. С. 30–33.

3. Нужна О. Про шахрайство, яке завжди на часі, розповідають у Вільногірському бюро правової допомоги. URL: https://www.legalaid.gov.ua/novyny/pro-shahrajstvo-yake-zavzhdy-na-chasi-rozpovidayut-u-vilnogirskomu-byuro-pravovoyi-dopomogy/

Романенко П. П., курсант 3-го курсу
факультету підготовки фахівців
для підрозділів кримінальної поліції
Науковий керівник – Гребенюк А. М.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ІНФОРМАЦІЙНІ ПІДСИСТЕМИ, ЯКІ ДОПОМОГАЮТЬ РОЗСЛІДУВАННЮ ПІД ЧАС КРИМІНАЛЬНОГО АНАЛІЗУ

Розгляд цієї теми зумовлений розслідуванням правопорушень, які потребують використання кримінального аналізу. Інформаційні підсистеми допомагають досягнути очікуваного результату, але важливо правильно використовувати обрану підсистему аби прискорити процес пошуку.

Інформаційні підсистеми, які функціонують на базі Національної поліції України, допомагають розкриттю правопорушень різної складності,

бо в підсистемах міститься інформація, яка може прямо стосуватись правопорушення. Головним є правильність використання кожної підсистеми та спрямування її у правильне русло.

Наказ Міністерства внутрішніх страв України від 14.06.2019 р. № 508 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» містить в собі положення, які регламентують порядок формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України», призначеної для обробки відомостей під час прийняття та реєстрації заяв і повідомлень про кримінальні правопорушення та інші події. Тобто працівник поліції повинен забезпечити повноту та своєчасне внесення до Єдиного обліку відомостей, з якими працівники поліції будуть працювати або використовувати у кримінальному аналізі, тому від правильності введеної інформації буде залежати подальший хід справи [1].

Наявні деякі проблемні питання стосовно доступу до деяких підсистем, з якими працює Національна поліція. Проблема щодо здійснення доступу до ІПС ОНП («Цунамі», «Армор»), яка полягає у можливості входу одночасно з декількох робочих станцій під одним логіном та паролем, що може призводити до витоку інформації службового характеру, повинна бути у найкоротший час остаточно вирішена. Доступ до інформаційних підсистем має мати абсолютну захищеність, бо важливість збереження персональних даних у цьому контексті на першому плані [2].

Загалом досить поширеними інформаційними ресурсами залишаються соціальні мережі, за допомогою яких можна знаходити інформацію та використовувати її під час розслідування. Зараз, за результатами різних експертних оцінок, американські розвідувальні служби з відкритих джерел добувають від 35 % до 95 % розвідданих. У провідних країнах світу система OSINT є важливим інструментом захисту національних інтересів та основною складовою в діяльності профільних силових відомств [3].

Звісно, що інформаційні системи Національної поліції України досить ефективно виконують свої завдання та функції, але перед тим як безпосередньо переходити до пошуку, потрібно відібрати максимум інформації з відкритих джерел. Можливо, що саме технологія OSINT стане поштовхом до розкриття кримінального правопорушення або іншого протиправного діяння.

OSINT (Open Source INTelligence) – це збір, аналіз, обробка даних, які є в загальному доступі, але ці дані завжди специфічні, тобто зібрані та структуровані особливим способом для відповіді на конкретне питання [6].

Швидкість розслідування цілком залежить від аналітичних вмінь та вмінь правильно користуватися пошуком за відповідними даними. За кожною отриманою інформацією кримінальному аналітику необхідно

ухвалити рішення про її необхідність, зберігання і подальше використання. Засоби аналітичної обробки допомагають знизити витрати й заощадити час на пошук інформації, істотної для розкриття та розслідування злочинів [4].

Одним з головних критеріїв ефективності розслідування є захищеність даних інформаційних підсистем, які використовуються в діяльності поліції. Одним з головних шляхів захисту є криптографія. Стійкість будь-якої системи закритого зв'язку визначається ступенем таємності використовуваного в ній ключа. Проте цей ключ повинен бути відомий іншим користувачам мережі, щоб вони могли вільно обмінюватися зашифрованими повідомленнями. У цьому змісті криптографічні системи також допомагають вирішити проблему автентифікації (встановлення дійсності) прийнятої інформації. Для класичної криптографії характерне використання однієї секретної одиниці – ключа, що дозволяє відправникові зашифрувати повідомлення, а одержувачеві розшифрувати його [5].

Отже, інформаційні підсистеми під час розслідування мають важливе значення під час кримінального аналізу. Інформаційні підсистеми є неабиякою допомогою працівникам не тільки поліції, але й всіх правоохоронних органів загалом. В епоху інформатизації суспільства інформаційні ресурси стали допоміжним елементом пошуку для поліції. Тому потрібно, щоб інформаційні підсистеми правильно використовували, інформація повинна містити загально визначений характер, а також інформація повинна перебувати під абсолютним захистом, аби дані, які зберігаються, не потрапили до рук злочинців.

Бібліографічні посилання

1. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» : наказ МВС України від 14.06.2019 р. № 508. URL: https://zakon.rada.gov.ua/laws/show/z0739-19#Text (дата звернення: 22.03.2021).

2. Рижков Е. В., Дзех Я. С. Проблемні питання інформаційно-аналітичного забезпечення в системі органів Національної поліції та проблемні питання щодо захисту під час виконання службових обов'язків : зб. наукових статей за матеріалами доп. Всеукр. науково-практ. конф. 21 грудня 2018 року / упорядник Т. В. Магеровська. Львів : ЛьДУВС, 2018 С. 83–86.

3. Пащенко Т. П. Гібридна війна та соціальні мережі. *Інформаційний вимір гібридної війни: досвід України* : матеріали Міжнар. науково-практ. конф. Київ : НУОУ, 2017. С. 62–65.

4. Фаріон О. Б. Сфери застосування таких систем різноманітні. *Алгоритм опрацювання оперативно-розшукової інформації для забезпечення потреб кримінального аналізу злочинної діяльності* : зб. наукових пр. Націон. академії держав. прикордонної служби України. Серія : військові та технічні науки. 2013. № 1 (59). С. 194–203.

5. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека : навч. посіб. : у 2 ч. Харків : Вид-во ХНЕУ, 2008. Ч. 2. С. 78–79.

6. Политическое Экспертное Сообщество (Модель OSINT. Открытые источники в мире разведки). URL: http://strateger.net/model_osint_otkritie_istochniki_v_mire_razvedki (дата звернення: 29.10.2021).

Рукіна Д. О., студентка 1-го курсу
юридичного факультету
Науковий керівник – Насонова С. С.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Невід'ємною частиною сучасного світу є інформаційні технології. Вони охоплюють усі сфери життя людей та сприяють розвитку держави на всіх її рівнях. Із розвитком інформаційних технологій постала проблема формування системи кібербезпеки, яка протидіятиме інформаційним загрозам та захистить інтереси суспільства. Ця проблема не минула і Україну. Для її вирішення були розроблені державно-правові норми, які деякою мірою поліпшили роботу соціальної інфраструктури.

Метою цієї публікації є вивчення сучасного стану питання правового забезпечення інформаційної безпеки України.

Кожна держава для убезпечення власної діяльності вводить низку заходів, які спрямовані на подолання кібератак та несення кримінальної відповідальності хакерів за скоєне діяння. До країн з високим рівнем інформаційної безпеки належать Великобританія та США. Політика цих країн спрямована на поліпшення та поглиблення знань про інформаційні ресурси, які забезпечують захист від небезпеки в інформаційному просторі. Підтвердженням активних дій у напрямі боротьби з інформаційними загрозами є, наприклад, підписання президентом США Джо Байденом указу про оголошення жовтня 2021 року – місяцем обізнаності у сфері кібербезпеки [1] та утворення у Великобританії системи кібербезпеки [2], яка почала функціонувати з 2018 року.

На жаль, наша країна на цей час розвивається у цьому напрямі не так активно, як Великобританія та США. Проте перший крок на шляху створення сучасної системи кіберзахисту в України все ж таки було зроблено. Забезпечення кібернетичної безпеки нашої країни базується на принципах верховенства правових норм, дотримання яких регламентовано законодавством. Зокрема, 19 червня 2019 року було ухвалено Постанову Кабінету Міністрів України № 518 «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [3], а 26 серпня 2021 року Президент України Володимир Зеленський Указом № 447/2021 затвердив рішення Ради національної безпеки і оборони України «Про стратегію

кібербезпеки України» [4].

Варто зазначити, що розуміння українською владою поняття «забезпечення інформаційної безпеки» продукується на тому, щоб упорядкувати, модернізувати та забезпечити правомірні суспільні відносини на просторах інформаційних ресурсів. В основу цих відносин покладені такі твердження:

1. Держава має повністю взяти відповідальність за національну, у тому числі за інформаційну безпеку та захищення індивідуальних інтересів кожного громадянина. А отже, мають бути відповідні правові акти, які будуть регламентовані та регульовані законодавством.

2. Підвищення рівня міжнародних інтеграційних процесів впливає на співробітництво з іншими державами, покращує міжнародні зв'язки. Держава має сприяти формуванню міжнародної співпраці між країнами в інформаційній сфері.

Отже, для забезпечення інформаційної безпеки в країні необхідно упорядкувати систему, яка відповідає за правотворчий процес. Конструктивізація цієї системи спрямує владні інстанції на вдосконалення правових основ законодавства [5], отже, буде сформована система правового забезпечення інформаційної безпеки України.

Висновки. Зараз Україна не належить до числа країн з високим рівнем інформаційної безпеки. Для підвищення рівня захисту від інформаційних загроз необхідно вжити низку спеціальних заходів, у тому числі упорядкувати систему, яка відповідає за правотворчий процес. Для цього треба розробити закони, які б забезпечували правомірні суспільні відносини між споживачами в інформаційній сфері.

Бібліографічні посилання

1. Кібербезпека стане головним питанням для США в жовтні – Байден. URL: https://www.ukrinform.ua/rubric-world/3325206-kiberbezpeka-stane-golovnim-pitannam-dla-ssa-v-zovtni-bajden.html

2. Британська мережа кібер-безпеки. URL: https://uk.wikipedia.org/wiki/%D0%91%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0_%D0%BA%D1%96%D0%B1%D0%B5%D1%80-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8

3. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

4. Стратегія кібербезпеки України: цілі та пріоритети. URL: https://armyinform.com.ua/2021/08/strategiya-kiberbezpeky-ukrayiny-czili-ta-priorytety/

5. Рибальченко Л. В., Кишкань М. А. Правове забезпечення інформаційних технологій в правоохоронній та юридичній діяльності. *Використання сучасних інформаційних технологій в діяльності національної поліції України* : матеріали Всеукр. науково-практ. семінару. Дніпро : Дніпропетр. держав. ун-т внутр. справ, 2019. С. 99–100.

Сафонова Т. Р., слухач
магістратури юридичного факультету
Науковий керівник – Косиченко О. О.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

КРАДІЖКА ЦИФРОВОЇ ОСОБИСТОСТІ

Крадіжка цифрової особистості – злочин, за якого незаконно використовуються персональні дані людини для отримання матеріальної вигоди. Англійський термін Identity theft виник у 1964 р., його переклад «крадіжка цифрової особистості» є неточним, оскільки саму особистість вкрасти неможливо. Термінологія в цьому разі тільки заважає. По суті, крадуть персональні дані, які потім використовують для різних злочинних дій. Розглянемо, яку інформацію і навіщо крадуть.

Крадуть фотографії, паспортні дані, копії документів, селфі з документами, копії банківських карток. Ви можете через пошук в Google знайти чимало пропозицій купити копії паспортних даних, можете зустрити серед продаваних і свої.

Насамперед персональну інформацію крадуть для шахрайства. Розглянемо приклад. Якщо ви – красива дівчина, у вашому інстаграмі чоловіки зависають годинами і все у вас добре, поки за інформацією про вашу особу не прийде шахрай. Ваші дані і фотографії можуть прикрасити сторінку на сайті знайомств, з якої потім будуть виманювати передоплату у чоловіків, які бажають з вами познайомитись. Одна з подібних схем працює так: красива дівчина, за акаунтом якої ховається шахрай, знайомиться на сайті знайомств з чоловіком, якому відведена роль жертви. За допомогою шаблонних фраз і повідомлень зловмисник знаходить спільну мову, що закінчується запрошенням у кіно. Але це не звичайний кінотеатр, а квитки на приватні місця, де вони зможуть дивитися кіно лише удвох. Ну як від такого відмовитися? Подібні квитки продаються на спеціальному сайті і надаються як особлива послуга в кінотеатрах. На сайті є можливість оплатити карткою, можливість повернення коштів за квитки за годину до початку, і інші приємні для покупця моменти. Є тільки один маленький нюанс – сайт належить шахраю, і після оплати гроші підуть в кишеню зловмисника, а «красуня» припинить спілкування. Є й інші способи монетизації: фотографії в купальнику відмінно підійдуть для шахрайського сайту інтим-послуг і якщо ваші знайомі потраплять на нього, вам доведеться довго розповідати історію про крадіжку ваших фотографій і даних.

Розглянемо ще приклад щодо отримання бонусів і послуг з післяплатою. Можливо, ви бачили рекламу букмекерських компаній, форекс-сайтів, онлайн покер-румів або інших сайтів, що пропонують новим клієнтам гроші на рахунок, за які ви можете скористатися послугами. Все дуже просто: ваші дані будуть використані зловмисником для створення облікового запису з метою отримання бонусів. Як правило, це досить необразливо для жертви, хіба що ви не зможете скористатися рекламною пропозицією в майбутньому.

Куди менш райдужними можуть бути наслідки придбання на ваші дані послуг з післяплати, коли зловмисник реєструє на ваші дані акаунт, використовує послуги, а в кінці замість їх оплати просто зникає. У цьому разі від вашого імені відбувається повноцінне шахрайство.

Ще приклад. Фотографії красивих дівчат використовуються при створенні акаунтів для спаму в соціальних мережах, це збільшує частоту успішних атак. Найчастіше зловмисники не обтяжують себе міняти дані і беруть реальні дані жертви, включно з ім'ям і прізвищем.

Але не тільки красиві дівчата цікаві шахраям, будь-які крадені дані можуть бути використані для створення вебсторінок. Наприклад, відома російська фабрика тролів, яка була обвинувачена у втручанні у вибори США, використовувала для поширення даних сотні акаунтів. Як ви можете здогадатися, реальні власники даних не знали, що їх фотографії використовуються в політичній кампанії проти одного з кандидатів.

В мережі ви можете знайти пропозиції щодо продажу акаунтів в різних соціальних мережах та інших сайтах. Для реєстрації подібних акаунтів зловмисники також використовують крадені дані, рідше подібні акаунти збираються внаслідок фішингу або витоків даних.

Сьогодні, в умовах великої конкуренції, компанії, що займаються онлайн позиками повсюдно знижують планку вимог до позичальників, спрощуючи процедуру отримання невеликої суми. Подібні ризики цих шахрайських компаній окупають високі відсотки по позиках, які іноді доходять до тисячі відсотків на рік, і великі штрафи за будь-яке прострочення. Мінімізація перевірок і наданих даних перетворила онлайн позики в добре джерело доходів для шахраїв, що беруть позики на чужі персональні дані. У деяких випадках шахраям вистачить електронних копій двох документів жертви, наприклад, паспорта і прав водія. Можна для їх отримання створити оголошення про роботу і просити у потенційних претендентів після «прийняття» на роботу копії документів. Шахраї знають багато способів отримати копії документів і взяти на них позику.

Бувають і більш витончені схеми шахрайства з отриманням позик без відома власника. На одному з російськомовних андеграунд форумів якось з'явилася пропозиція про продаж авіаквитків за 50 % від їх реальної вартості. Власник сервісу, який пропонував послугу, запевняв, що ніякого шахрайства немає, авіаквитки не купуються на крадені кошти. Перший час відвідувачі

форуму ставилися з недовірою до пропозиції, потім позитивні відгуки почали залучати все більше і більше клієнтів. Клієнти відправляли зловмисникові всі персональні дані, включно з копіями документів. У жодного з клієнтів не виникло проблем з польотом. Проблеми виникли пізніше, коли банк, в якому ці квитки оформлялися в кредит без відома клієнтів, почав вимагати повернути суму за авіаквитки, відсотки і значні пені за прострочення. В результаті жертви заплатили по 200–300 відсотків від реальної вартості придбаних квитків.

Становить інтерес приклад шахрайства проти корпорацій. У соціальних мережах створюються профілі співробітників якої-небудь компанії, які там не зареєстровані, й додаються як друзі до реальних. Потім зав'язується спілкування з реальними співробітниками; наступні методи атаки вибирає зловмисник – це може бути компрометація реального співробітника або використання методів соціальної інженерії для одержання необхідних персональних даних для майбутнього шахрайства. Якщо в соціальній мережі до вас додався колега по роботі «як друг», обов'язково верифікуйте його, оскільки за його акаунтом можуть ховатися шахраї.

Висновки. Пам'ятайте: легше запобігти крадіжці цифрової особистості, ніж намагатися видалити персональну інформацію про себе з мережі. Практично це зробити дуже важко. Якщо десь в мережі хочуть отримати від вас персональну інформацію, то спочатку оцініть, що ви отримаєте натомість і чи варто це тих ризиків, які ви отримуєте. Особливо це стосується ваших паспортних даних, номерів телефону, домашньої адреси, акаунтів тощо.

Якщо вам все-таки хочеться десь зареєструватися, наприклад, для скачки книг, то заведіть собі для цих цілей акаунт, у логіну якого немає ваших прізвища й імені. Потім купіть собі нову сім-карту і зареєструйтеся під іншим прізвищем, іменем та по батькові. При цьому природно, дата народження й усе інше повинні бути вигаданими. Ви будете майже в безпеці. Крім того, є багато інших методів для забезпечення своєї особистої інформаційної безпеки.

Бібліографічні посилання

1. Макаров А. Как киберпреступники добывают и используют персональные данные. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Personal-data-dark-side
2. Косиченко О. О., Рибальченко Л. В. Проблеми безпеки персональних даних в Україні. *Регіональна економіка та управління*. Запоріжжя, 2019. № 4 (26). Ч. 2. С. 68–71.
3. Колисниченко Д. Н. Секреты безопасности и анонимности в Интернете. Санкт-Петербург : БХВ-Петребург, 2021. 256 с.

Свистун Я. В., курсант
3-го курсу факультету № 1
Науковий керівник – Шевчук Т. А.,
доцент кафедри кримінального права
і кримінології факультету № 1,
кандидат юридичних наук, доцент
*(Харківський національний
університет внутрішніх справ)*

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОТИДІЇ ЗЛОЧИННОСТІ

Принципи та завдання розвитку технологій штучного інтелекту (далі – ШІ) в Україні законодавчо визнані одним з пріоритетних напрямів у сфері науково-технологічних досліджень. Концепція розвитку штучного інтелекту в Україні передбачає необхідність впровадження інформаційних технологій, частиною яких є технології ШІ, в соціально-економічну, науково-технічну, оборонну, правову та інші види діяльності [1].

Використання можливостей ШІ у роботі правоохоронних органів, зокрема у напрямі протидії злочинності є практично затребуваним та актуальним. Можливості програмного забезпечення в частині підтримки правопорядку дають значну перевагу людському потенціалу щодо передбачення, фіксації, попередження та завчасного реагування на правопорушення. Уже сьогодні вітчизняні правоохоронні органи активно використовують технології ШІ за такими напрямами:

– *ідентифікація та нейтралізація кіберзагроз, насамперед кібертероризму та кіберекстремізму. С*истеми ШІ здатні попереджувати атаки на охоронювані об’єкти, в автоматичному режимі виявляти віруси та вірусні «шкідливі» програми, за допомогою відповідних алгоритмів блокувати або нейтралізувати їх вплив, що значно знижує подальші негативні прояви в цій сфері;

– р*озпізнавання облич,* що часто відіграє головну роль у виявленні та розкритті кримінальних правопорушень по «гарячих слідах», встановленні місця знаходження осіб, оголошених у розшук, та забезпеченні публічного порядку та безпеки;

– *використання безпілотників*, що значно підвищує ефективність виявлення наркозлочинців (полів з наркопосівами), браконьєрів, місць незаконного видобутку корисних копалин, незаконної рубки лісу, пошуку заблукалих в лісі чи горах, а також моніторингу ситуації на дорогах і трасах великих міст, пошуку викраденого транспорту тощо;

– *використання комплексів автоматичної фіксації правопорушень на дорогах,* що дозволяє в автоматичному режимі здійснювати виявлення та

документування в базах даних фактичних подій, які містять ознаки адміністративних правопорушень у сфері забезпечення безпеки дорожнього руху;

– *використання програмного забезпечення для аналізу та прогнозування злочинності.* За допомогою технологій ШІ можливе створення обґрунтованих прогнозів щодо темпоральних, територіальних і якісних показників злочинності. Ці прогнози призначені сприяти правоохоронним органам в оптимізації використання наявних ресурсів та виконання поліцейських функцій [2, с. 103].

Невпинний розвиток інформаційних технологій в стрімко мінливих умовах цифровізації суспільства сприяє підвищенню ефективності інформаційного забезпечення діяльності правоохоронних органів і слугує міцним підґрунтям застосування штучного інтелекту в цій сфері. З іншого боку, розвиток комп'ютерних технологій в усіх напрямах науки і техніки продукує зростання рівня кіберзлочинності, яка в сучасному світі є однією з найбільших загроз інформаційній та економічній безпеці держави. Тому в процесі використання технологій ШІ необхідним є дотримання етичних та законних основ забезпечення захисту основних прав і свобод людини і громадянина. В подальшому актуальним вбачається ініціація та подальша державна підтримка проведення кримінологічних досліджень у довгостроковій перспективі щодо особливостей використання ШІ у правоохоронній діяльності з дотриманням фундаментальних принципів.

Бібліографічні посилання

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 01.09.2021).

2. Юртаєва К. В. Використання технологій штучного інтелекту в реалізації стратегій «predictive policing»: можливості, проблеми та перспективи для України. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 99–104.

Ставніцер Б. В., Сумцова Б. В.,
здобувачі вищої освіти
спеціальності 051 «Економіка»
Науковий керівник – Кононова І. В.,
професор кафедри аналітичної
економіки та менеджменту,
доктор економічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ЕКОНОМІЧНА БЕЗПЕКА ФУНКЦІОНУВАННЯ ПІДПРИЄМСТВА ЯК ОБ'ЄКТ УПРАВЛІННЯ

Сучасний стан розвитку економіки України характеризується постійною зміною умов функціонування підприємств, що потребує їх швидкої і навіть превентивної реакції на трансформацію ринкового середовища. Під час посилення процесів економічної глобалізації успішне функціонування підприємств значною мірою залежить від рівня їхньої економічної безпеки. Але одним з головних недоліків систем менеджменту вітчизняних підприємств є їх низька спроможність оперативно і з мінімальними витратами реагувати на такі зміни [1].

На українських підприємствах заходи щодо управління економічною безпекою переважно проводяться несистематично, а сам процес управління економічною безпекою підприємств є хаотичним, який ускладнюється значною кількістю різноманітних загроз зовнішнього і внутрішнього походження [2]. Тобто в основі забезпечення безпечного функціонування та розвитку підприємства лежить система управління його економічною безпекою, спрямована на попередження загроз його діяльності, появу яких спричиняють різноманітні чинники економічної безпеки.

Дослідження проблем економічної безпеки підприємства як об'єкта управління висвітлювали у своїх працях О. Власюк, О. Ляшенко, Д. Комарков, К. Фень, І. Отенко, В. Франчук тощо. Однак, незважаючи на проведені цими вченими дослідження, залишаються не повністю вирішеними проблеми забезпечення економічної безпеки підприємства як об'єкта управління.

Безперечно, з погляду управління – значущість дослідження підприємства, яке було і залишається основною структурною ланкою економіки будь-якого типу, в межах проведення спеціальних досліджень щодо їх економічної безпеки не викликає сумнівів.

Як об'єкт управління економічну безпеку підприємства треба розглядати одночасно з кількох позицій. З одного боку, необхідним є розгляд з позиції інтегрованості до загальної системи управління підприємством, зважаючи на той факт, що головною метою безпечного функціонування

підприємства є забезпечення досягнення власних цілей, серед яких забезпечення прибутковості, відповідного рівня конкурентоспроможності або збільшення ринкової вартості тощо [3]. З іншого буку, на особливу увагу в межах вивчення економічної безпеки підприємства як об'єкта управління заслуговує той факт, що рушійною силою функціонування та розвитку підприємства є діяльність, яка завжди пов'язана з інтересами різних суб'єктів, ступінь узгодження яких і формує його економічну свободу, досягаючи того чи іншого рівня економічної безпеки.

Об'єктами впливу для реалізації управління економічною безпекою підприємства можуть бути: ресурси, прибуток, обсяг виробництва або виробничий процес, попит, кваліфікація працівників, капітал, інвестиції, інші джерела формування і використання усіх видів ресурсів тощо [4].

Функції, поставлені перед управлінням економічною безпекою підприємства, можна об'єднати у дві групи: 1) функції, характерні для управління будь-якого рівня; 2) спеціальні функції. При цьому до спеціальних функцій управління економічною безпекою підприємства треба віднести синтезуючі, які створюють підґрунтя для відповідної реакції на загрози, що виникають (до цих функцій мають відноситися генеруюча та діагностична функції управління) та реакційні, як безпосереднє реагування на загрози, що виникають в процесі функціонування підприємства (до цих функцій відносимо превентивну та адаптивну функції). Тобто синтезуючі функції управління економічною безпекою створюють базу для реагування підприємства на загрози, що виникають, а реакційні функції визначають досягнутий рівень економічної безпеки підприємства.

На наш погляд, виконання цих функцій з врахуванням принципів безпечного функціонування підприємства у тісній взаємозалежності із застосуванням методів та інструментів забезпечення економічної безпеки дозволить отримувати позитивні результати, що відповідають цільовій установці діяльності підприємства.

Отже, економічна безпека підприємства є специфічним об'єктом управління, який маємо віднести до класу частково керованих систем, в складі якої повинні буди інструменти ідентифікації можливостей та обмежень господарювання з такими характеристиками, як здатність протистояння руйнівному впливу загроз шляхом використання запасу міцності, гнучкість щодо використання різних способів узгодження інтересів та адаптивність щодо виконання специфічних функцій та результативність щодо досягнення поставлених цілей.

Бібліографічні посилання

1. Бондаренко-Берегович В. В. Економічна безпека підприємства як об'єкт управління. *Вісник Національного технічного університету «ХПІ». Економічні науки.* Харків : НТУ «ХПІ». 2020. № 5 (7). С. 63–67.

2. Комарков Д. В. Методичне забезпечення аналізу економічної безпеки розвитку підприємств. *Економіка і регіон*. 2017. № 6 (67). С. 130–133.

3. Лойко В. В. Оперативна оцінка рівня економічної безпеки за допомогою експертної системи. *Управління проектами та розвиток виробництва.* Луганськ : Вид-во СНУ ім. В. Даля. 2013. №1(45). С. 22–26.

4. Ляшенко О. М. Категорії управління економічною безпекою підприємства. *Вчені записки Університету «КРОК»*. 2011. Вип. 27 (2). С. 17–22.

Стоєва Т. І., студентка 1-го курсу
юридичного факультету
Науковий керівник – Насонова С. С.,
доцент кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Сучасне суспільство стоїть на шляху інформатизації: зростає роль інформації, формується телекомунікаційна інфраструктура, розширюється застосування інформаційних технологій [1]. Водночас постають питання забезпечення захисту інформації. Саме інформаційна безпека є однією з головних складових частин національної безпеки країни, тому питання захисту інформації від внутрішніх та зовнішніх інформаційних загроз є вкрай важливими та актуальними.

Мета роботи – визначити, чому сьогодні, в епоху розквіту інформаційних технологій, в Україні виникають проблеми з інформаційною безпекою.

Сьогодні в Україні є достатня кількість науково-практичних знань та технологій для вдосконалення системи інформаційної безпеки. Але все одно українці та державні органи стикаються з проблемами захисту інформації у різних сферах життєдіяльності суспільства.

По-перше, однією з таких найважливіших проблем є недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в межах національних інтересів України [2]. Ефективний розвиток інформаційної безпеки можливий лише за наявності розвинутої інформаційної інфраструктури. Через відсутність якісної інфраструктури роль інформаційної безпеки знижується, що призводить до масштабних проявів інформаційної злочинності, яка загрожує безпеці функціонування інформаційно-телекомунікаційних систем. Саме тому Україна змушена створювати та реалізовувати програми з інформатизації, орієнтуючись на здобутки розвинутих країн. По-друге, проблема виникнення непередбачених ситуацій у системах та процесах, що базуються на використанні

інформаційних технологій [3]. Також проблема неефективності державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, недостатній рівень медіакультури суспільства [2]. Хоча в наш час рівень медіакультури дуже розвинений, у більшої частки населення виникають проблеми навіть щодо взаємодії з масмедіа.

Одним зі шляхів вирішення зазначених вище проблем може бути створення та розвиток системи цивілізованого співробітництва українців з обізнаними закордонними фахівцями в інформаційній сфері. Це сприятиме державному процесу формування інформаційних ресурсів країни.

Висновки. Інформаційна безпека є однією зі складових стійкого розвитку всієї держави, необхідною умовою розбудови інформаційного суспільства. Дослідження проблеми інформаційної безпеки в Україні показало, що інформаційна сфера країни потребує надійного захисту. Вирішення цієї проблеми можливе за умови плідної співпраці з обізнаними закордонними фахівцями у сфері інформаційних технологій.

Бібліографічні посилання

1. Гребенюк А. М., Кишкань М. А. Роль інформаційних технологій в правоохоронній та юридичній діяльності. *Використання сучасних інформаційних технологій в діяльності національної поліції України* : матеріали Всеукр. науково-практ. семінару. Дніпро : Дніпропетр. держав. ун-т внутр. справ, 2019. С. 96–98.
2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лютого 2017 року № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text
3. Боднар І. Р. Інформаційна безпека як основа національної безпеки. URL: https://core.ac.uk/download/pdf/141443493.pdf

Таранюк А. Г., курсант 4-го курсу
факультету підготовки фахівців для
органів досудового розслідування
Науковий керівник – Юр'єв Д. С.,
викладач кафедри фінансових
та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ,
підполковник поліції

МІСЦЕ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Економічна сфера життєдіяльності української держави завжди мала мінливий характер. Це твердження передусім пов'язане з економічною нестабільністю та недостатньою кількістю інвестицій в економіку держави з

боку інвесторів.

Незважаючи на вищевказані причини погіршення економічної ситуації в країні, ми вважаємо за необхідне виокремити одну з головних проблем, від якої потерпає вся економічна інфраструктура країни. Цією проблемою є невідповідність інформаційних технологій, які використовуються в економічній діяльності, сучасним вимогам та стандартам, які мають на меті не лише примножити прибуток держави, але й забезпечити інформаційну безпеку [1, с. 160].

Треба зазначити, що якісні сучасні інформаційні технології є необхідною умовою для нормального функціонування економічної інфраструктури України. Для цього в країні проводиться низка впроваджень та реформ, які повинні не лише поліпшити економічну ситуацію в країні, але й забезпечити економічну безпеку держави.

Інформаційні технології являють собою комплекс засобів та заходів, які використовуються на підприємствах, установах або організаціях з метою досягнення завдань, які чітко вказані в їх статуті.

Завдяки перевіреним інформаційним ресурсам можна не лише спокійно вести бізнес, але й розробляти нові концепції для його розвитку відповідно до міжнародних стандартів.

Інноваційні технології надають змогу суттєво зекономити власний час та зусилля на ту чи іншу роботу, наприклад паперову документацію. Завдяки новітнім базам даних та реєстрам можна вищевказану роботу зробити за допомогою комп’ютерів, що значно полегшить процес самого створення документації та її подальший пошук у разі потреби [2, с. 54].

Повертаючись до питання економічної безпеки, треба наголосити, що інформаційні технологій відіграють дуже важливу роль у забезпеченні вищевказаного питання, оскільки завдяки якісній системі захисту, яка буде інтегрована згідно з усіма принципами законодавства та відповідно до найостанніших новітніх технологій, економічна база, реєстри, звіти, договори та інші економічно-значущі документи буде збережено від використання їх не за призначенням. Тобто буде в перспективі зменшена кількість вчинених злочинів з використанням підроблених документів чи інформації.

Окрім інформаційних технологій, важливе місце посідає мережа «Інтернет», бо без цього ресурсу сучасна діяльність неможлива. Більшість грошових операцій, транзакцій, перекази відбуваються за допомогою Інтернету, тому досить важливим є наявність якісної системи захисту особистої інформації осіб та їх грошових активів від незаконної діяльності з боку інших людей або навіть держав.

Підсумовуючи все вищевказане, можна зробити висновок, що інформаційні технології посідають дуже важливе місце в забезпеченні економічної безпеки України, бо в разі низького рівня вищевказаного питання економічна ситуація в країні не налагодиться.

Бібліографічні посилання

1. Линник О. І. Стратегія економічної безпеки підприємства як фактор зменшення впливу зовнішніх та внутрішніх загроз. *Вісник НТУ «ХПІ»*. Серія : Технічний прогрес і ефективність виробництва. Харків : НТУ «ХПІ». 2013. № 67 (1040). С. 159–169.
2. Рибальченко Л. В., Рижков Е. В., Тютченко С. М., Гавриш О. С., Варяниченко А. О. Безпека підприємництва : монографія. ДДУВС, 2020. 180 с.

Туряк Ч. Д., курсант 4-го курсу
факультету підготовки фахівців
для підрозділів стратегічного
розслідування Дніпропетровського
державного університету внутрішніх справ
Науковий керівник – Гребенюк А. М.,
доцентт кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

СУЧАСНИЙ СТАН ЗАХИСТУ ІНФОРМАЦІЇ НА МОБІЛЬНИХ ПРИСТРОЯХ В КОНТЕКСТІ РОЗВИТКУ ЗАГРОЗ ТА ВИКОРИСТАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Захист інформації на мобільних пристроях – це прийняття правових, організаційних і технічних заходів для забезпечення захисту інформації від несанкціонованого доступу, знищення, перекручення, блокування інформації, копіювання, надання, поширення та інших незаконних дій щодо такої інформації. Конфіденційність інформаційних ресурсів з обмеженим доступом, реалізація основоположного права на вільний доступ до інформації є запорукою основних прав і свобод людини.

Варто почати з того, що сучасна проблематика інформаційної безпеки на мобільних пристроях містить разом з забезпеченням безпеки інформації та інформаційних систем ще два компоненти: захист від впливу шкідливої інформації, забезпечення ухвалення обґрунтованих рішень за максимального використання доступної інформації [1].

Забезпечення інформаційної безпеки на мобільних пристроях повинно вирішувати такі основні завдання:

– виявлення, оцінка та запобігання загрозам інформаційним системам і ресурсів;

– захист прав юридичних і фізичних осіб на інтелектуальну власність;

– збір, накопичення і використання інформації;

– захист державної, службової, комерційної, особистої та інших таємниць.

Загрози інформаційним системам і ресурсів для користувачів сучасних мобільних пристроїв умовно можна поділити на чотири основні групи:

1) програмне забезпечення – впровадження «вірусів», апаратних і програмних закладок; знищення і зміна даних в інформаційних системах;

2) технічні, в тому числі електронне перехоплення інформації в лініях зв'язку, електронне придушення сигналу в лініях зв'язку і системах управління;

3) фізичне знищення технологічного обладнання і носіїв інформації; крадіжка медіа та апаратних або програмних ключів та/або паролів;

4) інформація – порушення правил обміну інформацією; незаконне збирання і використання інформації; несанкціонований доступ до інформаційних ресурсів; незаконне копіювання даних в інформаційних системах; дезінформація, приховування або фальсифікація інформації; викрадення інформації з баз даних [2].

Цим загрозам можна протистояти, створивши і запровадивши ефективні системи захисту інформації від шкідливого ПЗ на мобільних пристроях.

Події останніх років вказують на те, що досить часто обговорюється і є дискусійною проблема інформаційного протиборства в Інтернеті – так званої кібервійни. Її основна мета – дестабілізувати інформаційні системи і доступ до Інтернету в державних установах, фінансових і ділових центрах, а також створити безлад і хаос в державах, які покладаються на Інтернет у своєму повсякденному житті.

Міждержавні відносини і політичні протистояння можуть тривати в Інтернеті у формі кібервійни: вандалізм, пропаганда, шпигунство і прямі атаки на комп'ютерні системи і сервери, шкідливе ПЗ на мобільних пристроях.

З поширенням інформаційних технологій на мобільних пристроях громадяни, підприємства і державні установи буквально стали залежати від Інтернету у повсякденному житті. Їх використання для атаки на інформаційні системи іншої держави може завдати значних економічних збитків і призвести до розбіжностей в повсякденному житті держави.

У міру того як нові технології переходять на мобільні пристрої, масштаби кібервійни постійно збільшуються і підвищують її загрози. Деякі держави приділяють особливу увагу захисту від кібервійни і надають необхідні ресурси для організації систем захисту і підтримки спеціальних сил, завданням яких є підвищення і поліпшення інформаційної безпеки. Контроль над мобільними пристроями з доступом до мережі «Інтернет» в наш час визначає стан національної безпеки держави [3].

Міжнародне право відіграє дуже важливу роль в боротьбі з кіберзлочинністю. Створення цілодобових контактних центрів, юридичне

визначення кіберзлочинності, екстрадиція злочинців, міжнародна взаємодія компетентних органів, проведення навчань і обмін інформацією – все це сприяє впровадженню ефективних методів реагування на міжнародні злочини і боротьби зі злочинами, скоєними в кіберпросторі.

Розвиток інформаційних технологій для користувачів сучасних мобільних пристроїв має тенденцію до все більшого прискорення, тому правова база повинна не тільки йти в ногу з часом, а й змінюватися для вирішення всіх нагальних проблем людей, суспільства та міжнародної спільноти в галузі інформаційної безпеки.

Бібліографічні посилання

1. Дмитренко М. Проблеми інформаційної безпеки України. URL: http:// socialscience.com.ua/article/807 (дата звернення: 25.03.2021).

2. Логінов О. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління. *Науковий вісник Юридичної академії МВС України*. Київ, 2003. Вип. 3. 224 с.

3. Кормич Б. Інформаційна безпека: організаційно-правові основи : навч. посіб. Київ : Кондор, 2004. 384 с.

Утвенко В. В., курсант 2-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник – Гребенюк А. М.,
доцентт кафедри економічної
та інформаційної безпеки,
кандидат технічних наук, доцент
*(Дніпропетровський державний
університет внутрішніх справ)*

ПРОБЛЕМАТИКА УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННИХ ОРГАНІВ

Детально розглянувши сучасний стан розвитку суспільства, потрібно звернути увагу на значне підвищення ролі інформаційних технологій у людській життєдіяльності, а також у суспільстві і державі. Стрімкий розвиток інформаційних процесів, започаткування нових винаходів, досягнень та технологій у виробничі та управлінські процеси – ці події зумовили не лише можливості поступального розвитку нашої держави, але і стали факторами зростання кількості злочинів, які, зі свого боку, вдосконалили засоби і способи вчинення кримінальних правопорушень. Ця

ситуація значно ускладнює запобігання, виявлення та протидію злочинності і зумовлює необхідність вдосконалення впроваджених і розробку нових методів та засобів її здійснення. Розвиток інформаційних систем в Україні на сучасному етапі недостатній.

Зважаючи на це, можна зробити висновок, що впроваджені інформаційні системи на сьогодні не здатні в повному обсязі реалізувати своє призначення у процесі діяльності правоохоронних органів. Саме тому питання вдосконалення інформаційного забезпечення правоохоронних органів набуває актуальності [2].

Система інформаційного забезпечення Національної поліції України – це сукупність взаємопов'язаних і взаємодіючих організаційних елементів і технічних засобів, яка здійснює інформаційне забезпечення Національної поліції України.

Формування загальновідомчих та галузевих інформаційних підсистем, які становлять основу системи інформаційного забезпечення Національної поліції України, здійснюється згідно з такими принципами:

1. Нормативно-правової забезпеченості.
2. Доцільності впровадження й експлуатації.
3. Фактичності даних.
4. Розвитку.
5. Функціонального призначення (інформаційні підсистеми кримінальної статистики, спеціалізовані інформаційні підсистеми).

Структурна побудова інформаційних підсистем Національної поліції України поєднує в собі сукупність принципів. До них належать принципи територіально-розподіленої та централізованої топології, яка організована у вигляді ієрархічної моделі з трьох рівнів. Належність інформаційної підсистеми до певного рівня визначається завдяки принципам територіальності, специфіки використання та обсягом інформації, яка обробляється.

Інформаційно-аналітичне забезпечення Національної поліції України залежно від підпорядкування здійснюється на трьох рівнях. Перший рівень – центральний, що інтегрує інформаційні підсистеми поліції загальновідомчого значення та галузевих служб Національної поліції України. На цьому рівні об'єднується вся інформація, що використовується для аналізу, ухвалення рішень і проведення у межах оперативно-розшукових, слідчих та інших спеціальних заходів щодо протидії злочинності. Другий рівень – регіональний, який охоплює інформаційні обліки, які є складовими частинами загальновідомчих інформаційних підсистем та використовуються обласними службами Національної поліції України. В складі таких баз даних регіонального рівня інтегрується інформація, що має регіональний характер і містить дані про надзвичайні події, кримінальні й адміністративні правопорушення. Третій рівень – місцевий, що охоплює інформаційні обліки, які використовуються у міських, районних підрозділах, слідчих та інших

підрозділах Національної поліції [3, 5].

Оптимізація вирішення завдань пошуку,

відбору та систематизації інформації, необхідної в діяльності поліції, базується в єдиному інформаційному просторі системи МВС України, який є сукупністю спеціалізованих баз і банків даних, технологій їх ведення та використання, суб'єктів інформаційно-аналітичної діяльності, що функціонують на основі єдиних принципів і за загальними правилами забезпечують інформаційну взаємодію системи Міністерства внутрішніх справ України і громадян [4].

Отже, можемо дійти висновку, що для вирішення завдань сучасного інформаційного забезпечення підрозділів поліції має бути розроблено комплексний підхід для досягнення високого рівня в діяльності правоохоронних структур, серед яких: упровадження єдиної політики інформаційного забезпечення; створення багатоцільових інформаційних підсистем діяльності ОВС; правове виховання через засоби масової інформації; удосконалення законодавства; створення умов для ефективного функціонування інформаційних обліків; забезпечення їх вірогідності, актуальності та безпеки; установлення взаємодії поліції з населенням у розробці ефективних способів такого забезпечення.

Бібліографічні посилання

1. Про Службу безпеки України : Закон України від 25.03.1992 р. № 2229-XII. URL: http://zakon.rada.gov.ua/laws/show/2229-12
2. Про Національну поліцію : Закон України від 02.07.2015 р. № 580-VIII. URL: http://zakon.rada.gov.ua/laws/show/580-19.
3. Лазур Я. В. Поняття, сутність та елементи адміністративно-правового механізму забезпечення прав і свобод громадян у державному управлінні. URL: http://nbuv.gov.ua/ UJRN/FP_index.htm_2009.
4. Закон України «Про Національну поліцію» : науково-практ. комент. МВС України, Харків. нац. ун-т внутр. справ; за заг. ред. В. В. Скакуненка. Харків, 2016. 408 с.
5. Вишня В. Б., Ісмайлов К. Ю., Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційні технології : підручник. Дніпро : Дніпропетр. держ. ун-т внутр. справ, 2020. 492 с.

Чепеляк К. В., слухач магістратури
2-го курсу факультету соціально-
психологічної освіти та управління
Науковий керівник – Верхоглядова Н. І.,
доктор економічних наук, професор,
завідувач кафедри
*(Дніпропетровський державний
університет внутрішніх справ)*

АКТУАЛЬНІ ПИТАННЯ ЗАГРОЗ ЕКОНОМІЧНІЙ БЕЗПЕЦІ ДЕРЖАВИ В УМОВАХ ГЛОБАЛІЗАЦІЇ

На сучасному етапі розвитку суспільства в умовах глобалізації та суттєвих перешкод на шляху досягнення стабільності і рівноваги основоположним є економічна безпека, яка посідає центральне місце у структурі національної безпеки України. Аналіз останніх подій нашої держави демонструє значне зниження економічної безпеки як соціально-економічної системи на мезорівні та на макрорівні. На сьогодні виявлення головних ризиків та загроз безпеці економіки є вкрай актуальним для забезпечення умов стабільності та незалежності нашої країни.

Ця тема не нова: до неї неодноразово звертались як зарубіжні, так і вітчизняні вчені, які здебільшого зосереджували увагу на протидії загрозам економічній безпеці держави, серед яких можна виділити: А. Гальчинського, О. Барановського, О. Білоуса, Т. Васильціва, Г. Дарнопиха, Г. Андрощука, С. Мочерного, С. Довбня, І. Лазарєва, Т. Момота, А. Гриценко, О. Новікова, В. Франчука, Є Панченка та інших. Проте, незважаючи на велику кількість наукових доробок за цією проблематикою, необхідним вбачається по-новому оцінити впливові загрози та заходи протидії в цьому контексті.

Варто почати з того, що економічна безпека держави є невід'ємною складовою національної безпеки, що забезпечує сталий розвиток суспільства та запобігає загрозі національним інтересам. Економічна безпека здатна забезпечити економічний розвиток, реалізацію дієвої соціальної політики, зростання національної конкурентоспроможності, вчасно виявити загрози економічним інтересам держави і суспільству в цілому.

Аналізуючи виклики глобалізації, маючи на меті ефективне забезпечення економічної безпеки держави, необхідним є окреслити сукупність загроз економічній безпеці. В цьому контексті загрози економічній безпеці держави можна розглядати як події та явища, які загрожують нормальному функціонуванню економічної та політичної системи. Зокрема, вчені поділяють такі загрози на зовнішні та внутрішні.

До внутрішніх загроз економічній безпеці України треба віднести: низький технологічний рівень більшості галузей, високі витрати виробництва, низьку якість продукції і, як наслідок, низьку конкурентоспроможність національної економіки; втрату значної частини

науково-технічного потенціалу, позицій на важливих напрямах науково-технічного прогресу; деформовану структуру виробництва; зруйнування системи відтворення виробничого потенціалу; неефективність державного управління соціально-економічними процесами та інші.

До головних зовнішніх загроз належать: імпортна залежність України з багатьох видів продукції, включно із стратегічними товарами, енергоносіями, комплектуючими виробами для машинобудування, продовольчими товарами; нераціональна структура експорту; перебування в зародковому стані фінансової, організаційної та інформаційної інфраструктури підтримки конкурентоспроможності українського експорту; некерований відтік за кордон інтелектуальних і трудових ресурсів; недостатній експортний та валютний контроль і недосконаліть митної політики; слабка розвиненість транспортної інфраструктури зовнішньоекономічних відносин [1, с. 69].

Також варто зазначити, що основними загрозами, безпосередньо макроекономічній безпеці, на сучасному етапі є:

– низькі темпи подолання деформації в економіці;
– нестабільність економічного зростання;
– недостатні темпи збільшення внутрішнього ринку;
– значна тінізація економіки;
– абсолютна залежність національної економіки від конкуренції зовнішніх ринків.

В. Сенчагов вважає, що внутрішні загрози економічній безпеці викликані нездатністю економіки до самозбереження та саморозвитку, слабкістю інноваційного початку в розвитку, неефективністю системи державного регулювання економіки. Зовнішні загрози відображають поточний стан світової економіки і можуть підривати основи її розвитку [5].

Підсумовуючи вищенаведене, варто вказати, що економічна безпека України вбирає в себе широкий спектр взаємопов’язаних елементів, а також самостійних систем. Саме тому загрози, які постають перед економічною безпекою, варто розглядати в контексті усіх складових елементів останньої.

На сьогодні наша держава подолала важкий період перехідної економіки, але це не означає, що в Україні наявна надійна та ефективна система забезпечення національної економічної безпеки. Тому необхідним є розробити та затвердити національну стратегію економічної безпеки України, що визначатиме провідні напрями реалізації політики держави у цьому аспекті та значно знизить загрози, які постають перед останньою.

Бібліографічні посилання

1. Варналій З. С., Мельник П. В., Тарангул Л. Л. Економічна безпека : навч. посіб. / за ред. З. С. Варналія. Київ : Знання, 2009. 647 с.

2. Сенчагов В. Стратегические цели и механизм обеспечения экономической безопасности. *Проблемы теории и практики управления*. 2009. № 3. С. 18–23.

3. Акімова Л. М. Сутнісна характеристика основних загроз в економічній безпеці держави. *Державне управління: удосконалення та розвиток*. 2016. № 10. URL: http://www.dy.nayka.com.ua/?op=1&z=1247

Чечель А. О., курсант 4-го курсу
факультету підготовки фахівців
для органів досудового розслідування
Дніпропетровського державного
університету внутрішніх справ.
Науковий керівник – Юр'єв Д. С.,
викладач кафедри фінансових
та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ,
підполковник поліції

ПЛАНУВАННЯ ЯК ОДНА З ОБОВ'ЯЗКОВИХ ВИМОГ ДО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ З ЕКОНОМІКОЮ

Злочинність, пов'язана з економічною сферою суспільних відносин, все ще залишається негативним чинником впливу на нормальне функціонування держави.

Економічні злочини характеризуються складними методами здійснення своєї злочинної діяльності, тому досить необхідним є підвищення кваліфікації та професіоналізму слідчих підрозділів, які будуть спроможні якісно та ефективно розслідувати кримінальні правопорушення у сфері економіки.

Варто зауважити, що розслідування будь-якого виду кримінальних правопорушень являє собою багатоетапний процес дій, які спрямовані на збирання доказового матеріалу, який буде направлено до суду. Очевидно, що перед розслідуванням економічних злочинів слідчому варто ретельно скласти план процесуальних дій, які необхідно провести в межах кримінального провадження.

Планування завжди залишалося невід'ємною частиною підготовки до розслідування будь-якого виду кримінальних правопорушень.

План – попередньо намічений порядок послідовності виконання програми шляхом здійснення роботи, проведення заходів [1, с. 1021].

Інструкція з організації діяльності слідчих підрозділів Національної поліції України Міністерства внутрішніх справ України чітко передбачає обов'язковість планування у діяльності органів досудового розслідування.

Планування розслідування – це складна діяльність слідчих, результатом якої є розробка плану розслідування, який містить основні процесуальні дії, які необхідно здійснити з метою розслідування кримінального правопорушення. План розслідування формується на основі ретельного вивчення всіх фактичних даних, доступних слідчому до

складання. Він також враховує спеціальні знання, професійний досвід та уяву слідчого, а також його погляди на природу кримінального правопорушення та метод встановлення істини [2, с. 57].

План розслідування у кримінальному провадженні має бути добре продуманим. Слідчі (розшукові) дії, які зазначені в плані, повинні відображати тактичний план слідчого та внутрішню логіку розслідування. Це означає, що план повинен передбачати найбільш розумне поєднання та послідовність слідчих (розшукових) дій для встановлення та перевірки доказів.

Звичайно, неможливо спланувати таку систему дій відразу під час всього розслідування, оскільки неможливо заздалегідь передбачити, яка інформація буде отримана під час проведення слідчих (розшукових) дій. Ця система дій впроваджується в план розслідування на певних етапах розслідування і впроваджується під час отримання інформації про розслідувану подію. З огляду на це розрізняють планування на початковому етапі розслідування та подальше планування.

На практиці розрізняють планування розслідувань у кримінальних провадженнях та планування окремих слідчих (розшукових) операцій. У першому випадку визначаються загальні методи та засоби вирішення слідчих завдань у кримінальному провадженні. Планування окремих слідчих (розшукових) дій спрямоване на визначення ефективних шляхів і засобів вирішення проміжних завдань (обшук, допит) [3, с. 62].

Кожен вид плану розслідування економічних злочинів є специфічним. Крім того, під час складання планів розслідування економічної злочинності треба дотримуватися деяких загальних правил. Ці правила називаються принципами планування розслідування і мають індивідуальність, динамічність, реальність та конкретність.

Індивідуальність плану пов’язана з особливостями конкретного злочину, і це необхідно враховувати під час складання плану. Особливість не унеможливлює виявлення загальних тенденцій у подібних ситуаціях. Спільні характеристики однорідних злочинів призводять до того, що можуть проводитися ті самі слідчі (розшукові) дії та негласні слідчі (розшукові) дії, що становлять певний алгоритм. Водночас індивідуальність кожного економічного злочину завжди вимагає творчого методу складання плану з урахуванням загальної закономірності та конкретних обставин інциденту, що розслідується.

Зрештою, треба зауважити, що правильне планування розслідування економічних злочинів є запорукою успішного встановлення істини. Якісний план є своєрідною підказкою для слідчого під час проведення досудового розслідування. Однак під час складання плану необхідно враховувати особливості кожного виду економічного злочину та розробляти слідчі (розшукові) дії відповідно до цих особливостей з метою ефективності досудового розслідування.

Бібліографічні посилання

1. Словник української мови / відп. ред. В. В. Німчук та ін. Київ : ВЦ «Просвіта», 2012. 1320 с.
2. Алєксєєва О. О. Розслідування окремих видів злочинів : навч. посіб. 2-ге вид. перероб. та допов. Київ : Центр навчальної літератури, 2014. 320 с.
3. Криміналістична тактика : навч. посіб. / за ред. д-ра юрид. наук, проф. М. А. Погорецького та д-ра юрид. наук, доц. Л. Б. Сєргєєвої. 2-ге вид., перероб. та допов. Київ : Алерта, 244 с.

Штундер В., студентка 3-го курсу
юридичного факультету
Науковий керівник – Тютченко С. М.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПОЛІЦЕЙСЬКОЇ ДІЯЛЬНОСТІ: ОСОБЛИВОСТІ ЗАРУБІЖНОГО ДОСВІДУ

Інформаційне забезпечення поліцейських структур є актуальним питанням не тільки для України, але й для багатьох зарубіжних країн, в яких значна увага приділяється створенню і використанню інформаційних систем поліцейської діяльності.

Збільшення кількості інформаційних процесів істотно впливають на рівень адаптації Національної поліції до нових умов та потребують удосконалення порядку контролю за управлінськими процесами, суттєво впливають на організацію систематизації та аналізу інформації. Вирішення цих викликів полягає у застосуванні широкої автоматизації управлінських процесів у сферах відповідальності органів системи МВС, у тому числі щодо ідентифікації та верифікації особи, екстреної допомоги населенню в разі надзвичайних ситуаціях, реагування на адміністративні та кримінальні правопорушення [1].

Вивчення досвіду зарубіжних країн та міжнародного досвіду в цій сфері дозволяє виявити найбільш ефективні й сучасні способи забезпечення інформацією, які можуть бути використані підрозділами Національної поліції під час виконання професійної діяльності.

Зарубіжний та вітчизняний досвід діяльності Нацполіції в особливих умовах та досвід збройних конфліктів та антитерористичних операцій засвідчив, що одним із найважливіших і специфічних видів оперативного (бойового забезпечення) на сьогодні стає інформаційне забезпечення. За поширеною у вітчизняній літературі позицією, інформаційне забезпечення

здійснюється у великомасштабних операціях за допомогою налагодженого механізму державного контролю над процесом інформаційної політики та впливу через засоби масової інформації на суспільну свідомість як усередині країни, так і за її межами [2, с. 94].

Нашій державі треба врахувати позитивний досвід розвинутих світових країн. Варто звернути увагу на досвід застосування інформаційних технологій у діяльності правоохоронних органів країн ЄС, адже в умовах євроінтеграції співробітництво у галузі юстиції, свободи та безпеки є одним із важливих напрямів руху нашої держави до набуття статусу повноцінної держави-члена ЄС. В умовах реформування системи правоохоронних органів важливим для підвищення ефективності її інформаційного аналітичного забезпечення є вивчення досвіду успішного функціонування інформаційних систем країн ЄС.

На особливу увагу у сфері застосування інформаційних технологій правоохоронними органами заслуговує Великобританія [3, с. 37; 3, с. 86]. У цій країні введено систему новітніх комп'ютерних відеоспостережень, створених завдяки фінансуванню міських адміністрацій та приватних підприємств, що сприяє підвищенню рівня попередження правопорушень та швидкого їх розкриття. Запроваджена корпоративна об'єднана інформаційна модель даних для потреб поліції ґрунтується на створенні каталогу інформаційних об'єктів, завдяки якому встановлюються і наочно демонструються ієрархічні взаємовідносини між інформаційними об'єктами [4, с. 169].

Заслуговує на увагу також досвід застосування інформаційних технологій правоохоронними органами Франції, Німеччини, Литовської республіки, Ізраїлю та ін. У кожній країні поліцейські структури мають свою назву і свої функції, але всіх їх об'єднує залежність від якісного інформаційного забезпечення. Інформаційні системи правоохоронних органів зарубіжних країн створюються на загальнонаціональному рівні і мета їх функціонування полягає у забезпеченні виконання стратегічного аналізу даних, що стосуються здійснення правопорушень. Правоохоронні органи зарубіжних країн приділяють значну увагу створенню та забезпеченню функціонування інформаційних систем як важливому інструменту забезпечення ефективності запобігання та протидії злочинності.

Бібліографічні посилання

1. Тютченко С. М., Штундер В. Є. Вдосконалення системи інформаційного забезпечення правоохоронних органів URL:https://er.dduvs.in.ua/bitstream/123456789/5944/1/25.pdf
2. Губанов А. В. Полиция зарубежных стран. Организационно-правовые основы, стратегия и тактика деятельности. Москва : МАЭП, 2017. 288 с.
3. Денисюк Д. С. Стан і перспективи реформування органів внутрішніх справ України: досвід поліції зарубіжних держав. *Науковий вісник Ужгородського національного університету*. Серія : Право. 2014. 29 (2.2). С. 36–39.
4. Нефедова Н. А. Інформаційне забезпечення спеціальної поліцейської діяльності. *Адміністративне право і процес*. 2019. № 2 (8). С. 167–173.

Янченко О. І., курсант гр. ФЕБ-942
Науковий керівник – Паршин Ю. І.,
доктор економічних наук, професор,
професор кафедри фінансових
та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ

СПОСОБИ ТА ПІДХОДИ БОРОТЬБИ З ТІНЬОВОЮ ЕКОНОМІКОЮ

Дедалі більше світову економічну арену поглинає тіньова економіка. Цей процес також не оминув і Україну. Варто зазначити, що з кожним роком рівень тінізації не зменшується, а залишається на одному рівні чи навіть збільшується. Тому важливим питанням є шляхи та способи подолання тінізації. Щоб зрозуміти, як подолати цей процес, потрібно визначити, що таке тіньова економіка.

Тіньова економіка – це господарська діяльність, яка розвивається поза державним обліком та контролем, а тому не відображається в офіційній статистиці [1].

Коли ми визначили, що є тінізацією, то ми можемо виділити деякі шляхи боротьби. Але варто розуміти, що не всі способи спрацюють так, як написано на папері. Проте залишити їх поза увагою ми не можемо.

На нашу думку, для ефективної боротьби з тінізацією економіки потрібно вжити такі заходи:

1. Підвищення ефективності управління державними фінансами.

Ефективне управління державними фінансами передбачає реалізацію комплексу заходів на кожній стадії планування та використання бюджетних коштів.

2. Вдосконалення зовнішньоекономічної діяльності та поліпшення міжвідомчої взаємодії.

Однією з головних умов цього пункту є систематичне розслідування кожного випадку виходу з ладу обладнання з контролю на митних постах, в разі виявлення порушень забезпечити притягнення до відповідальності.

3. Вдосконалення законодавства у сфері боротьби з економічними злочинами.

Низка досліджень наголошують, що в довгостроковій перспективі саме розвиток інститутів є головним фактором зменшення обсягів тіньового сектору економіки. Поступове вдосконалення законодавчої бази, незалежний суд, ефективна діяльність правоохоронних органів є обов'язковими умовами ефективного функціонування економіки, а також, в перспективі, створять належні умови для системної детінізації економіки України. Варто зазначити,

що Україна почала робити певні кроки в цьому напрямі, створивши Бюро економічної безпеки.

4. Розвиток безготівкового розрахунку.

Розвиток безготівкового розрахунку є одним з основних заходів щодо зниження тіньового обороту у фінансовому секторі. Цей пункт є одним з найважливіших, бо відстежувати фінансові операції, які проводяться безготівково, надійніше та зручніше. А саме тому виявити спробу ухилення від податків набагато легше.

5. Вдосконалення фіскального адміністрування.

Варто наголосити на необхідності проведення систематичної роботи з виявлення нових схем ухилення від сплати податків, а також створення ефективних механізмів обміну інформацією між державними та приватними структурами.

6. Створення сприятливих та ефективних умов для ведення бізнесу.

На нашу думку, це найважливіший пункт, бо створення належних умов для бізнесу – це прямий шлях до детінізації економіки в нашій державі. Одним із підпунктів є зменшення податків для приватних підприємців, бо саме високий податок і підбурює осіб вдаватися до незаконних дії. Також надавати правову підтримку малому та середньому бізнесу.

7. Боротьба з корупцією та підвищення рівня правової культури населення.

Також це є важливим пунктом. Можна додати те, що треба проводити заняття з правової культури зі старшої школи, зокрема щодо відповідальності, яка настає за економічні злочини [2].

Підсумовуючи, можна сказати, що основними способами боротьби з тінізацією економіки є: підвищення ефективності управління державними фінансами, вдосконалення зовнішньоекономічної діяльності та поліпшення міжвідомчої взаємодії, вдосконалення законодавства у сфері боротьби з економічними злочинами, створення сприятливих та ефективних умов для ведення бізнесу, боротьба з корупцією та підвищення рівня правової культури населення.

Бібліографічні посилання

1. Тенденції тіньової економіки. Загальні тенденції тіньової економіки в Україні. URL : https://me.gov.ua/Documents/List?lang=uk-UA&id=e384c5a7-6533-4ab6-b56f-50e5243eb15a&tag=TendentsiiTinovoiEkonomiki (дата звернення: 28.09.2021).

2. Савич О. В. Основні чинники та шляхи протидії тінізації економіки України. *Ефективна економіка*. 2015. № 2. URL: http://www.economy.nayka.com.ua/?op=1&z=3827 (дата звернення: 1.10.2021).

Наукове видання

ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА: АКТУАЛЬНІ ПИТАННЯ ТА ІННОВАЦІЇ

Матеріали Міжнародної науково-практичної конференції

(м. Дніпро, 4 листопада 2018 р.)

Упорядники:
Косиченко О. О., Насонова С. С. –
доценти кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидати технічних наук, доценти

Редактор, оригінал-макет – *А.В. Самотуга*
Редактор – *О.М. Врублевська*

Підп. до друку 24.12.2021. Формат 60х84/16. Гарнітура – Times.
Друк трафаретний (RISO), цифровий. Папір офісний. Ум.-друк. арк. 23,75.
Обл.-вид. арк. 25,00. Тираж 50 прим. Зам. № 12/21-зб.

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49000, м. Дніпро, просп. Гагаріна, 26, rvv_vonr@dduvs.in.ua
Свідоцтво суб'єкта видавничої справи ДК № 6054 від 28.02.2018