МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА ТА ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА ТА ІННОВАЦІЙНОЇ ОСВІТИ
КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Матеріали Всеукраїнського науково-практичного семінару

10 листопада 2022 року

м. Дніпро

УДК 351.74+004
С 90

Рекомендовано до друку Науковою радою Дніпропетровського державного університету внутрішніх справ (протокол № 4 від 21.12.2022 р.)

С 90 Сучасні інформаційні технології в діяльності національної поліції України: матер. Всеукр. наук.-практ. семінару (м. Дніпро, 10 листопада 2022 р.). Дніпро : ДДУВС, 2023. 204 с.

Збірник містить матеріали однойменного Всеукраїнського науково-практичного семінару. 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.

ЗМІСТ

КУРСАНТИ ТА СТУДЕНТИ

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

ФЕЙКИ ЯК ЕЛЕМЕНТИ ГІБРИДНОЇ ВІЙНИ: ОЗНАКИ ТА ІНСТРУМЕНТИ ВИЯВЛЕННЯ

24 лютого 2022 року розпочалася відкрита збройна агресія російської федерації (принципово, з маленької літери) проти України. Разом із тим, гібридна війна триває вже давно. Це війна, де агресор має наміри досягти політичних цілей шляхом використання методів дезінформації (відвертої, як-то пропаганда через державні ЗМІ та дипломатів, та прихованої, як-то через тролів, ботів та підробки), та інших активних заходів, як-то кібератак, агентів впливу, шантажування, військового обману, провокацій та інших у поєднанні з традиційними методами війни [2].

У гібридних війнах використовується велика кількість методів та засобів, серед яких особливе місце займає дезінформація, що стала невід'ємною частиною нашого інформаційного простору. Фахівцями дезінформація визначається як неправдива, маніпулятивна та/або оманлива інформація, що цілеспрямовано розповсюджується для досягнення певної політичної мети [2]. Для України дезінформація залишається серйозною загрозою, адже саме вона стала одним з головних інструментів російської федерації під час гібридної війни. При цьому, для дестабілізації ситуації та поширення дезінформації використовуються усі доступні канали комунікації: телебачення, Інтернет, радіо, пресу, чутки, дипломатію, експертне середовище тощо. Головним об'єктом ураження залишається людина, прихований вплив на яку здійснюється через її нервову систему та психіку, здебільшого на підсвідомому рівні [1, с. 8].

На теперішній час російська федерація доволі часто застосовує радянську практику активних заходів поширення дезінформації, що полягає у діях прихованого або оманливого характеру, які мають на меті здійснення вигідного впливу на цільове суспільство. Серед таких дій необхідно виділити створення та розповсюдження наративів та фейків.

Наратив (від латинської «nararre», пояснювати) це інтерпретація подій, яка не базується на фактах або точних даних. Найкращий приклад наративу – це міф або легенда [3, с. 30]. Для «підтвердження» наративів, як правило, використовуються фейки. Фейк (з англ. «Fake», підробка) це свідомо перекручена або повністю вигадана новина. При цьому, основними наративами російських фейків про Україну є: державний переворот на Майдані; Україна – це «нацистська» держава; Україна – це «недодержава» (failed state); спотворення та невизнання історії України; дискредитація української армії; територіальний розпад України; «територіальні претензії» сусідніх держав; «легітимізація»

тимчасової окупації окремих територій України; в Україні воюють війська НАТО; Захід втомився від України; маніпулювання міжнародними організаціями та відносинами України з ЄС; наявність в Україні лабораторій зі створення біологічної зброї тощо.

На сьогодні фейки – одна з найпоширеніших форм маніпуляцій у медіа. Не всі фейки вочевидь абсурдні. Часто маніпуляцію важко помітити з першого погляду. Такі фейки створюються для того, щоб поступово, крок за кроком, досягати бажаного ефекту – зміна ставлення та формування відношення до певного явища, соціальної або етнічної групи тощо. Саме накопичувальний ефект притаманний фейкам. При цьому, крім текстових відрізняють і візуальні фейки (фото, відео, у тому числі і дипфейки, створені з використанням штучного інтелекту).

Фейкам притаманні певні ознаки. По-перше, це підвищена надемоційність змісту та сенсаційність заголовків (наприклад, «розп'ятий хлопчик»), що унеможливлює критичний аналіз. По-друге, категоричність суджень та викладу (наприклад, «всім відомо, що…»). По-третє, драматичність «новини». По-четверте, посилання на «псевдоджерело» (наприклад, «як наголошують експерти», «за результатами опитувань» тощо). По-п'яте, швидкість розповсюдження (як наголошують фахівці, фейки поширюються на 70 % швидше ніж достовірна інформація та перевірені новини [2]). По-шосте, глибина розповсюдження (широке коло споживачів). По-сьоме, примітивізм (масовий продукт завжди створюється в досить спрощеній формі, без цього він не може отримати швидкого поширення). По-восьме, феки ніколи не мають продовження, вони розраховані виключно на оперативну маніпуляцію суспільною думкою виключно зраз, у короткотерміновій перспективі.

За наявності вказаних ознак, прийнятність фейків для використання у гібридних війнах обумовлена, за нашим переконанням, небажанням споживачів перевіряти інформацію та аналізувати викладені «факти». Разом із тим, дієвим інструментом їх виявлення є фактчекінг (з англ. «Fact checking», перевірка фактів). Це один із напрямів контролю, спрямований на виявлення невідповідностей між фактами та дійсністю. На професійному рівні виявленням та спростуванням фейків займаються фактчекінгові агентства. Існують і спеціалізовані програмні продукти та доступні сервіси для самостійного здійснення фактчекінгу, серед яких слід вказати «Images Google», «TinEye», «Fotoforensics», «InVID Project» тощо. Разом із тим, слід зазначити, що одним з основних інструментів виявлення та спростування фейків як елементів гібридної війни, має бути критичне мислення та інформаційна гігієна.

Список використаних джерел:

1. Албул С. В. Протидія інформаційним загрозам в умовах антитерористичної операції. *Кібербезпека в Україні: правові та організаційні питання*: матер. Всеукр. наук.-практ. конф. (м. Одеса, 21 жовтня 2016 р.). Одеса: ОДУВС, 2016. С. 7-9.
2. Дезінформація: види, інструменти та способи захисту: онлайн-курс. URL: https://courses.prometheus.org.ua/courses/course-v1:Prometheus+DISINFO101+2021_T2/about.
3. Ожеван М. А. Глобальна війна стратегічних наративів: виклики та ризики для України. *Стратегічні комунікації*. 2016. № 4 (41). С. 30-40.

Баліна І. В.,
директор Центру ІТ та
дистанційного навчання
Слов'янський університет
в Республиці Молдова,
кандидат економічних наук, доцент

КІБЕРСОЦІАЛІЗАЦІЯ СУЧАСНОГО СВІТУ: ВИКЛИКИ ТА РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Дослідження кіберсоціалізації, як процесу комп'ютерної, віртуальної соціалізації особистості, дозволяє сформувати основні ризики та виклики інформаційної безпеки сучасного світу [1].

Ризик інформаційної безпеки розглядається з точки зору можливості порушення ІБ з негативними наслідками. При цьому під ризиком розуміємо можливість того, що станеться несприятлива подія, яка має свою ціну (розмір очикуваної втрати) та ймовірність настання [2].

Основними сучасними ризиками інформаційної безпеки є: ризик неправомірної прихованої експлуатації інформаційно-обчислювальних ресурсів (наприклад, при створення бот-мережі), ризик втрати чи недоступності важливих даних, ризик використання неповної чи викривленої інформації, ризик розповсюдження до зовнішнього середовища інформації, яка загрожує репутації.

Роки пандемії 2020 та 2021 виявили багаточисельні проблеми кібербезпеки, виникла необхідність швидкої адаптації до «норми» віддаленої та гібридної роботи, що спричинило за собою зростання числа вразливостей та ризиків таких як: 1) захист кінцевих точок – це захист процесів, бізнес-даних та конфіденційних відомостей, які зберігаються або передаються через пристрої, підключені до мережі; 2) управління доступом – це механізм безпеки, який керує процесом взаємодії користувачів з системами та ресурсами, а також систем між собою. Цей механізм захщає системи та ресурси від несанкціонованого доступу і приймає участь у виявленні рівня авторизації після вдалого проходження процедури аутентифікації.

14 травня 2021 року компаняя Microsoft представила підсумки дослідження, проведеного аналітичною компанією IDC в шести країнах Центральної та Східної Європи. Дослідження показало, що бізнес не готовий у повній мірі відповісти на виклики у сфері ІБ: больше половини компаній (58 %) не мають комплексної стратегії кібербезпеки.

Рис. 1. Основні виклики у сфері безпеки в Центральній та Східній Європі

Дослідження проводилося в Угорщині, Греції, Польщі, росії, Румунії та Чехії, у ньому взяли участь фахівці з безпеки, а також ІТ-фахівці та керівники підприємств із різних галузей. Компанії відповідали на запитання щодо подій 2020 року та планів на два роки вперед. У дослідженні взяли участь 1500 осіб, з яких 48 % склали представники малого та середнього бізнесу [3].

В якості виявлених основних тенденцій кібербезпеки у 2021 р. та на перспективу 2022-2023 рр. можна виділити наступні:

1. ненавмисні дії співробітників – ТОП-5 атак: соціальна інженерія, тактика залякування, «уейлінг», «перехоплення сеансу», цільовий фішинг;
2. найбільш уразливі галузі – ТОП-5 мішеней: інфраструктурні об'єкти, охорона здоров'я, фармацевтичні і медичні організації, машинобудування, промисловий Інтернет речей;
3. наслідок COVID-19 – ТОП-5 вразливостей: домашні мережі, VPN, незахищений віддалений доступ, споживчі IoT-пристрої та пристрої периферії; здирники, двоетапні здирницькі кампанії.

При цьому головними проблемами економічної безпеки Євросоюзу є: забезпечення безпеки працівників, які працюють віддалено – це відзначили 47 % респондентів, захист від фішингу та атак з використанням соціальної інженерії – 42 %, надання безпечного віддаленого доступу – 41 %, захист хмарних додатків та інфраструктури – 39 %.

На рівні Євросоюзу питаннями регулювання інформаційної безпеки займається Європейський регламент захисту персональних даних GDPR (General Data Protection Regulation). Поряд із позитивними факторами впливу в положеннях Регламенту GDRP можна виділити такі протиріччя: війна з ботами та роботами. Так звана «вибухова» новація GDPR – право на заперечення проти результатів автоматичної обробки даних, створення профілів та прийняття на їх основі рішень (ст. 22). Тобто потенційний позичальник, який надав персональні дані, може вимагати скасувати рішення скорингової системи банку, яка відмовила йому в кредиті, якщо воно було винесене повністю без участі людини.

З точки зору заходів реагування, що використовуються в Республіці Молдова, можна навести такий позитивний приклад: Постановою Служби інформації та безпеки РМ узаконено блокування на період надзвичайного стану анонімних сайтів (понад 50), що поширювали неправдиву інформацію та нагнітали напругу в суспільстві, страх і паніку серед населення. «Анонімні адміністратори цих сайтів, видаючи новини типу fake-news, дезінформують населення, провокують ненависть у суспільстві, масові заворушення тощо. Таким чином вони становлять загрозу державній безпеці», – наголошувалося в повідомленні, розміщеному на сайті СІБ.

Головними завданнями безпеки на наступні 2 роки можна вважати: забезпечення віддаленої роботи, безпеку кінцевих точок та мобільних пристроїв, захист публічних та гібридних хмар.

Яскравим прикладом реалізованих загроз є 4 жовтня 2021 року, коли хакери отримали доступ до даних 1,5 млрд користувачів Facebook. За версією Business Insider, в даний час дані користувачів цієї соцмережі продаються на хакерському форумі [4]. Кожен користувач соціальних мереж та месенджерів WhatsApp та Instagram, а також сервісів Google, Facebook, Twitter та інших великих майданчиків по всьому світу відчули на собі збої та масове відключення доступу до on-line ресурсів у США та Великій Британії, Канаді, Нідерландів, Німеччині, Італії , Франції, України та Молдови, інших країн.

Аналогічна ситуація відбулася 25 жовтня 2022 – за даними ресурсу Downdetector, який відстежує відключення, в Мережі стався глобальний збій у роботі месенджеру у Великобританії, Німеччині, Греції, Іспанії, Італії, Нідерландів, Росії, Франції, Швеції [5]. Більшість користувачів месенджера WhatsApp компанії Meta (78 %) повідомили, що не можуть надіслати повідомлення в месенджері, 19 % відзначили проблеми з роботою програми в цілому, решта 3 % зіткнулися з проблемами при спробі зайти на веб-сайт сервісу WhatsApp [6]. Про проблеми в роботі сервісу з Німеччини надійшло понад 183 тис. повідомлень, з Великобританії – понад 60 тис., з Індії – майже 29 тис., з Індонезії – близько 9 тис., із Франції – майже 8 тис., із США – близько 3,5 тис.

На основі проведеного дослідження можна сформулювати такі висновки:

I. Слабкість можливого законодавчого механізму регулювання ІБ у країнах Євросоюзу веде до того, що основні дії порушників ІБ не можна зупинити штрафами та регламентами.

II. З точки зору вигоди порушення ІБ не завжди є виразом злої волі, а виступають таким наслідком еволюційних механізмів, як бажання ділитися негативними емоціями та попереджати про небезпеку.

III. Соціальний, фінансовий та технічні аспекти можливих викликів та ризиків, наслідків здійснення загроз ІБ слід відстежувати та формулювати у кожний конкретний часовий період, описуючи їх біполярність з погляду позитивних перспектив та негативних впливів як у кожній окремій країні Євросоюзу, так і загалом на його території.

Таким чином, досліджувані проблеми позитивних та негативних аспектів ІБ та кіберзлочинності є затребуваними як ніколи на сучасному етапі, а правильна поведінка до, під час та після атак зловмисників багато в чому сприятиме зниженню ризиків та викликів інформаційної безпеки та сприятиме регулюванню європейської дипломатії в цілому на новому рівні.

Список використаних джерел:

1. Довідник-24. Кіберсоціалізація. URL: https://spravochnick.ru/sociologiya/kibersocializaciya/
2. Ризики інформаційної безпеки. URL: https://arinteg.ru/articles/riski-informatsionnoy-bezopasnosti-26222.html.
3. Аналітика в: «CONNECT. Світ інформаційних технологій». URL: https://www.connect-wit.ru/issledovanie-check-point-kazhdaya-vtoraya-organizatsiya-soobshhaet-ob-uvelichenii-kiberatak-vo-vremya-pandemii.html.

4. Рибін О. Хакери злили дані 1,5 млрд користувачів Facebook. URL: https://rg.ru/2021/10/04/hakery-slili-dannye-15-mlrd-polzovatelej-facebook.html.
5. В роботі WhatsApp відбувся збій. URL: https://rg.ru/2022/10/25/v-rabote-whatsapp-proizoshel-sboj.html.
6. В роботі WhatsApp відбувся глобальний збій. URL: https://www.rbc.ru/rbcfreenews/63578d329a7947a58aefbf4c.
7. В роботі WhatsApp відбувся глобальний збій. URL: https://lenta.ru/news/2022/10/25/whatsapp/

Бадалова Т. Г.,
ад'юнкт
Дніпропетровського державного
університету внутрішніх справ,
майор поліції
Гребенюк А. М.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ОКРЕМІ ПРОБЛЕМНІ ПИТАННЯ ЩОДО ЗДІЙСНЕННЯ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА ПІД ЧАС ПРОВЕДЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРОВАДЖЕНЬ ПОВ'ЯЗАНИХ З КІБЕЗЛОЧИНАМИ

Становлення інформаційного суспільства в Україні, розвиток та поширення комп'ютерних технологій та комп'ютерної техніки, використання телекомунікаційних мереж майже в усіх сферах життєдіяльності людини полегшило можливість передання інформації, створивши низку проблем, пов'язаних зі створенням безпечних умов використання віртуального простору. У період глобалізації швидкий розвиток інформаційних технологій та комп'ютерних мереж супроводжується зловживанням цими технологіями зі злочинною метою та надає широкі можливості для вчинення традиційних злочинів, створюючи при цьому умови для реалізації зовсім нових схем і методів злочинної діяльності. Рівень можливостей, які отримують зловмисники, й тенденція до збільшення кількості злочинів у сфері комп'ютерних інформаційних технологій становлять загрозу не лише демократичним перетворенням та розвитку інформаційного суспільства.

Нині офіційна державна статистика містить відомості про вчинені кримінальні правопорушення, передбачені Розділом XVI КК України, які відображаються у звітах Офісу Генерального прокурора України (далі – ОГП) [1] та у відомчій статистичній звітності Національної поліції України (за даними Офісу Генерального прокурора) представлені в табл. 1.

Таблиця 1

Рік	Облікові кримінальні правопорушення	Кількість осіб, яким вручено повідомлення про підозру
2014	443	207
2015	598	263
2016	865	472
2017	2573	1272
2018	2301	1608
2019	2204	1481
2020	2498	1675
2021	2790	2034

Питома вага злочинності у сфері електронно-обчислюваних машин у структурі злочинності в Україні за 2014 рік становила приблизно 0,08 %, у 2015 р. – 0,01 %, у 2016 р. – 0,15 %, у 2017 р. – 0,49 %, у 2018 р. – 0,5 %, у 2019 р. – 0,49 %, у 2020 р. – 0,7 %, а у 2021 р. (станом на жовтень) – 0,93 % [2]. Рівень судимості за 2014 рік склав 37 осіб, за 2015 – 31 особу, за 2016 – 24 особи, за 2017 – 42 особи, за 2018 – 49 осіб, за 2019 – 50 осіб, за 2020 – 56 осіб. Отже, зазначений показник є досить мізерним порівняно з кількістю облікованих щорічно злочинів [3]. За звітними даними Голови Національної поліції України, ціна кіберзлочинності в Україні за 2019 рік становила 28 мільйонів гривень, а станом на 2020 рік зросла до 241 мільйона гривень [4]. Американська компанія McAfee, яка спеціалізується на комп'ютерній безпеці, та Центр стратегічних і міжнародних досліджень (CSIS) стверджують, що хакерські атаки протягом 2020 року коштували світовій економіці понад трильйон доларів, або 820 мільярдів євро [4]. Аналізуючи дані за 2020 рік щодо структури, можемо дійти висновку, що найбільшу питому вагу серед злочинів, передбачених розділом XVI КК України (49 %) становлять дії з несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 ККУ).

На сьогодні в українському законодавстві відсутнє визначення поняття «кіберзлочин» або «кіберзлочинність», є лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку (розділ XVI Кримінального кодексу України (далі – КК України)) [5], зокрема: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (стаття 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361-1 КК України); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних

машинах 8 (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (стаття 361-2 КК України); 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 (стаття 362 КК України); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (стаття 363 КК України); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 363-1 КК України). Крім того, діяльність кіберзлочинців кваліфікується за статтею 200 КК України – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

Банківська система України є однією зі сфер, де найбільш широко та активно використовуються сучасні можливості інформаційних технологій та мережі Інтернет. А враховуючи, що зазначені технології використовуються для грошових переказів, зазначена сфера привертає все більшу увагу злочинців.

Важливу роль у боротьбі та розслідуванні кіберзлочинів мають значення міжнародні угоди, Конвенції Ради Європи, рішення Ради Европейского Союзу та ін.

Питання кібербезпеки перебуває на особливому контролі з боку міжнародної спільноти, про що свідчить прийняття 23 листопада 2001 р. Конвенції про кіберзлочинність, яку Україна ратифікувала 07.09.2005 [6].

У преамбулі цієї Конвенції вказано, що вона «*є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, як це описано у Конвенції, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва*».

Конвенція закріплює чимало різних положень, які декларують можливості отримати міжнародну допомогу країнам-учасницям у боротьбі з кіберзлочинністю, серед яких слід виділити принцип надання міжнародно – правової допомоги, це насамперед пов'язано з отриманням необхідної інформації або документів, які суттєво впливають на процес доказу скоєного кримінального правопорушення.

Поняттям міжнародна правова допомога включає в себе проведення компетентними органами однієї держави процесуальних дій, виконання яких необхідне для досудового розслідування, судового розгляду або для виконання вироку, ухваленого судом іншої держави або міжнародною судовою установою.

Згідно до вимог ст. 542 КПК України міжнародне співробітництво під час кримінального провадження полягає у вжитті необхідних заходів з метою надання міжнародної правової допомоги шляхом вручення документів, виконання окремих процесуальних дій, видачі осіб, які вчинили кримінальне правопорушення, тимчасової передачі осіб, перейняття кримінального переслідування, передачі засуджених осіб та виконання вироків. Міжнародним договором України можуть бути передбачені інші, ніж у цьому Кодексі, форми співробітництва під час кримінального провадження.

Під час міжнародного співробітництва у сфері протидії кіберзлочинів реалізується у відповідності до чинного законодавства, але аналіз законодавства, вказує про відсутність спільного та узгодженого підходу до міжнародного співробітництва.

Одними із основних проблем міжнародного співробітництва під час розслідування кримінальних правопорушень у сфері кіберзлочинів є недосконаліть чинного законодавства України, щодо здійснення міжнародно – правової допомоги. Це насамперед стосується отримання відповідних ухвал щодо тимчасових доступів до інформації та документів.

Розглянемо проблематику проведення екстрадиції за злочинами, передбаченими ст. 361 КК України на прикладі кримінального провадження, внесеного до Єдиного реєстру досудових розслідувань СУ ГУНП в Дніпропетровській області.

Так, згідно з матеріалів кримінального провадження: «*в період часу з лютого 2016 року по березень 2016 року невстановлені особи за допомогою програмного забезпечення здійснили втручання в локальну обчислювальну мережу Публічного Акціонерного Товариства «БКД», міжнародну систему «Society for Worldwide Financial Telecommunications» – «S. W. I. F. T.», та отримали доступ до операційних дій з міжнародного переказу грошових коштів. Тобто невстановлені особи, отримавши доступ до локальної обчислювальної мережі ПАТ «БКД», увійшли до системи «S. W. I. F. T.», та використовуючи отримані злочинним шляхом платіжні документи, внесли в них фіктивні дані. Після обробки платіжних документів, системою «S. W. I. F. T.» було підтверджено операцію і здійснено переказ грошових коштів, з кореспондентських рахунків ПАТ «БКД» на рахунки банку Туреччини. Після цього невстановлені особи видалили створені ними файли, що призвело до зупинки роботи системи «S. W. I. F. T.». В результаті злочинних дій невстановлених осіб ПАТ «БКД» було спричинено значну матеріальну шкоду у розмірі 951 838, 95 доларів США, 1 468 593 доларів США, 1 833 956, 18 євро».*

У подальшому під час проведення досудового розслідування вказаного кримінального провадження СУ ГУНП у порядку ст. 552 КПК України та Європейської конвенції про взаємну правову допомогу в кримінальних справах 1959 року звернулася до компетентних органів Туреччини з запитом про надання міжнародної правової допомоги та висловила своє прохання здійснити тимчасовий доступ до речей та документів банківських рахунків банків Туреччини. Формування вказаного запиту довго тривало у зв'язку з тим, що треба було отримати відповідні ухвали та здійснити переклад на дуже рідкісну мову – турецьку. Також СУ ГУНП планувалися заходи, щодо арешту відповідних банківських рахунків, але судом на підставі ч. 7 ст. 173 було відмовлено у зв'язку з тим, що власники рахунків банків Туреччини не викликано у засідання суду для вирішення питання щодо арешту. Вказані слідчим суддею в ухвалі про відмову обставини не можливо було здійснити у зв'язку з тим, що офіційно сповістити турецьку сторону про розгляд клопотання про арешт майна можливо лише за міжнародним запитом. Всі заходи, щодо підготовки всіх необхідних матеріалів та їх переклад тривав більш ніж 2 місяці, що негативно впливало на повернення грошових коштів та отримання інформації, щодо власників рахунку та рух коштів по вказаним рахункам.

Ситуацію щодо повернення грошових коштів до ПАТ «БКД» вдалося вирішити лише завдяки співпраці ПАТ «БКД» та банків Туреччини, у подальшому запит було надіслано до компетентних органів Туреччини та отримано необхідну інформацію, але завдяки співробітників ПАТ «БКД» вдалося уникнути зняття з рахунків банків Туреччини грошових коштів у розмірі 951 838, 95 доларів США, 1 468 593 доларів США, 1 833 956, 18 євро.

На нашу думку слід враховувати законодавства іноземних держав під час здійснення міжнародного співробітництва та внести відповідні зміни до ст. ст. 170 – 173 КПК України, щодо розгляду клопотань про арешт майна у випадку здійснення міжнародно – правової допомоги та внести відповідні зміни до глави 44 КПК України, при цьому слід розробити відповідний механізм застосування чинного законодавства України та не допускати випадки втрати можливості отримання доказів під час здійснення міжнародно-правової допомоги у кримінальних провадженнях даної категорії кримінальних правопорушень.

Список використаних джерел:

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування: Єдиний звіт Офісу Генерального прокурора. URL: https://www.gp.gov.ua/ua/stat_n_st?dir_id=113653&libid=100820.
2. Судова статистика. Форма № 7 «Звіт про склад засуджених». URL: http://court.gov.ua/inshe/sudova_statystyka/
3. Звіт Національної поліції України про результати роботи у 2020 році. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf.
4. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів – дослідження. URL: https://tsn.ua/groshi/kiberzlochinci-u2020-roci-zavdali-u-sviti-zbitkiv-na-trilyon-dolariv-doslidzhennya-1683076.html.
5. Головкін Б. М., Голіна В. В., Лисодєд О. В. Кримінологія: підручник. Право, 2020. 259 с.
6. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 р. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

Bogdanova V.,
senior lecturer
Department Informatics and
Information Technology
Tiraspol State University,
Ph.D. in education science

METHODOLOGICAL ASPECTS OF TEACHING INFORMATION SECURITY TO FUTURE ECONOMISTS

Modern rapidly occurring changes in society and the economy, the rapid development of science and technology, place high demands on the digital competencies of specialists in various fields. The state is interested in the development of education in the field of information security (IS), as well as in specialists and qualified personnel of the public and private sectors, including economists [1].

The organization of training in the basics of information security for future economists requires a systematic approach, because has its own characteristics associated with the complexity and ambiguity of the conceptual apparatus, insufficient development of methodological approaches to teaching the basics of information security to students of non-technical specialties, a variety of content in various educational and methodological materials.

The process of teaching information security to students of economic specialties is modeled from the point of view of a systematic approach. When determining the purpose and objectives of training, the requirements of the labor market for future economists, the standards for the preparation of bachelors in the direction of «Economics» were taken into account.

The purpose of the discipline is to develop students' stable skills of working in a complex network information environment of a modern enterprise, office, taking into account the basic requirements of information security. The main objectives of the discipline: obtaining information about the current state of the problems of providing information security for computer systems, existing threats, types of security, methods and means of protecting information, the basics of building complex protection systems, the basics of legal regulation of relations in the information sphere, constitutional guarantees of citizens' rights to receive information and mechanisms their implementation, concepts and types of protected information.

Taking into account the goals set, the theoretical sections of the discipline are defined:

- Basic concepts and definitions;
- IS threats and information leakage channels;
- Legal means of information protection;
- Organizational means of information protection;
- Physical and technical means of information protection;

– Information security software;
– Identification and authentication;
– Cryptographic approaches to information security and digital signature;
– Moral and ethical ways to protect information.

Laboratory (L) and practical (P) classes are aimed at developing practical skills and abilities in the field of information security: P1. Windows security policy; L2. Disk space optimization; L3. Archiving; L4. Password protection; L5. Protection of flash drives; L6. Antivirus protection of information; L7. Protection of text documents; L8. Spreadsheet protection; P1. Symmetric encryption methods; P2. Methods of asymmetric encryption and digital signature.

An important part of the learning process is the organization of students' independent activities. Particular attention is paid to information and communication technologies that support the implementation of this process: the program for creating electronic textbooks SunRav; PowerPoint; digital publishing platform Joomag [2]; Google tools: Google Sites, Google Forms; Online Test Builder Testmoz.

To determine the effectiveness of the learning process, training control was introduced; accumulative point-rating system; final testing. A simplified model of the «composition of the system» of the process of teaching the basics of information security to future economists is shown in the figure 1.

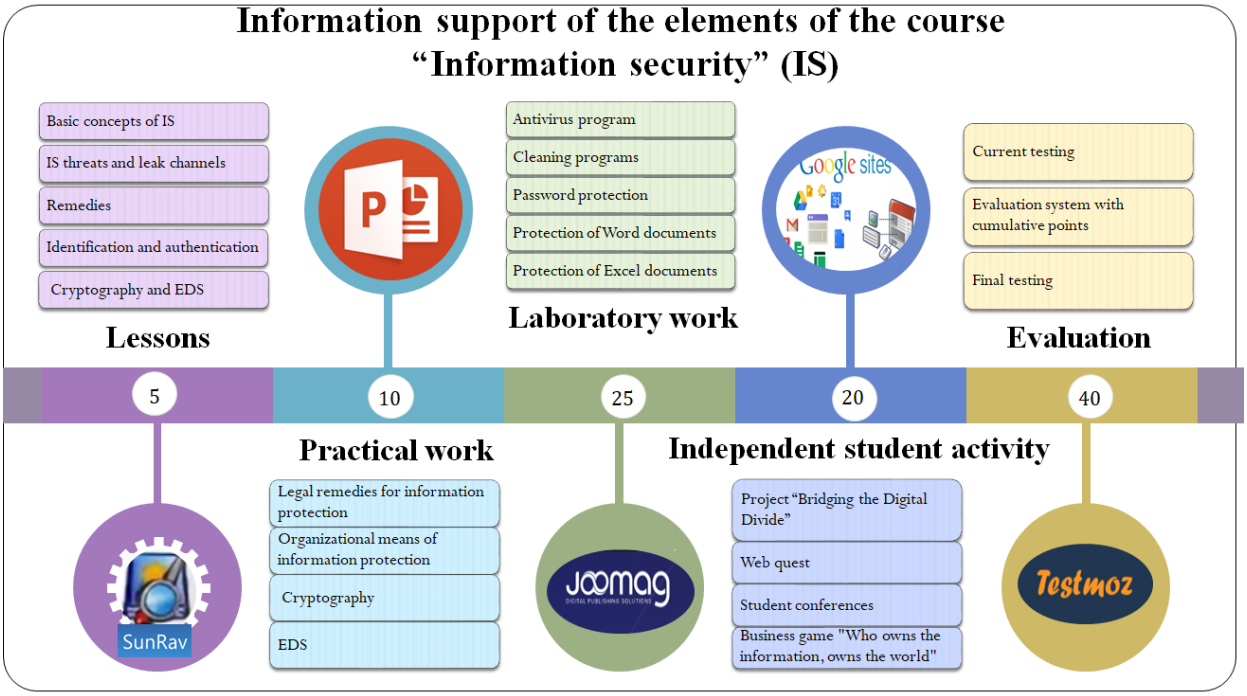


Fig. 1. Components of the course IS and applied ICT

The model ensures the successful mastering of the discipline, increasing the level of training, and contributes to the formation of skills for independent assimilation of educational material and its practical application. [3].

References:

1. Охріменко С. А., Скліфос К. Ф. Інформаційна безпека для економістів. Лабораторія Інформаційної безпеки. URL: http://security.ase.md/publ/ru/pubru106/o_s.html.
2. Bogdanova V., Chiriac L. The digital publishing platform joomag for organizing independent work of students. *Розбудова єдиного відкритого інформаційного простору освіти впродовж життя:* II Міжнар. наук.-практ. WEB-форум (March 25, 2020). Харків: «Мадрид», 2020. С. 201-202.
3. Bogdanova V., Chiriac L. Pedagogical modeling of the process of teaching the university discipline «Information security». The XXIX Conference on Applied and Industrial Mathematics (August 25-27, 2022). Chişinău: US Tiraspol, 2022. Pp.61-66.

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

КРИПТОВАЛЮТА ЯК ІНСТРУМЕНТ ЗЛОЧИННОГО СВІТУ

На теперішній час криптовалюта вже відкрила нові ринки та зробила світову економіку більшою та глибше інтегрованою. Ми бачимо лише початок того, що може запропонувати ця технологія. На сьогоднішній день як в Україні так і в світі зростає ажіотаж навколо криптовалюти, оскільки використання криптовалюти різко зростає, а вартість біткойнів досягає рекордних значень. Також в світі зростає тенденція проведення злочинних оборуток а не тільки використання криптовалюти для легальних законних транзакції.

Криптовалюти служать фінансовою основою для багатьох незаконних оборуток, таких як:

- відмивання грошей;
- шахрайство;
- незаконним обігом наркотиків;
- торгівля людьми;
- експлуатація дітей;
- торгівля на темному ринку;
- кіберзлочинність;
- фінансування терору.

Криптовалюти як цифрові активи легко зберігати. Зберігання інформації криптогаманця не потребує фізичного простору, на відміну від купи купюр. Це означає, що вони не привертають увагу ні злодіїв, ні, що найголовніше для злочинців, влади. Криптовалюти також легко переказувати як на місцевому, так і на міжнародному рівнях, без ризику конфіскації.

Легкі перекази створюють умови для крадіжки та відмивання коштів злочинцями. Криптовалюти передаються за лічені хвилини, і немає можливості скасувати транзакції після їх підтвердження майнерами.

У 2021 році злочинність, пов'язана з використанням криптовалюти, досягла нового історичного максимуму: протягом року незаконні адреси отримали 14 мільярдів доларів США проти 7,8 мільярдів доларів у 2020 році.

Але ці цифри не розповідають всю історію. Використання криптовалюти зростає швидше, ніж будь-коли раніше. За всіма криптовалютами, які відстежує Chainalysis, загальний обсяг транзакцій зріс до 15,8 трильйона доларів у 2021 році, що на 567 % більше, ніж у 2020 році [6].

Криптовалюта є цифровими грошами, в основі якої лежит технологія криптографії, тобто шифрування даних. Така валюта не має фізичного вигляду, а існує тільки в електронному вигляді, тобто є комп'ютерним кодом. Криптовалюта створюється шляхом майнінгу (англ. mining – видобуток в шахті). Під майнінгом називают вирішення певного криптозавдання шляхом повного перебору завданого алгоритму за допомогою спеціального технічного обладнання для підтвердження транзакцій та забезпечення безпеки криптовалютної мережі.

З огляду на чинні норми законодавства України (Цивільний кодекс України, Закон України «Про Національний банк України», Декрет Кабінету Міністрів України «Про систему валютного регулювання і валютного контролю», Закон України «Про платіжні системи та переказ коштів в Україні», Закон України «Про інформацію» та інші) поняття «крипто валюта» та регулювання операцій з нею не підпадають під режим регулювання [1-4]:

- криптовалюта не існує у формі банкнот, монет, записів на рахунках у банках, вона не може бути визнана грошима;
- оскільки криптовалюта не має прив'язки до грошової одиниці жодної з держави, вона не може бути визнана валютою або законним платіжним;
- не може бути визнана електронними грошима;
- криптовалюта не може бути цінним папером;
- криптовалюта не може бути визнана грошовим сурогатом (згідно з його визначенням у Законі України «Про Національний банк України»).

Зростання ринку криптовалют в Україні призвело до прийняття спеціального Закону «Про віртуальні активи»№ 2074-IX від 17.02.2022 (не набрав чинності). Цей Закон набирає чинності з дня набрання чинності законом України про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами, але не раніше дня опублікування цього Закону. Цей Закон врегулює правовідносини, що виникають у зв'язку з оборотом віртуальних активів в Україні, визначає права та обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обороту віртуальних активів [5].

На сьогодні серед регуляторів провідних країн світу, зокрема країн Європейського Союзу, немає єдиного підходу до визначення правового статусу криптовалют та регулювання операцій з ними.

Сьогодні нараховується біля тисячі видів криптовалют (їх кількість постійно змінюється), серед яких найбільшого поширення набули такі як Bitcoin, BitcoinCash, Ethereum, Litecoin та інші. Зростання їх популярності у світі відбувається на тлі відсутності єдиного поняття «крипто валюта» («cryptocurrency») − воно варіюється від ототожнення з поняттями «товар», «платіжний засіб», «розрахункова одиниця» до понять «нематеріальний цифровий актив», «інвестиційний актив», «фінансовий актив», «окремий вид цінних паперів» тощо. Більшість криптовалют працюють на технології блокчейн, тобто кожна транзакція містить інформацію про всі проведені раніше операції в мережі з моменту створення цифрової валюти. Тому, складність обробки транзакцій з криптовалютами постійно зростає, до того ж винагороду отримує лише один майнер, який перший обробив операцію.

Хоча всі транзакції, які відбуваються в блокчейні, зберігаються в загальнодоступному записі та доступні будь-кому для перегляду, особи виконавців транзакцій залишаються невідомими.

Транзакції здійснюються з однієї чи кількох криптоадрес на одну чи декілька адрес призначення. Криптоадреса – це випадковий набір символів, що приблизно є криптоеквівалентом номера банківського рахунку.

В Україні є достатньо торгових точок, ресторанів, кафе й інших закладів, які приймають до оплати ті ж самі біткойни. Поступово й інші криптовалюти в цій сфері отримують застосування.

Оскільки криптовалюта продовжує розвиватися, вкрай важливо, щоб державний і приватний сектори працювали разом, щоб гарантувати, що користувачі можуть здійснювати безпечні транзакції, і щоб злочинці не могли зловживати цими новими активами. Потрібно проводити навчання з правоохоронними органами для більш ефективного запобігання, пом’якшення та розслідування злочинів, пов’язаних із криптовалютою.

Список використаних джерел:

1. Про запобігання корупції: Закон України № 2849-IX від 13.12.2022 р. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text.
2. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України № 2736-IX від 04.11.2022 р. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text.
3. Рада легалізувала віртуальні валюти в Україні. URL: https://www.epravda.com.ua/news/2021/09/8/677595/
4. Про віртуальні активи: Закон України (не набрав чинності). URL: https://ips.ligazakon.net/document/T222074?an=1.
5. Платформа даних блокчейн URL: https://www.chainalysis.com/company/

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

ЗНАЧЕННЯ ЦИФРОВИХ, КРЕАТИВНИХ ТА ТРАДИЦІЙНИХ ІНДУСТРІЙ У ПОВОЄННИЙ ПЕРІОД

До початку Національно-визвольної війни в Україні цифрова та креативна індустрії визначали високотехнологічні напрями інноваційної діяльності і були пріоритетними для країни. У сьогоднішніх умовах, до них додаються традиційні індустрії, які є остовом соціально-економічного відновлення держави. До війни Україна мала потужний металургійний комплекс, що слугував базою для розвитку машинобудування, але залишалася країною із сировинною економікою. Нині є шанс реалізації розумної стратегії держави, що має на меті не лише відновлення довоєнних потужностей, а і розбудову сильної інноваційної країни.

Важливим методичним та нормативно-правовим забезпеченням поновлення згаданих вище індустрій є удосконалення відповідно до вимог часу та продовження реалізації таких стратегій як:

- Національна економічна стратегія 2030;
- Експортна стратегія для сектору інформаційних технологій;
- Експортна стратегія для сектору машинобудування;
- Експортна стратегія для сектору креативних індустрій (нові медіа та ІКТ: програмне забезпечення, цифрові технології в мистецтві – 3D-друк, AR/VR, змішана реальність);
- Експортна стратегія для сектору технічного обслуговування та ремонту повітряних суден;
- Пріоритети розвитку національного підприємництва в умовах цифрових трансформацій;
- Стратегія розвитку сфери інноваційної діяльності на період до 2030 року тощо [1].

Роль цифрових, креативних та традиційних індустрій постійно зростає, разом з тим, змінюються підходи до визначення ефективності та інноваційності, тим більше, змінюються самі економічні моделі, світові інституції, глобальна система безпеки та ставлення до середовища [2].

І саме інновації мають пов’язати провідні сфери та види діяльності, а також різні галузі науки у найближчій перспективі. Прикладом застосування інновацій у військових технологіях уже зараз є C4ISR: (C4 – командування, управління, зв’язок, комп’ютери; ISR – інтелект, спостереження та розвідка. Розширені можливості C4ISR забезпечують перевагу завдяки ситуаційній обізнаності, знанню супротивника й оточення та скороченню часу між

зондуванням та реакцією). При цьому застосовуються знання таких сфер діяльності як (біо)інформатика, авіоніка, аеростатика, медицина, кінематика, токсикологія, когнітологія, STEM та інші.

Можливі сценарії розвитку для України у повоєнний період, на думку експертів, представляють її як простір свободи і творення, фронтир цивілізації, світовий інноваційний, технологічний і логістичний хаб, країну розвинутого людського капіталу, світовий центр культури, освіти і науки, країну нової економіки, випереджального економічного зростання і бізнес-можливостей [2].

Першими кроками відбудови економіки мають стати подолання корупції, перерозподіл національного доходу, виробничих потужностей, усіх матеріальних, трудових і фінансових ресурсів в інтересах мирного будівництва.

Список використаних джерел:

1. Горященко Ю. Г. Вплив змін цифрових технологій бізнесу на формування інтелектуального капіталу. *Актуальні проблеми та перспективи розвитку обліку, аналізу та контролю в соціально-орієнтованій системі управління підприємством*: матер. Всеукр. наук.-практ. конф. Полтава: ПДАУ, 2022. С. 458-459.
2. Длигач А. Україна майбутнього – погляд із 2030 року. *Економічна правда*. URL: https://www.epravda.com.ua/rus/columns/2022/03/24/684560/

Дурєєв В. О.,
доцент кафедри автоматичних систем безпеки та інформаційних технологій Національного університету цивільного захисту України, кандидат технічних наук, доцент
Христич В. В.,
заступник начальника кафедри автоматичних систем безпеки та інформаційних технологій Національного університету цивільного захисту України, кандидат технічних наук, доцент

УДОСКОНАЛЕННЯ МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ БЕЗПЕКИ

В умовах військового стану в Україні, виникла гостра потреба в проведенні безпечних робіт зі спеціальною технікою. Одним із можливих шляхів забезпечення таких робіт є можливість застосування дистанційного доступу та вивчення роботи приладів, які забезпечують безпеку об’єктів виробництва та громадської інфраструктури.

Пропонується для вивчення роботи систем безпеки та протипожежного захисту застосувати електронний тренажер, що моделює роботу приймального приладу контрольного пожежного (ППКП) в усіх практичних умовах та режимах експлуатації. Метою використання такого підходу є підвищення безпеки та якості підготовки спеціалістів при вивченні роботи спеціального обладнання систем безпеки. Для досягнення поставленої мети, були сформульовані і вирішені наступні актуальні задачі: виконано аналіз вітчизняних та міжнародних патентів для приладів систем безпеки, які використовуються у навчальному процесі ВНЗ України; розроблено електронний тренажер [1], що моделює роботу приладів систем безпеки [2] і дозволяє проводити дистанційно: вивчення технічних даних сучасних і перспективних зразків обладнання; дії користувачів ППКП в чотирьох режимах роботи та чотирьох рівнях доступу; виконувати контроль отриманих знань; розроблена методика та проведена апробація використання електронного тренажера ППКП в умовах дистанційного навчання фахівців систем безпеки.

В алгоритмі роботи (рис. 1) тренажеру закладені можливості по визначенню приладу безпеки, роботу якого досліджується; його основні технічні данні; інтерактивне вивчення чотирьох режимів роботи в чотирьох рівнях доступ. Закладена можливість проведення контролю рівня отриманих знань вбудованою системою опитування.

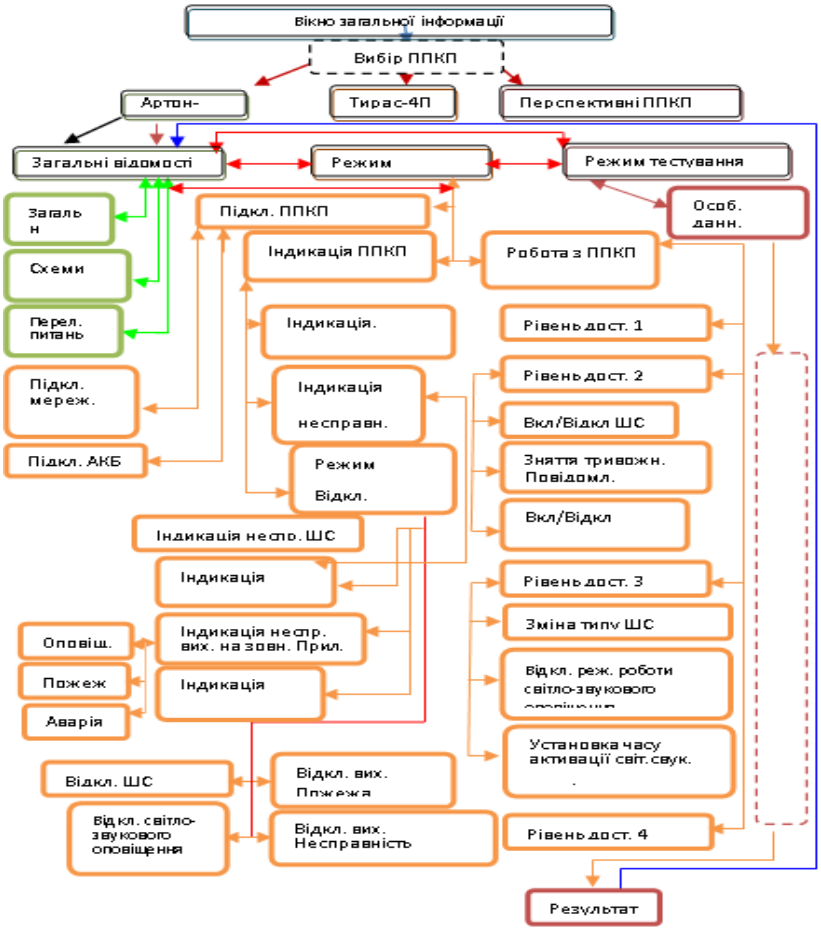


Рис. 1. Алгоритм роботи електронного тренажеру

Для зручності користувачів та кращої наочності, програма містить робочі вікна, в яких представлені: можливість вибору типу приладу системи безпеки, зовнішній та внутрішній вигляд приладу, технічні данні та характеристики приладу, інформація про виробників систем безпеки, зразки технічної документації, зразки приладів для навчання (рис. 2).

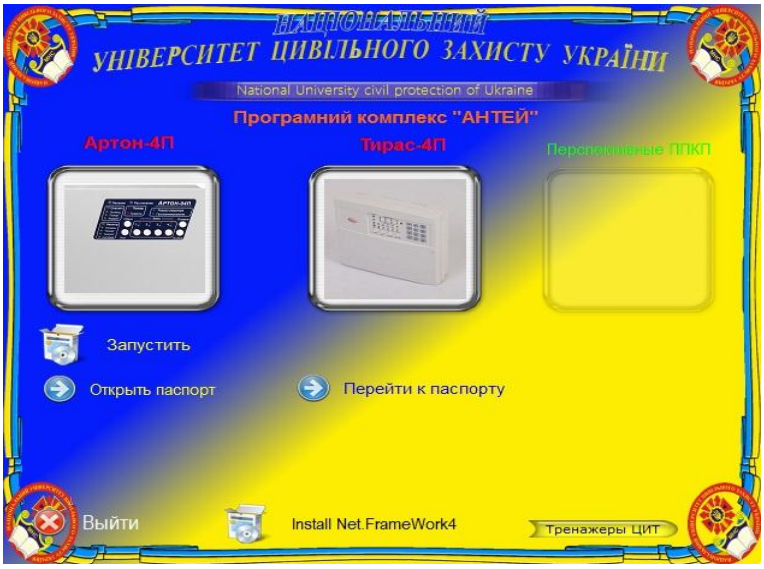


Рис. 2. Стартове вікно програми

Після визначення приладу, який користувач тренажера вибирає для навчання, програма відтворює робочи місця для навчання, а саме: загальна інформація приладу, робота приладу (рис. 3.а); контроль та перевірка результатів вивчення роботи приладу (рис. 3.б).

Перевірка отриманих знань відбувається шляхом постановки тестових питань з виставленням оцінки. Час перевірки – 20 хвилин.

З метою апробації застосування електронного тренажера для дистанційного навчання, було проведено: заняття з обмеженням часу для фахівців ліцензованих видів робіт, курсантів і студентів НУЦЗ України, які вже вивчали раніше системи безпеки; заняття без обмеження часу для курсантів НУЦЗ України, які не вивчали раніше системи безпеки.

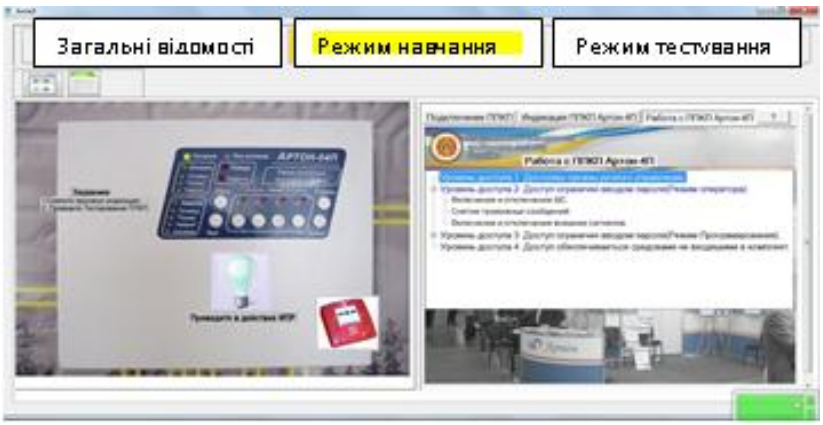


Рис. 3.а. Робочі місця програми

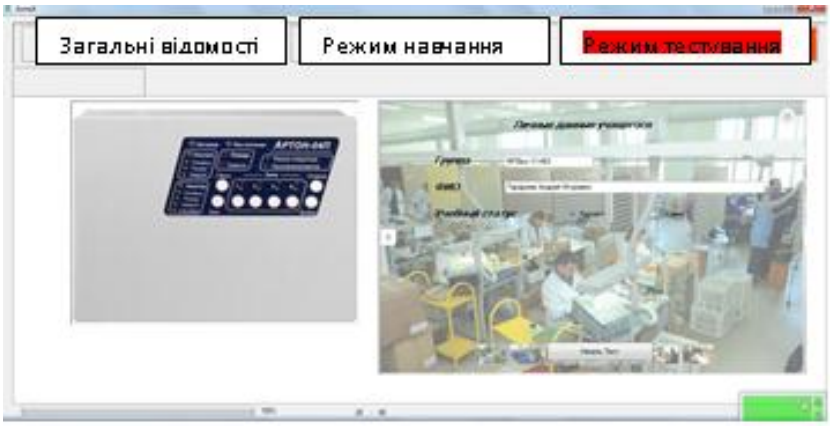


Рис. 3.б. Робочі місця програми

Результати застосування програми представлені на рис. 4.

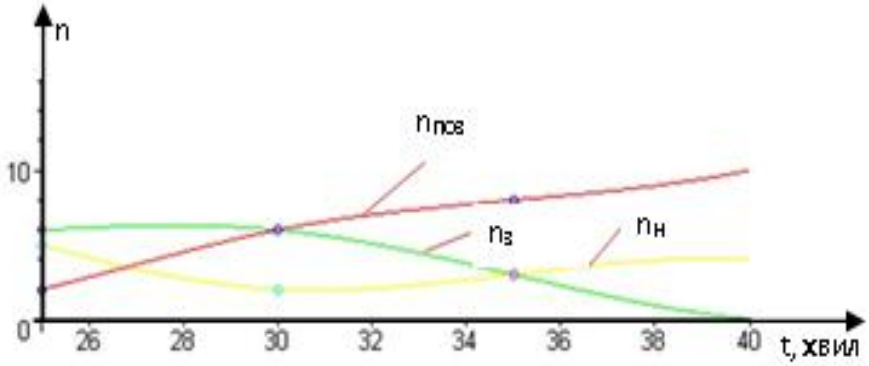


Рис. 4. Результати тестування: $n_{поз}$ – позитивні результати; $n_з$ – задовільні результати; $n_н$ – негативні результати

Практичне значення використання програми полягає в: безпечна підготовка фахівців сучасним і перспективним систем безпеки; розробка рекомендацій виробникам систем безпеки щодо технічних характеристик, конструкційному виконанню та інтерфейсу приладів безпеки.

Список використаних джерел:

1. Петцольд Ч. Програмування з використанням Microsoft Windows Forms. Університет «Україна». 2015. 137 с.
2. Системи протипожежного захисту. К.: Міністерство регіонального розвитку та будівництва України. 2015. 127 с.

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

ОКРЕМІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ ВІЙНИ У КІБЕРПРОСТОРІ ПІД ЧАС ВОЄННОГО СТАНУ

Кіберзлочинність у XXI столітті є дуже великою загрозою, а з початком війни, яку держава-агресор РФ здійснює проти України, ця загроза значно зросла. Адже хакерські атаки на комп'ютерні мережі та об'єкти критичної інфраструктури можуть спричиняти наслідки, порівняні з ракетними ударами. Тому кількість кібератак з початку війни значно зросла.

У квітні Microsoft запобігла спробам хакерського угруповання Strontium, пов'язаного з російським ГРУ, здійснити атаки на комп'ютерні мережі України, США та Євросоюзу, щоб «забезпечити тактичну підтримку фізичного вторгнення та вилучити конфіденційну інформацію» [1-2].

За повідомленням Держспецзв'язку у квітні відбулося розсилання електронних листів з темою «№ 1275 від 07.04.2022», а також з темою «Військові злочинці рф», у разі відкриття яких зловмисники можуть отримати повний контроль над комп'ютером та викрасти чи пошкодити дані. 28 березня цього року зазнав атаки хакерів провайдер Укртелеком, коли зловмисники намагалися вивести з ладу обладнання та сервіси компанії та отримати над ними контроль. А 23 березня була здійснена кібератака на державні установи України за допомогою шкідливої програми Cobalt Strike Beacon [2].

За повідомленням Reuters Росія стоїть за масштабною кібератакою наприкінці лютого цього року на супутникову інтернет-мережу, яка вивела з ладу десятки тисяч модемів, та яка на думку Ентоні Блінкена мала на меті «порушити українське командування та контроль під час вторгнення, і ці дії мали побічний вплив на інші європейські країни». Також Ілон Маск заявив, що мережа Starlink, яка використовується ЗСУ для забезпечення зв'язку, чинила опір російським блокуванням та спробам злому, але російські хакери нарощують свої зусилля [3].

21 жовтня 2022 року Міністерство оборони України надіслало у Telegram попередження про розсилання електронних листів на електронні скриньки та у месенджери нібито від Пресслужби Генштабу ЗСУ, а насправді з адрес, що не мають жодного стосунку до Збройних Сил України, та можуть спричинити зараження комп'ютера шкідливими програмами у разі їх відкриття [4].

І таких прикладів можна навести чимало. Це свідчить про те, що інформаційна безпека України під час воєнного стану є під значною загрозою.

Багато українських науковців розглядали проблеми нормативно-правової бази забезпечення кібербезпеки в України, зокрема Сеник В., Рудий Т., Живко З., Родченко С. та інші. На їх думку нормативно-правова база України не охоплює всіх сучасних загроз інформаційній безпеці держави та має бути доповненою [5, с. 24].

Розуміючи те, що війна у кіберпросторі шкодить не менше за бойові дії на полі бою, Верховна Рада України протягом перших двох місяців війни одноголосно прийняла зміни у Кримінальний кодекс України та у Кримінальний процесуальний кодекс України, прийнявши два закони:

1. «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24.03.2022 року;

2. «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137-IX від 15.03.2022 року [6, с. 38-39].

Але це нормативно-правове забезпечення регламентує лише оборонні заходи, посилює відповідальність за кіберзлочини. Українські ІТ-фахівці мають високу кваліфікацію і здатні не лише здійснювати захист інформації, але і можуть здійснювати ефективні кібератаки. Зараз, під час війни, активно діє громадський рух «КіберАрмія», учасники якого завдають збитків ворогу шляхом атак у кіберпросторі [1]. Але, незважаючи на те, що вони діють в інтересах України, їх дії формально містять склад злочинів статей 361, 361^1, 361^2 та 363^1 Кримінального кодексу України [7]. Тому є нагальна необхідність нормативно-правового регламентування активних атакуючих дій у кіберпросторі, які здійснюються в інтересах України.

Список використаних джерел:

1. Microsoft зірвала спробу російської кібератаки проти України. LIGA.Tech від 08.04.2022 р. URL: https://tech.liga.net/ua/other/novosti/microsoft-sorvala-popytku-rossiyskoy-kiberataki-protiv-ukrainy.
2. Єрема М. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX від 13.04.2022 р. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.
3. Pearson J. Russia downed satellite internet in Ukraine – Western officials. Reuters, May 11, 2022. URL: https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10/
4. Увага: остерігайтесь спам-розсилки листів, що містять віруси. Повідомлення Міністерства оборони України від 21.10.2022 р. URL: https://t.me/ministry_of_defense_ua/2451.
5. Живко З. Б., Рудий Т. В., Сеник В. В., Родченко С. С. Проблеми нормативно-правової бази забезпечення кібербезпеки в Україні: стан і перспективи. *Соціально-правові студії.* 2020. Вип. 3 (9). С. 18-25. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/3234.
6. Мальцева І. Р., Черниш Ю. О., Штонда Р. М. Аналіз деяких кіберзагроз в умовах війни. *Кібербезпека: освіта, наука, техніка.* 2022. № 4 (16). С. 37-44. URL: https://csecurity.kubg.edu.ua›article›download.
7. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

Калугін В. Ю.,
професор кафедри кібербезпеки
та інформаційного забезпечення
Одеського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ОСНОВНІ ЗАВДАННЯ ТАКТИЧНОГО КРИМІНАЛЬНОГО АНАЛІЗУ

Одним із напрямків використання аналітичної інформації в протидії злочинності є моніторинг ситуації стосовно можливих тактичних рішень щодо розміщення ресурсів у визначених проміжках часу.

З цією метою аналітичними підрозділами НП України проводиться тактичний кримінальний аналіз який являє собою когнітивний/пізнавальний і технічний процес, метою якого є оцінка характеру злочину, виявлення ризиків, тенденцій та моделей злочинності, встановлення пов'язаних фактів, інцидентів або місць імовірного скоєння злочинів. Ця форма аналізу має короткострокову та середньострокову перспективу [1, с. 170].

Тактичний аналіз являє собою метод аналізу даних з центром навколо короткострокових і середньострокових проблем, що покликаний виявити закономірності, особливості та специфічні елементи в серії злочинів. З його допомогою проводиться ідентифікація підозрілих осіб та групи, визначення зв'язків між декількома фактами (чинниками), сфери чи ділянки території з високим потенціалом кримінальної активності, типи людей, схильних стати жертвами злочинів, та сприятливі проміжки часу для злочинних проявів.

Тактичний кримінальний аналіз дозволяє підключати інтуїцію – здатність відчувати і розуміти – для пошуку альтернативних рішень, під контролем свідомості. По цій причині з'ясовується важливість методу візуалізації: свідомості простіше фокусуватися і контролювати хід аналізу [2, с. 19].

Тактичний кримінальний аналіз передбачає вирішення наступних основних завдань:

– провести аудит правопорушень [3, с. 34], встановивши місця, час концентрації злочинів, що вчиняються на конкретному адміністративно-територіальному регіоні, тобто;

– визначити види найбільш розповсюджених злочинів. На підставі результатів проведеного аналітичного дослідження надати рекомендації щодо розміщення правоохоронних сил та засобів з метою запобігання злочинній діяльності та своєчасного (найкоротші терміни) реагування;

– проведення моніторингу вивчення профілю злочинця та потерпілого, з метою встановлення передумов та визначення напрямів дій щодо запобігання злочинам та контролю за станом оперативної обстановки;

– провести аналіз зв’язків між різними правопорушеннями та можливими їх виконавцями, виокремити можливі зв’язки між серією злочинів, які мають загальні характеристики та у яких підозрювані особи використовують аналогічні способи вчинення кримінальних правопорушень;

– надання керівникам структурних підрозділів картину постійних чи виникаючих шаблонів злочинів в рамках їх юрисдикції: динаміка злочину; часовий аналіз; просторовий аналіз, географічний аналіз, аналіз місць концентрації злочинів; спосіб вчинення злочину; профіль жертви та підозрюваного; генеруючі чи фактори які впливають на розвиток подій (економічні, соціальні, демографічні);

– визначити проблеми, з якими стикається поліцейський підрозділ, та передбачити можливість використання аналітичної інформації в управлінській діяльності;

– висвітлити можливості запобігання та зниження рівня злочинності. виявлення та зниження сприятливих умов та покарання за правопорушення.

– виявлення нових тенденцій зростання чи зменшення кримінальних подій, зареєстрованих на певних територіях;

– оцінити результати, отриманих внаслідок вжитих заходів.

Слід зазначити , що фундаментальною базою яка використовуються в тактичному аналізі, є бази даних Національної поліції, статистичні данні, матеріали кримінальних проваджень та оперативно-розшукових справ.

Зміст тактичного кримінального аналізу повинен базуватися на документально підтвердженій інформації, якість якої безпосередньо залежить від точності та кількості отриманих даних

Слід зробити висновок, що результати тактичного аналізу є потужним інструментом у протидії кримінальним правопорушенням.

Список використаних джерел:

1. Федчак І. А. Основи кримінального аналізу: навч. посібник. Львів: ЛьвДУВС, 2021. 288 с.
2. Некрасов В. А. Сучасне розуміння кримінальної розвідки як напряму діяльності правоохоронних органів. *Кримінальна розвідка: методологія, законодавство, зарубіжний досвід*: Міжнар. наук.-практ. конф. Одеса: ОДУВС, 2016. С. 19-20.
3. Бабенко А. М, Користіна О. Є. Основи кримінального аналізу: підручник. Одеса, 2019. 296 с.

Ковний Ю. Є.,
адвокат,
кандидат економічних наук

ІНФОРМАЦІЙНА БЕЗПЕКА В КОНТЕКСТІ ЕТНОНАЦІОНАЛЬНОЇ ПОЛІТИКИ

В межах державно-правової комунікації можуть проявлятися групи з різною етнічною ідентичністю, що безумовно стосується політичної сфери суспільства, впливає на правову політику. Зокрема на національному рівні потребують вирішення принаймні такі питання як адміністративно-територіальний устрій, статус національних меншин, запобігання дискримінаційним проявам, мовна політика, релігійна толерантність у праві тощо. Все це потребує належного механізму забезпечення у тому числі інформаційної сфери.

Інформаційна безпека є критично важливим аспектом і відіграє значну роль у захисті державного життя, органи публічної влади зобов'язані захищати свою інформацію та активи, щоб підтримувати свою цінність і репутацію.

Щодо етнонаціональної політики така проблема має особливе значення, оскільки належний інформаційний простір створює мирний аспект комунікації між національними меншинами, корінними народами, окремими етносами. В той же час розпалювання етнічної ворожнечі провокує соціальний супротив, в широкому розумінні стає загрозою територіальної цілісності держави.

Збереження належності, конфіденційності, цілісності та доступності інформації, протидія атакам і загрозам є проблемою в цю цифрову епоху. Державні інституції в усьому світі роблять величезні інвестиції в технологічні засоби протидії інформаційній безпеці. Тим не менш, держава в багатьох випадках не можуть захистити свої інформаційні активи, оскільки вони покладаються в основному на технічні рішення, які контекстуально недостатньо сумісні.

Однак простого зосередження на технічних аспектах інформаційної безпеки недостатньо, оскільки інформаційна безпека є мультидисциплінарною за своєю природою, і людський аспект відіграє в ній головну роль. Значна кількість інцидентів організаційної інформаційної безпеки пов'язана з використанням людських елементів [1].

Насправді значна кількість інцидентів організаційної інформаційної безпеки пов'язана з використанням людських елементів, які прямо та/або опосередковано викликають більшість інцидентів безпеки. Людський фактор щодо помилковості, викривлення та неналежності інформації, безумовно може мати контекст казусу, проте під час військових дій та загрози територіальної цілісності такі дії зазвичай мають умисний характер.

За останні роки кількість кіберзлочинів і витоків даних різко зросла. Відповідно до звіту Cybersecurity Business Report, очікується, що кіберзлочин коштуватиме «понад 6 трильйонів доларів до 2022 року, порівняно з 3 трильйонами доларів у 2015 році» [2].

На державному рівні комплекс інформаційних гарантій має включати не тільки загальну систему протидії інформаційним атакам, але й передбачати можливі етнічні, мовні, національні конфлікти як породження суттєвого суцільного обурення, що в умовах війни підриває та розхитує громадянське суспільство.

Ідеальна або сильна культура інформаційної безпеки може характеризуватися виключно комплексним підходом, у тому числі шляхом визначення факторів, необхідних для впровадження ідеальної культури інформаційної безпеки [3].

Необхідно репрезентувати управління інформаційною безпекою як комплексне рішення, розробку цілісної основи для управління інформаційною безпекою, яка (1) поєднує цілі держави та етнонаціональних суб'єктів та їх захист, (2) розглядає кожен аспект стратегії, контролю та регулювання, (3) забезпечує відповідність процедур і настанов з політичною стратегією розвитку суспільства та держави та (4) забезпечує постійну оцінку та відповідність.

Список використаних джерел:

1. Stahl B. C., Doherty N. F., Shaw M. Information security policies in the UK healthcare sector: a critical evaluation *Infor. Syst. Jour*., 2012. Vol. 22 (1). Pp. 77-94.
2. Morgan S. Cybersecurity business report. 2016. URL: https://www.csoonline.com/article/3110467/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html.
3. Veiga A., Astakhova L., Botha A. Herselman M. Defining organisational information security culture. Perspectives from academia and industry. *Computers & Security*. 2020. Vol. 92.

Коростельова Л. А.,
інспектор відділу супроводження програм інформатизації та роботи із відкритими даними УІАП ГУНП у Луганській області

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У РОБОТІ КРИМІНАЛЬНОГО АНАЛІТИКА

Розвиток технологій і сучасна трансформація суспільства. Обумовлює перегляд принципів роботи у правоохоронних органів, зокрема в умовах війни.

У межах наданих повноважень підрозділи кримінального аналізу здобувають достатній масив інформації про злочинну діяльність, зокрема про представників організованої злочинності, а наразі і інформацію про військові злочини, скоєними російськими солдатами.

У зв'язку із зазначеним, надважливим завданням є застосування інструментів заснованих на технології штучного інструменту, які надали б можливість аналізувати значні обсяги наявних даних та покращували роботу із ідентифікації окупантів.

Загалом, воєнні конфлікти та війни двох перших декад XXI ст. мають свої особливості. Обумовлені вони поступовим скороченням кількості особового складу і тим, що на озброєння армій провідних країн світу взято сучасні системи розвідки, передачі даних, управління та ураження, як матеріальна основа збройної боротьби. І головним знаряддям в них поступово стають бойові системи зі «штучним інтелектом», а також інновації у зборі даних [1].

Наразі перспективним напрямом роботи кримінального аналітика є використання технологій штучного інтелекту у контексті розпізнання обличчя та подальша ідентифікація їх у соціальних мережах, робота із аудіофайлами щодо встановлення аудіодипфейків, OSINT-розвідка.

Наразі, поєднання зібраної у ході OSINT-розвідки та візуалізації даних у поєднанні із ШІ є сучасним підходом розслідування таких кримінальних правопорушень.

Сучасним прикладом є можливе використання мультимодальних моделей на основі машинного навчання *(Deep Multimodal Models*) у кримінальному аналізу щодо вивчення сайтів російської федерації на знаходження і зв'язуванні інформації.

Метою *Deep Multimodal Models* є використання і створення моделей, які можуть обробляти і зв'язувати інформацію із різними модальностями [2].

У кримінальному аналізу зазначена технологія вже була запропонована у використання щодо торгівлі людьми, де може доповнювати не автоматизовану роботу кримінального аналітика у роботі із ескорт сайтами. Основною метою підходу, є обробка та комп'ютерне бачення щодо виявлення та повідомлення про рекламу торгівлі людьми. Набір даних містить два джерела інформації для вивчення кожного оголошення: текст і зображення. Отже варто зазначити, Deep Multimodal Models дозволяє знаходити жертву та злочинця торгівлі людьми, які знаходяться серед великої кількості онлайн сайтів. Нейронне моделювання зазначених 98 моделей вивчає модальність мови і бачення понад 10000 рекламних оголошень із ймовірними ознаками торгівлі людьми [3].

Отже, підсумовуючи вище зазначене необхідно сказати, що саме розвиток AI в підрозділах кримінального аналізу є напрямом швидкого і якісного реагування на злочинність, зокрема в умовах війни.

Список використаних джерел:

1. Штучний інтелект на полі бою російсько-української війни. URL: https://www.ukrinform.ua/rubric-ato/3444808-stucnij-intelekt-na-poli-bou-rosijskoukrainskoi-vijni.html.
2. Summaira J., Li X., Shoib A. M., Li S., Abdul J. Recent Advances and Trends in Multimodal Deep Learning: A Review. Computer Vision and Pattern Recognition. 2021. URL: https://arxiv.org/abs/2105.11087.
3. Коростельова Л. А. Сучасні можливості використання в кримінальному аналізі Deep Multimodal Models у межах протидії торгівлі людьми. Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України: матер. міжвідом. наук.-практ. конф. (м. Київ, 11 серпня 2022 р.). К. : НАВС, 2022. С. 96-98.

Косиченко О. О.,
доцент кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ОСНОВНІ ПРОБЛЕМИ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ХМАРНИХ ПОСЛУГ ПІДПРИЄМСТВАМИ

Популярність хмарних послуг останніми роками стрімко зростає. Перспективи економії на капітальних та операційних витратах, а також масштабованість та еластичність спонукали компанії переходити на хмарні послуги. Однак перехід на хмарні технології пов'язаний із великою кількістю проблем. Одна з них – безпека, величезна проблема для організацій, які хочуть перейти на хмарні технології.

Дані організації – один із самих коштовних активів. Тому їх безпека відіграє важливу роль для багатьох організацій при переході на хмарні технології. Постачальники хмарних послуг (CSP – cloud service providers) тримають у секреті точне місце розташування своїх центрів обробки даних. Хоча це й передова практика в області фізичної безпеки, багато організацій – потенційні клієнти бояться не знати місцезнаходження зберігання своїх даних і відмовляються від хмарних сервісів.

Інформаційний суверенітет також відіграє велику роль у питанні переходу на хмарні технології. Організації не хочуть втрачати доступу до своїх даних через юридичні складнощі. Дотримання нормативних вимог відповідно Європейського загального регламенту захисту персональних даних (GDPR) – одна з ключових проблем для компаній. Порушення GDPR та інших нормативних актів спричиняє великі фінансові штрафи, чого більшість організацій хочуть уникнути. З цієї причини багато організацій вважають за краще зберігати конфіденційні дані (персональну інформацію тощо) локально.

Вирішальне значення для організації, яка використовує хмарне сховище, грають системи запобігання втрати даних (DLP – Data Leak Prevention). Випадкове видалення даних може статися з боку самої організації. У угоді про рівень послуг (SLA – Service Level Agreement) може бути обговорено про сприяння відновленню систем та інформації з боку CSP. Якщо CSP не зможе виконати SLA, клієнт зазнає великих збитків. Тому організації хочуть бути впевненими у безпеці своїх резервних копій, адже у разі втрати чи пошкодження даних їм потрібно, щоб дані були відновлені в рамках цільового часу відновлення (RTO – Recovery time objective) та цільових точок відновлення (RPO – Recovery Point Objective).

Багато компаній для вирішення своїх завдань використовують програмне забезпечення та послуги від різних постачальників. У зв'язку з цим подібні

організації при переході в хмару іноді змушені прийняти багатохмарну модель. За даними дослідження, проведеного компанією Tripwire у 2021 році, 98% фахівців з безпеки, що працюють у сфері багатохмарних середовищ, вважають таку модель більш ризикованою з точки зору безпеки. Респонденти того ж опитування зазначили, що важко знайти фахівців з безпеки, які є експертами у всіх хмарних середовищах, що використовуються різними CSP.

Підвищені ризики мультихмарної моделі змушують організації відмовлятися від деяких переваг кількох хмарних послуг на користь одного CSP. Вибір одного CSP замість іншого – не завжди просте рішення. Деякі постачальники послуг хмари можуть ускладнити перехід організації до інших постачальників. Перед вибором CSP компанія має ретельно вивчити умови використання хмарних послуг конкретного CSP.

Відсутність належної обачності може сповільнити реагування служб безпеки на кібератаки. Більшість CSP працюють за моделлю спільної відповідальності, коли йдеться про забезпечення безпеки у хмарі, тому клієнтам хмарних сервісів дуже важливо розуміти свою роль і роль CSP у цій моделі. Кібератаки неминучі, тому компаніям необхідно мати плани реагування на різні інциденти та бути впевненими у методах захисту провайдерів.

При оцінці варіанта публічної хмари організація повинна розуміти, що в такій моделі для скорочення витрат використовується розрахована на багато користувачів ліцензія. Клієнти сервісів повинні бути впевнені в CSP та методах «глибокого захисту», адже відсутність багаторівневого захисту дозволить хакеру здійснювати серії кібератак після однієї успішної спроби.

Організації, які використовують критично важливі сервіси у хмарі, можуть серйозно постраждати від DoS та DDoS-атак, що паралізують бізнес-операції. Щоб мінімізувати ризик таких атак, компанії повинні прагнути усунення єдиних точок відмови при виділенні робочих навантажень.

Більшість завдань із забезпечення, керування та моніторингу робочих навантажень у хмарі виконуються через виклики способів взаємодії однієї комп’ютерної програми з іншими (API – Application Programming Interface, інтерфейс прикладного програмування). Тому важливість надійних API не можна недооцінювати, адже від них залежить безпека та доступність спільних хмарних сервісів. Відсутність грамотно налаштованої авторизації, контролю доступу та моніторингу API може призвести до різних порушень та руйнівних атак хакерів.

Можливість стихійного лиха, хоча і не відноситься до атак, все ж таки є подією, що порушує роботу хмарних сервісів. Якщо стихійне лихо зруйнує центри обробки даних CSP, це призведе до серйозних порушень у роботі підприємств, які використовують центри обробки даних, адже навіть, незважаючи на передові методи резервування, у разі стихійного лиха ризик втрати інформації досить високий.

Перехід у хмару – важливе, але ризиковане бізнес-рішення, що вимагає грамотної оцінки всіх «за» і «проти». Помилкове рішення здатне завдати непоправної шкоди організації, але при ретельному дотриманні заходів безпеки та оцінки ризиків можна зробити хмарні послуги чудовим інструментом для розвитку компанії.

Список використаних джерел:

1. Prinzlau M. 6 security risks of enterprises using cloud storage and file sharing apps. URL: https://digitalguardian.com/blog/6-security-risks-enterprises-using-cloud-storage-and-file-sharing-apps.
2. Semeney A. What are the Top Cloud Computing Security Issues for Businesses. URL: https://www.devteam.space/blog/author/alexey-semeney/
3. Dotson C. Practical Cloud Security. USA : O'Reilly Media Inc. 195 p.

Костенко О. В.,
завідувач науково-дослідної лабораторії теорії і права цифрових трансформацій науково-дослідного центру цифрових трансформацій і права Національної академії правових наук України, доктор філософії в галузі права
Прокопович-Ткаченко Д. І.,
в. о. завідувача кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів, кандидат технічних наук, доцент

УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНИМИ ДАНИМИ: ІДЕНТИФІКАЦІЯ IoT ЯК БАЗОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Одним із ключових елементів технологій та систем передачі даних є наявність інформації за якою можливо ідентифікувати суб'єктів та об'єктів за притаманні їм ідентифікаційні атрибути – ідентифікаційними даними.

Ідентифікаційними даними вважається інформація про конкретного суб'єкта в формі одного або декількох атрибутів, що дозволяють суб'єкту бути в достатній мірі відмінним в певному контексті або набір атрибутів особи, які дозволяють цій особі відрізнятися від інших осіб у конкретному контексті, а саме е-екосистемі IoT.

Разом із тим, управлінням ідентифікаційними даними в широкому сенсі прийнято вважати набір прийомів, що дозволяють управляти процесами ідентифікації, автентифікації і авторизації фізичних і юридичних осіб, пристроїв IoT в режимі он-лайн з метою отримання електронних сервісів та даних.

Сучасний IoT являє собою локальні об'єднання автономних мікро електромеханічних систем (MEMS), радіотехнологій передачі даних, програмних продуктів, електронних сервісів, Інтернету та галузевих або соціальних інформаційно-комунікаційних хабів (е-екосистем).

Структурно IoT умовно можна поділили на елементи за принципом мережевої моделі OSI (The Open Systems Interconnection model). До першого рівня моделі (media layers) відносяться фізичний, мережевий та рівень додатків, тобто, безпосередньо IoT пристрої, радіотранспортна мережа та мережеве обладнання, протоколи передачі даних та інтерфейси, модулі та алгоритми ідентифікації. До другого рівня (host layers) доцільно віднести модулі управління, аналітики та зберігання даних, Інтернет-комунікації, програмні платформи, хаби.

На рівні Media layers протоколами передачі даних пристроїв IoT вважаються HTTP, сенсор-сенсор (DDS), сенсор-сервер (CoAP, XMPP, MQTT, STOMP), сервер-сервер (AMQP).

Для передачі даних пристроїв IoT застосовують такі радіо технології, як LoRaWan, LTE-M, Sigfox, NB-IoT, NFC BLE, Wi-Fi, Z-Wave, ZigBee. Одні, такі як Zigbee, BLE, WiFi, мають малу дальність дії, інші, як 3G і LTE, мають проблеми енергоспоживання і нестабільний радіус або сектор радіопокриття.

До відомих платформ IoT відносяться: Amazon Web Services, Microsoft Azure, ThingWorx IoT Platform, IBM's Watson, Cisco IoT Cloud Connect, Salesforce IoT Cloud, Oracle Integrated Cloud, GE Predix.

Ідентифікатори стандарту IoT сьогодні прийнято розділяти на такі категорії: Ідентифікатори об'єктів, які використовуються для ідентифікації фізичних або віртуальних об'єктів (URIs, URL); Ідентифікатори зв'язку, які застосовуються для унікальної ідентифікації пристроїв у межах комунікації з іншими пристроями, включаючи Інтернет-зв'язок (IPv4, IPv6, E.164); Ідентифікатори додатків, які визначають унікальні програми, що використовуються в межах IoT додатків (EPC, UPC, Handle/DOI, UUID, MAC, URI, URL, Ecode, OID, CID).

Нині в світі існують різні універсальні ідентифікаційні системи, такі як Object IDentifier (OID), електронний код продукту (EPC), універсально унікальний ідентифікатор IDentifier (UUID) і міжнародний ідентифікатор мобільного обладнання Identity (IMEI) тощо.

Сучасне IoT середовище неоднорідне і в механізмах ідентифікації. Це наслідки не стільки значної кількістю пристроїв, скільки різноманітності унікальних схем ідентифікації (ISS) або оригінальних методів ідентифікації різних виробників, що стає бар'єром обміну даними між неспорідненими хабами, додатками або платформами. Найбільш поширеними схемами ідентифікації є OID, EPC та UUID.

OID – широко використовуваний механізм ідентифікації, спільно розроблений ITU-T (Міжнародний сектор телекомунікаційної стандартизації телекомунікацій) і ISO/IEC (Міжнародна організація зі стандартизації/ Міжнародної електротехнічної комісії), призначений для встановлення унікального та стійкого в часі реквізиту об'єкта або пристрою, за яким буде здійснюватися його ідентифікація.

EPC – універсальний ідентифікатор будь-якого фізичного об’єкту, унікальний серед усіх існуючих об’єктів. Ідентифікатор EPC дозволяє контролювати розташування об’єктів в інформаційних системах, що входять до мережі EPCglobal.

UUID – це 128-розрядне число, яке використовується для унікальної ідентифікації сутності або об’єкта в просторі та часі або стандарт ідентифікації, який використовується при створенні програмного забезпечення, затверджений Open Software Foundation (OSF), як частина розподіленого комп’ютерного середовища (DCE).

Різноманітність підходів ідентифікації торкнулась і технічних стандартів, рішень безпеки та платформ сумісності IoT, які розроблюють багато організацій і галузевих груп. Існує декілька популярних стандартів і платформ для надання послуг IoT таких як «oneM2M», «GS1», «OCF» та «FIWARE».

Так, в 2012 році проект oneM2M заснували вісім провідних світових організацій інформаційно-комунікаційних технологій. Основною метою oneM2M є визначення комплексної платформи M2M для надання послуг з взаємодії в організації та між організаціями. Архітектура oneM2M походить від багаторівневого підходу, при якому кожен рівень відповідає за певний набір дій: рівень програм, загальний рівень послуг і мережевий рівень.

Проект GS1 створено в 1973 році Uniform Code Council, Inc. (UCC), відомий зараз як GS1 US. Метою проекту є розробка стандартів, таких як штрих-коди та RFID. Стандарти ідентифікації GS1 надають ключі ідентифікації GS1, які є унікальними ідентифікаторами для позначення реальних суб’єктів або об’єктів. Комбінована система стандартів GS1 відіграє невід’ємну роль у підключенні пристроїв на базі IoT. GS1 виконує вимогу ідентифікації об’єктів за допомогою ключів ідентифікації GS1.

Проект OCF – це галузева група, яка спрямована на впровадження рекомендацій щодо сумісності та стандартів специфікації для пристроїв IoT. OCF є однією з найбільших організацій промислової стандартизації IoT і має більш ніж 300 компаній-членів. За проектом створено набір специфікацій, референційне впровадження та сертифікація для пристроїв на базі IoT, з метою забезпечення сумісності та створення загальної моделі даних для взаємодії пристроїв IoT.

Проект FIWARE ініційований Європейською Комісією в рамках державно-приватного партнерства Future Internet і був започаткований 3 травня 2011 року спільно з основними партнерами з інформаційно-комунікаційних технологій та компаніями Європи. Основна мета FIWARE є надання майбутніх інтернет-послуг і додатків із використанням універсальних ідентифікаторів. FIWARE використовує специфікацію інтерфейсу служби Open Mobile Alliance Next Generation (OMA NGSI) для обміну інформацією та керування даними. Проект підтримується грантом Інституту інформаційно-комунікаційних технологій, що фінансується Корейським урядом.

Окремо слід звернути увагу на нові проекти альянсів – FIDO та AIOTI.

Альянс з інновацій Інтернет речей AIOTI (The Alliance for Internet of Things Innovation) створено у 2015 році з ініціативи Єврокомісії. Мета альянсу – розвиток та підтримка діалогу й взаємодії між різними країнами Європейського Союзу, які прогнозують прогрес IoT у власних економіках [12-13].

Проект FIDO Alliance (Fast IDentity Online) засновано у 2013 році компаніями Agnitio, Infineon Technologies, Lenovo, Nok Nok Labs, PayPal та Validity. Згодом до них приєдналися Google, Microsoft, Samsung, Yubico та NXP. Метою Альянсу є створення стандартизованого підходу до автентифікації в Інтернеті та випуску відповідних пристроїв, захисту користувачів Інтернету від фішингу, вирішенням проблем використання паролів, а також розвиток доступності та безпеки біометричних технологій.

FIDO розробляє стандарти WebAuthn и CTAP, які будуть основою для різноманітних методів безпарольної автентифікації: біометричної, голосової, 2D-, 3D-фото, одноразових паролів та USB-ключів. На практиці користувачу буде запропоновано два типи ключів FIDO: ID-ключ – унікальний ідентифікатор, підключений до облікового запису в Інтернеті (аналог – соціальні мережі) та карта автентифікації. Стандарти FIDO генерує нову унікальну пару ключів на кожну нову і окрему транзакцію або реєстрацію, при цьому всі ключі зберігаються в безпечному сховищі типу SecureEnclave, TPM або TEE. Крім того, у FIDO потрібна тільки підтримка базової криптографії, ключі та біометрична інформація зберігається на безпечних чіпах і ніколи з них не вилучається.

В Україні також здійснюються заходи в напрямі організації та розвитку процесів електронної ідентифікації, які спрямовані на виключно технічні способи ідентифікації. Так статтею 15 Закону України «Про електронні довірчі послуги» визначені схеми електронної ідентифікації.

Схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації, що використовуються в них. Схема електронної ідентифікації визначається Кабінетом Міністрів України.

Низький, середній та високий рівні довіри до засобів електронної ідентифікації повинні відповідати таким критеріям:

– низький рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує обмежений ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є зниження ризику зловживання або спростування ідентичності;

– середній рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує суттєвий ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на

технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є істотне зниження ризику зловживання або спростування ідентичності;

– високий рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує найвищий ступінь довіри до заявлених ідентифікаційних даних особи і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є запобігання зловживанню повноваженнями або підміні особи.

Постановою Кабінету Міністрів України від 19 червня 2019 № 546 «Про затвердження Положення про інтегровану систему електронної ідентифікації» визначено, що інтегрована система електронної ідентифікації це інформаційно-телекомунікаційна система, яка призначена для технологічного забезпечення зручної, доступної та безпечної електронної ідентифікації та автентифікації користувачів системи, сумісності та інтеграції схем електронної ідентифікації, їх взаємодії з офіційними веб-сайтами (веб-порталами), інформаційними системами органів державної влади, органів місцевого самоврядування, юридичних осіб і фізичних осіб-підприємців, забезпечення захисту інформації та персональних даних з використанням єдиних вимог, форматів, протоколів та класифікаторів, а також задоволення інших потреб, визначених актами законодавства.

Відповідно до постанови Кабінету Міністрів України від 19 червня 2019 року № 546 та згідно ЄААД.468244.209 Д7.01 «Загальний опис. Інтегрована система електронної ідентифікації» Міністерством цифрової трансформації України ведуться роботи по створенню інтегрованої системи електронної ідентифікації. Нині ця система надає тільки послуги перевірки цифрового підпису та підписання файлів цифровим підписом користувача без додаткових заходів ідентифікації підписантів і виступає в ролі транскодера між різноманітними системами ідентифікації, що створює низку суттєвих ризиків та правових невизначеностей і не сприяє зростанню довіри до державних цифрових сервісів, інформаційних ресурсів та технологій.

Крім того, наказом Державного агентства з питань електронного урядування від 27.11.2018 р. № 86 встановлено вимоги до засобів електронної ідентифікації (далі – Вимоги), рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування. Вимоги встановлюють організаційні, методологічні, технічні та технологічні умови використання засобів електронної ідентифікації у сфері електронного урядування залежно від рівнів довіри до засобів електронної ідентифікації. Ці Вимоги обов’язкові для виконання надавачами електронних довірчих послуг, підприємствами, установами та організаціями незалежно від форм власності, діяльність яких пов’язана з розробленням, виробництвом, сертифікаційними випробуваннями, експертними дослідженнями та експлуатацією засобів електронної ідентифікації, що видаються фізичним, юридичним особам або представникам юридичних осіб, та використовуються для автентифікації у сфері електронного урядування.

Наразі в Україні функціонують такі схеми ідентифікації, як «QsignID» (ідентифікатор – засоби кваліфікованого електронного підпису чи печатки), «BankID» (ідентифікатор – електронна анкета з ідентифікаційними даними користувача Системи BankID Національного банку України), «MobileID» (ідентифікатор – ідентифікаційна телекомунікаційна картка, в якій зберігається особистий ключ кваліфікованого електронного підпису), «PasscardID» (ідентифікатор – безконтактний електронний носій, в якому зберігається особистий ключ кваліфікованого електронного підпису та ідентифікаційні дані власника) та «Дія/Мій ID» (проект, ідентифікатор – електронна анкета з ідентифікаційними даними власника облікового запису у Національній системі електронної ідентифікації «Дія»).

Лізунов С. І.,
доцент кафедри захисту інформації
Національного університету
«Запорізька політехніка»,
кандидат технічних наук, доцент
Верещака М. П.,
аспірант кафедри радіотехніки
та телекомунікацій
Національного університету
«Запорізька політехніка»

ЗАСТОСУВАННЯ БРАНДМАУЕРІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Системи захисту інформації в комп’ютерних мережах полягають в умінні забезпечувати їх цілеспрямовану роботу, тобто вся інформація повинна бути прихованою і цілісною. В більшості випадків всі мережі офісів і компаній підключаються до всесвітньої павутини. Для захисту локальних мереж, використовують міжмережеві екрани, які називаються брандмауерами. Даний екран є засобом диференціального доступу. Це означає що мережа розосереджена на дві половини. Тобто є межа між інтернет-мережею і локальною мережею. Брандмауери бувають програмними та апаратними.

Для аналізу брандмауерів використовують утиліти з сайту, а саме Jumper, DNStester і CPIL Suite (розробка компанії Comodo). Ці утиліти використовують такі ж самі методи, що і шкідливі програми, роботу яких вони симулюють. Під час тестування всі засоби антивірусного захисту повинні бути деактивовані.

Розглянемо наступні утиліти:

– Jumper – дозволяє обійти брандмауер, використовуючи методи «DLL injection» і «thread injection». Програма дозволяє швидко змінити поточний

DNS-сервер, через який відбувається звернення до ресурсів інтернету, і пропонує для цього свій перелік відомих адрес, серед яких розташувалися Google, Yandex, Comodo, Norton та інші. При цьому утиліта залишає можливість вручну ввести значення будь-якої іншої адреси;

– DNS Tester – використовує рекурсивний DNS-запит, щоб обійти брандмауер. Після ініціалізації DNS Tester запитує дозвіл на спробу рекурсивного DNS-запиту. Щоб пройти тест, брандмауер повинен заблокувати цей запит і видати попередження;

– CPIL Suite – набір CPIL містить три окремі тести, спеціально розроблені інженерами Comodo для перевірки захисту брандмауера від атак витоку батьківських ін'єкцій. У кожному з трьох тестів користувач вводить довільний текст у текстове поле, яке CPIL намагатиметься передати на сервери Comodo.

Розглянемо ці тести більш детально:

– Тест 1: намагається вимкнути перехоплення брандмауера шляхом прямого доступу до фізичної пам'яті, а потім модифікує explorer.exe, щоб обійти брандмауер, запустивши iexplore.exe за допомогою командного рядка;

– Тест 2: спроба ін'єктувати cpil2.dll у explorer.exe за допомогою Windows Accessibility API, а потім намагається обійти брандмауер, запустивши iexplore.exe за допомогою командного рядка;

– Тест 3: спроба ін'єктувати cpil3.dll у explorer.exe за допомогою Windows Accessibility API, а потім намагається обійти брандмауер, запустивши iexplore.exe та змінивши iexplore.exe за допомогою зв'язку DDE.

Усі ці утиліти потрібно запускати безпосередньо з досліджуваних комп'ютерів, а з зовні потрібно сканувати мережу за допомогою програми nmap.

Апаратні брандмауери використовують для ефективного захисту кожного вузла мережі. До їх недоліків можна віднести те, що вони не можуть забезпечити захист кожної окремої робочої станції, безсилі при атаках всередині мережі, а також не можуть виконувати розмежування інформаційної системи персональних даних.

Програмні брандмауери використовують для захисту всієї мережі в цілому. Їх стандартні настройки не можуть забезпечити максимальний захист від усіх типів загроз, тому правильно налаштовані програмні брандмауери дають гарантовану безпеку роботи в мережі.

Захист інформаційної системи повинен бути комплексним та включати: програмні і апаратні брандмауери, антивіруси і правильні налаштування операційної системи.

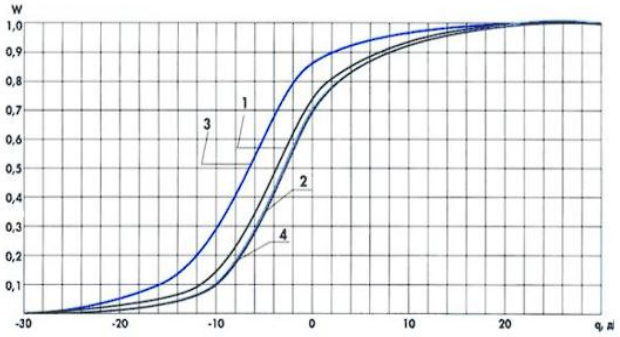
Лізунов С. І.,
доцент кафедри захисту інформації
Національного університету
«Запорізька політехніка»,
кандидат технічних наук, доцент
Філобок Є. В.,
аспірант
Національного університету
«Запорізька політехніка»

АНАЛІЗ ВАРІАНТІВ РОЗРАХУНКУ РОЗБІРЛИВОСТІ МОВИ У СФЕРІ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Проведення заходів, щодо забезпечення безпеки мовної інформації на режимних об'єктах, підпорядковує у собі аналіз розповсюдження акустичних сигналів поза межами контрольованої зони. Задля забезпечення безпеки мовної інформації використовують пасивні (послаблення сигналу) і активні (створення маскуючих шумів) методи захисту. Показником оцінювання ефективності захищеності та об'єктом аналізу є розбірливість мови (РМ), за IEC 60268-16:2020 – це процентне значення, того наскільки точно люди розуміють промовлене повідомлення. Метою методів акустичної безпеки є мінімізація значення РМ в усіх можливих місцях витоку мовної інформації.

Умовно поділяють два класи вимірювання і розрахунку розбірливості мови: об'єктивні і суб'єктивні – пара яких, у свою чергу, налічує декілька десятків різних методів [1].

Під об'єктивними (інструментально-розрахунковими) розуміють, ті методи, при яких здійснюються інструментальні виміри параметрів мовних сигналів. Це основний метод в оцінці ефективності шумових завад. Один з популярних об'єктивних методів – це метод співвідношення рівнів мовного сигналу до шуму. Він полягає у тому, що існує залежність – задля забезпечення зменшення РМ, потрібно зменшити рівень сигнал/шуму, у вразливих місцях виділеного приміщення. Це досягається використанням пасивних і активних методів захисту акустичної інформації. Після аналізу, простежується, що рожевий шум є найбільш ефективним шумом. Можливо досягти РМ у 40 % при перевищенні рівня завад на 4.9…5.0 дБ, для приховування змісту розмови, що ведеться, та значення РМ у 20% при перевищенні – на 8.8…9.0 дБ, для приховування тематики розмови (рис. 1) [1].



1 – «білий» шум;

2 – «рожевий» шум;

3 – шум зі спадом спектральної щільності 6 дБ на октаву у бік високих частот;

4 – «мовоподібна» завада

Рис. 1. Залежність словесної розбірливості W від відношення сигнал/шум q у смузі частот 180…5600 Гц

До суб'єктивних методів оцінки РМ відносять – артикуляційні випробування, методика яких заснована на експертних оцінках. Створюються спеціально натреновані групи, вони проводять вимірювання РМ. При досить великій кількості вимірів, тобто коли відсоток розбірливості розраховується з урахуванням великої кількості прийнятих складів (слів), вплив різних чинників і суб'єктивних особливостей окремих операторів осереднюється, і артикуляційні виміри дають стабільні, об'єктивні результати. Вони передбачають оцінку ефективності «мовоподібних» завад або тих, що сформовані з реверберацій, чи сигналу, який приховується. Метод потребує великих витрат, починаючи від тривалого часу задля проведення випробувань, формуванням артикуляційної групи чи створення нових артикуляційних таблиць. Нажаль розробці артикуляційних таблиць української мови приділяють не так багато уваги, але дослідження в цієї галузі продовжуються. Так у [2] було проведено артикуляційне випробування, з використанням власно зроблених таблиць. Одним із результатів якого було узгодження отриманих результатів РМ з інструментально-розрахунковими методами – «рожевий» шум є ефективнішим, задля зменшення розбірливості (рис. 2).

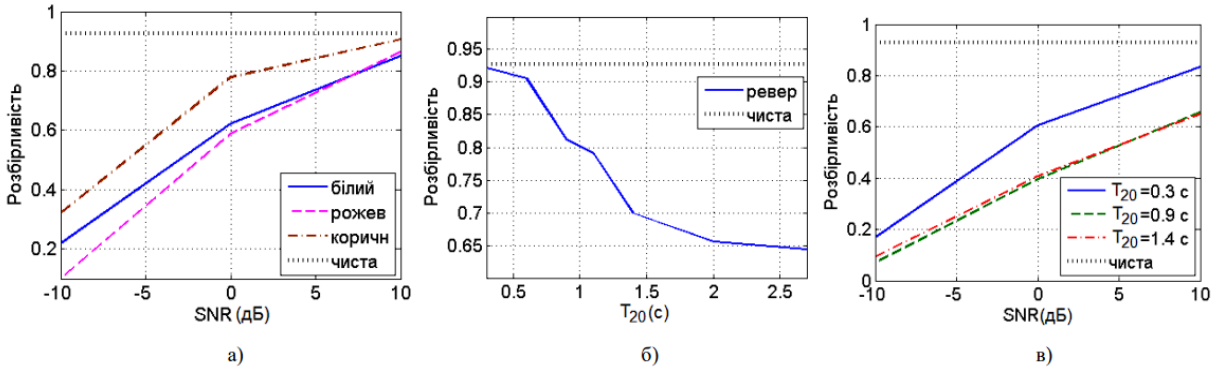


Рис. 2. Оцінки розбірливості при слуханні через навушники: шум (а), реверберація (б), рожевий шум+реверберація (в)

Кожен з двох методів має свої недоліки та переваги.

Об'єктивні – мають високу оперативність, варіативність параметрів у вимірюваннях звукового сигналу (спотворення, реверберації, тощо), але завдяки цьому обмежуються лише унітарними, а не комплексними сферами застосування.

У суб'єктивних – висока ресурсна витратність, трудомісткість, але метод надає точну кількісну оцінку розбірливості мови, яка може бути як розрахована, так і виміряна. Результати артикулярних методів також використовуються у об'єктивних методах, задля отримання стабільних значень.

Список використаних джерел:

1. Prodeus A. M., Vityk A. V., Didenko D. Y. Суб'єктивне оцінювання якості та розбірливості мовних сигналів, спотворених синтезованими шумами. *Мікросистеми, Електроніка та Акустика*. Вип. 6 (22), с. 56-63.
2. Продеус А., Вітик А., Дворник О., Котвицький І., Чайка О., Ярошенко М. Суб'єктивне оцінювання розбірливості мови на тлі шуму та реверберації. *Мікросистеми, електроніка та акустика*. 2018. № 2 (23), с. 66-73.

Лунгол О. М.,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ, кандидат педагогічних наук
Габорець О. А.,
доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки Донецького державного університету внутрішніх справ, доктор філософії

ЦИФРОВА ДАКТИЛОСКОПІЯ

Захист індивідуальних даних в Інтернеті – актуальна потреба сьогодення. Зважаючи на швидкий розвиток та розповсюдження шкідливого програмного забезпечення в мережі, сучасні загрози інформаційної безпеки, як фішинг, соціальна інженерія та ін., важливим питанням залишається анонімність користувача в мережі Інтернет.

Технологія ідентифікації користувача Інтернету Fingerprinting дозволяє за непрямими ознаками, що пов'язані як з hardware, так і з програмним забезпеченням software, отримати значний об'єм інформації про браузер та комп'ютер користувача, що становить його індивідуальність. Суть технології полягає в тому, що Web-серверу браузер користувача надає певну інформацію

в процесі запиту адреси сайту. А саме: роздільну здатність дисплею; вид операційної системи, яка встановлена на комп'ютер; місцезнаходження пристрою; мовні параметри інтерфейсу тощо. За допомогою скриптів Fingerprinting, як от FingerprintJS, можливо отримати додаткову інформацію про браузер та властивості комп'ютера. В результаті обробки цієї сукупності даних засобами технології Fingerprinting отримується Hash-сума у вигляді унікального 32-бітового числа, наприклад, 11348f1d2a96620ef122b6e54946224a. Цю Hash-суму ще називають Fingerprint користувача або цифровим відбитком комп'ютера чи цифровим відбитком браузера. Проаналізувати дану інформацію можна за допомогою цифрової дактилоскопії.

Щоб перевірити цифровий відбиток власного браузера та комп'ютера, можна скористатися послугами сайту AmIUnique. Цей веб-сайт створено та підтримується командою дослідників, які вивчають програмне забезпечення та досліджують різноманіття цифрових відбитків браузера. Результати дослідження розробники вбачають у можливості автоматичного переналаштування платформи користувача, щоб реалістично «розмивати» цифровий відбиток браузера. Ступінь реалістичності важливий, щоб забезпечити анонімність користувача в Інтернеті. З цифровими відбитками комп'ютерів пов'язана також робота сайтів: Fake Vision, 2IP.ua, CoverYourTracks та ін. Ці сайти збирають інформацію про браузер та комп'ютер через дані HTTP-заголовків. HTTP – це протокол, який використовується комп'ютерами для запиту та надсилання даних через Інтернет. HTTP-заголовки (Message Headers) – це спеціальні параметри, які містять службову інформацію про з'єднання HTTP. Деякі заголовки мають лише інформаційний характер для користувача чи комп'ютера, інші передають певні команди, з яких, сервер чи клієнт буде виконувати певні дії. Іншими словами, це рядки, які браузер користувача надсилає на сервер при відкритті певного сайту. Спеціальна програма на сервері обробляє ці рядки для подальшого правильного відображення сайту саме для браузера користувача. До надісланих даних входить: тип та версія браузера, налаштування параметрів конфіденційності, встановлена мова, вид операційної системи, відомості про типи текстових файлів, що підтримує система, інформація про налаштування щодо файлів Cookie, часовий пояс, наявність блокувальників реклами, роздільна здатність екрану, часовий пояс, відео та аудіо формати та ін. Цю інформацію про себе користувач може переглянути та проаналізувати на сайтах: Fake Vision, 2IP.ua, CoverYourTracks, AmIUnique тощо.

Деякі комп'ютерні експерти в галузі IT безпеки розглядають цифрові відбитки браузерів, як уразливість браузера та порушення конфіденційності користувача. Використання на одному комп'ютері декількох браузерів призводить до можливості існування певної кількості цифрових відбитків у одного користувача. З метою ідентифікації особи за цифровими відбитками декількох браузерів розвивається нова технологія – Cross-Browser Fingerprinting, яка є тематикою наших подальших досліджень та публікацій.

Пиріг І. В.,
професор кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, професор

ВИКОРИСТАННЯ КРИМІНАЛІСТИЧНИХ ОБЛІКІВ МВС УКРАЇНИ В ЗАЛЕЖНОСТІ ВІД ТИПОВИХ СЛІДЧИХ СИТУАЦІЙ

Криміналістичні обліки використовуються в діяльності з розслідування кримінальних правопорушень в залежності від поставлених завдань, етапів розслідування та слідчої ситуації на кожному з етапів. На думку М. Салтевського, слідча ситуація є сукупністю актуалізованої суб'єктами кримінального процесу доказової інформації, що відображена у матеріальній обстановці події злочину [1, с. 302].

Процес розслідування в криміналістиці прийнято ділити на три етапи: початковий, подальший і заключний. Переважна більшість вчених-криміналістів приділяють увагу початковому етапу розслідування, оскільки відомості, отримані на цьому етапі, значною мірою визначають дії на подальшому етапі та успіх усього розслідування в цілому [2, с. 164].

Розглянемо типові слідчі ситуації розслідування та можливість використання при цьому інформаційних баз даних. Однією з несприятливих ситуацій розслідування є така, при якій є ознаки злочину, особа злочинця невідома але є матеріальні сліди, ним залишені; відсутні свідки та очевидці. У такій ситуації для встановлення особи злочинця використовуються криміналістичні обліки в залежності від виду слідів, залишених злочинцем. Першочергове значення при цьому має дактилоскопічний облік, що реалізується у формі АІПС «Дакто-2000». Перевірка слідів, вилучених на місці події дає позитивні результати, якщо особа раніше була затримана та її дактилокарта є у базі даних. Перспективним напрямком використання дактилоскопічного обліку є підвищення мобільності систем вводу інформації та, відповідно, швидкості її перевірки. Це можливо досягти шляхом створення пересувних комплексів вводу слідів рук з використанням «живого» сканування безпосередньо на місці їх вилучення, об'єднаних з системою «Дакто-2000», що починала б перевірку відразу після вчинення кримінального правопорушення. Впровадження такої системи могла б приносити позитивні результати у ситуації затримання підозрюваного на місці події, його дактилоскопіюванні та перевірці по базі даних. Подібного роду діяльність могли б виконувати інспектори-криміналісти або, навіть слідчі поліції. Досвід створення таких пересувних дактилоскопічних систем показав позитивні результати у США та країнах Європи. В окремих штатах США дактилоскопічні сканери встановлено у машинах патрульної поліції. Поряд з дактилоскопічними у цій ситуації можуть бути використані обліки слідів взуття, транспортних засобів, знарядь зламу, профілів ДНК.

Інша ситуація, коли є ознаки злочину, є свідки та очевидці, які запам'ятали злочинця та можуть його описати або є його відеозображення, зафіксоване відеокамерою спостереження. У цьому випадку з початку потрібно скласти суб'єктивний портрет злочинця зі слів свідків-очевидців. Серед сучасних систем програмного забезпечення можна відмітити програмний комплекс «Фоторобот» розроблений для автоматизації процесу створення суб'єктивних портретів шляхом компонування на екрані дисплея графічних образів з бази готових елементів обличчя, що пропонується компанією «Експертні системи» (м. Київ). Складений композиційний портрет перевіряється з використанням автоматизованої система портретної ідентифікації «Портрет». Система призначена для централізованого обліку та розшуку осіб і суб'єктивних портретів. Ця ж система дозволяє введення і завантаження зображень, отриманих з відеокамер спостереження, сканерів та графічних файлів. Незважаючи на простоту у використанні та відносно невелику вартість обладнання цієї ідентифікаційної системи, вона поки що не знайшла свого застосування на центральному рівні. Окремі обласні НДЕКЦ її використовують, але база зображень злочинців є незначною, а звідси й ідентифікаційні можливості встановлення правопорушника за його зображенням зменшуються.

Більш сприятливою для розслідування є слідча ситуація, коли особу підозрюваного встановлено, але його не затримано та місцезнаходження невідомо. У цьому випадку потрібне комплексне використання інформації криміналістичних обліків НДЕКЦ та інших підрозділів МВС, зокрема ДІАП на центральному та їх управлінь (відділів) поліції на обласному рівнях. Також для перевірки особи можуть використовуватись інформаційні бази інших відомств, зокрема: Державної міграційної служби, Прокуратури України, СБУ, НАБУ та ін., а в окремих ситуаціях Інтерполу та Європолу. Поряд з цим можливо використання баз даних підприємств та організацій банківської системи, медичних установ, транспортних підприємств тощо. Перевірка особи правопорушника за означеними базами є завданням органів досудового розслідування поліції, але отриману при цьому інформацію потрібно використовувати в комплексі з даними обліків інших відомств.

Список використаних джерел:

1. Салтевський М. В. Криміналістика (у сучасному вигляді): підручник. К. : Кондор, 2005. 588 с.
2. Пиріг І. В. Поняття та характеристика етапів розслідування в криміналістиці. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. Спец. вип. № 2 (115). С. 163-168.

Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ТРЕНІНГИ ІНФОРМАЦІЙНОГО СПРЯМУВАННЯ ДЛЯ ПІДГОТОВКИ КУРСАНТІВ ДНІПРОПЕТРОВСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ

Процес навчання курсантів у навчальних закладах системи Міністерства внутрішніх справ призначений для підготовки та якнайкращого адаптування майбутніх правоохоронців до діяльності підрозділів Національної поліції. Важливу роль у підготовці поліцейських відіграє отримання ними навичок уміння знаходити необхідну інформацію в процесі виконання службових обов'язків, аналізувати та систематизувати отримані інформаційні потоки, а у подальшому, вміти презентувати та правильно відображати цю інформацію у службовій документації.

У навчальних закладах системи Міністерства внутрішніх справ в рамках інформаційної підготовки майбутніх поліцейських викладаються дві дисципліни: це «Інформаційні та комунікаційні технології» та «Інформаційне забезпечення професійної діяльності». Під час вивчення першої дисципліни «Інформаційні та комунікаційні технології», яка викладається на першому курсі, курсанти опановують загальні інструментарії роботи з інформацією на персональному комп'ютері, до яких належать майкрософтівські та гуглівські офіси, основи побудови мережі Інтернет, принципи обміну інформацією та основи інформаційної безпеки користувача комп'ютерних пристроїв. Під час вивчення дисципліни «Інформаційне забезпечення професійної діяльності», яка викладається на другому, або третьому курсі, курсанти отримують навички користування відомчими інформаційними ресурсами та вчаться добувати інформацію з відкритих джерел мережі Інтернет, обробляти та аналізувати її з подальшим використанням у процесуальних та службових відомостях.

Для кращої підготовки курсантів та слухачів Дніпропетровського університету внутрішніх справ, авторським колективом був підготовлений навчальний посібник «Інформаційні технології» [1], у якому містяться всі необхідні відомості для опанування зазначених вище двох інформаційних дисциплін «Інформаційні та комунікаційні технології» та «Інформаційне забезпечення професійної діяльності».

Для якнайкращого закріплення теоретичних знань та практичних навичок по кожній з тем навчальної дисципліни потрібно проводити поліцейські квести. У попередній доповіді ми ділились досвідом проведення ділової гри «Лінія 102», яка покращує практичні навички курсантів під час роботи з інформаційно-телекомунікаційною системою Національної поліції

«Цунамі» [2]. У цій доповіді ми запропонуємо порядок проведення рольової гри, яка завершує вивчення методів та інстументаріїв пошуку інформації з відкритих джерел.

При вивченні дисципліни «Інформаційне забезпечення професійної діяльності» достатньо багато уваги приділяється темі «Методика організації пошуку інформації працівниками Національної поліції у відкритих джерелах мережі Інтернет». Курсантам та слухачам пропонується отримати навички пошуку інформації за допомогою GOOGLE, Yandex, мета-пошукових систем та систем анонімного пошуку інформації, пошукових систем в соціальних мережах (Facebook, Вконтакте), державних реєстрів України, а також застосування поліцейськими чат-ботів у месенджері Telegram. Завершує вивчення теми рольова гра, методику проведення якої опишемо нижче.

При проведенні квесту з теми «Методика організації пошуку інформації працівниками Національної поліції у відкритих джерелах мережі Інтернет» (4 навчальні години) курсантів поділяють на групи до п’яти осіб. Кожній групі надаються установчі дані на 4 фігурантів, інформацію про яких необхідно знайти у відкритих джерелах мережі Інтернет. Курсанти систематизують інформацію та готують доповіді-презентації по кожному фігуранту. Після, по черзі, кожна підгрупа презентує зібраний та систематизований матеріал. По закінченню доповіді, курсанти команди, що доповідала, надають відповіді на поставлені інформаційні запитання курсантів інших команд. Якщо відповіді команда, що презентує зібрану інформацію на фігуранта, не знає, то відповідь на запитання дає курсант, який задав це питання. В залежності від активності курсантів під час проведення поліцейського квесту та якості зібраної інформації, викладачі виставляють підсумкову оцінку кожному курсанту кожній підгрупі.

Проведення таких інформаційних квестів значно мотивує курсантів та слухачів щодо вивчення навчального матеріалу дисципліни «Інформаційне забезпечення професійної діяльності», надає необхідні практичні навички щодо пошуку необхідної інформації з використанням великої кількості джерел, вчить проводити аналіз джерел отриманої інформації, враховуючи їх достовірність, допомагає систематизувати та підготувати інформаційні звіти та вчить презентувати зроблену роботу та знаходити відповіді на питання по зібраній інформації. Все це, безумовно, підвищує рівень інформаційної підготовки майбутніх правоохоронців.

Список використаних джерел:

1. Вишня В. Б., Ісмайлов К. Ю., Краснобрижий І. В. Інформаційні технології: підручник Дніпро : ДДУВС, 2021. 492 с. URL: http://er.dduvs.in.ua/handle/123456789/6820.
2. Прокопов С. О. Використання поліцейських квестів у навчальному процесі Дніпропетровського державного університету внутрішніх справ. *Економічна та інформаційна безпека: актуальні питання та інновації:* матер. Міжнар. наук.-практ. конф. (м. Дніпро, 4 листопада 2021 р.). Дніпро : ДДУВС, 2021. С. 186-193. URL: https://er.dduvs.in.ua/handle/123456789/8578.

Рибальченко Л. В.,
завідувач кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент
Чупілко С. І.,
викладач ліцею № 18 (м. Кам'янське)

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ЇХ ВПЛИВ НА ЕКОНОМІЧНУ БЕЗПЕКУ УКРАЇНИ

Економічна безпека країни є однією із важливих складових національної безпеки держави. Незалежність, суверенітет та конкурентоспроможність держави виступають головними чинниками на шляху економічного розвитку країни, залучення іноземних інвестицій, зростання валового внутрішнього продукту, зростання макроекономічних показників та зростання рівня якості життя населення.

Побудова стабільної національної економіки, її міцність та надійність економічної системи, створення ефективного розвитку підприємницької діяльності, забезпечення надійної системи захисту від можливих ризиків та загроз спрямовано на збалансований розвиток могутньої національної економічно системи.

Важливим чинником економічної безпеки є захищеність національних інтересів від внутрішніх та зовнішніх загроз, створення умов надійного захисту на усіх рівнях розвитку економічної системи. Забезпечення належного стану виробничого на науково-технічного потенціалу, високий технологічний розвиток галузей економіки, висока якість продукції та конкурентоспроможність національної економіки сприяють зростанню рівня захисту економічної безпеки країни.

Розглядаючи чинники впливу загроз економічній безпеці, необхідно сказати, що одним з факторів загроз виступає тіньова економіка, яка охоплює майже всі сектори економіки для отримання величезних прибутків, які не оподатковуються і з яких не сплачуються податки державі. У 2021 році тіньовий сектор України досяг 31 % ВВП. За результатами діяльності банківського сектору спостерігалося зростання тіньового сектору від операцій з фінансовими активами, зобов'язаннями в іноземній валюті та значний рівень накопичених непрацюючих кредитів. Створюються офшорні зони для витоку капіталу та сплати найменших податків, при цьому не сплачується прибутковий податок та існують жорсткі правила захисту комерційної таємниці та банківської [1].

Одними з чинників зростання рівня тінізації економіки є низький рівень захисту прав власності, низький рівень ліквідності фондового ринку, захисту прав інвесторів поряд із недостатньою спроможністю регулятора протидіяти зловживанням на ринку, недосконаліть судової системи країни, високий рівень корупції в країні, недосконаліть законодавчої бази та інше.

Для створення надійної системи захисту національної економіки та економічної безпеки необхідно впровадження нових правових норм та відповідного контролю за його дотриманням, створення системи гарантування економічної безпеки та механізмів її контролю.

Економічна безпека є важливою складовою і соціальної безпеки, яка визначає її рівень соціально-економічної безпеки, захист населення, регіонів країни та суспільства. Концепція Національної безпеки є нормативно-правовим документом, в якому зазначено основні положення щодо захисту національних інтересів в усіх сферах діяльності та виділено напрями виявлення та усунення можливих загроз національній економіці.

Однією з функцій надійної системи економічної безпеки є формування інформаційної безпеки. Інформаційні технології сьогодні широко використовуються в усіх сферах діяльності. Підприємницька діяльність та бізнес вже неможливі без застосування сучасних інформаційних технологій, програмного забезпечення та інформаційних систем. Але якраз із застосуванням інформаційних технологій виникають питання щодо створення загроз і небезпек, які впливають на діяльність не лише великих підприємств, установ, організацій, а й населення. Підприємства мають створювати та формувати нові методи протидії будь-яким загрозам для забезпечення економічної безпеки [2].

Отримання та доступ до інформації відбувається із застосуванням інформаційних технологій. Тут виникає питання щодо захисту інформації від загроз, які можуть відбуватися під час роботи в мережі Інтернет.

Більшість покупок відбувається через Інтернет, що дозволяє зменшити час на пошук на придбання товару. Але трапляються і такі випадки, коли продавець виявляється шахраєм, якого зразу немає можливості виявити. Для багатьох підприємств важливим є потенційно надійні постачальники продукції та замовники послуг, якими можуть бути як вітчизняні так і зарубіжні компанії. Тут розглядаються питання надійної та добросовісної конкуренції з перевіреними компаніями.

Застосування сучасних інформаційних технологій дає можливість розширення ринків надання будь-яких послуг на вітчизняному інформаційному просторі та охоплення нових ринків провідних країн світу. Проведення платежів за надані послуги, сплата за отримання товару чи обладнання виконується через банківські інформаційні системи і технології.

Моделювання економічних процесів та прогнозування діяльності підприємств у довготривалому періоді стає можливим саме із застосуванням сучасних інформаційних технологій, які призначено для ведення бізнес-процесів, створення та реалізацію міжнародних проектів [3].

Використання хмарних технології є надійним для зберігання великих обсягів інформації, її обробка та робота з різними базами даних є найбільш привабливим та надійним. Використання таких технологій є зручним для ведення контролю за процесами виробництва та розвитку бізнесу у будь-який час та з будь-якої країни світу. Зберігання, захист інформації від

несанкціонованого доступу, протидія загрозам, управління безпекою та контроль доступу в хмарних технологіях забезпечується через багатофакторну аутентифікацію, надійну систему паролів та ефективну архітектуру безпеки хмарного середовища, що забезпечує високий рівень захисту даних. Щороку відбувається зростання попиту на застосування хмарних технологій в бізнесі та інших сферах життя.

Формування надійних та довготривалих відносин між постачальниками та клієнтами є можливим через застосування корпоративних порталів та мереж, де зосереджено інформаційні ресурси підприємств для створення спільного доступу до участі у конференціях, проектах, проведення вебінарів, обміну інформацією, тощо.

Таким чином, сучасний розвиток інформаційних технологій сприяє не лише швидкому доступу до інформації, а й зростанню рівня її економічної безпеки, захисту від витоку та несанкціонованого доступу, зменшенню рівня ризиків, застосуванню механізмів управління інформаційною та економічною безпекою не лише на рівні підприємств, а й в Україні.

Список використаних джерел:

1. Міністерство економіки України. Загальні тенденції тіньової економіки в Україні у січні-вересні 2021 року. URL: https://me.gov.ua/
2. Rybalchenko L., Ryzhkov E., Ciobanu G. Global consequences of the loss of business in countries around the world caused by fraud. *Philosophy, Economics and Law Review*. 2022. Vol. 2 (1). Pp. 93-101.
3. Rybalchenko L., Ryzhkov E. Modeling economic component of national security. *Philosophy, Economics and Law Review*. 2021. Vol. 1 (1). Pp. 25-36.

Рибальченко Л. В.,
завідувач кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент
Чупілко Т. А.,
доцент кафедри комп'ютерних наук
та інженерії програмного забезпечення
Університету митної справи та фінансів,
кандидат технічних наук, доцент

ВИКОРИСТАННЯ ЕКСПЕРТНИХ СИСТЕМ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Експертні системи (ЕС) – то цілий клас комп'ютерних програм, які проводять аналіз на основі знань спеціалістів у конкретній галузі, класифікують, пропонують рекомендації, консультують та ставлять «діагноз» [1].

Експертні системи створені для розв'язання задач у вузькій, конкретній ділянці експертизи. Такі системи відрізняється від інших прикладних програм тим, що моделюють механізм мислення людини стосовно до розв'язання задач у певній проблемній області. Основна увага приділяється відтворенню комп'ютерними засобами методики вирішення проблем, що застосовується експертом, тобто виконанню деякої частини задач так само (або навіть краще), як це робить експерт. Система, крім виконання обчислювальних операцій, формує певні розуміння й висновки, ґрунтуючись на тих знаннях, якими вона володіє. Знання в системі представлені, як правило, на деякій спеціальній мові й зберігаються окремо від власне програмного коду, що і формує висновки й розуміння. «Знання» – це інформація у формі правил та фактів, необхідна ЕС для того, щоб її поведінка була інтелектуальною. Таким чином, базою для роботи ЕС є знання, а точніше – їхня структурована сукупність. База знань ЕС створюється шляхом збору, систематизації, організації та індексації інформації, отриманої від спеціалістів конкретної галузі.

Важливим аспектом діяльності ЕС є вміння експертно пояснювати свої рішення користувачу, особливо в умовах неточності інформації, для того, щоб і підвищити рівень довіри до системи, і віднайти за наявності дефект роботи. Однією з основних характеристик експертної системи є її продуктивність, тобто швидкість одержання результату і його вірогідність (надійність).

Експертні системи в юриспруденції застосовують задля наступного:

– забезпечення схеми подання юридичних понять і методології перетворень для виявлення взаємозв'язків між поняттями, що в подальшому стає базою для аналізу доказової бази;

– планування та прогноз подальших дій для досягнення того чи іншого завдання;

– визначення зв'язку між вихідними даними та юридичною теорією відповідно до законодавчих актів;

– навчання.

ЕС в галузі юриспруденції – системи, які можуть вирішувати завдання з юридичної практики, інколи навіть заміняючи юриста.

Використовуючи знання експертів, що закладено в їх базу знань ЕС, система пояснює, аргументує і робить висновки.

Далі наведено два приклади ЕС, що знайшли застосування в розслідуванні злочинів на території України:

1. «STOP кілер» – дана ЕС будує версії щодо особи людини, що вчинила вбивство та його мотивів. Система адаптована до українського законодавства і містить значну базу даних, що підвищує репрезентативність результату.

В основному даною системою користуються співробітники органів кримінальної юстиції під час розслідування справ, в основі яких – вбивство.

2. «RICAS» – ЕС, створена для кримінального аналізу даних. Система в реальному часі здійснює кримінальний аналіз та пошук, що вагомо підвищує результативність розкриття злочинів по гарячих слідах, а також – раніше нерозкритих злочинів.

Система має миттєвий доступ до відеокамер на інтерактивній мапі як в реальному режимі, так і в записі, тому дозволяє оперативно відстежувати дії правопорушників, фіксувати обставини злочинів, збирати доказову базу, а також швидко реагувати на ситуації на вулицях міста.

Ці ЕС та інші сприяють підвищеній ефективності роботи правоохоронних органів шляхом автоматизації процесів пошуку доказової бази, фіксації правопорушень і прийняття рішень щодо них.

Найбільшою перевагою подібних систем у кожній області є те, що це, фактично, усі знання з певної галузі, акумульовані в одній системі. Варто зазначити, що ЕС не може приймати рішення за співробітника, її функція – якісне, об'ємне консультування.

Експертні системи в галузі права будуються на загальних та спеціальних знаннях в праві: існуючих правових концепціях, структурі правил, особистісному сприйнятті права, правової системи та підсистем, юридичної аргументації, логіці, семантиці, соціології та психології права, а також філософських теоріях, що носять загальний характер.

Список використаних джерел:

1. Експертні системи: особливості застосування. URL: https://osvita.ua/vnz/reports/management/13574
2. Мазниченко Н. Місце і значення експертних систем в області права. 2020. URL: http://ir.librarynmu.com/bitstream/123456789/2120/1/2020.10.6-8.pdf#page=193.

Рижков Е. В.,
професор кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, професор

ПРОБЛЕМНІ ПИТАННЯ ФОРМУВАННЯ КІБЕРВІЙСЬК В ПЕРІОД ВОЄННОГО СТАНУ В УКРАЇНІ

Повномасштабному вторгненню росії в Україну передувала серія глобальних кібератак на об'єкти нашої кібернетичної інфраструктури. Було атаковано понад 70 урядових та державних інформаційних ресурсів та систем. Фактично, ми отримали повномаштабну кібервійну, яка в попередні 8 років мала підготовчий період з боку агресора та безліч кібератак по відношенню до нашої країни.

Готуючись до цього, в Україні було вжито певних заходів. Так протягом 2021 року видана низка нормативних актів. Серед них Указ Президента Укріни від 26 серпня 2021 року №446/2021 «Про невідкладні заходи з кібероборони держави» та Указ Президента України від 26 серпня 2021 року № 447/2021 «Про Стратегію кібербезпеки України» [1].

Фактично, вказаними документами було запроваджено створення в Україні кібервійськ. Рекрутування фахівців у сфері ІТ було розпочато у різних формах: від ананімного через спеціалізовані чат-боти:

Хоча кібервійська і будуть частиною Міноборони після прийняття відповідного закону, майбутніх кібербійців планувалось розподілити між різними структурами, що відповідають за кібербезпеку: СБУ, Держспецзв'язку, кіберполіцією, РНБО, НБУ, Мінцифри, Міноборони, ЗСУ та розвідкою.

На прикладі США структура кіберкомандування кібервійськ виглядає наступним чином:

Рис. 1. Структура Кіберкомандування США

Кібервійська США (United States Cyber Command або USCYBERCOM) офіційно сформувалися у 2009 році, а неофіційно – як мінімум 20-30 років тому. Основними завданнями USCYBERCOM – є централізоване проведення операцій кібервійни, управління і захист військових комп'ютерних мереж США [3].

За різними оцінками експертів якість системи вітчизняного кіберзахисту у період війни коливається від достатнього (очами фахівців державницького сектору) до незадовільного (на думку незалежних фахівців). У цих умовах безумовним є той посил, що допомога ІТ-фахівців та реалізована з боку держави ініціатива була б вкрай актуальною.

Проте, по факту маємо ситуацію в якій залучено до співпраці лише десятки фахівців з тисяч, що подали анкети. Виникає питання чому склалася така ситуація? Чому у глухому «резерві» вже протягом року знаходяться вкрай цінні для країни фахівці, які не можуть знайти собі прямого застосування, щоб протидіяти ворогові у кіберпросторі? Або кураторів з числа представників державницького сектору у спеціалізованих суб'єктів не вистачає чи мета анкетування була зовсім та, що продикларована? Картинка налагодження співпраці з представниками населення є. Результат мінімальний від можливого.

Ще одна проблема чітко позначилась напередодні повномасштабного вторгнення. Це відкриття кримінальних проваджень відносно найбільш кваліфікованих вітчизняних ІТ-фахівців, що пропонували свої послуги державі задля боротьби з рашистами. Після декількох спроб встановлення конструктивної взаємодії та обєднання зусиль з відповідними державними структурами вони були як мінімум деморалізовані, а за фактом нейтралізовані в цьому напрямі [4]. Типовим прикладом цьому є Ukrainian Cyber Alliance «Украинский кибераль янс» (УКА) [5]. «Тепер не буде жодних нічних дзвінків про допомогу, не буде публікацій, не буде консультацій удень і вночі для різних державних силових відомств. Все зупинилося», – заявив, у свою чергу, співзасновник компанії Олександр Галущенко [6].

Головна міжнародна мережа хакерів Anonymous оголосивши війну владі Росії [7]. Наразі вона також діє самостійно, демонструючи свою безумовну ефективність у кіберпросторі ворога [8].

За період війни з росією маємо безліч ганебних фактів саботажу, колобаранства та державної зради з боку представників різних ланок державницького сектору (безвійськова здача Криму, Іловайський котел для добробатів, размінування проходів до Херсонщини, знаходження джевелінів у амбарах замість передовій у лютому 2022 р. та інш.), які отримають свою правову оцінку після перемоги [9]. Що стосується захисту представників Українського кіберальянсу від кримінального переслідування, то такі спроби з боку представників законодавчого органу влади вже мали місце [10].

Чи виправиться ситуація і коли з вказаних нами вище проблем – є риторичним питанням. Причина в тому, що сфера кіберзахисту держави в Україні у силу своєї специфіки є вкрай консервативна, закрита та практично не досяжна для здійснення контролю з боку громадськості.

Безумовно, одним із можливих вариантів співпраці кібер-аматорів з правоохоронними структурами може бути реалізована в рамках конфіденційності [11]. Проте, вказані приклади поки що свідчать про протилежне.

Безумовним є той факт, що кіберзахист є однією з основних складових безпеки держави, а його ефективність – запорукою перемоги над ворогом у кіберпросторі. Сама ж ефективність повинна реалізовуватись через конструктивну співпрацю правоохоронних та військових структур із населенням – у нашому випадку фахівцями у ІТ сфері. Проте, темпи розробки вітчизняного законопроекту щодо створення кібервійськ суттєво відстають від успіхів ЗСУ на фронті, а його прийняття та вступ в дію ризикує відбутися вже після перемоги України над рашизмом.

Список використаних джерел:

1. Указ Президента України від 26.08.2021 р. № 446/2021 Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про невідкладні заходи з кібероборони держави». URL: https://www.president.gov.ua/documents/4462021-40009.
2. Указ Президента України від 26.08.2021 р. № 447/2021 Про рішення Ради національної безпеки і оборони України від 14.05.2021 р. «Про Стратегію кібербезпеки України». URL: https://www.president.gov.ua/documents/4472021-40013.
3. Українців запросили долучитися до кібервійськ – заступник секретаря РНБО. URL: https://fakty.com.ua/ua/ukraine/suspilstvo/20220217-ukrayincziv-zaprosyly-doluchytysya-do-kibervijsk-zastupnyk-sekretarya-rnbo/
4. РНБО видала розпорядження створити Кібервійська в Україні. Що це буде? URL: https://www.ukrinform.ua/rubric-technology/3316171-rnbo-vidala-rozporadzenna-stvoriti-kibervijska-v-ukraini-so-ce-bude.html.
5. Про українських хактивістів, кібервійну та вразливості в держсекторі. Інтерв'ю з членом Ukrainian Cyber Alliance Андрїєм Барановичем. URL: https://dou.ua/lenta/interviews/story-of-ukrainian-cyber-alliance/
6. Український кіберальянс. URL: https://ru.wikipedia.org/wiki.
7. «Український кіберальянс» припиняє діяльність в Україні. URL: https://censor.net/ua/n3178085.
8. Хакери Anonymous 3 березня обіцяють спустошити рахунки росіян і направити кошти на ЗСУ. URL: https://uagit.tv/2022/2/28/16206-hakery-anonymous-3-bereznya-obitsyayut-spustoshyty-rahunky-rosiyan-i-napravyty-koshty-na-zsu-video.
9. Хакери Anonymous збільшили атаки на офіційні сайти російських органів влади у два-три рази. URL: https://uagit.tv/2022/3/19/16641-hakery-anonymous-zbilshyly-ataky-na-ofitsiyni-sayty-rosiyskyh-orhaniv-vlady-u-dva-try-razy.
10. Рижков Е. В. Протидія корупції в ОВС. *Науковий вісник ДДУВС*. 2015. № 3. С. 19-24.
11. В «ЄС» вимагають від влади припинити переслідування «Українского кіберальянсу» URL: https://www.5.ua/ru/polytyka/v-es-trebuiut-ot-vlasty-prekratyt-presledovanye-ukraynskoho-kyberaliansa-209613.html.
12. Рижков Е. В., Маклаков Г. Ю. Особливості оперативно-розшукової діяльності при розслідуванні злочинів у сфері високих технологій. *Використання сучасних досягнень криміналістики у боротьбі зі злочинністю*: матер. міжвуз. наук.-практ. конф. студентів, курсантів і слухачів (м. Донецьк, 12 квітня 2002 р.). Донецьк: ДІВС, 2002. С. 19-29.

Рижкова С. А.,
старший викладач кафедри адміністративного права, процесу та адміністративної діяльності Дніпропетровського державного університету внутрішніх справ
Карпець Т. І.,
здобувач вищої освіти Дніпропетровського державного університету внутрішніх справ

ІНФОРМАЦІЙНО- КОМУНІКАТИВНА СКЛАДОВА ОРГАНІВ ТА ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЇ ЩОДО ПРОТИДІЇ НЕЗАКОННОМУ ОБІГУ НАРКОТИЧНИХ ЗАСОБІВ

В Україні від 1 до 1,5 млн жителів вживають наркотичні засоби, відповідно тенденція таких статистичних показників щороку збільшується серед українців та зростає на 8-10 %. Темпи зростання наркоманії в Україні є одними із найвищих у світі. Щороку від наркоманії та пов'язаних із нею хвороб помирають близько 120 тисяч людей. Близько 20 % наркотиків в Україні розповсюджується через Інтернет [1].

Важливим в контексті зазначеної проблематики є належна протидія незаконному обігу наркотичних засобів правоохоронними органами та правозахисними організаціями щодо протидії незаконному обігу наркотичних засобів із використанням інформаційно-телекомунікаційних технологій.

Зловмисники, використовуючи надбання сучасних технологій, постійно вдосконалюють свою злочинну діяльність, переводять її на нові рівні. В Україні, як і у світі загалом, наркозлочинність активно реалізується через мережу Інтернет, смартфони, мобільні месенджери та спеціальні додатки для розповсюдження психоактивних речовин, наркотичних засобів та їх аналогів.

Привертає увагу стрімке поширення цього явища серед дітей та молоді як основної вікової групи користувачів всесвітньої мережі, адже Інтернет є потужним інструментом впливу на свідомість підліткової та молодіжної аудиторії, яку нескладно підкупити на нав'язану інформацію.

Тенденція до переходу наркозлочинності у віртуальний простір є вкрай небезпечною, адже він не має кордонів і вирізняється транснаціональним характером. Замовлення наркотиків, відправлення їх та легалізація отриманих від незаконного обігу наркотиків коштів можуть відбуватися в абсолютно різних точках планети.

Мережа Інтернет є комунікативним полем, її активно використовують як інтерактивний інформаційний канал, а сприяє цьому анонімність інтернет-користувачів й «онлайн дилерів», а тому їх кількість збільшилася не тільки в Україні. В умовах пандемії коронавірусу перехід значної частини суспільних контактів в інтернетпростір, що стосується і наркозлочинності, лише посилився, про що йдеться і в щорічному звіті ООН.

На сайтах пронаркотичного спрямування розміщено чимало текстів з описом різних видів наркотичних засобів і психотропних речовин, рецептів їх виготовлення, виробництва та споживання. Надають навіть поради, як поводитися під час затримання працівниками правоохоронних органів за зберігання та перевезення наркотиків. Інтернет – це потужний інструмент для впливу на свідомість підліткової та молодіжної аудиторії.

На найпопулярніших про наркотичних сайтах є «чат-кімнати» – інтерактивні сторінки, на яких можна спілкуватися в реальному часі на теми, що найбільше цікавлять споживачі наркотиків (вартість, де дістати, як спожити). Спілкування відбувається без жодних обмежень. Крім того, є численні тематичні мережеві конференції з допомогою електронної пошти, соціальних мереж. Отже, Інтернет використовують як інтерактивний анонімний інформаційний канал, що надає можливість наркодилерам майже без ризику для себе пропонувати товар для реалізації [2, с. 85].

Важливе значення у протидії незаконному обігу наркотичних засобів серед населення, а особливо серед молоді є використання тієї ж «зброї», а саме використання інформаційно-комунікативного зв'язку із населенням щодо інформування про протиправні дії пов'язаних із незаконним розповсюдженням наркотичних засобів [3]. Позитивним прикладом такої взаємодії є створення чат-боту DrugHunters, що з англійської перекладається як «мисливець на наркотики» у месенджері Telegram Патрульної поліції [4]. Завдяки якому особи мають можливість анонімно повідомляти про «закладки» наркотиків та «закладників». Зокрема долучити фото та відео матеріали, для оперативного реагування органами та підрозділами Національної поліції на виявлені факти.

Досить позитивним прикладом у протидії незаконному обігу наркотичних засобів є чат-бот «ДійПротиНаркотиків» розроблено співробітниками управління боротьби з наркозлочинністю в Донецькій області ДБН Національної поліції України у партнерстві з ГУНП в Донецькій області в рамках реалізації «Регіональної програми з профілактики правопорушень, протидії поширенню наркоманії, боротьби з незаконним обігом наркотичних засобів, психотропних речовин та прекурсорів» в Донецькій області. Унікальність такого проєкту є в тому, що бот діє одразу на всій території Донецької області. Громадяни можуть анонімно надати інформацію про відомі факти наркозлочинів, навіть знаходячись в іншому місті. Наразі до чат-боту долучилися більше 1600 громадян. Від початку роботи чат-боту надійшло 461 повідомлення про ймовірне розповсюдження наркотиків серед населення. Здебільшого повідомлення надходили з Краматорська, Бахмута та Костянтинівки. Інформація, яка надходить у скриньку бота, всебічно аналізується та перевіряється працівниками кримінальної поліції територіальних підрозділів. Так, поліцейські встановили 19 осіб, причетних до наркозлочинів. Чат-бот «ДійПротиНаркотиків» було створено для викриття збувачів, постачальників та організаторів каналів збуту наркотиків [5].

Отже, на підставі вищезазначеного, важливим у протидії незаконному обігу наркотичних засобів, викриттю каналів збуту наркопрепаратів через мережу інтернет, протидії вуличній торгівлі наркотиками є ефективне запровадження в діяльності правоохоронних органів нових методів роботи, а саме використання інформаційно-комунікаційних технологій, в тому числі моніторинг онлайн ресурсів, щодо виявлення та реагування на зазначені правопорушення.

Список використаних джерел:

1. Щороку в Україні кількість наркозалежних зростає на 10 %. URL: https://zn.ua/ukr/UKRAINE/shchoroku-v-ukrajini-kilkist-narkozalezhnikh-zrostaje-na-10.html.
2. Пряхін Є. В. Особливості використання слідчим інформації, що поширюється через мережу Інтернет. *Основні напрями та проблеми протидії наркоманії:* матер. наук.-практ. круг. столу (м. Київ, 6 лютого 2017 р.). Івано-Франківськ : НАВС, 2017. С. 85-88.
3. Рижкова С. А. Використання чат-ботів у профілактиці правопорушень. *Сучасні інформаційні технології в діяльності Національної поліції України:* матер. всеук. наук.-практ. семінару (м. Дніпро, 16 листопада 2020 р.). Дніпро : ДДУВС, 2020. С. 82-84.
4. DrugHunter: Українська поліція запустила чат-бот для боротьби з поширенням наркотиків. URL: v5.zp.ua/news/drughunter-ukrainska-policija-zapustila-chat-bot-dlja-borotbi-z-narkotikami/
5. Поліцейський чат-бот «ДійПротиНаркотиків» обробив пів тисячі повідомлень, більшість – з Краматорська, Костянтинівки та Бахмута. URL: https://kramatorsk-police.dn.ua/news/view/9095.

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
Сеник С. В.,
доцент кафедри європейського права Львівського національного університету ім. І. Франка, доктор філософії

ОКРЕМІ АСПЕКТИ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ОБІГУ ІНФОРМАЦІЇ

У довоєнний час Україна, як держава, проводила значну кількість реформ стосовно використання інформаційних ресурсів, інформаційно-телекомунікаційних технологій і пов’язаних із ними знань у правовій галузі.

Прикладом цього може слугувати запровадження у 2020 році мобільного застосунку, вебпорталу і бренду цифрової держави в Україні – «Дія»; прийняття у березні 2022 року Закону України «Про хмарні технології» [1] тощо. Такі запровадження стали вимагати своєчасного та відповідного удосконалення інформаційного законодавства. Не дивлячись на те, що в Україні продовжуються бойові дії, на один із перших планів виходить питання щодо потреби вдосконалення системи та розроблення відповідних рекомендацій щодо регулювання суспільних відносин у галузі роботи з інформаційними ресурсами.

Не заглиблюючись у класифікацію, перелік та аналіз основних нормативно-правових актів нинішнього законодавства України про інформацію (дане питання більш конкретизовано описано в роботі [2]) хочемо акцентувати увагу на те, що сьогодні в Україні фактично діє нова галузь законодавства – інформаційне законодавство, основою якого стало закріплене у ст. 34 Конституції України, право на свободу думки і слова. При цьому основним гарантом конституційного права на інформацію є держава, адже зазначене право є можливим лише у демократичній, правовій державі і може реально розвиватися лише у демократичному суспільстві. Аналіз розвитку суспільства показує, що послаблення чи відсутність демократії безпосередньо по’язано із обмеженням інформаційних прав, передусім, права на свободу слова.

Сьогодні, однією із негативних ознак, яка впливає на стан права на отримання інформації громадянами, є низька інформаційна культура, низька кібергігієна громадянського суспільства. З іншого боку, проблемою є і недоліки, неузгодження у самому нормативно-правовому забезпеченні, де:

– частина положень є застарілою;

– недостатньо розроблені правові механізми реалізації та захисту прав на інформацію;

– наявна термінологічна невпорядкованість;

– наявні суперечності у регулюванні окремих суспільних відносин різними нормативно-правовими актами, що є причиною для неоднозначного тлумачення окремих їх норм тощо.

Така ситуація створює перешкоди для отримання інформації від органів державної влади та органів місцевого самоврядування. Інколи названі органи неправомірно застосовують право на встановлення грифів обмеження доступу до інформації, тим самим, по-суті, відмовляючи у наданні інформації. Зокрема, в окремих випадках утруднюється доступ до інформації про процеси прийняття ними рішень з цих чи інших питань. Звичайно, у даному випадку ми не розглядаємо питання, що пов’язані із утрудненням отримання інформації, через військову агресію росії.

З огляду на наведене, є потреба у вдосконаленні державної політики у галузі інформаційних правовідносин, наприклад, стосовно реформування законодавства про інформацію. Такий процес має відбуватися не хаотично, а з урахуванням міжнародних стандартів (оскільки Україна як держава прагне до Європейської інтеграції) та вітчизняних особливостей.

Так, на наш погляд, уже сьогодні є потреба у внесені змін до Закону України «Про інформацію» [3], у частині уточнення чи встановлення окремих термінологічних понять, уточнення порядку надання режиму доступу до інформації, а також інших критеріїв інформаційних ресурсів, доступ до яких може чи не може бути обмежено. Тому можемо констатувати, що на сьогодні Закон України «Про інформацію» не відповідає сучасному рівню розвитку інформаційних правовідносин. Це створює передумови для неможливості вирішувати окремі проблеми, що виникають у галузі інформації, інформаційних та інформаційно-телекомунікаційних технологій. Зазначимо, що Закон України «Про інформацію» приймався до прийняття Конституції України. Не дивлячись на те, що упродовж тривалого періоду до нього вносились певні доповнення і зміни, на сьогоднішній день він залишається застарілим для забезпечення нинішніх потреб. Прикладом наведеного може бути невизначеність критеріїв віднесення інформації до категорії конфіденційної інформації та, відповідно, вичерпного переліку таких відомостей, що надає можливість суб'єктам інформаційних правовідносин обмежувати доступ до інформації на власний розсуд. Таким чином створюються перешкоди, наприклад, для здійснення права громадян на доступ до інформації. Тому даний аспект є одним із важливих для вдосконалення державного управління у сфері інформаційних правовідносин. Адже, як показує розвиток суспільства і стверджують провідні вітчизняні та міжнародні фахівці у галузі інформаційно-телекомунікаційних технологій, XXI століття є відрізком часу, де інтелектуальна власність та інформаційні технології займають провідне місце у розвитку суспільства. Звідси випливає потреба у включені питання розвитку ІТ-галузі у найпріоритетніші напрями політики держави. Зрештою, це дасть змогу забезпечити розвиток вітчизняного ринку високих технологій.

На думку авторів, врахування викладених вище думок під час розроблення нових та удосконалення діючих нормативно-правових актів, які регламентують суспільні відносини в інформаційній сфері, безумовно, сприятиме вдосконаленню інформаційного законодавства в цілому та наблизить його до відповідних міжнародних стандартів.

Список використаних джерел:

1. Про хмарні технології: Закон України від 17.02.2022 р. № 2075-IX. URL: https://zakon.rada.gov.ua/laws/show/2075-20#Text.
2. Сеник В. В., Сеник С. В. Сучасні проблеми інформаційного законодавства України та напрями їх вирішення. *Сучасний конституціоналізм: проблеми теорії та практики:* матер. наук. семінару (м. Львів, 25 червня 2021 р.). Львів : ЛьвДУВС, 2021. С. 231-235.
3. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: http://zakon2.rada.gov.ua/laws/show/2657-12/

Синиціна Ю. П.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ПИТАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНІСТІ В ПРАВООХОРОННІЙ ГАЛУЗІ

Активні трансформаційні процеси в системі суб'єктів правоохоронної діяльності відбуваються у зв'язку з різними глобальними чинниками, зокрема інформаційними.

Збільшення обсягу даних та виникнення нових інформаційних технологій підвищує продуктивність праці, впливає на розвиток суспільства, розширенню соціальної комунікації, що в свою чергу формує нові поняття такі як інформатизація та цифровізація.

За результатами ретроспективного аналізу визначено, що основні питання інформаційно-аналітичної діяльності в правоохоронній сфері вивчали наступні видатні вчені: Вербенський М., Антонов К., Буржинський В., Никифорчук Д. та інші.

Інформаційно-аналітична діяльність (ІАД) – сукупність інформаційних процесів (збір, пошук, переробка інформації), необхідних для якісного та ефективного процесу управління.

До основних форм роботи інформаційно-аналітичної діяльності відносяться:

- моніторинг – складання інформаційних зведень та оглядів;
- аналіз ефективності прийняття рішень;
- дослідження актуальних проблем (інформаційні розробки, оперативні дослідження, аналітичні дослідження).

Підрозділи Національної поліції відповідно до покладених на них завдань аналізують рівень злочинності, чинники, від яких він безпосередньо залежить, прогнозують криміногенну ситуацію; розробляють і вносять пропозиції керівництву Національної поліції України щодо організації уповноважених підрозділів; аналізують ефективність використання сил, засобів та обліків у протидії кримінальним правопорушенням, визначають основні напрями й тактику розвідувальної діяльності, пов'язаної з виявленням кримінальних правопорушень, формулюють на цій підставі пропозиції керівництву Національної поліції щодо підвищення ефективності оперативно-службової діяльності [1].

Інформаційно-аналітичне забезпечення органів внутрішніх справ являє собою самостійну систему, яка характеризується певними принципами організації та управління, що має властиві їй функції й чітко сформульовані цілі розвитку як на найближчий, так і на перспективний періоди, і складається і з підсистем, між якими існують стійкі структурні зв'язки.

Особливе значення для ефективної діяльності підрозділів Департаменту інформаційно-аналітичного забезпечення МВС України має будь-яка соціальна інформація, що містить відомості, які можна використовувати для протидії злочинності, в тому числі отримана з відкритих джерел інформації.

До основних загальних характеристик і типових проблем інформаційно-аналітичного забезпечення органів внутрішніх справ України відносить – не досконаліть методичної та методологічної бази організаційно-управлінської діяльності ОВС. Інформаційно-аналітична діяльність та аналітичні дослідження є новітнім напрямком діяльності правоохоронних органів.

Інформаційно-аналітичне діяльність у сфері правоохоронної галуззі – це творчо-інтелектуальна діяльність аналітика (експерта) з отримання нового знання (інформаційно-аналітичного продукту) на підставі зібраних та оброблених (переважно засобами автоматизації) даних про осіб, процеси, події, явища.

До основних етапів вдосконалення інформаційно-аналітичної діяльності в правоохоронній галузі можна віднести:

− розробка та впровадження системи моніторингу та прогнозування стану безпеки держави;

− розробка і впровадження методик комплексного аналізу та оцінки оперативної обстановки та діяльності органів внутрішніх справ;

− проведення розрахунків обсягів злочинної діяльності та оцінки збитків, завданих нею;

− визначення рівня латентності злочинності.

Використання уповноваженими підрозділами Національної поліції інформаційно-аналітичного забезпечення у протидії злочинності сприятиме:

– суттєво покращиться ефективність практичних результатів щодо виявлення та документування злочинів, а саме ріст показника ефективного співвідношення виявлених та задокументованих до вчинених;

– зниження рівня злочинності, що свою чергу, призведе до поліпшення стану криміногенної ситуації в регіоні та країні;

– реальному оцінюванню ризиків та своєчасному впровадженні оперативно-профілактичних заходів у межах регіонів та держави;

– оптимізації процесуальних й управлінських рішень;

– створення практичної методики аналітичного аналізу великих за обсягом масивів інформації;

– збільшення ефективності процесу збирання, зберігання, накопичення та використання інформації.

Список використаних джерел:

1. Про затвердження Положення про Національну поліцію: Постанова Кабінету Міністрів України від 28.10.2015 р. № 877. URL: https://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF#Text.

Станіна О. Д.,
доцент кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ЦИФРОВІЗАЦІЯ ЯК КРОК В МАЙБУТНЄ

Персональні комп'ютери, мережа Інтернет, штучний інтелект, цифрові технології, біоінженерія тощо – все те, що раніше здавалося фантастикою, сьогодні є буденною реальністю. Експоненційний розвиток інформаційних технологій стосується всіх сфер життя та безумовно призводить до оптимізації виробничих процесів, зменшення необхідності використання людської праці.

Повсемісне впровадження цифрових технологій в повсякденне життя, виробничу сферу спричиняє збільшення виробничих потужностей, дозволяє знизити витрати (чи втрати) бізнесу, збільшує доступність інформації та відкриває границі і можливості для подальшого розвитку кожної окремої країни та світу в цілому. Цифрові технології, насправді, у значній мірі перетворили світ та спричинили зміну звичних моделей роботи всіх сфер життя людини. Сьогодні все більше відмічаються тенденції для перенаправлення інвестицій з більш традиційних сфер у цифрову.

Цифровізація, окрім наглядної зміни у вигляді економії ресурсів, має й деякі побічні ефекти, про які також слід сказати: 1) підвищення економічної конкуренції між різними країнами внаслідок загальної глобалізації; 2) зміна характеру моделі вибору тих чи інших товарів та послуг; 3) виникнення окремої сфери для товару «інформація», який у майбутньому в значній мірі може вплинути на прийняття вкрай важливих економічних рішень.

Цифровізація та автоматизація суттєво змінила ті тенденції в області економіки, які довгий час були незмінними. Так, для прикладу візьмемо сферу праці. Протягом багатьох сторіч ми спостерігали стійку тенденцію до збільшення вимог до кваліфікації робітника, підвищення його відповідальності тощо. З настанням четвертої промислової революції можна було спостерігати зворотну тенденцію, яка характеризується повсемісним впровадженням штучного інтелекту та зниженням вимог до спеціаліста, який, власне, й буде з цією системою працювати. З іншого боку, напевно, невірно розповідати про зниження вимог для усіх спеціалістів, бо тут мова, скоріше, йде саме про перерозподіл та модифікацію ринку праці. Так, якщо до спеціаліста, який буде взаємодіяти з системою штучного інтелекту, вимоги дещо зменшуються, у той же час до самого розробника такої системи з кожним роком такі вимоги будуть тільки збільшуватися, і їх підвищення – прямий результат ускладнення самої системи.

Тут також слід зазначити нездорову тенденцію в сфері зайнятості, яка характеризуюся значним переформатуванням в процесі швидкої зміни на ринку праці. І, скоріше за все, такі зміни будуть стосуватися не лише (а може, і не стільки) робітників з низькою заробітною платою, а поруч з ними – всього середнього класу. І справа в дійсності у доцільності самої оптимізації, оскільки інколи вигідніше залишити низькокваліфікованого робітника з невеликою зарплатнею, ніж купувати нову автоматизовану систему. Зовсім інша ситуація відбувається у випадку, коли робітник має достатньо високу заробітну платню, і тоді, як наслідок, роботодавцю є сенс її скорочувати та піти шляхом заміни десяти робітників всього одним спеціалістом разом з установленням на виробництві сучасної автоматизованої системи.

З іншого боку, як зазначають деякі дослідники [1], проблема з безробіттям, справді, не така однозначна, і наразі в першу чергу слід говорити саме про модифікацію ринку праці та перерозподіл ринку праці з пріоритетом переключення на ІТ-сферу.

Окрім цього, важливо відмітити, що тенденції, які прослідковуються на ринку праці, потягнуть за собою певні зміни і в інших сферах. Так, наприклад, чи не найпершою постраждає сфера освіти (вже зараз ми бачимо певні тенденції в цьому напрямі), адже кожного року буде все зменшуватися потреба у базовій середній освіті і будуть все більше підвищуватися вимоги до вищої освіти, причому сама освіта, скоріше за все, матиме направленість на досить невелику групу людей. Вже зараз можна казати про зміни пріоритетів – від базових «енциклопедичних» знань до сфери цифрових технологій. Також можна прогнозувати зміни, наприклад, у сфері культури, яка безпосередньо пов’язана з рівнем та якістю освіти, а через зміни у сфері культури відбудуться вкрай важливі і водночас з тим небезпечні зміни у всіх інших сферах, оскільки зміняться загальні тенденції, правила поведінки, світосприйняття тощо.

Крім того, в результаті четвертої промислової революції виникла нова проблемна сфера – кіберзлочинність [2], яка в свою чергу потребує окремого підходу для боротьби з нею [3].

Отже, повсемісні зміни в економічний та соціальній сферах, що є наслідком цифровізації, зараз є не просто тенденцією, а нашим буденним сьогоденням. Ігнорувати такі зміни наразі неможливо і навіть шкідливо, а взагалі – досить небезпечно. Тепер вбачається важливою задача розробки нових підходів та принципів життя і соіснування у світі разом з останніми тенденціями, що прослідковуються і значно впливають на населення цілої планети.

Список використаних джерел:

1. Bukht R., Heeks R. Defining, Conceptualising and Measuring the Digital Economy. *International Organisations Research Journal.* 2018. Vol. 13 (2). Pp. 143-172.
2. Рибальченко Л. В. Кіберзлочинність та її вплив на економічну безпеку країни. *Економічна та інформаційна безпека: актуальні питання та інновації:* матер. Міжнар. наук.-практ. конф. (м. Дніпро, 4 листопада 2021 р.). Дніпро : ДДУВС, 2021. С. 198-200.
3. Гребенюк А. М., Рибальченко Л. В., Прокопов С. О. Моніторинг кіберінциндентів хмарних сервісів та захист цифрових каналів зв’язку. *The First Special Humanitarian Issue of Ukrainian Scientists. European Scientific e-Journal.* 2022. Vol. 3 (18). Pp 40-53.

Струков В. М.,
професор кафедри кібербезпеки
та DATA-технологій
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ПРИСКОРЕННЯ ШВИДКОСТІ РОЗВИТКУ ВИСОКОТЕХНОЛОГІЧНИХ ПРОЦЕСІВ У СУЧАСНОМУ СВІТІ

Сучасний світ переживає епоху Четвертої промислової революції і, відповідно, епоху докорінних змін у всіх сферах життєдіяльності, і, зокрема, в кримінальному світі. Все потужніше і доступніше стають високотехнологічні інструменти, використання яких надає суспільству принципово нові, нечувані до сих пір можливості, але в той же час несуть в собі великі ризики і загрози і в руках злочинців можуть заподіяти людству дуже великої невиправної шкоди.

Інтегрована назва цього явища сформульована на Всесвітньому економічному форумі і отримала назву «Четверта промислова революція». Подальше більш детальне дослідження цього феномена виконано в роботі засновника Всесвітнього економічного форума Клауса Шваба «Технології четвертої промислової революції».

Однією з найважливіших характерних рис цього явища є зростаюча швидкість темпів розвитку технологій, які є драйверами Четвертої промислової революції. Це означає, що завтра можливості, які сьогодні вважаються фантастикою, будуть буденним явищем.

Цю особливість яскраво можна охарактеризувати прогнозом творця андроїда Софія канадського експерта у галузі робототехніки голови лабораторії Hanson Robotics Девіда Хенсона.

На його погляд, до 2029 року розумові здібності андроїдів будуть порівнянні з інтелектом однорічної дитини. Такі машини зможуть займати посади у військових і правоохоронних органах. Ще через одне десятиліття світ зміниться раз і назавжди.

Люди будуть жити зовсім в іншому соціумі, хоча ще довгі роки андроїди не зможуть звільнитися від статусу «представників другого сорту». Хенсон не виключає, що «законодавці намагатимуться легально пригнічувати емоційну зрілість машин, щоб люди могли відчувати себе в безпеці».

Однак це не зупинить штучний інтелект, і людство докладе максимальних зусиль: «Вимоги людей до розумних машин будуть зростати, що підштовхне розвиток штучного інтелекту. Відбудеться переломний момент, коли машини «прокинуться і почнуть наполягати на своїх правах, щоб вести вільне існування».

Вже в 2035 році, на думку Хенсона, варто очікувати, що андроїди перевершать людей в будь-яких професіях. Нове покоління розумних машин буде складати іспити нарівні з випускниками і отримувати докторські ступені.

Це призведе до виникнення глобального руху за громадянські права в суспільстві роботів, а до 2038 року США стануть першою країною, що надала такі права андроїдам.

Давайте порахуємо, скільки залишилося до 2038 року – 16 років. Таким чином, переважна більшість сучасників буде свідками і учасниками цих подій.

Це, на перший погляд, може здаватися певною мірою футуристичним прогнозом. Але я б зауважив, що такий прогноз робить не дилетант або письменник-фантаст (як свого часу це робив відомий письменник-фантаст Г. Уелс у книгах «Машина часу» і «Боротьба світів»), але один з провідних фахівців у найсучаснішій технологічній галузі – робототехніці. І цей факт, на мій погляд, вимагає ставитися до його прогнозу з повагою і увагою.

Найважливішим результатом сучасних процесів у сфері високих технологій є усвідомлення правоохоронними органами розвинених країн необхідності зміни парадигми своєї діяльності – перехід від реактивного принципу до предикативного, що і відбувається в останні декілька років. І головним інструментом реалізації такої парадигми є застосування інтелектуальних аналітичних систем типу Palantir, ePOOLICE.

Ткач Ю. О.,
ад'юнкт
Дніпропетровського державного університету внутрішніх справ,
майор поліції
Науковий керівник:
Гребенюк А. М.,
завідувач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх справ

СУЧАСНІ ПИТАННЯ ДЕЗІНФОРМАЦІЇ В УМОВАХ ВІЙНИ

Так, 24 лютого 2022 року російська федерація розпочала повномасштабне вторгнення в Україну. Щодня в інформаційному просторі з'являється багато інформації різного характеру, серед якої є недостовірна інформація, яка публікується у Facebook, Instagram, Twitter, Telegram та інших соціальних мережах. Поширення такої інформації тягне за собою дезінформацію населення, залякування, введення громадян в оману, при цьому здійснюється психологічний тиск на них за допомогою цієї інформації, яку використовує ворог у своїх цілях.

Так, дезінформація – це очевидно неправдива або така, яка вводить в оману, інформація, що в сукупності: створена, представлена і поширена з

метою економічної вигоди або умисного введення в оману громадськості; та може заподіяти шкоду суспільству через загрозу демократичним політичним процесам і процесам вироблення політики, а також таким суспільним благам, як захист здоров'я громадян, довкілля і безпека. Таке поняття як «дезінформація» не охоплює недостовірну рекламу, помилки у звітності, сатиру і пародію чи очевидні необ'єктивні новини й коментарі, та не є порушенням юридичних зобов'язань, кодексів саморегулювання рекламних послуг і стандартів щодо недостовірної реклами [1].

До дезінформації не можуть бути визнано: по-перше оціночні або критичні судження; по-друге сатира; по-третє недостовірна інформація про особу, яка не шкодить суспільним інтересам [1].

За поширення дезінформації відповідальність може бути як адміністративна або кримінальна залежності від дій осіб, які поширюють дезінформації.

Адміністративна відповідальність може настати у разі одноразового поширення дезінформації без ознак замовлення; відсутність вихідних даних про медіа [1].

Кримінальна відповідальність може настати у разі умисного, систематичного поширення дезінформації; умисного поширення дезінформації на замовлення третьої особи або якщо спричинено шкоду; втручання в діяльність журналіста або медіа, підкуп. Також необхідно звернути увагу, що відповідальність за дезінформацію настає виключно на підставі рішення суду [1].

Необхідно звернути увагу, як поводитися у мережі, щоб протидіяти дезінформації та фейкам під час війни:

1. Бажаєте бути корисними в інформаційному фронті? Знайдіть собі команду, яка вже зосередила сили на окремому напрямку боротьби з дезінформацією.
2. Не поширювати інформацію з не офіційних джерел. Навіть, якщо вам її надіслала близька людина, кум, сват або ще хтось. Не впевнені, то ж не робіть репост.
3. Не вірити сліпо в інформацію в інтернеті. Виключення – правила або вказівки, опубліковані на офіційних сторінках військового керівництва держави чи органів державної влади, або тих, які лунають в ефірі «Українського радіо» чи інших офіційних каналів оповіщення. Критично аналізуйте будь-яке джерело.
4. Намагатись не реагувати на масові розсилки та зупиняти за змогою їх поширення. Залиште в підписках лише офіційні сторінки та канали влади і місцевого уряду.
5. Не залишати свої дані у відкритому доступі – онлайн-форми, петиції та будь-які анкети є небезпечними наразі. Лише громадяни відповідальні за особисту конфіденційність.
6. Не відкривати сумнівних листів та повідомлень та не робити їх репост або пересилку.
7. Не захоплюватись історіями з неперевірених джерел – під час війни сарафанне радіо працює не на нашу користь, та інше [2-3].

Підсумовуючи вважаємо за необхідним проводити роз'яснювальну роботу з населенням щодо поведінки в мережі з метою протидії дезінформації та фейкам, пояснювати громадянам, що останні не повинні залишати свої дані у відкритому доступі – онлайн-форми, петиції та будь-які анкети, тощо. Правоохоронним органам необхідно посилити моніторинг для виявлення дезінформації та подальшого документування загрози та виправлення недоліків, які використовує агресор. Також необхідно посилити покарання за поширення дезінформації та вжити всіх необхідних заходів правоохоронними органами для стримування агресора в інформаційному просторі.

Список використаних джерел:

1. Ясність? Міністерство культури, молоді та спорту України: веб-сайт. URL: https://mkip.gov.ua/files/pdf/Ясність%20fin.pdf?__cf_chl_tk=Q65s0J_RVOlCJoKRbs_g01T5zNW.SJnPzdOWDSIOiVM-1668295307-0-gaNycGzNCKU.
2. Моє місто? Інформаційна війна: як вийти з нею переможцем: веб-сайт. URL: https://mycity.one/blog/faktcheking?utm_source=google&utm_medium=cpc&utm_campaign=inweb_My_City_Informatsijna_Vijna_Ukraine&utm_content=611396250363&utm_term=дезінформація%20це&gclid=EAIaIQobChMIxe2z16qj-wIV7kKRBR0J_AlSEAAYASAAEgKg6_D_BwE.
3. Плескачова В. С. Дезінформація як один із способів інформаційно-психологічного впливу на суспільство. *Міжнародна та національна безпека: теоретичні і прикладні аспекти*: матер. V Міжнар. наук.-практ. конф. (м. Дніпро, 12 березня 2021 р.). Дніпро: ДДУВС, 2021. С. 406-407. URL: http://er.dduvs.in.ua/jspui/handle/123456789/6262.

Форос Г. В.,
т. в. о. завідуча кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ОКРЕМІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В СУЧАСНИХ УМОВАХ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади. На сьогодні актуальність проблеми забезпечення кібернетичної безпеки не викликає жодних сумнівів. Щодня кожен з нас стикається із необхідністю користування інформаційними технологіями. Від соціальних мереж, розміщення інформації про свої персональні дані в інтернеті до користування банкоматами, банківськими рахунками і т.п.

Водночас переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Особливу занепокоєність викликає можливість розробки, застосування та розповсюдження інформаційної зброї, виникнення у зв'язку з цим загрози інформаційних війн та кібертероризму, чиї негативні наслідки можна порівняти з наслідками застосування зброї масового знищення.

Військовий напад російської федерації вимагає невідкладного удосконалення національної системи кібернетичної та інформаційної безпеки як складової системи забезпечення національної безпеки України.

Загрози національним інтересам та національній безпеці України в інформаційній сфері визначено у Стратегіях національної безпеки та інформаційної безпеки України, затверджених, відповідно, Указами Президента України від 14.09.2020 р. № 392/2020 та від 28.12.2021 р. № 685/2021. Слід зазначити, що Стратегією інформаційної безпеки України перше введено в офіційний обіг термін «інформаційна безпека України» – складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєвоважливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії завдаванню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Саме інформаційна безпека дає гарантію того, що можуть бути досягнути наступні цілі: конфіденційність інформації; цілісність інформації і пов'язаних з нею процесів; доступність інформації, коли вона потрібна; облік усіх процесів, пов'язаних з інформацією, тобто завдяки інформаційній безпеці виконуються функції щодо дотримання вимог, що ставляться до інформації.

Як ми вже вказували, сьогоднішня економіка, політика, туризм повністю залежать від зовнішніх чинників. Інформаційний статус держави, її представлення в світовому інформаційному просторі є часткою її політичної чи економічної ваги в світі. Немає держав, статус яких в інформаційній площині, суттєво відрізнявся би від статусу в інших площинах. Але це не є випадковим процесом, сильна держава займається своїми іміджевими процесами на рівні з іншими.

Дослідники міжнародних відносин нині виділяють четвертий вимір відносин – інформаційний, констатуючи його рівність з такими відомими вимірами, як дипломатичний, економічний та військовий. Йдеться вже не просто про інформаційну цивілізацію, в яку вступили розвинуті держави, а про постінформаційну. Останні події яскраво демонструють важливість такої складової держави, як інформаційна. У випадку збройних конфліктів виникає потреба в легітимізації застосування сили, у змінах ставлення до цінностей, оцінок однієї культури іншою.

Якщо зв звернути увагу на ситуацію щодо інформаційної безпеки громадян України в умовах воєнного стану, то вона умовно може бути класифікована на кілька категорій, а саме: інформаційна безпека громадян України, що проживають АР Крим та на тимчасово окупованих територіях; інформаційна безпека населення України, що проживає на неокупованих територіях та інформаційна безпека військовослужбовців та інших осіб, що безпосередньо беруть участь в військових діях та членів їх сімей. Згідно Конституції України, обов'язком саме держави є захист людини від реальних та потенційних загроз, в тому числі і в інформаційній сфері.

Особливе занепокоєння викликає інформаційна безпека громадян України, що проживають АР Крим та на тимчасово окупованих територіях. Військова операції щодо російської інтервенції до Криму, Донецької та Луганської областей в 2014 році виступала військовим фактором, який був вирішальним для початку активних дій України стосовно впровадження політики із захисту прав, свобод громадян, які проживали на тимчасово окупованих територіях. Зважаючи на історичні умови розвитку, можемо зауважити, що весь період державотворення незалежної України з 1991 р. до моменту анексії з боку росії Україна не зазнавала викликів такого характеру, хоча і відбувались події, які могли стати наочним прикладом розвитку ситуації, зокрема, в Грузії, Молдові тощо. Відповідно, вплив військового фактору обумовив поступовий розвиток інформаційної політики України стосовно забезпечення прав, свобод громадян на окупованих територіях.

На цей час з'явилось багато доказів, що підтверджують порушення окупаційною владою росії прав та свобод громадян, які проживають на тимчасово окупованих територіях. Постійний збір, обробка, аналіз, передавання інформації світовій спільноті має стати одним із інструментів інформаційного забезпечення захисту таких прав і свобод з боку держави, громадських організацій. Слід відмітити, що діяльність держави в сфері інформаційного забезпечення в даній сфері є важливим інструментом залучення міжнародної спільноти до забезпеченні прав, свобод громадян на тимчасово окупованих територіях.

Яровий К. В.,
викладач кафедри
інформаційних технологій
Національної академії внутрішніх справ,
кандидат юридичних наук

ВИКОРИСТАННЯ ПРАВООХОРОННИМИ ОРГАНАМИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ ЗЛОЧИННОСТІ

Внаслідок потужного розвитку технологічного прогресу та інформаційних систем, сучасні технології широко використовуються в різних сферах життєдіяльності людини, у тому числі у правоохоронній діяльності.

Використання правоохоронними органами інформаційних технологій міцно закріпилось у її роботі, як інструмент для розкриття та протидії злочинності та захисту прав і свобод людини та громадянина.

Безумовно, що за допомогою сучасних інформаційних технологій відбувається модернізація правоохоронної діяльності, підвищується ефективність роботи окремих підрозділів.

Натомість результати цієї роботи безпосередньо залежать від якості інформаційної підтримки, оскільки основні зусилля практичних працівників із розслідування, розкриття та запобігати злочинам пов'язані з отриманням необхідної інформації. Основну роль в інформаційному забезпеченні правоохоронних органів займають обліки, що використовуються для реєстрації первинної інформації про злочини, а також осіб, які їх вчинили.

У свою чергу, під інформаційними технологіями необхідно розуміти – процес, який використовує засоби та методи збору, обробки та передачі даних (первинної інформації) для отримання нової якісної інформації про стан об'єкта, процесу чи явища (інформаційного продукту) [1, с. 9].

В правоохоронній діяльності запровадження нових інформаційних технологій продовжується за допомогою побудови на основі сучасних комп'ютерів локальних, регіональних та загальнодержавних галузевих інформаційно-обчислювальних мереж, які сприятимуть подальшому вдосконаленню інформаційного забезпечення правоохоронної системи [2, с. 148].

Правоохоронні органи використовують інформаційні технології не лише для розшуку та обліку злочинців та злочинів, але й для надання послуг населенню. Наразі громадяни та організації можуть скористатися деякими з державних послуг, що надаються в електронному вигляді. У разі інформаційно-технічного прогресу інформаційні технології є ключовим чинником оптимізації правоохоронної діяльності.

Враховуючи вищевикладене, слід зазначити, що на сьогоднішній день рівень злочинності потребує впровадження сучасних інформаційних технологій в правоохоронну діяльність. Необхідно переглянути підходи до запровадження сучасних інформаційних технологій у діяльність правоохоронних органів, збільшити фінансування для придбання сучасного та ліцензованого програмного забезпечення.

Крім цього, сучасний стан нормативно-правового забезпечення правоохоронної діяльності не дозволяє повною мірою використовувати інформаційний потенціал у правоохоронній діяльності, навіть у разі їх активного запровадження та використання.

Список використаних джерел:

1. Косичено О. О. Правові інформаційні ресурси Інтернет: довідник. Дніпро: ДДУВС, 2017. 64 с.
2. Вишня В. Б. Інформаційне забезпечення юридичної діяльності: підручник. Дніпро : ДДУВС, 2018. 245 с.

Bradu N.,
student of Theoretical Lyceum
«Children's Academy»
Scientific supervisor:
Ohrimenco S. A.,
professor
Moldova Economics Academy,
D.Sc. in Economics

CYBER SECURITY THREATS

Cyber security threats continue to escalate in frequency and variation. This has led to major security threats thus the need for installation of better security measures to prevent the occurrence of these threats. Typically, the threats could be categorized into three: malicious codes, network abuses, and network attacks. In addition, I will describe each of these threats and their characteristics.

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. The malicious code describes a broad category of system security terms like: attack scripts, viruses, worms, Trojan horses, backdoors time bombs, deliberate information and others. These threats are hidden in software and mask their presence to evade detection by traditional security technologies. Malicious codes can become a security threat if they are found and exploited by hackers or unauthorized users.

Network abuse is the use of a computer network for purposes prohibited by the network's acceptable use policy. It usually includes internet crime and other malicious uses, that may interfere with other users' ability to access network services. It is not uncommon for networks to prohibit the access or transmission of obscene, profane, or controversial material, especially considering employer and school networks. Some networks employ content filters or firewalls, designed to block objectionable activity. Most network operators maintain a specific email address or other contact for reporting network abuse.

A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity. There are two main types of network attacks: passive and active.

A passive network attack could be described as attackers which gain access to a network by monitoring or stealing sensitive information, without making any change to the data. However, an active network attack is used by attackers who also gain unauthorized access, but they modify the data as well. These attackers can either delete, encrypt or harm that data.

By analysing the information above, I came to the conclusion that cyber security is as important as ever. Due to the fact that cybersecurity threats exist and cause harmful damage to businesses, a robust security solution is absolutely essential. We've all heard of enterprises paying huge fines or even going out of business because of a simple hack to their systems. There are simply far too many threats out there to ignore the risks. Threats like the ones I described, could endanger our livelihood. Prevention is the key to reducing the risk of cyber attacks. By investing in cybersecurity software, using a VPN, and being aware of common attack methods, individuals and organizations can deter hackers and keep their data private.

References:

1. Kuah A., Dillon R. Digital Transformation in a Post-COVID World. *Sustainable Innovation, Disruption, and Change.* 2021.
2. West L. The Coronavirus Cybersecurity Survival Guide. Top Tips to Protect You from a Cyber Attack. 2020.
3. Slade R. Cybersecurity Lessons from COVID-19. CRC Press, 2021.
4. The Global Risks Report. 16th Edition. 2021.

Gnediuc I.,
student
Academy of Economic Studies of Moldova
Scientific supervisor:
Ohrimenco S. A.,
professor
Moldova Economics Academy,
D.Sc. in Economics

CYBER SECURITY AND CYBER THREATS

Abstract. The article examines the impact of cybersecurity in the digital space on the international economy. The classification (today, yesterday, and in the future) and analysis of cyber threats are carried out. The practical significance of the research results is obvious, since the active spread of IT technologies and their application in many areas of human activity, as well as the active policy of many countries in the field of digital economy formation, lead to the inevitable emergence of new threats at all levels. In this regard, the purpose of this work is to consider the impact of cybersecurity on the world, what types of cybercriminals exist, and what threats they pose.

Currently, the development of the digital world makes it increasingly interconnected with various spheres of human activity, so it becomes extremely important to know the security threats to protect people, organizations, the environment, infrastructure, and almost everything that we value and rely on for health and prosperity.

The purpose of this work is to consider the impact of cybersecurity on the world, what types of cybercriminals exist and what threats they pose.

To determine the importance of cybersecurity and knowledge of cyber threats, it is necessary to study this section of information security, define spheres of influence, who and how influences it, and what risks it brings with it.

At the World Economic Forum, Carnegie Mellon University [1] presented the Cyber Security Scheme, which represents the main cyber threats and areas of our life that are subject to them. They identified eight cyber threats such as:

- Gaps in cybersecurity skills;
- Cyber diplomacy and international security;
- Critical infrastructure and cyber resilience;
- Cyber risk management;
- Cyber security and new technologies;
- Cyber risk and supply chain risk;
- Cybercrime;
- Cybersecurity and regulation.

Behind all this are cybercriminals, which can be functionally divided into three types [2]:

1. Money-motivated criminals who commit identity theft, privacy breaches, and cybercrime for financial rewards.
2. State-sponsored attackers and terrorist organizations wishing to damage critical infrastructure systems and other vulnerable databases.
3. Thrill seekers who find satisfaction in being able to interfere in the work and life of individuals and organizations that possess protected information, such as identity information.

There have been many changes in the cyber threat landscape in recent years. However, there are many continuing trends in the way cybercriminals operate and the responses of public and private defenders.

The speakers of the Romanian company Bitdefender [3], which offers one of the best cybersecurity solutions in its class, identified the main cyber threats (their landscape) of today, yesterday, and the future. They are:

- Cybercriminal groups;
- Dark web;
- Supply chain attacks;
- Internal threats;
- Effect of Covid-19.

To understand the importance of knowledge of cyber threats, the breadth of the cybersecurity concept, the main scenarios of cybercriminal activity, and the landscape of cyber threats were examined.

As the dangers change, so must our responses; digital threats require vigilance, determination, and determination to respond accurately to the ever-expanding cycle of risk.

Over the past years, tools and methods used by cybercriminals to carry out their exploits (Exploit is a computer program, a piece of program code, or a sequence of commands that exploit vulnerabilities in software and are used to attack a computer system. The purpose of an attack can be to seize control over a system, and disruption of its functioning). Thus, responses tended to focus on exploit-by-exploit methods rather than more general criminal acts.

An st constant for cybercriminals is the phenomenon of social engineering, otherwise known as target manipulation to gain access to confidential information to which the criminal is not entitled, and then use that information to commit fraudulent use of personal information.

The simplest and most prevalent representative of the above phenomenon is fraud. Born in the information environment with spam calls and messages, in which the attacker, using manipulative scenarios, pretends to be a family member or trusted organization, seeking to obtain confidential information, information from the target person or company.

With the development of the Internet, email scams following the same scenarios have become very popular. And further, with the growing use of various platforms and social networks, smishing (text messages of a provocative nature), as well as hyperlinks through which data (often passwords) are stolen, began to spread.

Another important threat is ransomware and malware, which growth is constantly growing. The trend is shifting from simple data breaches to ransomware attacks.

Malware is software that intrudes into the systems of a target organization and either prevents them from working as intended or gives criminals access and control.

Ransomware is a more specialized attack in which the cybercriminal demands payment for the data they have accessed and holds encryption or public disclosure hostage.

The COVID-19 pandemic has accelerated the use of digital tools in business and at home, and these advances in digitalization have led to increasingly frequent, costly, and destructive cyber incidents. In connection with this change, people and organizations should pay special attention to cyberspace events and know the cyber threat landscape.

Thus, we can summarize the key conclusions:

– Cybercriminals have been successful in ransomware and data theft;
– Ransomware is a global threat;
– Understanding how to access and investigate dark web content will enable cybersecurity professionals to identify activities that may be targeted at businesses;
– A large number of business credentials are being sold and leaked to the dark web. These leaks can pose a severe threat to our customers.

Significant digitalization provided an opportunity for interaction and communication at a time when the world had to remain separate. Its advantages are obvious, but so are the threats. To ensure that we maintain a trusted, secure, and secure digital environment, managers and employees must know the main cyber threats and take all necessary measures to ensure cybersecurity.

References:

1. Carnegie Mellon University. Cybersecurity. *World Economic Forum.* 2022. URL: https:// intelligence.weforum.org/topics/a1Gb00000015LbsEAE.
2. Zivanchev P. W. How Criminals Have Migrated Through Identity Theft and Privacy into Cyber Attacks. Institute of Consumer Financial Education.
3. The Cyber Threat Landscape: Today, Tomorrow, and in the Future. Bitdefender MDR.

Niculin. E.,
student
Academy of Economic Studies of Moldova
Scientific supervisor:
Ohrimenco S. A.,
professor
Moldova Economics Academy,
D.Sc. in Economics

MODERN THREATS TO CYBER SECURITY

In today's world there is a rapid increase in the number of cyber threats. At the moment a new digital society is being built that brings both positive aspects and threats. The question of how the Internet will be governed and what control can be established over the information flowing through it has become important not only at the user level, but also at the political level.

The purpose of this paper is to look at cyber threats and their impact on the world, what types of threats there are, and how to deal with them [1].

Internet governance and the involvement of world states and international organizations is now a serious area of political debate. WSIS has demonstrated the growing politicization of the Internet and the cyber space. What fifteen years ago was largely run by a small group of technicians, scientists and engineers has now attracted the attention of a much larger group of stakeholders, both inside and outside governments. As the group grew, so did a broader range of issues. However, the issue of information or cybersecurity was hardly mentioned.

Users also use the Internet to propagandize and impose their values. The governments of China and Russia view the topic of information security as a way to shield their public from information that is unpopular with the regime and that can sow the seeds of discontent. These views conflict with the ideals of openness and freedom of speech held by many participants in the Internet governance process.

Today there are more than 100 positions and types of threats to the information system. It is important to analyze all risks using different diagnostic techniques. Based on the analyzed indicators with their detailing, it is possible to competently build a system of protection against threats in the information space.

Depending on different ways of classification, all possible threats to information security can be divided into the following main subgroups:

- information leakage;
- fraud;
- cyberterrorism;
- unauthorized access;
- unwanted content;
- data loss;
- Cyber Wars.

The most frequent and dangerous threats are: information leaks, fraud, and cyberterrorism.

Information leaks are the inappropriate transfer of confidential information. Causes can be many things, such as insiders, hacking or malware. Information leaks as a result of uncontrolled distribution of secrets outside an office, building, or company. The loss of valuable information can happen when the rules and regulations of security policies are not properly used [1]. Non-compliance with data protection and storage regulations leads to data leakage and dissemination in public places. So, for example, with the advent of social networks – Twitter, YouTube and Facebook – new ways of transmitting information and new ways of wiretapping and spying on people began to emerge. Eavesdropping has become web-based eavesdropping, listening to anything that is transmitted digitally. The Mark Klein exposé, first reported in the press, made the idea of mass eavesdropping on the Internet public.

Fraud is one of the most popular threats, the goal of which is usually to embezzle money from the victim. Malware, social engineering and targeted attacks help scammers do this. Social engineering is an attack technique based on human interaction. Attackers gain the trust of the victim and force them to give up confidential information, or they use a phishing attack by sending emails or text messages on behalf of trusted sources to lure out banking information.

Cyberterrorism is a set of illegal actions in cyberspace that threaten national security, individuals and society. These include, for example, hacking into computer systems, disabling hardware or software, hijacking the media and spreading misinformation there [2].

Common terrorists also use the Internet. For example, social networks have been used by various terrorist organizations to recruit people and coordinate their activities.

The above-mentioned range of threats does not exhaust the variety of contemporary threats. As the Internet develops, the number of threats grows in proportion to the number of benefits. This topic is increasingly relevant in today's times and requires a great deal of attention. First of all cyber security is about people. People who create programs that protect against cyber threats, people who find vulnerabilities before cybercriminals get to them, leaving cybercriminals no chance. Today's cybersecurity threats are vast and can cause enormous harm to users. So it's a very important issue to understand and be able to deal with.

References:

1. Bronk C. Cyber Threat. The Rise of Information Geopolitics in U.S. National Securit. Praeger Security International. 2016.
2. Gaufman E. Security Threats and Public Perception. Digital Russia and the Ukraine Crisis. Springer. 2016.

Skurtul M.,
student
Academy of Economic Studies of Moldova
Scientific supervisor:
Ohrimenco S. A.,
professor
Moldova Economics Academy,
D.Sc. in Economics

PROTECTING CRITICAL INFORMATION INFRASTRUCTURE

The modern world is rapidly developing the vector of digitalization, process automation, cybersecurity in the vast majority of countries. But at the same time, the number of various risks and threats is growing, which can adversely affect each of the areas of critical infrastructure.

To support the identification of the Critical Information Infrastructure (CII) elements, a conceptual model has been developed that represents the various areas of ICT/OT, a number of which need to be monitored for need to be managed at the national level or even at the international level:

1. Key manufacturers. The area is home to a small number of major hardware and software manufacturers operating worldwide. They produce key components for ICT systems. The products of these companies are widely used both in other production areas and in the mass consumer market. Examples include processors, operating systems, and software. But the fact is that not all subcomponents of these products are home-grown. Multiple manufacturers may use the same embedded software libraries created by specialized companies or open source software vendors. When a serious security vulnerability is found and made public in such a product, hundreds of millions of systems in both CII and core services, as well as consumer systems, can become vulnerable overnight. Such vulnerabilities can be actively attacked within hours of becoming public knowledge.
2. Sector of critical communications and IT (ICT). This is a critical element of CII, which provides a national critical core – services and functions of the classical communications industry (wire and cable infrastructure, mobile communications, navigation systems, terrestrial and space segments of satellite communications, broadcasting). The problem in this second area relates to the risk

of foreign influence on the national CII or core services through mergers and acquisitions. Several countries have actively developed or are developing legislation to block foreign takeovers of CII operators.

3. ICT and OT embedded in other CIIs. Major technological changes in embedded ICT and OT in «traditional CI services» such as the energy and financial sectors may necessitate the addition of important new services to the national set of CI and core services. As a result, the criticality of one or more CIIs and essential services may decrease over time. An example of a possible new CII is blockchain infrastructure, including cryptocurrency services, while the use of national beeper infrastructures is rapidly declining as their functionality is replaced by Internet and mobile technologies. The main threat to these systems is interruptions or lack of electricity in general.

4. Critical third party services to ICT service providers. Some services provided by third parties in the ICT sector, such as name and address services, may be critical to CII operations and core services, as well as implicitly CI. Both technological and organizational changes in this area can (imperceptibly) cause shifts in the set of CII. These services support the operation of critical and essential ICT services. They are often provided out of sight and overlooked by the political elite of the state. The main threat may be the active impact of cybercrime in this area, massive attacks on the Internet resources of companies using the services of these organizations. Thus, regulatory measures similar to those applied to CIIs and major operators in the telecom and IT sector(s), for example, could be considered. by applying the same breach reporting requirements that apply to a set of digital service providers.

5. Mass market of ICT. Here we have consumer electronic products. Psychologically, people are dependent on everything that makes their life more convenient, brings us happiness or pleasure. Increasingly, consumer and professional product features rely on IT and OT built into the product. More often than not, these products connect to and interact with the Internet. These mass-produced devices offer great opportunities for cyberattacks, as these products are widely distributed in different countries and are connected to a wide range of telecommunications and Internet service providers.

Summing up, it is worth noting the most important thing – the above is only a small step towards solving big problems. After all, it is the analysis, forecast and understanding of the problem that has arisen that solves it by half. Although problems tend to change constantly, but a number of developed solutions will be able to take the hit and solve them.

References:

1. Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies.

Spinachi V.,
Master student
Academy of Economic Studies of Moldova
Scientific supervisor:
Ohrimenco S. A.,
professor
Moldova Economics Academy,
D.Sc. in Economics

ANALYSIS OF CYBER ATTACKS

Our society is increasingly dependent on the development of information technology. On the one hand, informatization processes concern all aspects of human life, and on the other hand, new challenges and threats to the individual, society and the state are emerging.

The purpose of this work is to consider cyber-attacks as the basis of criminal activity. The digital transformation of all aspects of activity is accompanied by a rapid growth of cyber-attacks on various critical infrastructure facilities. The purpose of cyberattacks is access to personal data, operations management processes, financial reporting results, etc., as well as monetization of the results obtained. Under these conditions, there is a need for a comprehensive analysis of information characterizing all aspects of cyber-attacks. The report presents the results of a study to identify possible scenarios, stages and levels of cyberattacks, highlighting the motives, goals, objects, means of attack used, specific actions and the final result.

The history of attacks on information systems dates back several decades, and it began with the introduction of computer viruses into a personal computer. Over time, cyberattacks have changed significantly in terms of the tools used, penetration methods, and so on. and have become a serious weapon of attack against government and commercial organizations.

Most analysts distinguish targeted or targeted cyber-attacks (APT – Advanced Persistent Threat) into a separate class. A feature of targeted attacks is that attackers are interested in a specific company or government organization. Targeted attacks are usually well planned and include several stages – from intelligence and implementation to as a rule, as a result of a targeted attack, attackers gain a foothold in the infrastructure of the victim and remain undetected for months or even years – during all this time they have access to all corporate information. According to the well-known consulting firm A. Kearney, the main targets of such attacks are the following [1]:

– Office of the board of the company. Often, equipment is not adequately protected from physical damage (for example, by cleaning or maintenance personnel);

– R&D. This is usually the department that requires the highest level of protection, but is often no better protected than other departments;

– Data centers provide a secure environment for hosting a private cloud. The problem is to ensure the secure functioning of numerous servers, as well as applications running on these servers;

– Network of suppliers. With the increasing use of networked solutions for vendors, there are risks associated with the fact that relatively small vendors tend to be less secure;

– Cloud computing. Basically, using an external cloud is secure. The problems are related to the fact that the level of data protection depends on the legislation and that access by intelligence agencies is possible;

– Production. Many old specialized systems are increasingly being networked and difficult to monitor and control. Attacks by intruders in this case can lead to production losses or even to the collapse of the company;

– Databases provide secure storage of important information. The main weakness is that hackers can use administrators as «tools» to break into databases;

– End products activated by information technology.

The growing use of networked solutions to ensure the operation of end products facilitates cyberattacks. By remotely controlling users' devices in order to cause breakdowns, hackers are able to illegally obtain confidential information through these devices. In this regard, the company may face loss of reputation and receive claims from users who have become victims of fraud:

– Office networks. The growing level of networking, involving the interconnection of almost all systems, provides a rich opportunity for a hacker if he can penetrate the network;

– Sales. Leakage of marketing plans, pricing and customer information undermines the reputation of the company and deprives it of competitive advantages;

– Mobile devices. When buying smartphones available on the commercial market, users often enter sensitive data into their memory, which, as a rule, can be easily stolen by hackers. The most tried and true security concepts can be rendered useless when company employees use their own mobile devices for work tasks;

– Online stores. For illegal access under the guise of real buyers and committing fraudulent actions, hackers use credit card details and personal data of customers;

– Phone calls. By exploiting people's willingness to help each other, attackers can use phone calls as a way to easily get the information they need.

The composition of threats is constantly changing and we should expect an increase in the number of negative digital impacts on the resources of information systems.

References:

1. APT – Targeted_or_targeted_attacks. URL: https://www.tadviser.ru/index.php/

Азаров Д. В.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ТЕХНІЧНЕ ОСНАЩЕННЯ ТЕРИТОРІАЛЬНИХ ПІДРОЗДІЛІВ ПОЛІЦІЇ: ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ. ЗАКОРДОННИЙ ДОСВІД

Стрімкий розвиток інформаційних технологій пов'язаний з усіма сферами життєдіяльності. Правоохоронна структура не є виключенням. В Міністерстві внутрішніх справ України постійно відбуваються зміні. Слід зауважити, що зміни є як позитивними так і негативними.

Досить важливу роль в ефективному функціонуванні всієї правоохоронної структури відіграє запровадження новітніх інформаційних технологій. Не останнє місце займає саме технічне обладнання, адже використання сучасних комп'ютерів та інших технічних пристроїв значно покращує роботу поліцейських.

За допомогою комп'ютерів виконується безліч функцій, зокрема, це значно полегшує пошук відповідної інформації щодо конкретної ситуації або правопорушення. Також сучасні технічні пристрої допомагають в роботі з доказовим матеріалом при проведенні різноманітних судових експертиз, які мають невід'ємне значення задля розслідування злочинів. Також новітні технології забезпечують активну взаємодію між всіма територіальними підрозділами поліції [1, с. 21].

Слід зауважити, що проблема сучасного технічного оснащення в правоохоронних органах є досить актуальною проблемою, адже більша частина підрозділів має відповідне технічне обладнання, але воно застаріле. Також досить часто такі пристрої купуються за власні кошти.

У порівнянні з зарубіжними країнами, де оснащення поліцейських підрозділів наявне на досить високому рівні, Україні знаходиться значно в гіршій ситуації.

На нашу думку, перш за все це пов'язано з економічними можливостями кожної країни. Для прикладу, в таких країнах як США та Великобританія технічне оснащення відповідає всім останнім тенденціям, які необхідні задля ефективної діяльності всіх закордонних правоохоронців [2, с. 43].

Науковці вважають, що така ситуація представлена тим, що на правоохоронну структуру виділяється велика кількість бюджету держави та держава може це собі дозволити без збитку для себе.

Окрім США та Великобританії, такі країни як Чехія та Норвегія створили спеціальні фонди підтримки поліцейських райвідділів. Особливість даних фондів полягає в тому, що будь-яка особа може внести благодійний внесок задля покращення технічного оснащення своїх територіальних підрозділів поліції [2, с. 55].

На нашу думку, це є гарним прикладом допомоги від населення, адже якщо держава не спроможна виділяти величезні кошти на надсучасні технології, громадяни, які спроможні виділити такі кошти, або бажають зайнятися благодійністю мають таку можливість. Також, досить позитивним є те, що громадяни, які роблять такі благодійні внески потім бачать той чи інший результат своїх внесків, що відображає прозорість діяльності та звітування поліції перед місцевим населенням.

Варто зауважити, що в Україні, нажаль, відсутні такі благодійні фонди, через те, що в Україні досить низький рівень довіри населення до поліції, що проявляється в відсутності впевненості прозорої діяльності правоохоронців.

Проаналізувавши позитивний закордонний досвід, зокрема досвід США та Великобританії з приводу виділення коштів з державного бюджету, а також досвід Чехії та Норвегії у вигляді створення благодійних фондів є гарними можливими методами вдосконалення технічного оснащення підрозділів поліції.

У підсумку, варто зазначити, що завдяки активній взаємодії поліції з місцевим населенням можливо буде досягти довіри від населення з приводу прозорості, тоді вже можливо запроваджувати такі благодійні фонди. Завдяки допомозі з боку держави та громадян можливо значно поліпшити технічне оснащення своїх територіальних підрозділів. Завдяки надсучасному оснащенню райвідділів вдасться значно підвищити ефективність діяльності поліцейських.

Список використаних джерел:

1. Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС і навчальному процесі: зб. наук. статей за матеріалами доповідей Всеукр. наук.-практ. конф. (м. Львів, 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.
2. Сокуренко В. В. Управління органами Національної поліції України: підручник. Харків: Стильна типографія, 2017. 580 с. URL: http://univd.edu.ua/science-issue/issue/2179.

Анісімов О. Ю.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Калякін С. В.,
викладач кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ

БЕЗПЕКА ОСОБИСТИХ ДАННИХ ТА ОБЕРЕЖНІСТЬ В СОЦІАЛЬНИХ МЕРЕЖАХ ПІД ЧАС ВОЄННОГО СТАНУ

На початку 21-го століття злодій - це не завжди і не обов'язково холоднокровна людина яка хоче зробити щось погане тій або іншій особі [1]. Інформаційна революція призвела до того, що злодієм може бути звичайний студент або навіть школяр або звичайний студент із ноутбуком та доступом до різних видів мережі кіберпростору.

В умовах війни такий злодій є бойовою одиницею, а його основні інструменти – це кібератаки і злами. Окрім того, під час військового стану в країні атаки можливі не лише з боку ворога, який використовує інфопростір для завдання різного виду шкоди обороноздатності України, а й з боку тих, хто вирішив ганебно скористатися цією ситуацією, коли правоохоронні органи перевантажені важливою роботою, та поживитися коштами громадян нашої країни [1]. Протягом останніх місяців війни кіберзлочинність в Україні стабільно зростає.

В наш час війна в інформаційному просторі може завдати не меншої шкоди, ніж війна на справжньому полі бою. Розуміючи це, у перший місяць війни парламент оперативно оптимізував кримінальне та кримінально-процесуальне законодавство, покращивши підстави та процесуальні механізми притягнення до кримінальної відповідальності кіберзлочинців. Зміни зосереджено у двох законах.

Мета таких дій – розкрадання або руйнування інформації в інформаційних системах і мережах. В умовах війни кіберзлочини можуть здійснюватися з метою погіршення ситуації в країні, крадіжки необхідних (конфіденційних) даних, виведення з ладу державних інституцій, техніки, та завдання іншої матеріальної шкоди.

З початку війни стало зрозуміло про велику небезпеку кібератак на Україну: Варто згадати спробу атаки хакерського угруповання Strontium, які намагалися отримати доступ до комп'ютерних мереж в Україні і не тільки, щоб забезпечити тактичну підтримку фізичного вторгнення росії в Україну та викрасти різну важливу конфіденційну інформацію.

Нещодавно Держспецзв'язку повідомило про отримання українськими користувачами нових небезпечних електронних листів з темою «№ 1275 від 07.04.2022» [1], відкриття яких призводить до отримання хакерами повного контролю над вашим пристроєм та загрожує крадіжкою та пошкодженням комп'ютерних даних.

Раніше, 4 квітня, Держспецзв'язку попереджувало про розповсюдження електронних листів з назвою «Військові злочинці росії», відкриття яких призводить до того, що зловмисники отримують віддалений доступ до комп'ютеру жертви.

Під прицілом знаходяться також об'єкти критичної інфраструктури. Український провайдер Укртелеком зазнав потужної атаки 28 березня 2022 року, під час якої хакери намагались проаналізувати, як влаштована ІТ-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії.

23-го березня ворог намагався здійснити кібератаку на державні установи України з використанням шкідливого софту Cobalt Strike Beacon, яка уражає комп'ютер у випадку її відкриття.

Відповідальність за кіберзлочини передбачена розділом XVI ККУ, саме 2 норми із цього розділу і зазнали змін відповідно до нового Закону 2149-IX.

Мета нового Закону 2149-IX полягає у посиленні спроможностей та оптимізація національної системи кібербезпеки для протидії кіберзагрозам [2].

Впровадження дієвих кримінально-правових механізмів протидії кіберзлочинності. Також Закон 2149-IX передбачає, що втручання в роботу інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж не вважатиметься несанкціонованим, якщо таке втручання вчинено відповідно до Порядку пошуку та виявлення потенційних уразливостей таких систем чи мереж, текст якого Держспецзв'язку зараз активно напрацьовує.

Ще до початку війни, після кібератак 14 січня на сайти державних органів влади, відчувалася необхідність запровадження невідкладних змін в українському законодавстві для узаконення процедури Bug Bounty (залучення зовнішніх фахівців до пошуку помилок і уразливостей програмних продуктів, інформаційно-комунікаційних систем тощо). Тож на сьогодні ІТ-спільнота зможе легально тестувати державні інформаційні системи на наявність уразливостей, а держава отримає інструмент для значного підвищення ступеня захисту таких систем.

З іншого боку, запровадження ч. 6 ст. 361 ККУ є логічним продовженням змін у конструкції ч. 1 ст. 361 ККУ. Адже те, про що вказано у частині 6, раніше не визнавалося злочином відповідно до частини 1.

Список використаних джерел:

1. Yerema M., Borysenko A. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. *Lexology*. URL: https://www.lexology.com/library/detail.aspx?g=d37e1715-7526-4626-9cde-26d1f6982c17.

2. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. Ліга законів: сайт. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.

Афанасьєв Д. С.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Рижкова С. А.,
старший викладач кафедри
адміністративного права, процесу
та адміністративної діяльності
Дніпропетровського державного
університету внутрішніх справ

ПРОФІЛАКТИКА ЗЛОВЖИВАННЯ НАРКОТИЧНИХ ЗАСОБІВ НЕПОВНОЛІТНІМИ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

На сучасному етапі розвитку нашої держави, досить актуальною і поширеною соціальною проблемою є вживання наркотичних засобів або психотропних речовин серед молоді

Відповідно до результату останніх досліджень фонду ЮНІСЕФ за 2019 рік 18 % опитаних підлітків повідомили про те, що вони хоча б один раз в житті вживали яку-небудь з наркотичних речовин (серед хлопців – 17,9 %, серед дівчат – 18,1 %). Результати досліджень 2015 року показують, що спочатку відбулося невелике збільшення рівня вживання марихуани, а відповідно аналізу 2019 року зафіксували стабільність рівня поширення серед дівчат та зменшення серед хлопців. Також треба зазначити, що знизився і вік, коли неповнолітні вперше пробують наркотичні засоби, який наразі складає 14-17 років [1, с. 53-54].

З розвитком технологій в Україні, як і у світі загалом наркоділери використовують найсучасніші методи розповсюдження наркотичних речовин: публікації в інтернет-магазинах або у соціальних мережах та мессенджерах, написи на фасадах з адресами нарко крамниць та інші. Сьогодні все популярнішим методом продажу наркотиків стає публікації в Telegram-каналах. Завдяки цьому, наркодилерство стало більш анонімною діяльністю ніж раніше.

Національна поліція разом з громадськістю протидіє поширенню наркотиків у всіх сферах його можливого прояву. Кіберпростір не є тому виключення. Курсанти факультету кіберполіції Харківського національного університету внутрішніх справ розробили чат-бот «СтопНаркотик», який покликаний об’єднати зусилля громадян у блокуванні у месенджері Telegram електронних адрес користувачів, ботів та чатів, якими користуються дилери з метою пропаганди вживання наркотиків та їх незаконного збуту. До користувачів чат-боту вже долучилось понад 30 тисяч осіб, серед яких не тільки мешканці України, а й зарубіжних країн. За їх допомогою, вже заблоковано

не лише майже 1600 електронних адрес нарко крамниць, але й адреси, які використовувалися для вчинення інших злочинів: продаж підроблених банкнот України; шахрайство; розміщення фейкових новин та інших повідомлень [2]. На основі такого чат-боту правоохоронними органами були створені й інші, наприклад чат-бот «ДійПротиНаркотиків», у якого принцип діяльності також базується на основі співробітництва з громадськістю. Для повідомлення про обіг наркотиків користувач має вказати: населений пункт; адресу, за якою побачили потенційного зловмисника; опис місця, де на думку заявника може бути схованка, так звана «закладка». Дуже корисною є можливість надіслати геолокацію, а також фото й відеоматеріали з місця, де були приховані наркотики [2].

Як і в нашій державі, в Японії теж звернулись до сучасних ІТ-технологій. Спеціалісти створили чат-бот «Anti-Drug Buddy» для поширення загальних знань про наркотики та їх шкідливий вплив на організм людини, а також підвищення обізнаності людей щодо боротьби з наркотиками. Цей чат-бот вже працює онлайн та налічує близько двохсот користувачів, які є кваліфікованими лікарями та, на сьогоднішній день, мають понад 500,000 запитів та відповідей на них. У цій специфічній сфері боротьби з наркотиками «Anti-Drug Buddy» може відповісти користувачеві на такі запити: інформація про наркотики; як боротися з проблемами наркотиків; останні новини та інформація про боротьбу з наркотиками [3].

Отже, на підставі вищезаначеного профілактичні заходи органів та підрозділів Національної поліції шодо зловживання наркотичних засобів неповнолітніми з використанням інформаційно-телекомунікаційних технологій, в тому числі за допомогою месенджерів є надійним ефективним та перспективним методом роботи з молоддю, який потребує подальшого розвитку та дослідження.

Список використаних джерел:

1. Балакірєва О. М., Павлова Д. М. та ін. Куріння, вживання алкоголю та наркотичних речовин серед підлітків, які навчаються: поширення й тенденції в Україні: за результатами дослідження 2019 року в рамках міжнародного проекту «Європейське опитування учнів щодо вживання алкоголю та інших наркотичних речовин – ESPAD». К. : ТОВ «ОБНОВАКОМПАНІ», 2019. 214 с.
2. Підсумки роботи чат-боту «СтопНаркотик» за рік. URL: https://osvita.mvs.gov.ua/news/pidsumki-roboti-chat-botu-stopnarkotik-za-rik.
3. Поліція запустила чат-бот «Мисливці за наркотиками». Як він працюватиме. URL: https://suspilne.media/179262-policia-zapustila-cat-bot-mislivci-za-narkotikami-ak-vin-pracuvatime/
4. The 35th Annual Conference of the Japanese Society for Artificial Intelligence, 2021. URL: https://www.ai-gakkai.or.jp/jsai2021/en.

Батура Д. В.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТ-РЕСУРСАХ

На початку XXI століття стрімко почали розвиватися інформаційні технології, які і наразі є невід'ємною частиною нашого життя. Тим самим, технологічний процес створює для нас все ширше коло потреб та можливостей для обробки та збору персональних даних, а самі персональні дані використовуються в найрізноманітніших сферах, починаючи від соціальних мереж та закінчуючи бізнесом і політикою. І їх використання стає багатогранним, окрім допомоги в роботі та побуті, вони, також можуть існувати для декого інструментом порушення прав та свобод людини,а саме порушення права на приватність.

Тому, розвиток системи захисту персональних даних є одним із найактуальніших завдань на сучасному етапі становлення розвитку суспільства та інформаційних технологій. Захист персональних даних та його вдосконалення є не просто обов'язком держави, але й предметом державно-правового регулювання, тим самим – це повинно розглядатися, як захист прав та свобод людини, в поєднанні з захистом її приватного життя. Створення дієвої системи захисту персональних даних належить до міжнародних зобов'язань України [1].

На сьогодні, де б ми не звернулися, всюди потрібно зазначати свої дані, незалежно від того, соціальні мережі це, надання послуг чи інші обставини. Та доволі часто, люди свідомо зазначають їх, не підозрюючи, що ці дані можуть в майбутньому використовуватися проти них в шахрайських схемах чи в інших протиправних діяннях. Особливо в карантинний період збільшилася кількість комунікацій в електронному просторі і захист персональних даних став актуальною проблемою. Тим паче, що останнім часом персональні дані українських громадян періодично з'являються в мережі Інтернет.

Отже, щоб захистити свої особисті дані, по-перше, перед тим як надавати згоду на обробку персональних даних слід ознайомитись з метою, процедурами обробки персональних даних, а також політикою конфіденційності. По-друге, не повідомляти особисті дані особам, з якими не плануєте укладати юридичні правочини, а також, залишати у цифрових сервісах, якими користуєтесь

мінімально необхідний набір даних для користування ними. По-третє, не дозволяти обробку особистих даних, якщо від вас вимагають інформацію в більшому обсязі, ніж потрібно для повідомленої вам мети обробки персональних даних. До того ж, винятки з цього правила можуть визначатися лише за законом. По-четверте, коли припиняються відносини з володільцем персональних даних, а саме, особою, яка відповідно до закону чи договору уповноважена визначати мету та підстави обробки персональних даних, вимагати видалення чи знищення інформації про себе [2].

У разі, якщо відбулася незаконна обробка персональних даних або ж відбулося втручання в особисте життя особи, то суб'єкт персональних даних може звернутися до того, хто володіє або розпоряджається персональними даними з вмотивованою вимогою, а саме: заборонити таку обробку, змінити свої персональні дані (у випадку, якщо вони є недостовірними) та вимагати їх видалення або ж знищення.

Але, якщо цю вимогу суб'єкта персональних даних не буде виконано, то особа в праві оскаржити вказані дії чи бездіяльність того, хто володіє чи розпоряджається персональними даними, звернувшись до Уповноваженого Верховної Ради України з прав людини або до суду [3].

Захист персональних даних дійсно є проблемою. Доволі часто відбувається витік інформації та персональних даних в мережу Інтернет, через те, що законодавство не може в повній мірі забезпечити гарантований захист прав і свобод громадян. Проблема в тому, що законодавство не має реального діючого механізму, який би гарантував захист наших персональних даних. Тому, необхідно посилити дію законодавчих актів та механізм покарання за незаконне використання персональних даних та витік інформації в мережу Інтернет.

Отже, враховуючи вище викладене, можна зробити висновок, що захист персональних даних є актуальною проблемою. Тому, щоб запобігти порушенню прав і свобод людини та втручання в приватне життя необхідно уважно ознайомлюватися з умовами, перед тим як надавати згоду на обробку ваших особистих даних. Це допоможе запобігти правопорушенням та втручанням в приватне життя особи.

Список використаних джерел:

1. Авдєєва Г. К. Використання спеціальних знань у боротьбі з комп'ютерною злочинністю. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2016. Вип. 1. С. 268-277.
2. Крилова Ю. І. Захист персональних даних : вітчизняний та зарубіжний досвід (ст. 57-63). URL: http://ippi.org.ua/krilova-yui-zakhist-personalnikh-danikh-vitchiznyanii-ta-zarubizhnii-dosvid-st-57-63.
3. Про захист персональних даних: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

Бєльєва Н.В.,
ад'юнкт
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Гребенюк А. М.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ПРИТЯГНЕННЯ ЗАВІДОМО НЕВИННОГО ДО КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ З МЕТОЮ ПОКРАЩЕННЯ ПОКАЗНИКІВ ПРОФЕСІЙНОЇ ДІЯЛЬНОСТІ

У Конституції України закріплено, що людина, її життя, здоров'я, честь і гідність, недоторканість і безпека визнаються в Україні найвищою соціальною цінністю. Особливу роль у забезпеченні охорони зазначених цінностей належить державним органам, що здійснюють діяльність у сфері правосуддя [1].

Право кожної особи на справедливий розгляд її справи неупередженим судом гарантоване ст. 10 Загальної декларації прав людини 1948 року, ст. 6 Конвенції про захист прав людини і основоположних свобод 1950 року та ст. 14 Міжнародного пакту про громадянські і політичні права 1966 року [2-4]. Положення цих міжнародно-правових документів відображені в Конституції України та вітчизняних нормативних актах. Справедливе судове рішення має бути підтверджено та обґрунтовано достовірними доказами, які відтворюють усі фактичні обставини справи чи події. Однак аналіз судової практики свідчить про чималі випадки вчинення як працівниками правоохоронних органів, так і учасниками процесу, протиправних дій із доказами у різних формах судочинства, що перешкоджає здійсненню законного правосуддя та призводить до вкрай негативних наслідків.

Стаття 62 Конституції України проголошує, що особа вважається невинуватою у вчиненні злочину і не може бути піддана кримінальному покаранню, доки її вину не буде доведено в законному порядку і встановлено обвинувальним вироком суду [1]. При цьому обвинувачення не може ґрунтуватися на доказах, одержаних незаконним шляхом. У разі порушення цих вимог настає відповідальність за ст. 372 Кримінального кодексу України як за спеціальний вид (відносно ст. 364 Кримінального кодексу України) службового зловживання [5].

Незважаючи на високі вимоги, які пред'являються законодавством України до діяльності державних органів, ситуація у цій сфері є вкрай

негативною. Спостерігається чимало порушень під час досудового розслідування кримінальних проваджень: недотримання процесуальних норм, односторонність і неповнота розслідування справ тощо. Одним з найбільш небезпечних порушень у цій сфері є притягнення завідомо невинних до кримінальної відповідальності, як специфічний прояв зловживання владою або службовим становищем.

Приклади:

1. *Старший оперуповноважений К., вступивши у змову зі слідчим С. задля покращення показників професійної діяльності, змусив наркозалежного громадянина О., який перебував у СІЗО на території області, зізнатися у вчиненні крадіжок, які він не скоював. За це правоохоронець пообіцяв надати йому наркотичний засіб. У подальшому слідчий оперуповноважений, без слідчих дій та свідків штучно створив докази з фіктивними відомостями про обставини нібито вчинених злочинів, які скерував слідчому для долучення до матеріалів кримінального провадження. Той, у свою чергу, достовірно знаючи про непричетність громадянина до вчинення кримінальних правопорушень, використав зібрані «докази» та повідомив громадянину про підозру, а згодом направив обвинувальний акт до суду, чим притягнув потерпілого до кримінальної відповідальності[6].*

2. *Начальник рійвідділення поліції області переконав свого підлеглого В., начальника сектору кримінальної поліції, створити штучні умови для покрашення статистики з розкриття злочинів, пов'язаних із розкраданням лісу. Для цього правоохоронці запропонували місцевому мешканцю грошову винагороду в обмін на зізнання у вирубі дерев. Надалі обіцяли сприяти йому в ухиленні від покарання у вигляді позбавлення волі. Для реалізації злочину поліцейські відвезли громадянина в ліс, де вже були зрубані 9 дерев, вручили бензопилу і пальне до неї та викликали слідчо-оперативну групу. Слідча М. знаючи, що людина не має відношення до скоєння злочину, повідомила потерпілому про підозру у незаконній порубці деревини (ч. 1 ст. 246 Кримінального кодексу України). У рамках кримінального провадження задокументовано передачу поліцейськими потерпілому коштів у якості винагороди за зізнання в злочині, який той не вчиняв [6].*

Вищевказані приклади вказують на те, що це робиться з метою покращення показників професійної діяльності відділів та відділень органів поліції.

Так, з моменту набрання чинності Кримінального процесуального кодексу України 20 листопада 2012 року, одночасно запрацював Єдиний реєстр досудових розслідувань [7].

Єдиний реєстр досудових розслідувань (ЄРДР) – це створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення даних про кримінальні правопорушення та хід досудового розслідування у кримінальних провадженнях. Досудове розслідування розпочинається з моменту внесення відомостей до ЄРДР. Відомості з реєстру надаються у вигляді витягу. Порядок ведення реєстру затверджений наказом Генеральної прокуратури України від 6 квітня 2016 № 139 [8].

Водночас, відомості, які вносяться до Єдиного реєстру досудових розслідувань вносяться і до ІПНП «Кримінальні провадження» [9].

Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (ІПНП) – це сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення.

ІПНП «Кримінальні провадження» – це облік відомостей про кримінальні правопорушення, осіб, які їх вчинили або підозрюються в їх вчиненні, досудове розслідування за якими здійснюється слідчими органів поліції.

Подалі, з відомостей, які вже внесені до ІПНП «Кримінальні провадження» формується статистичні дані показників підрозділів поліції у «Форму-200», яка складається з кількості зареєстрованих злочинів, кількості кримінальних проваджень, по яких особі повідомлено про підозру (розкрито), направлено до суду тощо.

З вищезазначеної форми потім робляться звіти про результати роботи відділів та відділень поліції, які бачить керівництво та робить відповідні висновки про розкриття злочинів.

Отже, задля таких показників статистики, які вказані у прикладах, деякі працівники поліції йдуть на службові злочини.

Протидія злочинам, які вчиняють службові особи у сфері правосуддя, є важливим завданням для становлення України як демократичної та правової держави. Шкода, якої завдають такими діями, полягає не лише у порушенні законних прав та інтересів людей, а й у їх зневірі до діяльності державних органів, насамперед – правоохоронних, судових та прокуратури, у підриві престижу і авторитету цих структур.

Список використаних джерел:

1. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр/Text.
2. Загальна декларація прав людини 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text.
3. Конвенція про захист прав людини і основоположних свобод 1950 року. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text/
4. Міжнародний пакт про громадянські і політичні права 1966 року. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text/
5. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
6. Судова влада України. URL: https://court.gov.ua/fair/.
7. Кримінальний процесуальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

Блохіна О. А.,
ад'юнкт
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Гребенюк А. М.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

АНАЛІЗ І ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ «ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ» ТА ЇЇ ПІДСИСТЕМИ ІП «ПОСТАНОВИ ВИКОНАВЧОГО ПРОВАДЖЕННЯ» ІПНП В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Для виконання покладених завдань, органи Національної поліції користуються повноваженнями у сфері інформаційно-аналітичного забезпечення згідно ст. 25-27 Закону України «Про Національну поліцію», згідно з якими в рамках своєї діяльності вони можуть: формувати реєстри та бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; користуватися реєстрами та базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; здійснювати інформаційно-пошукову та інформаційно-аналітичну роботу та інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями [1].

В єдиній інформаційній системі МВС (далі – ЄІС МВС) виділяють функціональні підсистеми якими користуються відповідні підрозділи Національної поліції. Відповідно до предмету дослідження із них більш детально проаналізуємо Інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» (далі – система ІПНП), яку було розроблено з метою організації інформаційно-аналітичної підтримки поліції, та одну із її складових підсистем ІП «Постанови виконавчого провадження» ІПНП.

Відповідно до Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України», затвердженого Наказом Міністерства внутрішніх справ України від 03.08.2017 № 676, система ІПНП – є сукупністю технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення. Основними завданнями системи ІПНП є: інформаційно-аналітичне забезпечення діяльності Національної поліції України; забезпечення наповнення та підтримки в актуальному стані

інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС; забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу; забезпечення електронної взаємодії з МВС та іншими органами державної влади [2, 4].

Призначення системи ІПНП полягає в:

– формуванні інформаційних ресурсів ЄІС МВС;

– обробці інформації, яка утворена в процесі діяльності поліції;

– аналітична обробка інформації, отриманої з автоматичної фото- і відеотехніки;

– наданні безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС;

– генерації інтерфейсів та функціонування вебсервісів для здійснення інформаційної взаємодії органів (підрозділів) поліції з іншими органами державної влади, органами правопорядку іноземних держав, міжнародними організаціями;

– здійсненні пошукових та аналітичних функцій для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади в межах службової діяльності відповідно до рівня доступу і повноважень за запитом або регламентом;

– використанні програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об’єкта в залежності від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах;

– забезпеченні автоматизації процесів управління силами та засобами поліції;

– забезпеченні електронного документообігу в органах (підрозділах) поліції, обміну електронними документами з МВС;

– комплексному захисті інформації та розмежування доступу до інформації, що зберігається в базах даних системи ІПНП [2].

Власником системи і розпорядником інформації ІПНП є Національна поліція України, а її адміністратором - уповноважений структурний підрозділ апарату центрального органу управління Національної поліції України.

Користувачами системи ІПНП є:

– посадові особи органів (підрозділів) поліції, яким в установленому порядку надано відповідні права доступу до інформації в системі ІПНП;

– фізичні особи та інші уповноважені посадові особи суб’єктів ЄІС МВС, яким в установленому порядку надано відповідні права доступу до інформації в ЄІС МВС [2].

В системі ІПНП детально розглянемо інформаційну підсистему ІП «Постанови виконавчого провадження» ІПНП, яка узагальнює відомості про постанови державних виконавців щодо обмеження прав боржників у керуванні транспортними засобами та користуванні зареєстрованою зброєю.

Ведення обліку даної інформаційної підсистеми здійснюється автоматично відповідно до вимог наказу МВС, МінЮсту України від 31.01.2018 р. № 64/261/5 «Про затвердження Порядку взаємодії Міністерства внутрішніх справ України, Національної поліції України та органів і осіб, які здійснюють примусове виконання судових рішень і рішень інших органів» [3].

Функціонування механізму взаємодії усіх складових підрозділів, які приймають участь у обмеженні прав боржників у керуванні транспортними засобами починається з державного підприємства «Національні інформаційні системи», яке забезпечує передачу від автоматизованої системи виконавчого провадження (АСВП) до Єдиного державного реєстру МВС (ЄДР) запитів про зареєстровані за боржником транспортні засоби, сформованих державними, приватними виконавцями. В подальшому Головний сервісний центр МВС (далі – ГСЦ МВС) забезпечує передачу відповідей на запити про зареєстровані за боржником транспортні засоби від ЄДР до АСВП. Останнім етапом є: постанова про арешт майна боржника, винесена під час примусового виконання рішення, яка надсилається до ЄДР в електронному вигляді з використанням електронного цифрового підпису (далі – ЕЦП) державного, приватного виконавця, який виніс відповідну постанову, через АСВП [3].

Якщо арешт майна припиняється, то державний або приватний виконавець виносить постанову, яка надсилається до ЄДР в електронному вигляді з використанням їх ЕЦП через АСВП.

Під час розшуку транспортних засобів боржника у виконавчому провадженні, підставою для залучення поліцейських до розшуку транспортного засобу боржника є постанова державного, приватного виконавця про такий розшук, яка надсилається до ІПНП в електронному вигляді з використанням їх ЕЦП через АСВП. Про виявлення та затримання транспортного засобу боржника, оголошеного в розшук, поліцейський інформує державного, приватного виконавця шляхом надсилання повідомлення через ІПНП до АСВП».

Якщо тимчасове обмеження боржника у праві керування транспортними засобами припиняється , то постанова державного виконавця надсилається до ЄІС в електронному вигляді з використанням ЕЦП державного виконавця, який виніс відповідну постанову, через АСВП» [3].

Постанови про встановлення тимчасового обмеження боржника у праві користування вогнепальною мисливською, пневматичною та охолощеною зброєю, пристроями вітчизняного виробництва для відстрілу патронів, споряджених гумовими чи аналогічними за своїми властивостями метальними снарядами несмертельної дії, та припинення дії таких постанов, надсилаються до ЄІС в електронному вигляді з використанням ЕЦП державного виконавця, який виніс відповідну постанову, через АСВП.

Таким чином, враховуючи все вищевикладене, можна прийти до висновку, що використання системи ІПНП і її складових підсистем, це складний взаємопоєднаний механізм дії різних користувачів і підрозділів для отримання загального результату, який полягає у накопиченні, обробці та опрацюванні на практиці інформаційних ресурсів, з метою покращення та оптимізації функціонування підрозділів Міністерства внутрішніх справ, у тому числі Національної поліції України.

Список використаних джерел:

1. Про Національну поліцію: Закон України від 02.07.2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.
2. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України»: наказ МВС України від 03.08.2017 р. № 676. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.
3. Вишня В. Б., Ісмайлов К. Ю., Краснобрижий І. В. Інформаційні технології: підручник. Дніпро : ДДУВС, 2021. 492 с. URL : https://er.dduvs.in.ua/handle/123456789/6820.
4. Утвенко В. В. Проблематика удосконалення інформаційного забезпечення правоохоронних органів. Економічна та інформаційна безпека: актуальні питання та інновації: матер. Міжнар. наук.-практ. конф. (м. Дніпро, 4 листопада 2021 р.). Дніпро : ДДУВС, 2021. С. 389-391. URL: https://er.dduvs.in.ua/handle/123456789/8519.

Богомол А. І.,
курсант
Дніпропетровського державного
університету внутрішніх справ,
Науковий керівник:
Паршин Ю. І.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

ФІНАНСОВІ РОЗСЛІДУВАННЯ ЯК ПЕРЕДУМОВА ЗАБЕЗПЕЧННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ УКРАЇНИ

Останнім часом спостерігається зростання інтересу до питань безпеки. Безпека країни, суспільства, підприємництва і громадянина активно обговорюється в ЗМІ. За своєю суттю безпека – це стан мінімальної залежності від різного роду ризиків. Людина відчуває себе в безпеці, якщо в будь-якому випадку його стан і відчуття залишаються незмінними. Те ж саме можна сказати і про безпеку підприємства або держави. Потреба в безпеці, захисті від небажаних зовнішніх впливів і внутрішніх змін на життя окремої людини, сім'ї, власності, різних об'єднань людей, включаючи суспільство і державу, відноситься до типу основних фундаментальних потреб. Ідеї вивчення проблем забезпечення економічної безпеки почали проникати в нашу країну з початком перебудови. У 90-х роках XX століття в статтях економістів і в ЗМІ все частіше стала лунати стурбованість з приводу втрати економічної безпеки України [2].

У сучасній літературі економічна безпека розглядається як початкова основа зовнішньоекономічних видів безпеки, стабільного, сталого розвитку

держави і суспільства. Такий підхід об'єднує інші види безпеки, ускладнює визначення предметних областей аналізу політичної, військової, екологічної, інформаційної, технологічної та іншої безпеки [1]. Нестабільність економічного стану в Україні останнім часом має дуже загрозливий характер для її національної безпеки. Вона насамперед пов'язана з переділом українських земель, політичною нестабільністю, яка спричинена і внутрішніми, і зовнішніми факторами впливу, катастрофічним розвитком кримінальної економіки та розкраданням державного майна, переведення коштів у «тінь» із подальшим його використанням для розвитку кримінально-тіньової економіки.

Створюючи підрозділ фінансової розвідки в Україні, потрібно зважати на загальні характеристики правової системи країни та існуючі переваги й недоліки державних відомств, до складу яких може входити такий підрозділ. Деякі схеми розміщення розвідки у структурі органів державного управління розробляються з урахуванням конкретних особливостей адміністративно-правових систем тієї або іншої країни. Аналогічно необхідно оцінити відносні переваги та недоліки відомств, до системи яких потенційно може входити ПФР, оскільки видається не виваженим створювати даний підрозділ у межах адміністративного органу, який не має реального впливу [1]. Для забезпечення успіху необхідна політична підтримка. Вона потрібна не тільки задля гарантування ухвалення закону про створення відповідного органу, а й для того, щоб на постійній основі забезпечувати отриманнядостатніх бюджетних ресурсів для досягнення обраних цілей.

Упродовж багатьох років країни створювали підрозділи фінансової розвідки із загальною метою – для боротьби з відмиванням грошей [2]. У деяких країнах підрозділи організовується у структурі правоохоронного відомства, оскільки це найпростіший спосіб сформувати орган із відповідними правоохоронними повноваженнями без необхідності створювати нові адміністративно-правові основи. У операційному аспекті за такої схеми організації ПФР тісно взаємодіятиме з іншими правоохоронними підрозділами, зокрема з підрозділом боротьби з фінансовими злочинами, і зможе користуватися накопиченими цим підрозділом знаннями і практичним досвідом, а також його джерелами інформації [3]. Своєю чергою, інформація, отримана фінансовою розвідкою, стане доступнішою для правоохоронних органів і може бути використана в будь-якому розслідуванні, що підвищує її корисність. Обміну інформацією також може сприяти використання існуючих національних і міжнародних мереж. Проте, забезпечення економічної безпеки країни не є прерогативою якогось одного державного відомства або служби. Вона повинна підтримуватися всією системою державних органів, усіма ланками і структурами економіки.

Беручи до уваги вищевикладене, слід зауважити, що підрозділи фінансової розвідки полегшать виконання основного завдання – забезпечаеня національної економічної безпеки. Що, в свою чергу, передбачає діяльність із захисту економіки країни від небажаних і небезпечних впливів з точки зору можливих

наслідків. Стабільність і безпека – найважливіші параметри руху будь-якого соціального явища, характеристики економіки як єдиної системи. Стабільність економіки характеризує надійність і міцність його конструктивних елементів, зовнішніх і внутрішніх, горизонтальних, вертикальних та інших комунікацій цієї системи, здатність витримувати внутрішні і зовнішні впливи. Ефективно організована економічна безпека повинна створювати необхідні умови для забезпечення здатності економіки до саморозвитку і динамічного, стійкого, прогресивного руху.

Список використаних джерел:

1. Власюк О. Деякі аспекти внутрішньої економічної безпеки. URL: www.receps.com.ua/ukr/all/ journal/
2. Жихор О. Б. Економічна безпека: підручник з грифом МОНУ. К. : УБС НБУ, 2015. 467 с. URL: www.studmed.ru/zhihor-o-b-kucenko-t-m-ekonom-chna-bezpeka_7752503d01f.html.
3. Гальчинський А. С., Єщенко П. С., Палкін Ю. І. Основи економічної теорії. К. : Вища школа, 2015. 471 с.

Богуслав І. Д.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ЗДІЙСНЕННЯ ОПЕРАТИВНО-РОЗШУКОВИХ ЗАХОДІВ В МЕРЕЖІ ІНТЕРНЕТ

Вплив інформаційної сфери в розвитку сучасного суспільства призводить як до безсумнівним позитивним результатам, до розширення джерел соціальної небезпеки, зокрема пов’язані з явищами кримінального плану. Неухильно зростає кількість злочинів, скоєних з використанням інформаційно-телекомунікаційних технологій, значний і завданий ними збиток. Кіберзлочинність набуває все більш небезпечних форм, одержуючи при цьому яскраво виражений транснаціональний характер [1]. Відбувається зміна мотивації відповідної протиправної діяльності, активно освоюються нові її сфери. Наголошується на посиленні організованості кримінальних структур, які використовують можливості Інтернету для здійснення злочинної

діяльності та збору даних про потенційні жертви. Такі структури удосконалюють способи приховування слідів злочинів, намагаються отримати доступ до інформаційних систем правоохоронних органів. Всі ці факти вказують на те, що боротьба зі злочинністю в мережі Інтернет неможлива без застосування оперативно-розшукових сил, засобів та методів.

При аналізі впливу кіберпростору на зміст оперативно-розшукових заходів (ОРЗ), що застосовуються в ньому, важливо враховувати, що, з одного боку, цей простір прив'язаний до існуючої географії світу фізичними мережевими об'єктами (серверами, мережевим обладнанням, каналами зв'язку, комп'ютерами користувачів і т.п.), з іншого боку, воно має особливі «надгеографічні» і транскордонні властивості: державні кордони йому прозорі, у ньому відсутня фіксована топологія, воно постійно змінюється, модернізується, розширюється [2]. У разі скоєння в кіберпросторі злочину, як правило, можна встановити фізичне місце знаходження злочинця та жертви, а також місця збереження слідів в апаратних пристроях мережевої інфраструктури, проте спроба просторово локалізувати певні інформаційні об'єкти може залишитися безрезультатною. У кіберпросторі злочинець здатний одночасно здійснювати низку різних операцій у кількох обчислювальних системах, причому можливе здійснення дистанційних дій, у яких вплив виробляється інформаційний об'єкт, що знаходиться на значній відстані або не має фізичної прив'язки до конкретного місця. Певні операції можуть виконуватися з мобільних пристроїв (ноутбуків, смартфонів, планшетів тощо), тоді як їхній оператор переміщається у фізичному просторі. У подібних випадках можна в певному сенсі говорити про «розмивання» фізичного місця скоєння злочину, порушення його просторової локалізації. Крім того, в кіберпросторі застосовні методи, що дозволяють здійснювати заміну даних, що відображають реальне розташування певного суб'єкта або об'єкта. Подібні методи активно використовуються і для формування так званого тіньового Інтернету (dark net), що створює умови для функціонування майданчиків анонімного спілкування та торгівлі забороненими для поширення товарами та послугами (наркотики, зброя, дитяча порнографія, блокування сайтів тощо). Виявлення таких майданчиків та контроль над ними з боку правоохоронних органів становить особливу проблему.

Важливою умовою ефективного проведення ОРЗ у мережі Інтернет є знання особливостей злочинів, які відбуваються у мережному просторі. Такі злочини мають помітні особливості з погляду їхнього оперативно-розшукового документування. До кіберзлочинів належать передбачені кримінальним законодавством суспільно небезпечні діяння, вчинені на основі віддаленого доступу до об'єкта зазіхання з використанням ресурсів мережі Інтернет як основний засіб досягнення мети. У сукупність таких злочинів в основному потрапляють навмисні, ретельно плановані та масковані злочини [3]. Діапазон кіберзлочинів досить широкий. Серед найбільш поширених в Інтернеті злочинів можна назвати: неправомірний доступ

до комп'ютерної інформації; створення, використання та розповсюдження шкідливих програм для ЕОМ; порушення авторських та суміжних прав; поширення порнографії за участю неповнолітніх; здирництво; шахрайство; збут підроблених кредитних карток; розкрадання коштів із банківських рахунків; порушення недоторканності приватного життя; незаконне отримання та розголошення відомостей, що становлять комерційну таємницю; заподіяння майнової шкоди шляхом обману чи зловживання довірою; збудження національної, расової чи релігійної ворожнечі та ін.

Злочини, що відбуваються в мережі Інтернет, як правило, характеризуються підвищеною скритністю вчинення, що забезпечується за рахунок складності інфраструктури мережі та розвинених механізмів анонімності. Багато злочинів мають транскордонний характер, у якому злочинець, об'єкт злочинного посягання, жертва перебувають під юрисдикцією різних держав. Способи скоєння злочинів та застосовуваних спеціальних засобів відрізняються нестандартністю, складністю, різноманіттям та частим оновленням. При цьому реалізація складних сценаріїв може перетворити окремі комп'ютери на потужну зброю скоєння злочину при об'єднанні щодо слабких ресурсів. Прикладом цього є організація ретельно спланованих масштабних DDoS-атак, в яких задіяні тисячі заздалегідь «заражених» комп'ютерів, що централізовано керуються злочинцем для досягнення єдиної протиправної мети.

Список використаних джерел:

1. ОДУВС – Одеський державний університет внутрішніх справ. URL: https://oduvs.edu.ua/wp-content/uploads/2016/09/2-6.pdf.
2. Зняття інформації з транспортних телекомунікаційних та електронних інформаційних систем. План-конспект лекції. Оперативно-розшукова діяльність. URL: http://ord-irina.pp.ua/Зняття-інформації-з-транспортних-тел-1/
3. Бандурка О. М., Блажівський Є. М. та ін. Кримінальний процесуальний кодекс України. Науково-практичний коментар: у 2 т. Т. 1. Харків: Право, 2013.

Болобан Р. Ю.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Калякін С. В.,
викладач кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ

ДОСВІД ТЕХНОЛОГІЧНИХ ІННОВАЦІЇ ПОЛІЦІЇ СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ ЯКІ ДОПОМАГАЮТЬ ВИЯВЛЯТИ ЗЛОЧИНІ

Навіть побіжний огляд історичного розвитку наших зусиль із запобігання злочинності підкреслює важливість технології, точніше, технологічних інновацій була рушійною силою, яка призвела до реформування стратегій запобігання злочинності та боротьби зі злочинністю, як окремими громадянами та зацікавленими групами, так і офіційними поліцейськими органами. Існує два загальних типи технологічних інновації, які можна визначити: інформаційні технології (на які ми будемо посилатися тут як м'які технології) і технології, засновані на матеріалах (на які ми будемо посилатися тут як жорсткі технології). Обидва типи технологічних інновацій були пов'язані з «драматичними змінами в організації поліції» [1], особливо з кінця минулого століття, тоді як подібні зв'язки можна запропонувати для більш загальної профілактики, які використовують окремі особи та групи жителів.

В останні роки було розроблено цілу низку нових інновацій у галузі «м'яких» технологій, які використовуються як інструмент попередження злочинності [1]. Останні технологічні інновації включають останнє покоління інструменти класифікації ризиків правопорушників, поява протоколів оцінки загроз, інструменти виявлення хуліганів, програми, розроблені для запобігання злочинам.

Інструменти ідентифікації, програми, розроблені для запобігання крадіжці особистих даних та захисту конфіденційності даних, нові інструменти для моніторингу місцезнаходження та переміщення груп населення схильних до ризику, наприклад: психічно хворих і сексуальних злочинців [2]. Зовсім недавно з'явилися нові інструменти оцінки, призначені для виявлення осіб, які можуть стати жертвами домашнього насильства. Розроблені виявлення осіб, які можуть стати злочинцями (або жертвами) вбивств у визначені терміни. У той час як рівень впровадження кожної з цих нових технологій важко оцінити, ми можемо запропонувати таку попередню оцінку.

Сполучені Штати інвестували значні ресурси у «м'які» технології запобігання злочинності. Наприклад, вони відстежують місцезнаходження та переміщення приблизно 800 000 зареєстрованих осіб, які вчинили злочини на сексуальному ґрунті в Сполучених Штатах, за допомогою національної системи реєстрації осіб, які вчинили злочини на сексуальному ґрунті [2]. За допомогою національної системи реєстрації сексуальних злочинців, здатної забезпечити повідомлення громади про будь-якого нового сексуального злочинця, що прибув, та повідомлення правоохоронних органів про цих злочинців, які не зареєструвалися або порушили обмеження на місцезнаходження. Ризик рецидивізму серед цієї групи правопорушників, як правило, класифікується (високий, помірний, низький) на підставі проходження одного з багатьох інструментів оцінки ризику, які були введені останніми роками (наприклад, RRASOR, Static-99, SORAG, MnSOST, SONAR, SVR-20 для сексуальних злочинців) [2].

США також може використовувати картографічні програми ГІС у поєднанні з національними та окремими базами даних реєстру штатів для вивчення місцезнаходження правопорушників та оцінки впливу обмежень на проживання сексуальних злочинців на профілактику злочинності.

Другою галуззю важких фінансових інвестицій є оцінка ризиків управління. 7,5 мільйонів правопорушників [2], які зараз перебувають під виправним контролем у Сполучених Штатах, спирається на використання актуарно обґрунтованих систем класифікації ризиків. Запобігання злочинам, скоєним правопорушниками, коли вони після виходу з в'язниці чи умовно-дострокового звільнення, останніми роками привертає значну увагу та фінансову підтримку.

Третя область інновацій у сфері «м'яких» технологій, пов'язаних із запобіганням злочинності, що отримала значну увагу та фінансування після 11 вересня – це оцінка загроз. Менш ніж за десять років було створено цілу індустрію, засновану на простому понятті: можна визначити загрозу (тобто ймовірність) терористичної атаки та/або серйозної насильницької події, що відбувається на одному з таких об'єктів: аеропорти, атомні електростанції, школи, вокзали, урядові будівлі та приватні компанії [1]. У поєднанні з оцінкою загроз проводиться оцінка вразливості: що ми можемо і маємо зробити, щоб запобігти цій загрозі? Середня вартість цих оцінок варіюється від постачальника до постачальника та від об'єкта до об'єкта. В одному з нещодавніх звітів зазначається, що оцінка погроз та вразливостей в окремій школі може коштувати від 25 доларів США. Оцінка вразливості може коштувати від $25 000 до $50 000, а у коледжах – значно більше [2].

Висновки. Завдяки дослідженням і прикладу США можна зробити висновок, що за останній час з'явилось багато технологій які допомагають і покращують службу поліції. Якби Україна мала всі сучасні технології які має США, тоді поліція змогла би як мінімум спрогнозувати багато злочинів.

Список використаних джерел:

1. Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact – вебсайт. URL: https://www.connectedpapers.com/main/7cd2b8e78e61c5d2798215391abf469a3915a7ef/Technological-Innovations-in-Crime-Prevention-and-Policing.-A-Review-of-the-Research-on-Implementation-and-Impact/graph.
2. Taking advantage of new technologies: For and against crime. URL: https://www.researchgate.net/publication/222416247_Taking_advantage_of_new_technologies_For_and_against_crime.

Борисенко Т. В.,
ад'юнкт
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Гребенюк А. М.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ЗАПРОВАДЖЕННЯ ЄДИНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБЛІКУ ГУМАНІТАРНОЇ ДОПОМОГИ, БЛАГОДІЙНИХ ПОЖЕРТВ, БЕЗОПЛАТНОЇ ДОПОМОГИ ТА КОНТРОЛЮ ЗА ЇХ ВИКОРИСТАННЯМ НА ВСІХ РІВНЯХ

З 24 лютого 2022 року Україна протистоїть збройній повномасштабній агресії з боку Російської Федерації. У зв'язку з військовою агресією рф проти України, в країні введено воєнний стан. Протягом всього періоду дії воєнного стану громадяни країн усього світу спрямовують свої зусилля на допомогу українцям, кооперацію з волонтерськими організаціями, підтримку Збройних сил України та обороноздатності України. До України надсилається безліч гуманітарної допомоги від різних країн світу та приватних організацій як у вигляді предметів та товарів, так і у вигляді коштів,благодійної допомоги та пожертв. І в період воєнного стану, така допомога обов'язково має доходити до адресатів, до тих, хто її потребує, проте так трапляється не завжди. В цей важкий час з'являються випадки використання товарів гуманітарної допомоги для отримання прибутку.

Воєнний стан у державі та збурення в суспільстві через не доброчесні дії деяких громадян призвело до законодавчого врегулювання даних питань.

03 квітня 2022 року набрав чинності Закон України від 24 березня 2022 року № 2155-XI «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне використання гуманітарної допомоги».

Вказаним Законом КК України доповнено статтею 201² «Незаконне використання з метою отримання прибутку гуманітарної допомоги, благодійних пожертв або безоплатної допомоги» [1].

Виходячи зі статистичних даних Генеральної прокуратури України станом на 01.10.2022 у Єдиному реєстрі досудових розслідувань зареєстровано 345 кримінальних правопорушень за ст. 201² КК України [2].

Для того, щоб таких фактів ставало дедалі менше, є необхідним запровадження Єдиної інформаційної системи обліку гуманітарної допомоги, благодійних пожертв, безоплатної допомоги та контролю за їх використанням.

В цьому напрямку вже є позитивні напрацювання.

Створено автоматизовану систему реєстрації гуманітарної допомоги, яка призначена для забезпечення обліку отримувачів гуманітарної допомоги та вантажів, коштів, послуг, які вони отримують.

В Україні функціонує Державна система гуманітарної допомоги. Система в режимі реального часу вирішує три головні завдання: веде облік всієї завезеної на територію України гуманітарної допомоги в розрізі кожного окремого декларанта й отримувача; веде облік потреб отримання та відвантаження гуманітарної допомоги по складах; веде облік отримання гуманітарної допомоги по територіальних громадах з усіх джерел надходження [3].

Хоча сьогодні при ввезенні на територію України гуманітарної допомоги:

– не потрібно отримувати окреме рішення про визнання вантажу гуманітарною допомогою та отримувач не обов’язково має бути включеним до Єдиного реєстру отримувачів гуманітарної допомоги;

– митна та прикордонна служби забезпечують невідкладний пропуск через Державний кордон України гуманітарної допомоги, що в подальшому ускладнює облік такої допомоги.

Ефективним механізмом є розподіл медичної гуманітарної допомоги, який відбувається через інформаційно-аналітичну систему «MedData», що забезпечує контрольованість і прозорість процесу.

Крім того, Міністерство охорони здоров’я запустило інтерактивний дашборд, де можна подивитися, як розподіляється гуманітарна допомога від українських і міжнародний організацій та урядів країн світу.

Там доступна інформація про те, скільки вантажів доставлено в регіони і яка саме це допомога: лікарські препарати, обладнання, швидкі, витратні матеріали, засоби індивідуально захисту.

Дашборд інтерактивний, дані на ньому оновлюються щогодини [4].

Автоматизація складського обліку гуманітарної допомоги для України в умовах війни була розроблена та впроваджена командою BJet у співпраці з партнерами всього за кілька тижнів.

Система «Гуманітарна допомога та координація» (ГУДОК), створена на волонтерських засадах, оперативно вирішила відразу кілька важливих завдань для нашої держави:

– швидке опрацювання вантажів на складах;
– відправка їх у ті місця, де є найбільша потреба у людей;
– забезпечення належного контролю за надходженням та відвантаженням гуманітарної допомоги зі складів;
– уніфікований підхід до ведення обліку гуманітарної допомоги як на рівні категорій, так і на рівні процесів.

Відтепер гуманітарні вантажі, які проходять через склади обласних військових адміністрацій (всієї України), включено в єдиний контур у рішенні ГУДОК.

Проект передбачає збір та аналіз специфічних вимог від гуманітарних складів, розробку системи обліку на платформі Odoo, внесення та адміністрування даних про склади і користувачів, тестування, навчання операторів складу, організацію служби підтримки та масштабування системи на півтори сотні великих складів у всіх регіонах країни.

Задля належного контролю за рухом гуманітарної допомоги доступ до системи мають також уряд та офіс Президента України [5].

Процедура та критерії розподілу гуманітарної допомоги серед кінцевих набувачів нормативно не врегульовані, узагальнений алгоритм описати наразі не видається можливим. Сформовані продовольчі набори та інші види гуманітарної допомоги обласні військові адміністрації, передають до районних державних (військових) адміністрацій, які розподіляють їх між громадами. Видача гуманітарної допомоги населенню здійснюється у різний спосіб та у різних пунктах видачі. На офіційних веб-сайтах обласних військово-цивільних адміністрацій інформація щодо отримання та розподілу гуманітарної допомоги, звітності про її отримання в повному обсязі не відображається.

Беручи до уваги вищевикладене, можна дійти висновку, що в Україні запроваджено ефективні механізми для контролю гуманітарної допомоги.

Проте проблеми є, а саме: відсутній порядок взяття на баланс та належний облік отриманої гуманітарної допомоги, благодійних пожертв, безоплатної допомоги отримувачами, що може мати наслідком, подальше незаконне використання такої допомоги.

Для вирішення даної проблеми необхідно розробити і запровадити Єдину комплексну інформаційну систему, яка діятиме за принципами прозорості та підзвітності на усіх етапах. Є важливим, щоб дана система включала в себе дані про донорів (хто надає допомогу), отримувачів, набувачів (кому надається), вид та об’єм допомоги, а також про склади, де вона буде зберігатися.

Наявність такої системи сприятиме підвищенню рівня довіри як з боку вітчизняних, так і з боку міжнародних донорів.

Разом з тим, наявність такої системи сприятиме в роботі правоохоронних органів при виявлені фактів незаконного використання з метою отримання прибутку гуманітарної допомоги, благодійних пожертв або безоплатної допомоги.

Список використаних джерел:

1. Яка відповідальність за нецільове використання гуманітарної допомоги під час воєнного стану. URL: https://biz.ligazakon.net/news/211590_yaka-vdpovdalnst-za-netslove-vikoristannya-gumantarno-dopomogi-pd-chas-vonnogo-stanu.
2. Єдиний звіт про кримінальні правопорушення по державі за вересень 2022 року. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.
3. В Україні функціонує Державна система гуманітарної допомоги. URL: https://www.adm-km.gov.ua/
4. Як МОЗ використовує гуманітарну допомогу: на сайті запустили дашборд. URL: https://www.the-village.com.ua/village/city/city-news/326689-yak-moz-vikoristovue-gumanitarnu-dopomogu-na-sayti-zapustili-dashbord.
5. Облік гуманітарної допомоги для україни – автоматизовано BJET! URL: https://bjetpro.com/oblik-gumanitarnoyi-dopomogy-dlya-ukrayiny-avtomatyzovano-bjet.

Борисова К. Є.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

КОМПЮТЕРНА РОЗВІДКА – ЗАХІД ОПЕРАТИВНОГО ПОШУКУ

Одним з найбільш плідних та дієвих об’єктів отримання інформації є комп’ютер. В останні десятиліття набули активізації наступні види діяльності: отримання інформації шляхом гласного і негласного пошуку, добування інформації з інформаційних систем та баз даних, отримання інформації за допомогою контролю над повідомленнями мережі та інші. Говорячи про вищезазначені види діяльності визначають наступні терміни: «комп’ютерна розвідка», «кіберрозвідка», «комп’ютерний моніторинг», «аналітична розвідка за допомогою інтернету» тощо.

Поняття «комп’ютерна розвідка» трактується наступним чином – це оперативно-пошуковий захід, який полягає у цілеспрямованому пошуку та отриманні інформації з комп’ютерних систем та мереж, доступ до яких не обмежується їхнім власником, володільцем або утримувачем або не пов’язаний з подоланням системи логічного захисту, що здійснюється працівниками оперативних та оперативно-технічних підрозділів з метою виявлення відомостей криміногенного та кримінального характеру [1].

Сутність комп'ютерної розвідки полягає в добуванні інформації, що обробляється/зберігається/передається в інформаційних системах; добуванні даних і відомостей про методи/способи/механізми захисту інформації; добуванні персональної інформації про користувачів інформаційних систем.

Мета комп'ютерної розвідки – отримання інформації, яка міститься в комп'ютерних системах та мережах (на серверах).

Необхідність проведення комп'ютерної розвідки зростає с кожним днем та обумовлена сучасною організованою злочинністю. Мережа інтернету наразі використовується все більше і більше задля просування наступних правопорушень: збут зброї, людських органів, продуктів порнографії, вибухових пристроїв та речовин, кілерських «послуг», за допомогою створення нелегальних онлайн-ринків, а також: пропаганда національної ворожості та тероризму.

До основних напрямів здійснення комп'ютерної розвідки належать: пошук та збирання інформації, та здійснення активних заходів в мережі (оперативне опитування, оперативний експеримент, оперативна закупка тощо).

До програмних засобів комп'ютерної розвідки відносять мережеві пошукові системи: Яндекс, Rambler, Yahoo!, Google, Aport, Meta тощо, що в свою чергу дають змогу здійснювати пошук необхідної інформації в комп'ютерних мережах (за комбінацією ключових слів). Для здійснення комп'ютерної розвідки використовують спеціалізовані розвідувальні програми – прикладні програми, які виконують функції пошуку/отримання/аналізу інформації поза межами оперативних обліків.

Головною відмінністю розвідувальних програм від інших програм пошуково-аналітичного призначення є наявність в них специфічних функцій, спрямованих суто на вирішення розвідувальних завдань. До таких функцій відносять – пошук інформації (за неповними параметрами), на основі діаграми зв'язків/нечіткої логіки тощо. Перспективним вважається так званий інфомедійний пошук, який дає змогу в автоматичному режимі аналізувати інформацію, що міститься у відеоматеріалах, здійснюючи комплекс досліджень усного мовлення та зображень (розпізнавання мовлення, обличчя, переклад з однієї мови на іншу тощо). Отримана за допомогою спеціалізованих розвідувальних програм інформація зіставляється з наявною інформацією з оперативних обліків, що дає більшу результативність та чіткість в подальшому [1].

Комп'ютерна розвідка, а саме OSINT (Open Source Intelligence) – розвідка на основі інформації з відкритих джерел, є досить актуальною і в теперішній воєнний час. Чимало прикладів, починаючи з 2014 року, зафіксовано, коли така діяльність як OSINT допомагала викривати на теренах України проросійські діяння (злочини) і в цілому пропаганду Кремля (досить відомим прикладом є західний журналіст KremlinTrolls). OSINT – це збір і аналіз даних, отриманих із відкритих джерел, що має велике значення для розвідки під час війни в Україні. «Прочісуючи» інтернет, світова OSINT-спільнота, до якої входять переважно американці та європейці, активно допомагає Україні виявляти переміщення російських військ і місця дислокації їхньої техніки та документувати скоєні ними воєнні злочини. «Агенти-OSINT» не є професійними розвідниками, але мають надважливу роль у зборі інформації [2].

Резюмуючи сказане потрібно вимітити, що комп'ютерна розвідка – один з найбільш перспективніших заходів оперативного пошуку, адже вбачає в себе логічність, швидкість та дієвість. Отримана інформація може стати частиною процесу аналізу інформації щодо користувачів, подій у суспільстві та державі.

Методи комп'ютерної розвідки прискореними темпами удосконалюються. Масиви накопичуваної інформації збільшуються, тому росте і результативність здійснюваного нею аналізу.

Список використаних джерел:

1. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посіб. Львів: ЛьвДУВС, 2017. 244 с.
2. Як несекретна розвідка боронить Україну – KyivPost – Ukraine's Global Voice. KyivPost. URL: https://www.kyivpost.com/uk/war-uk/yak-nesekretna-rozvidka-boronyt-ukrayinu.html.

Борматов Р. С.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

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. На сьогодні важко уявити роботу будь-якого з підрозділів Національної поліції України без інформаційної підтримки та інформаційного забезпечення, накопичення та систематизації інформації в базах даних. Це є наочним підтвердженням загальновідомої тези «хто володіє інформацією, той володіє світом». Інформаційне забезпечення органів поліції – це комплекс методів, заходів, засобів різного характеру, які забезпечують створення та функціонування інформаційних технологій, а також їх ефективне використання для вирішення покладених на поліцію завдань. Інформаційні підсистеми як складові системи інформаційного забезпечення призначені для збирання, накопичення, зберігання та обробки інформації з певних напрямів обліків і орієнтовані на використання в діяльності більшості правоохоронних структур, мають загальний характер і належать до загальновідомчих інформаційних систем.

Сучасні інформаційні технології – це сукупність методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації в інтересах її користувачів. Види сучасних інформаційних технологій:

- інформаційна технологія опрацювання даних;
- інформаційна технологія керування;
- інформаційна технологія підтримки прийняття рішень;
- інформаційна технологія експертних систем [2, с. 396-397].

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є:

1. удосконалення форм та методів управління системами інформаційного забезпечення;
2. централізація та інтеграція комп'ютерних банків даних;
3. впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків;
4. розбудова та широке використання ефективних та потужних комп'ютерних мереж;
5. застосування спеціалізованих засобів захисту інформації;
6. налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні.

Все це забезпечує суттєве підвищення рівня боротьби зі злочинністю.

Як підсумок, відмітимо, що інтеграція інформаційних технологій в діяльність органів Національної поліції України дозволяє удосконалити механізми управління, забезпечує належне функціонування правоохоронних органів, а саме, оперативно отримувати доступ до певних відомостей, необхідних для виконання їх службових завдань, кваліфіковано здійснювати їх аналіз, використовувати досягнення науково-технічної думки для оптимізації слідчих дій. Розвиток комп'ютерних технологій дає змогу для створення нових методів роботи, підвищення професіоналізму кожного працівника правоохоронних органів.

Список використаних джерел:

1. Танкушина Т. Ю. Автоматизовані інформаційні системи в структурі реєстраційної діяльності міліції: становлення, розвиток, сучасність. *Вісник Запорізького національного університету:* зб. наук. праць. Юридичні науки: у 2 ч. Запоріжжя: ЗНУ, 2011. Ч. І. 224 с.
2. Варенко В. М. Інформаційно-аналітична діяльність: навч. посіб. К. : Університет «Україна», 2014. 417 с.
3. Кудінов В. А., Смаглюк В. М., Ігнатушко Ю. І., Іщенко В. А. Інформаційні технології в правоохоронній діяльності: посібник. К. : НАВСУ, 2013. 82 с.

Братішко Н. А.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Насонова С. С.,
доцент кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

КІБЕЗЛОЧИННІСТЬ У ВІРТУАЛЬНОМУ ПРОСТОРІ

Комп'ютерні злочини на сьогоднішній день – це одна з найрозповсюдженіших груп суспільно небезпечних посягань. Незважаючи на те, що це нове явище, однак швидко збільшуються показники поширення цих злочинів і постійно зростає їх суспільна небезпечність. Це зумовлено тим, що наука й технологія у сфері комп'ютеризації не стоїть на місці і постійно розвивається, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

У загальному понятті під кіберзлочинністю слід розуміти злочинність в так званому «віртуальному просторі». Віртуальний простір (або кіберпростір) – це модельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символічному або будь-якому іншому вигляді, що перебувають у процесі руху по локальних та глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного чи віртуального пристрою, а також іншого носія, спеціального призначення для їх зберігання, обробки та передачі [1, с. 19-20].

До кіберзлочинів слід віднести такі посягання:

1) правопорушення проти конфіденційності, цілісності і доступності комп'ютерних даних і систем, зокрема:

− незаконний доступ, тобто навмисний доступ до цілої комп'ютерної системи або її частин без права на це з метою отримання комп'ютерних даних або з іншою недобросовісною метою;

− нелегальне перехоплення комп'ютерних даних;

− втручання у дані, включаючи навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

− втручання у систему – навмисне створення серйозних перешкод функціонуванню комп'ютерної системи, наприклад, шляхом розподілених атак на ключову інформаційну інфраструктуру;

− зловживання пристроями, тобто виготовлення, продаж, придбання для використання, розповсюдження пристроїв, комп'ютерних паролів або кодів доступу з метою здійснення кіберзлочинів;

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема, дитяча порнографія, расизм і ксенофобія;

4) правопорушення, пов'язані з порушенням авторських прав, наприклад, незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг [2, с. 172-174].

Кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, але практично кожен чув про неї, або навіть особисто зіштовхнувся. Вона включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі Інтернет. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не лише на національному, а й на глобальному рівні. Наприклад, на рівні фізичних осіб кіберзлочинність пов'язана з використанням піратського програмного забезпечення: зловмисники можуть отримати доступ до персональних даних користувача. Згідно з дослідженням міжнародної компанії MUSO із січня по серпень 2022 року експерти зафіксували 141.7 мільярда відвідувань піратських сайтів, що на 21,9 % більше, ніж за аналогічний період 2021 року. За цим показником Україна знаходиться на 14 місці [3].

Тому варто зауважити, що для того, щоб вберегтися від кіберзлочинів необхідно: створення надійних паролів, захист інформації та періодична їх зміна; перевірка своїх облікових записів; використання захищених мереж; поінформованість про розповсюджені прийоми, які використовують злочинці для того, щоб розпізнавати їх; використання інструментів конфіденційності та безпеки Google чи інших браузерів; захист пристроїв і встановлення антивірусних програм.

Отже, підсумовуючи вищевикладене, можна сказати, що кіберзлочини являють одне із найбільш складних асоціальних явищ у сучасному інформаційному суспільстві, вони загрожують інформаційному суверенітету. Тому юридично правильне розслідування злочинів у даній сфері – це наразі одне із ключових питань для розвитку криміналістики будь-якої держави.

Список використаних джерел:

1. Олійник В. М. Кіберзлочинність як умова порушення громадської безпеки України. *Актуальні питання розслідування кіберзлочинів:* матер. Міжнар. наук-практ. конф. (м. Харків, 10 грудня 2013 р.). Харків: ХНУВС, 2013. С. 19-20.

2. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції.* 2016. № 3. С. 172-174.

3. В якій країні найбільш поширене медіапіратство? URL: https://mediasat.info/uk/2022/10/13/doslidzhennya-spolucheni-shtati-ta-rosiya-lideri-po-telepiratsvu-ukraina-na-14-misci/#:~:text=Із%20січня%20по%20серпень%202022,за%20аналогічний%20період%202021%20року.

Верзілов М. Р.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ПРОТИДІЯ ТОРГІВЛІ ЛЮДЬМИ В МЕРЕЖІ ІНТЕРНЕТ

Сьогодні у світі до глобальної мережі Інтернет має доступ близько трьох мільярдів осіб. Виявляється, що 17 % користувачів Інтернету в Європі мешкають у чотирьох країнах – Білорусії, росії, Молдові та Україні. За таким показником в Європі росія знаходиться на другому, а Україна – на дев'ятому місці [1].

Торгівля людьми у сучасному світі це протизаконні діяння в цілях збагачення та особистої вигоди (комерційна, сексуальна експлуатація або примусові праці). Ця діяльність є найшвидше зростаючою кримінальною діяльністю у світі, велику роль у якій відіграють інформаційні технології. І хоча основним об'єктом торгівлі людьми або іншої незаконної угоди щодо передачі людини (ст. 149 Кримінального кодексу України) виступає воля людини, однак додатковим факультативним об'єктом злочинних посягань можуть виступати статева недоторканність, честь і гідність, трудові та інші права. До цього виду злочину законодавчо віднесено також вербування, переміщення, переховування, передачу, одержання людини, вчинені з метою експлуатації з використанням обману, шантажу чи уразливого стану [2].

За оцінками експертів у світі щороку від двох до чотирьох мільйонів осіб стають жертвами торгівлі людьми. Особливо це стосується жінок та дітей. Отже, для когось це – «Великий бізнес», а для когось – це крах надій і сподівань на краще майбутнє [3].

У зв'язку із розвитком кіберзлочинності все частіше люди стають жертвами правопорушень, вербування людей, реклама. Зустрічі між жертвами та клієнтами організовуються за допомогою спеціальних веб-сайтів, соціальних мереж, при чому сучасні злочинці досягли такої майстерності що будь-яка людина сама того не розуміючи може бути введена в оману.

Зазвичай правопорушники використовують такі програмні технології [1, 3]:

1. Спеціальні веб-сайти із айпілогером;
2. Спеціалізовані веб-сайти;
3. Соціальні мережі;

4. Електронні скриньки;
5. Онлайн чати;
6. Дошки оголошень.

До спеціалізованих веб-сайтів та сайтів з айпілогером входять сайти неіснуючих кафе, барів, ресторанів, агенцій з пошуку нерухомості, банків, сайти знайомств, тощо. Також часто використовується практика копіювання популярного веб-сайту, його модифікація та видання як оригінал жертві.

У висновку зазначимо, що правоохоронні органи розслідуючи злочини з торгівлі людьми проводять первинний пошук й аналіз інформації. Місце знаходження, останні переписки, друзі, тощо. Різні випадки потребують різних методів підходу слідчих та інших оперативних підрозділів. Маємо лише те, що дуже важливим є узгоджені дії підрозділів боротьби з кіберзлочинністю та підрозділів боротьби зі злочинами пов'язаними із торгівлею людей.

Список використаних джерел:

1. Інститут інформації, безпеки і права Національної академії правових наук України. URL: http://ippi.org.ua/sites/default/files/12kvglmi.pdf.
2. Савчин Г. Я., Цмонь У. О. Сучасні механізми протидії торгівлі людьми: зб. тез Міжнар. наук.-практ. конф. (м. Львів, 4 грудня 2020 року). Львів : ЛьвДУВС, 2020. 180 с.
3. Що таке торгівля людьми? Основні поняття та види експлуатації. Таїровська селищна рада, об'єднана територіальна громада – вітаємо на офіційному веб-сайті. URL: https://tairovska-gromada.gov.ua/news/1632136460/

Візір В. Ю.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Рижков Е. В.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ПІДСИСТЕМ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ У ПРОТИДІЇ НЕЗАКОННИМ ЗАВОЛОДІННЯМ ТРАНСПОРТНИМИ ЗАСОБАМИ

Розшук автотранспортних засобів сьогодні є одним із тих напрямків діяльності МВС, які потребують особливої уваги та вивчення. Число скоєних крадіжок і викрадень транспортних засобів в Україні є досить високим, при

цьому залишається значна кількість нерозкритих злочинів цього виду. Все це вказує на необхідність вжиття комплексних заходів, спрямованих на вдосконалення діяльності МВС щодо запобігання та розкриття злочинів цієї категорії.

Як правило, чим більше часу пройшло з моменту скоєння злочину та початку розслідування, тим більше його слідів-наслідків зазвичай зникає, а особи, які вчинили злочин, мають більше шансів далеко втекти від слідства. І навпаки, швидкий початок розслідування дозволяє проводити його ще за свіжими, не видозміненими і незниклими слідами, що дозволяють вести швидку, цілеспрямовану, безперервну та ефективну діяльність з розшуку злочинця та його затримання. Тому сприятливі умови для швидкої та цілеспрямованої діяльності з розкриття злочину зазвичай складаються тоді, коли розслідування починається негайно після скоєння злочину за його добре збереженим, ще не видозміненим і незниклим матеріальним та ідеальним слідам [1].

Зарубіжні кримінологи на основі інтерв'ю із викрадачами визначили їхній психологічний портрет. Ризик під час скоєння був джерелом гордості для злочинця, свідченням його здатності долати екстремальні ситуації. Правопорушники знаходили заволодіння автомобілем захоплюючим дійством. Молоді люди говорили, що займалися цим не для заробітку, а заради азарту, щоби отримати адреналін. Свої відчуття вони порівнювали із вживанням кокаїну, називаючи це вмінням «танцювати» з небезпекою [2].

Знаходження викрадачів у стані сп'яніння від одурманюючих препаратів може породжувати з їхнього боку насильницькі дії щодо потерпілих. Інтерв'ю з такими злочинцями дозволило західним ученим встановити взаємозв'язок між споживанням наркотиків та застосуванням насильства, оскільки «нейтралізація» соціальних обмежень у наркотичному стані спонукає до «злочинного дрейфу» (відхилення), який злочинці виправдовують збігом обставин, тим, що вони не усвідомлюють власне «я», що жертва заслуговує на насильство, особиста відповідальність засудженими заперечується [2].

Вивчивши статистику викрадень на інших континентах, наприклад у Південній Африці, з'ясувавши можливі фактори впливу на вибір мети в процесі викрадення, фахівці зробили цікавий висновок, що викрадення не відбувається хаотично: викрадачі виборчі, і в основному вони виявляють інтерес до автомобіля, керованого водієм. Тому, незважаючи на те, що викрадення та розкрадання транспортних засобів є злочинами проти власності, вони не виключають небезпеки для життя та здоров'я автовласника, оскільки заволодіння автомобілем може вимагати від правопорушників нейтралізації потерпілих, які здатні використовувати свої транспортні засоби як зброю та щит. У зв'язку з цим у кримінології досліджують не тільки азарт і бешкетність викрадача, а й співвідношення його страху з упевненістю вчинити злочинне діяння

В українській юридичній науці таку впевненість злочинця зробити задум, що нерідко пов’язують з пияцтвом і алкоголізмом, які сприяють антигромадській поведінці, виступаючи в ролі його каталізатора. Безліч злочинних посягань на автомобіль відбувається особами у нетверезому стані. Це є ситуативної природою таких злочинів, їх імпульсивним характером. Алкоголь сприяє зниженню у злочинця почуття відповідальності за свою поведінку, знижує здатність до самоконтролю, правильної самооцінки та провокує протиправне самоствердження, що збігається зі «злочинним дрейфом», аналізованим у західній літературі.

Вітчизняні кримінологи роблять висновок, що найбільш тісно пов’язані з пияцтвом викрадення, які здійснюють саме неповнолітні [3].

Не менш важливим є вік злочинця, який сам по собі не може бути причиною злочинів, проте нестійка психіка неповнолітніх у період складних життєвих ситуацій сприяє формуванню негативних процесів у їхньому внутрішньому світі. У молодому віці люди зазвичай менш стримані, швидше ухвалюють рішення, не замислюючись про наслідки.

Проведене кримінологами дослідження свідчить про певне «омолодження» злочинних посягань на транспортні засоби (не тільки викрадень, а й розкрадань у різних формах). Так, у 2021 р. в Україні за викрадення транспортних засобівбуло виявлено неповнолітніх у віці 14-15 років – 7,4 %, 15-16 років – 12,3 %, 16-17 років – 34,9 %, 17-18 років – 45,4 %.

Інформаційною підсистемою (далі – ІП) «Гарпун» системи «ІПНП» об’єднано інформацію про розшук транспортних засобів та номерних знаків, забезпечення оперативного реагування, 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 транспортних засобів Міністерства внутрішніх справ України, знищено, а також забезпечення взаємодії з державними та приватними виконавцями під час розшуку ТЗ боржника у виконавчому провадженні [5].

Як свідчить цей перелік, ІП «Гарпун» системи «ІПНП» фактично поєднала відомості двох інформаційних систем: інформаційної підсистеми «Угон» ІІПС та автоматизованої інформаційно-пошукової системи відеофіксації номерних знаків транспортних засобів «Відеоконтроль-Рубіж» [4].

ІП «Гарпун» створено для:

– об’єднання інформації про розшук ТЗ та номерних знаків у єдиному інформаційному просторі з використанням сучасних інформаційних технологій, комп’ютерного та телекомунікаційного обладнання;

– моніторингу тимчасових потоків даних про номерні знаки, що надходять із систем відеофіксації, щодо їх розшуку, одночасного знаходження на різних ТЗ (номерні знаки – двійники), використання номерних знаків, які за даними ЄДР МВС знищені [5].

Практика застосування інформаційних підсистем Національної поліції характеризується позитивною тенденцією за останні 10 років. Проте, в процесі виникають проблемні аспекти, що у свою чергу потребують постійного вдосконалення [6, с. 19].

Правовий механізм забезпечення функціонування автоматизованих інформаційних систем та їх підсистем, використовуваних органами (підрозділами) поліції, що являє собою систему правових засобів, за допомогою яких упорядковано суспільні відносини відповідно до цілей і завдань правової держави, сьогодні перебуває у стані подальшого розвитку.

Список використаних джерел:

1. Кіріленко Ф. О., Мінаєв Д. Д. Профілактика та запобігання незаконному заволодінню транспортними засобами. *Правничий часопис*, 2018. 56 с.
2. Черниш М. О. Оперативно-розшукова характеристика незаконного заволодіння транспортними засобами. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*, 2018. № 2. С. 313-320.
3. Яремко Г. З. Кваліфікація викрадення, поєднаного з проникненням у транспортний засіб. Київ, 2019. 80 с.
4. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України». Наказ МВС України від 13.06.2018 р. № 497. URL: https://zakon.rada.gov.ua/laws/show/z0787-18#Text.
5. Бірюков В. В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів: монографія. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка. 2009. 664 с.
6. Рижков Е. В. Оптимізація деяких підсистем ІІПС ОВС та ІТС НПУ та інші питання в діяльності працівників ІАП ГУНП. *Використання сучасних інформаційних технологій в діяльності Національної поліції України*: матер. всеукр. наук.-практ. семінару (м. Дніпро, 23 листопада 2018 року). Дніпро: ДДУВС, 2017. С. 18-23.

Володько В. О.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

Воєнний стан – це особливий правовий режим, що вводиться в Україні або в окремих її місцевостях у разі збройної агресії чи загрози нападу, небезпеки державній незалежності України, її територіальній цілісності та

передбачає надання відповідним органам державної влади, військовому командуванню, військовим адміністраціям та органам місцевого самоврядування повноважень, необхідних для відвернення загрози, відсічі збройної агресії та забезпечення національної безпеки, усунення загрози небезпеки державній незалежності України, її територіальній цілісності, а також тимчасове, зумовлене загрозою, обмеження конституційних прав і свобод людини і громадянина та прав і законних інтересів юридичних осіб із зазначенням строку дії цих обмежень.

Як, коли та ким приймається рішення про введення воєнного стану? Рада національної безпеки та оборони, приймає рішення про введення воєнного стану. У подальшому Президент України указом вводить воєнний стан та негайно звертається до Верховної Ради України щодо його затвердження, після затвердження Верховною Радою даний указ підлягає негайному оприлюдненню та виконанню, на виконання вищевказаних дій надається два дні від прийняття рішення РНБО. Управління від держадміністрацій переходить до військово-цивільних адміністрацій, тобто по суті відбувається зміна влади на місцях. За вищевказаних умов під охорону армії та правоохоронних органів переходять об’єкти державного значення, об’єкти транспортної системи України та об’єкти, що забезпечують життєдіяльність населення, запроваджується особливий режим їх роботи. Крім того, може бути запроваджена трудова повинність для працездатних осіб, які не мобілізовані і не забронювані за підприємствами на період дії воєнного стану, для виконання робіт оборонного характеру або ліквідації наслідків надзвичайних ситуацій, або до суспільно корисних робіт, порядок залучення до таких робіт визначений Постановою КМУ №753 від 13.07.2011 року.

Понад 8 років війна, що точилася в нашій державі, була локалізована лише двома областями, але 24 лютого 2022 року все змінилося. Вся Україна стала ареною бойових дій. Розглянемо що ж треба знати та робити під час війни цивільним людям, аби захистити себе у інформаційному просторі.

Двохфакторна автентифікація має бути увімкнута скрізь, в усіх сервісах. Оновить паролі та зробіть їх безпечними – мінімум 8 символів, літери великого та малого регістру, цифри та спецсимволи; не повторюйте паролі у різних сервісах. Не відповідайте на дзвінки з незнайомих номерів. Також для дзвінків найкраще користуватися захищеними месенджерами, такими як Signal. Дзвінки по мобільній мережі перехопити набагато простіше. Читайте лише офіційні джерела інформації. Не довіряйте чуткам та пліткам – те що ви або члени вашої родини не бачили на власні очі, варто сприймати максимально-критично [1-2].

Дуже важливо – не можна допустити паніки! Тому будь які панічні пости ігнорувати, та блокувати їх авторів. Паніка – це найстрашніше під час війни. Не фотографувати та не викладати в соціальні мережі фото військових, бойових дій, ракет та літаків у небі, результатів обстрілів. Якщо ви вважаєте, що мажте важливу інформацію – є телеграмм-бот в який офіційно можна її відправляти – @stop_russian_war_bot Або ж повідомте найближчому військовому, бійцю тероборони, поліцейському.

Якщо ви знаходитеся у зоні окупації – сидіть вдома, почистить свій телефон від фото, переписок та підписок у соцмережах. Пам'ятайте: це – тимчасово.

Якщо можете – допомагайте одне одному та нашим захисникам. Якщо ви прихистили пораненого захисника – не пишіть й не кажіть цього, передайте інформацію його командуванню або по наданим вище каналам [3].

Список використаних джерел:

1. Безпека бізнесу: що потрібно розуміти й зробити перед загрозою воєнного стану. ЮРЛІГА. URL: https://jurliga.ligazakon.net/news/209142_bezpeka-bznesu-shcho-potrbno-rozumti-y-zrobiti-pered-zagrozoyu-vonnogo-stanu.
2. Правила інформаційної безпеки під час війни. URL: https://www.itguild.org.ua/blog/pravila-informaciynoyi-bezpeki-pid-chas-viyni.
3. Інститут інформації, безпеки і права Національної академії правових наук України. URL: http://ippi.org.ua/sites/default/files/12kvglmi.pdf.

Галушневська К. О.,
здобувач вищої освіти
Дніпропетровського державного університету внутрішніх справ
Науковий керівник:
Рижкова С. А.,
старший викладач кафедри адміністративного права, процесу та адміністративної діяльності Дніпропетровського державного університет внутрішніх справ, майор поліції

ПРОФІЛАКТИКА ПРАВОПОРУШЕНЬ СЕРЕД НЕПОВНОЛІТНІХ ЗА ДОПОМОГОЮ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Належний розвиток та виховання молоді, формування моральних та етичних принципів поведінки підлітків, пропагування здорового способу життя, в тому числі підвищення рівня правової свідомості є пріоритетним завданням держави.

В контексті зазначеного, важливим є й аспекти по'вязані з превентивною діяльністю (профілактикою) недопущення скоєння кримінальних та адміністративних правопорушень неповнолітніми. Слід зазначити, що питаннями профілактики правопорушень опікується відповідні суб'єкти, дотичні до вирішення зазначених проблем, наприклад, спеціалізовані державні органи та організації, які здійснюють функцію превентивного нагляду; державні та недержавні органи, громадські об'єднання та громадяни, які здійснюють функцію превентивного контролю, тощо.

Важливе значення у профілактиці правопорушень відводиться органам та підрозділам Національної поліції України, особливо зазначена проблематика актуальна в умовах воєнного стану, першочерговим завданням підрозділів поліції має стати захист від втягнення в криміногенне, злочинне середовище неповнолітніх.

Слід зазначити, що введення правового режиму воєнного стану в нашій державі, відобразилось й на питаннях проведення занять у навчальних закладах (школах), з метою забезпечення безпеки дітей, заняття проводяться он-лайн з перших початкових і випускних класів. У зв'язку з зазначеним, постає загроза отримання негативної інформації через мережу Інтернет, та формування девіантної поведінки серед неповнолітніх. Адже практично всі підлітки є активними користувачами мережі Інтернет, месенджерів, та соціальних мереж. Більшість інформації, а також формування поведінки підлітків в суспільстві, базується на перегляді контенту, який в подальшому ретранслюється у реальному житті. Важливим в цьому контексті є донесення інформації профілактичного змісту, наприклад про безпеку в Інтернеті, профілактику кібербулінгу [1], недопущення вживання алкогольних та наркотичних засобів. Окрема проблематика – це розповсюдження та продаж наркотичних засобів неповнолітнім, за допомогою месенджерів, тощо.

Досить позитивним та ефективним методом профілактики правопорушень серед підлітків є впровадження чат-ботів, метою створення яких, є донесення певної інформації та забезпечення належного алгоритму дій, як протистояти деяким антисоціальним явищам. Зупинимось на деяких позитивних прикладах використання чат-ботів у профілактиці правопорушень.

Спілкування учнівської молоді з однолітками частіше відбувається у соціальних мережах та месенджерах. У зв'язку з цим почастішали випадки кібербулінгу серед учнівської молоді. Кібербулінг – це новітня форма протиправної поведінки, яка виявляється в агресивних, жорстоких діях з метою дошкулити, нашкодити, принизити людину, використовуючи інформаційно-комунікаційні засоби: мобільні телефони, електронну пошту, соціальні мережі тощо. В українській мові поняттям кібербулінгу позначають процес лютого завзятого нападу, який характеризують дієсловами «роз'ятрювати», «задирати», «прискіпуватися», «провокувати», «дошкуляти», «тероризувати», «цькувати» тощо [1, с. 277].

Важливе місце цьому негативному явищу та профілактиці кібербулінгу серед учнівської молоді належить створений Міністерством цифрової трансформації у співпраці з ЮНІСЕФ та за інформаційної підтримки Міністерства освіти і науки України, Координаційного центру з надання правової допомоги та Міністерства юстиції України чат-бот #Кіберпес. Чат-бот #Кіберпес [2], надає певний правовий алгоритм дій, учасникам освітнього процесу щодо протидії проявам кібербулінгу. Чат-бот у Telegram і Viber допоможе дізнатись, як визначити кібербулінг, як самостійно видалити образливі матеріали з соціальних мереж, а також куди звертатись за

допомогою, тощо. Впровадження чат-ботів, суб'єктами які уповноважені здійснювати профілактичні функції у правоохоронній сфері, є новим інструментом комунікації з населенням, здатним не тільки підвищувати правосвідомість громадян, підвищувати рівень правового виховання серед населення, а також бути дієвим помічником у протидії правопорушенням.

Отже на підставі вищезазначеного, впровадження нових методів профілактики правопорушень серед неповнолітніх за допомогою інформаційних технологій, забезпечує досягнення позитивних результатів та підвищує якості виховного впливу на підлітків.

Список використаних джерел:

1. Рижкова С. А. Використання чат-ботів у профілактиці та протидії кібербулінгу серед учнівської молоді. *Актуальні питання взаємодії суб'єктів, які мають здійснювати заходи з реагування та профілактики на випадки насильства у закладах освіти:* матер. ІІ Міжрегіон. форуму «Дніпровська міжрегіональна платформа» Координаційного центру з надання правової допомоги (м. Дніпро, 16 грудня 2020 р.). Дніпро, 2020. С.86-90.
2. Миронюк Т. В., Запорожець А. К. Кібербулінг в Україні – соціально небезпечне явище чи злочин: визначення та протидія. *Юридичний часопис Національної академії внутрішніх справ*. 2018. № 2. С. 275-284.
3. Кіберпес: в Україні розробили чат-бот для боротьби з кібербулінгом. URL: https://nus.org.ua/news/kiberpes-v-ukrayini-rozrobyly-chat-bot-dlya-borotby-zkiberbuling.

Гарбузова Є. О.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

РОЗВИТОК ТА СТАНОВЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Як характеристика сучасного суспільного розвитку, інформаційні технології відіграють все більшу роль у житті людини, суспільства та країни. Інформаційне забезпечення Національної поліції відкриває нові можливості для запобігання злочинності та сприяє прийняттю ефективних і точних рішень щодо розкриття злочинів. Важлива роль системи інформаційного забезпечення управління в правоохоронних органах підтверджується на нормативному рівні, зокрема наказами та розпорядженнями Міністерства внутрішніх справ України [1, с. 55].

Досліджуючи питання розвитку та становлення інформаційного забезпечення, науковці виділяють шість етапів.

На першому етапі – поява людської мови, вона значною мірою сприяла обміну інформацією під час особистого контакту та для накопичення інформаційних ресурсів у подальшому з'явилися кадри, відповідальні за зберігання.

На другому етапі еволюції з'явилася писемність. Поява першого друкарського верстату в 1445 р. поклала початок третьому етапу інформаційних технологій, який тривав приблизно 500 років і важливим досягненням якого стала поява інформаційного забезпечення поліції як власне функції їхньої діяльності.

У четвертому періоді (кінець XIX – початок XX ст.) інформаційної еволюції була винайдена і стала широка гама способів передачі інформації: радіо, телеграфу, телефону та ін.

Із появою перших електронно-обчислювальних машин в 1946 р. розпочався п'ятий етап еволюції інформаційних технологій, а на шостому етапі, що триває досі, був винайдений мікропроцесор і персональний комп'ютер [2].

Фундамент інформаційного забезпечення українських правоохоронних органів склався на початку 1970-х років. У цей період ми почали використовувати накопичений в країні досвід для вирішення проблем управління промисловістю за допомогою комп'ютерів.

У 1985 році почала формуватися єдина автоматизована база даних, яка централізувала інформацію, необхідну правоохоронним органам для виконання своїх функцій. У всіх чергових підрозділах органів внутрішніх справ були встановлені автоматизовані системи оперативної інформації.

Відповідно до положення про Інтегровану інформаційно-пошукову систему (далі – ІІПС) органів внутрішніх справ України від 12.10.2009 року розроблено алгоритм дій, сформований організацією-користувачем ІІПС для використання під час виконання службових обов'язків у сфері правоохоронних органів. У той же час інформаційні записи ІІПС на регіональному та центральному рівнях надаються лише авторизованим користувачам ІІПС.

ІІПС внесла великий вклад у роботу правоохоронних органів: надала можливість доступу до необхідної інформації онлайн, що значно зберігає час правоохоронця. Кожен авторизований користувач має певний доступ до матеріалів справ та може їх знайти, використовувати одразу у своєму кабінеті в райвідділі.

Сучасна база даних була розроблена 03.08.2017 року з метою організації інформаційно-аналітичної підтримки поліції, про це зазначає Положення про інформаційно-телекомунікаційна систему «Інформаційний портал Національної поліції України».

У сьогоднішній час Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (далі – система ІПНП) – сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її

інформаційно-аналітичної підтримки. Існує багато інформаційних підсистем, що допомагають Національній поліції Україні у розкритті та протидії злочинності, наприклад: «Повідомлення «102», «Єдиний облік», «Особа», «Інспектор», «Адміністративне правопорушення», «Затримані та доставлені», «Розшук» та багато інших.

Однією з таких підсистем є система централізованого управління нарядами поліції (скорочено – система «ЦУНАМІ»). Вона представляє собою комплекс апаратних і програмних засобів, що забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Система фіксує, зберігає та робить доступними для аналізу та контролю повідомлення і результати реагування на них.

Мета впровадження системи «ЦУНАМІ» обумовлена необхідністю вдосконалення процесу організації діяльності з управління силами й засобами Національної поліції для ефективного реагування на повідомлення про злочини та події [3, с. 105-110].

Тому, історичний огляд чітко свідчить, що інформаційне забезпечення Національної поліції України є важливим фактором їх діяльності. Воно є масштабним та корисним, але все одно має свої проблеми. Одна з масштабних проблем – це недостатнє оснащення технічним забезпечення, що як результат впливає на якість обробки інформації. Але з кожним днем систему ІПНП допрацьовують та покращують, тому у подальшому недоліки будуть виправленні.

Список використаних джерел:

1. Фролова О. Г. Проблеми правового регулювання інформаційно-методичного управління в органах внутрішніх справ. *Проблеми правознавства та правоохоронної діяльності*. № 1. С. 53-62.
2. Цимбалюк В. І., Олексін Ю. П., Міщук І. В., Петровський О. М., Сахнюк В. В Правові засади інформаційного забезпечення діяльності правоохоронних органів України. 18 с.
3. Вишня В. Б., Ісмайлов К. Ю., Краснобрижий І. В. Інформаційні технології: підручник. Дніпро: ДДУВС, 2020. 492 с. URL: http://er.dduvs.in.ua/handle/123456789/6820.

Гуненко В. Д.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

SQL ІН'ЄКЦІЯ ТА ІН'ЄКЦІЇ КОДУ. ЩО ЦЕ ТАКЕ І ЯК З ЦИМ БОРОТИСЬ

Ін'єкція коду це введення в додаток шкідливого для функціональності, цілісності, приватності й конфіденційності бази даних. Часто використовується з метою несанкціонованого входу або крадіжки даних. Визначають чотири основні види атак на введення коду:

- введення сценарію;
- динамічна оцінка;
- ін'єкція оболонки;
- введення SQL.

SQL ін'єкція. Даний термін використовують щоб визначити одну із найбільш часто використовуваних різновидів атак на введення ін'єкцій коду, що взаємодіють з базами даних ,шляхом впровадження в данні спеціального SQL коду для їх компрометації.

Потенційні наслідки успішної SQL ін 'єкції:

- зламання облікового запису іншої особи;
- видалення даних системи;
- зміна даних системи;
- крадіжка та копія даних системи;
- загроза використання облікового запису адміністратора;
- перегляд приватної інформації;
- загроза змінення структур баз даних, видалення таблиць;
- виконання команд на сервері за власним бажанням.

Деякі введені користувачем дані можуть бути використані для кадрування Виписки SQL які потім виконуються додатком у базі даних. Додаток НЕ може правильно обробляти введені користувачем дані [1]. Попри на існування методів захисту від такого методу злому, ін'єкції залишаються найпоширенішими за популярність видами атак ,вони варіюються від простих до таких,які дуже важко знайти, сукупність цих ознак і вказує на високу загрозу даного метода.

Основні методи протидії ін’єкціям:

- перевірка вхідних даних;
- екранування спецсимволів для динамічних заходів;
- інструменти об’єктивно-реляційного відображення;
- елементи управління SQL.

Щоб провести досконале дослідження тестувальнику необхідно розуміти функціональні вимоги ,сценарій додатку ,основні тригери, також бізнес-логіку. Тестувальник повинен реагувати на будь-яку аномальну реакцію додатку, як-то більш довга загрузка сторінки, завантаження порожньої сторінки, відсутність повідомлень про помилки чи успіх.

Не можна нехтувати перевіркою усіх сторінок програми,які приймають введення від користувачів (поля для входу, поля для пошуку, поля коментарів, посилання на веб-сайт, будь-які інші поля введення та забезпечення даних), хоча найчастіше такий тип атаки використовують на сторінках входу.

Введення SQL може бути можливим у програмах, що використовують SSL. Навіть брандмауер може бути не в змозі захистити програму від цієї техніки [2]. Тому незважаючи на ефективність веб-сканерів на вразливості, ручна перевірка є не менш актуальною, бо дозволяє провести глибоке дослідження, виявити помилки й потенційний витік даних та навіть знайти нові,раніше невідомі вразливості,що значно підвищує рівень безпеки.

Наслідки SQL ін’єкції можуть бути набагато серйознішими ніж ін’єкція Javascript або HTML які виконуються на стороні клієнта, оскільки дозволяє отримати доступ до всієї бази даних.

Слід зазначити: гарний тестер має добре знати мову SQL й бази даних, як я які запити до них надходять, бути уважним оскільки будь-яка аномалія вже свідчить про наявність вразливості до ін’єкцій. Навіть якщо автоматизовані засоби заощаджують ваш час, вони не завжди вважаються дуже надійними. Якщо ми тестуємо банківську систему або будь-який вебсайт з дуже конфіденційними даними, настійно рекомендуємо перевірити його вручну. Де ви можете побачити точні результати та проаналізувати їх. Крім того, у цьому випадку ми можемо бути впевнені, що нічого не пропущено [2].

Список використаних джерел:

1. Тестування безпеки: SQL ін’єкції – QATestLab training center. URL: https://training.qa testlab.com/blog/technical-articles/security-testing-sql-injection/
2. Підручник з тестування ін’єкцій SQL (Приклад та запобігання атаці ін’єкцій SQL). URL: https://uk.myservername.com/sql-injection-testing-tutorial-example.

Гупалюк Я. Р.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

На сьогоднішній день задля підвищення ефективності функціонування спеціалізованих інформаційних систем Національної поліції все більше розвивають інформаційно-аналітичну діяльність. Інформаційно-аналітична робота виявляє та визначає закономірності щодо дослідження злочинності, порушення громадського порядку, ДТП та іншого. А також, інформаційно-аналітична робота підсумовує та узагальнює результати роботи Національної поліції, охоплює аналіз заходів протидії злочинності, спрямовані на охорону громадського порядку. Врегульовує використання інформації щодо запобіганню правопорушенням, охорони порядку та публічної безпеки та інші завдання Національної поліції визначені законодавством України. Закон України «Про національну поліцію» визначив як одну з напрямків своєї діяльності – інформаційно-аналітичну діяльність. Різноманітність завдань та функцій, які здійснюються в процесі функціонування системи МВС України, використовує різні форми діяльності. Найголовніші види інформаційної діяльності представлені в Законі України «Про інформацію». Такою є діяльність отримання, зберігання, використання, розповсюдження та захист інформації.

Структура інформаційно-аналітичної діяльності включає в себе створення баз даних, інформаційну підтримку, інформаційну та аналітичну обробку, пошук інформації та методи їх реалізації. Щоб ефективно реалізувати ці функції їх необхідно реалізовувати в окремих територіальних поліцейських органах з об’єктивно встановленими критеріями збору інформації та встановленим процесом їх обробки. Також беремо до уваги, що технологія збору та обробки даних повинна охоплювати всі сфери діяльності складових елементів Національної поліцейської системи, визначених Законом України «Про Національну поліцію» та компонентами Міністерства внутрішніх справ України, зовнішні показники оцінки зібраної та обробленої інформації.

Оптимізація завдання відбору, пошуку та систематизації інформації, необхідної для роботи Національної поліції, базується на розробці єдиного інформаційного простору системи Міністерства внутрішніх справ України,

який визначається як сукупність спеціальних баз даних з технологіями їх управління та використання, інформаційними та телекомунікаційними системами та мережами, а також інформаційно-аналітичні заходи, що діють на основі загальних принципів та загальних правил, що забезпечують інформаційну взаємодію між Міністерством внутрішніх справ України та громадянами [1].

Національна поліція здійснює аналітичну роботу за такими напрямами:

1) оперативний аналіз (робота за конкретними кримінальними провадженнями з локальними даними, такими як аналіз телефонних трафіків, транзакцій, даними стосовно конкретної особи, об'єкта тощо);

2) тактичний аналіз (аналіз несприятливої ситуації на конкретній території за нетривалий проміжок часу, за певним видом злочину);

3) стратегічний аналіз (виявлення тенденцій, закономірностей, прогнозування розвитку за тривалий період часу тощо) [2].

Використання уповноваженими підрозділами Національної поліції інформаційно-аналітичної діяльності у завданнях Національної поліції приятиме:

– значному покращенню результатів, які виявляють та документують працівники поліції щодо злочинів, і завдяки інформаційно-аналітичної діяльності збільшить кількість цих результатів;

– з цього випливає і зниження рівня злочинності, ефективнішого підтримання публічного порядку та громадської безпеки;

– правильна оцінка ризиків та своєчасне вживання оперативно-профілактичних заходів на даній місцевості;

– оптимізація процесу.

Отже, підрозділи інформаційно-аналітичного забезпечення та швидкого реагування займають центральне місце в інформаційно-аналітичному супроводі поліції. Найголовнішою особливістю профпридатності працівників на всіх рівнях є вимога досконалого знання інформаційних технологій, вміння аналізувати, обробляти та використовувати інформацію, залучаючи для цього найсучасніші інформаційно-технологічні засоби, прогресивний розвиток якого призведе до постійного вдосконалення навичок роботи з новітніми технологіями.

Список використаних джерел:

1. *Використання сучасних інформаційних технологій в діяльності національної поліції України:* матер. Всеукр. наук.-практ. семінару (м. Дніпро, 23 листопада 2018 р.). Дніпро: ДДУВС, 2018. 150 с

2. Використання інформаційно-аналітичних можливостей у протидії злочинності. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 4 (109). URL: https://scientbul.naiau.kiev.ua/index.php/scientbul/article/download/993/1004/

Гусева С. О.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРИНЦИП ДОСТУПНОСТІ ІНФОРМАЦІЇ У НАЦІОНАЛЬНІЙ ПОЛІЦІЇ УКРАЇНИ: МІЖНАРОДНИЙ ДОСВІД

З кожним роком інформація має зростаючу роль для сучасного населення, вона є провідною у кожній сфері суспільного життя. Особливого значення набуває принцип доступності інформації. Для розвитку демократичного суспільства є необхідним забезпечити доступ та відкритість до цієї інформації, особливо органів державної влади, місцевого самоврядування та правоохоронних структур. Кожному громадянину важливо мати двосторонній взаємозв'язок із даними соціальними інституціями. Не так давно в Україні почала функціонувати реформа правоохоронних органів, що перш за все пов'язана із створенням нового органу державної влади – Національної поліції України.

Одним із позитивних перших кроків на шляху реформування правоохоронних органів з метою наближення їх до громадян і формування взаємної довіри, стало розробка офіційного сайту Національної поліції України, де передбачена можливість доступу до різноманітної інформації, оформлення і подання звернень громадян, консультації з громадськістю тощо. Це стало відповіддю на запити громадян щодо подолання безпрецедентної за масштабами криміналізації суспільних відносин, зростання багатьох видів злочинності та у різноманітнення її форм. Особливе серед громадян викликають занепокоєння явища, що зумовлюють латентність злочинності, передусім відсутність дієвого механізму реагування з боку органів поліції на звернення громадян. Як наслідок, злочинність зростає, а суспільство втрачає довіру до будь-яких представників органів державної влади. Саме для унеможливлення таких дій в подальшому варто звернути увагу на налагодження інформаційно-комунікаційних каналів зв'язку між громадянами та правоохоронними органами влади, зокрема нагальну потребу в організації та налагоджені системи надання електронних послуг в правоохоронній діяльності України. Якщо якісно забезпечувати інструменти електронного урядування в поліції, то це дасть змогу оперативно повідомляти відповідні інстанції про злочини, цікавитися про фактичний стан перебігу справи злочинця, спростити процес надання адміністративних послуг для громадян, налагодити пошукову систему

отримання необхідної інформації, отримати доступ до нормативно-правових документів, долучитися до співпраці з поліцією шляхом проходження спеціалізованої он-лайн школи підготовки тощо.

Це сприяє управлінню органами поліції, як складною правоохоронною системою в мінливому соціальному середовищі, оптимізації самої системи та своєчасному розподілу її ресурсів. Усе це неможливе без розвитку інформаційно-технологічного забезпечення в управлінні, яке має бути постійним, безперервним, у режимі моніторингу [1, с. 580].

Результатом практичного впровадження електронних послуг в рамках правоохоронної системи є забезпечення доступності, прозорості та зручного користування для всіх без виключення громадян Варто зазначити, що дана практика вже впроваджена в багатьох країнах світу: Великобританія, США, Франція, Естонія, Данія, Фінляндія, Норвегія, Швеція, Японія, Сінгапур. Надання різноманітних електронних послуг стали вже звичними та природніми для цих країн, що значно оптимізує та покращує суспільне життя. Рушійним кроком до створення громадянського суспільства став Указ Президента України від 26 лютого 2016 року № 68/2016 «Про сприяння розвитку громадянського суспільства в Україні» [2].

Розроблення нової Стратегії обумовлено змінами основних тенденцій розвитку громадянського суспільства, зростанням його ролі в різноманітних сферах – від просування реформ на державному і місцевому рівнях, європейської інтеграції та розвитку електронного урядування до надання волонтерської допомоги Збройним Силам України, іншим військовим формуванням, правоохоронним органам, органам державної влади під час дії особливого періоду, проведення антитерористичної операції, надання допомоги внутрішньо переміщеним особам.

Розглянемо на досвіді поліції Швеції надання електронних послуг. Аналізуючи офіційний сайт Національної поліції Швеції можна зробити певні висновки, що в поліції налагоджений тісний взаємозв’язок з населенням [3]. Принцип роботи поліції Швеції як раз і ґрунтується в основному на довірі. Можливість он-лайн сповіщення про крадіжки чи шахрайство, наявність електронних звітів про злочинність за допомогою мережі Інтернет. Консультування представлено у формі різних форм допомоги і підтримки, підказок і порад у попередженні злочинності, та допомоги у наданні консультацій з будь-яких питань. Доступно показано всі етапи стану розгляду кримінальної справи від заяви потерпілого до стану справи в суді. Візуалізація сайта є легко доступною та простою у використанні для всіх категорій населення та з різними можливостями. Шведська поліція, як і будь-яка інша державна структура цієї країни, функціонує на основі клієнт-орієнтовної системи, в центрі якої права і комфорт громадян. Поліція працює на запит своїх клієнтів, громадян Швеції, а тому в неї чітке бачення власної місії і цілей [4].

Для України буде корисним вивчення та застосування досвіду надання електронних послуг в таких країнах, як Великобританія, Німеччина, Швеція,

Данія, особливо в аспекті впровадження та функціонування електронних послуг в правоохоронний структурах. З впровадженням правоохоронної реформи вже можна спостерігати тендецію становлення – послуг в даній галузі. Це не поганий початок, проте потрібно ініціювати проведення потужних реформ щодо розвитку електронних послуг і надалі. Уряд України має встановити прямий діалог з громадянами. Адже лише спільні дії та порозуміння між громадянами та правоохоронними структурами, зможе привести нашу країну до гідного та щасливого майбутнього, сформувати довірливі відносини та знизити рівень злочинності.

Список використаних джерел:

1. Сокуренко В. В. Управління органами Національної поліції України: підручник. Харків: Стильна типографія, 2017. С. 580.
2. Указ Президента України «Про сприяння розвитку громадянського суспільства в Україні» № 487/2021 від 27.09.2021 р.
3. Коваль Р. А. Інформаційно-аналітичне забезпечення діяльності органів влади: автореф. дис. канд. наук з держ. управ.: 25.00.02. Запоріжжя, 2020.
4. Мовчан А. В. Теоретичні засади інформаційно-аналітичного забезпечення оперативно-розшукової діяльності. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 2. URL: http://dspace.lvduvs.edu.ua/bitstream/1234567890/318/1/мовчан.pdf.

Загоровська І. О.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Гребенюк А. М.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ

З 24 лютого 2022 року російськими військовими було здійснено повномасштабне вторгнення на територію України. У зв’язку з чим було продовжено гібридну війну, в якій військовий фактор є лише однією складовою. На сьогоднішній день війна триває не тільки на фронті, а й в інформаційному просторі. Інформація дозволяє вигравати у війні не зробивши жодного пострілу, шляхом формування і розпалювання внутрішніх протиріч [2].

Тому важливого значення в умовах сьогодення займає питання інформації, як стратегічного інструменту перемоги. В час, коли джерелом інформації

і лідером суспільної думки може стати практично кожен, поширювана інформація не завжди може відповідати потребам, які диктуються захистом національної безпеки. З початку повномасштабного вторгнення кожен житель держави публікував велику кількість інформації в соціальних мережах, жодним чином не підтверджуючи її доказами. Всі були налякані, моніторили новини кожну хвилину і вірили усім новинам. Перший час такі дії дійсно підтримували бойових дух населення та допомогали тримати психіку у нормі в такий тяжких час, але згодом інформаційний потік почав погіршувати становище українця.

Гостроти проблематиці інформаційної безпеки додає спроможність ворога маніпулювати інформацією, прописувати власні наративи, відповідно, впливати на свідомість людей та формувати зручний для себе інформаційний простір. Окупаційною владою щоденно здійснюється інформаційний тиск на населення, публікуєтеся реклама, мітинги та інша журналістська діяльність із закликами «Україна покинула Херсон», «Росія тут назавжди» й інші абсурдні фрази, які нездорова психіка людини сприймає, як доведений факт [3].

З іншого боку, сучасні технічні можливості дозволяють практично в прямому етері слідкувати за розвитком воєнних дій і, відповідно, викривати злочинні дії агресора, що є визначальним у перевазі на інформаційному фронті.

Рішенням РНБО від 8 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» визначається, що в умовах воєнного стану пріоритетним питанням визначається реалізація єдиної інформаційної політики, наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини #UAразом»«. З огляду на це рекомендовано Національній раді України з питань телебачення і радіомовлення вжити заходів щодо реалізації цього рішення [1]. У той самий час канал «Інтер», що був рупором російської пропаганди, майданчиком для антиукраїнських сил став частиною проєкту «Єдині новини #UAразом» [2].

З боку законодавця необхідно здійснити ряд дій, для будування ефективної системи інформаційної безпеки:

1) технічна складова – передбачає створення і функціонування всіх необхідних технічних складових систем;

2) політична – державна політика повинна бути спрямована на забезпечення інформаційної безпеки;

3) правова – оформлення всіх пов’язаних елементів у якісні нормативно-правові акти [3].

Отже, підсумовуючи проведене дослідження, можна дійти висновку, що сьогоднішні воєнні реалії чітко демонструють, що інформація є зброєю «масового ураження». Тому необхідно створити ефективний механізм, який би забезпечив державну інформаційну безпеку і дотримання прав людини та водночас дозволив би людям не відчувати ефекту посягань на свободи та демократію. У воєнний час захист інформаційної безпеки держави є пріоритетним оскільки безпосередньо від нього залежить безпека суспільства і людини. У час війни публічно-правовий захист виходить за межі традиційного регулювання і поглинає приватно-правові відносини.

Список використаних джерел:

1. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану. Рішення РНБО. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#Text.
2. Детектор медіа. URL: https://detector.media/infospace/article/198490/2022-04-18-opzzh-ne-pratsyuie-shchobude-z-interom/
3. Інвестиційна підтримка державної інформаційної безпеки україни в умовах воєнного стану: аналіз актуальних законодавчих новацій. URL: http://appj.wunu.edu.ua/index.php/appj/article/view/1334.

Здоровець Т. О.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

КІБЕРАТАКИ ЯК РИЗИК ДЛЯ ДЕРЖАВИ

В епоху інформаційних технологій неможливо почуватися захищеним у кіберпросторі. З розвитком технологій стрімко зростає кількість злочинів у цій сфері, а тому з впевненістю можна стверджувати, що саме «кіберзлочини» у XXI столітті будуть одними з найчисельніших.

Кібератака – це шкідлива, свідома спроба людини або організації проникнути в інформаційну систему іншої людини або організації. Як правило, порушуючи роботу мережі жертви, хакер прагне отримати зиск.

Зловмисники сподіваються скористуватися вразливістю корпоративних систем, що зумовлює щорічне зростання кіберзлочинності. Часто хакери вимагають викупу. Як звітує світова статистика – у середньому одна з 53 % кібератак призводять до збитків у розмірі 500 000 дол. США або більше, за рік [1].

Кібератаки можуть мати приховані мотиви. Деякі спроби хакерів є своєрідними проявами «хактивізму», наприклад, знищити системні дані, або ж викрасти їх.

Хактивізм – використання комп'ютерів та комп'ютерних мереж для просування політичних ідей, свободи слова, захисту прав людини і забезпечення свободи інформації. Якщо такі політичні ідеї суперечать інтересам держави, то зазвичай наносять великий удар по економіці країни та політичній орієнтації суспільства, що є одним із негативних наслідків кібератак.

Такі протиправні діяння вже сьогодні складають для нашої держави, як і для багатьох інших країн світу, певну суспільну небезпеку, реально загрожуючи інформаційній безпеці – складовій національної безпеки.

В недалекому минулому, а саме в 2014 році, Україна стала учасником у кібервійни з державою «агресором», що триває й до нині. Російсько-українська кібервійна стала першим конфліктом в кіберпросторі, коли була здійснена успішна атака на енергосистему з виведенням її з ладу. На думку Адміністрації Президента США хакерські атаки на Україну з боку Росії в червні 2017 року із використанням вірусу NotPetya стали найбільшою відомою хакерською атакою.

В наш час, у мережі «Інтернет» зазначена низка заходів безпеки що допомагають мінімізувати випадкові, або ж цілеспрямовані, несанкціоновані проникнення у пристрої громадян та державні системи. Звичайно, неможливо повністю викорінити такі ризики, але держава активно бореться для того, щоб максимально уникати хакерських атак, та зламу національної безпеки.

В українських новинах сьогодення, вже з'являється інформація про створення специфічного підрозділу (кібервійська), сфера якого буде розповсюджуватися саме на кіберпростір, задля того, щоб активізувати засоби боротьби, та процес забезпечення національної безпеки на світовому рівні [2].

Кібервійськові виконують бойові завдання, поставлені командуванням. Тобто все те саме, що роблять і звичайні хакери, тільки мотивація інша – за наказом Батьківщини.

У якості висновку, можу зазначити, що неабиякий внесок у захист національної безпеки не лише України а й інших держав, може зробити саме обмін важливою інформацією між державами, спільні ідеї та об'єднання можливостей. Адже лише методом співробітництва та взаємної допомоги можливо розвиватись та еволюціонувати у сфері національної кібербезпеки.

Список використаних джерел:

1. Что такое кибератака? : веб-сайт. URL: https://www.cisco.com/c/ru_ru/products/security/common-cyberattacks.html#~definition.
2. Нові українські кібервійська: веб-сайт. URL: https://www.dw.com/uk/%D0%BD%D0%BE%D0%B2%D1%96-%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1.

Калашнік Д. О.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРОБЛЕМИ ПОШУКУ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ ПРАЦІВНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Якісне інформаційне забезпечення діяльності Національної поліції відіграє одну з ключових ролей у ефективності виконання покладених на неї задач. Багато інформації поліцейські отримують використовуючи відомчі бази даних Інформаційного порталу Національної поліції. Але у зв'язку з надпотужним розвитком інформаційних ресурсів загального користування мережі Інтернет, багато цінної інформації для виконання службових обов'язків можна черпати з відкритих джерел. Проблеми пошуку інформації з відкритих джерел розглядаються у цій доповіді.

Обсяг доступних інформаційних ресурсів у мережі Інтернет постійно зростає. Дані ресурси характеризуються величезним обсягом, слабкою структурованістю та високою розподіленістю інформації. Існуючі методи та підходи не забезпечують у багатьох випадках необхідний час та точність пошуку та обробки необхідних даних, тому розробка нових методів, що дозволяють підвищити ефективність використання інформаційних та обчислювальних ресурсів комп'ютерних та телекомунікаційних мереж з метою зменшення часу та підвищення точності пошуку та обробки інформації, актуальна.

Існує велика кількість пошукових машин (Google, Yandex, AltaVista та ін), які у відповідь на запит користувача, сформований у контекстній формі, тобто у вигляді набору слів та словосполучень, повертають набір посилань на документи, що містять дані слова та словосполучення. Для підвищення зручності формування запитів більшістю пошукових машин надається можливість використання у запитах операцій (кон'юнкції, диз'юнкції, заперечення та ін.) [1].

Також існує можливість пошуку в рубриках, пошук схожих документів та інші функції. Однак незважаючи на наявність великої кількості функцій, покликаних полегшити та прискорити процедуру пошуку інформації в Інтернет, основною проблемою, що виникає при використанні широко відомих пошукових машин, є відносно низька релевантність посилань, внаслідок чого користувачеві

додатково необхідно переглядати велику кількість документів. Причини криються в багатоваріантності людської мови, можливості використання синонімів, відсутності повноцінних засобів налаштування засобів пошуку для конкретної предметної області, що цікавить користувача.

При організації пошуку в мережі Інтернет доцільно використовувати існуючі пошукові машини як один із засобів отримання вихідного набору посилань для подальшого аналізу, також такими засобами можуть бути власні набори посилань по предметним областям користувача та різного роду каталоги. Отримання вихідного набору посилань є першим етапом виконання запиту, його виконання не є трудомістким завданням і не вимагає зчитування великого обсягу даних з Інтернету, тому розпаралелювання на даному етапі не потрібно.

Розглянемо застосування поліцейськими чат-ботів у месенджері Telegram. Взагалі, чат-боти створюються для загального доступу, але деякі з них містять важливу інформацію, за допомогою якої правоохоронці можуть отримувати інформацію про суб'єкта, його зв'язки або об'єкт посягання практично миттєво. Для використання чат-боту не потрібно додатково встановлювати додатки на свій пристрій, витрачаючи оперативну пам'ять, отримувати додатковий дозвіл та залишати особисту інформацію на незнайомих серверах. Серед недоліків використання чат-ботів є неофіційний характер отриманої інформації, іноді платний контент, а також те, що бот необхідно знайти та перевірити його на спроможність виконувати необхідну функцію, що в реаліях роботи правоохоронця дуже складно зробити через брак часу [2, с. 394].

Використання інструментаріїв, описаних у даній доповіді, для пошуку інформації з відкритих джерел працівниками Національної поліції значно покращує інформаційну підтримку діяльності поліції що підвищує її ефективність.

Список використаних джерел:

1. Бевз С., Бурбело С., Боднар П.. Спеціалізовані пошукові системи для глобальної мережі. *Сучасні проблеми радіоелектроніки, телекомунікацій та приладобудування (СПРТП – 2019):* матер. VIII Міжнар. наук.-техн. конф. (м. Вінниця, 19-21 травня 2019 р.). С. 32-33.
2. Вишня В. Б., Ісмайлов К. Ю.,Краснобрижий І. В. Інформаційні технології : підручник. Дніпро: ДДУВС, 2021. 492 с. URL: http://er.dduvs.in.ua/handle/123456789/6820.

Коваль А. Д.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ВИКОРИСТАННЯ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПРОТИДІЇ ЗЛОЧИННОСТІ НА ТЕРИТОРІЇ УКРАЇНИ

На сьогоднішній день стрімкий розвиток інформаційних технологій є притаманний для всіх сфер суспільного життя, не є виключенням і правова сфера, а саме сфера правопорядку. Такі процеси є досить необхідними для сучасного життя адже вони значно полегшують його, дозволяючи проводити різного роду операції, пов'язані з інформацією, докладаючи мінімум зусиль для цього. В сучасних умовах розвитку українського суспільства інформаційні технології є одним із засобів за допомогою яких окремі групи людей виконують покладені на них функції, не є виключенням і підрозділи Національної поліції України. Необхідність використання інформаційних технологій у підрозділах Національної поліції обумовлюється великою кількістю інформації, яка потрібна для виконання покладених на них повноважень.

Для початку треба з'ясувати поняття «Інформаційні технології». Так науковець Рогатюк І. визначає у своїй праці поняття «Інформаційні технології» як сукупність методів, інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування, об'єктом яких є інформація [1].

Проаналізувавши чинне українське законодавство у сфері інформаційно-аналітичного забезпечення, ми визначили, що використання підрозділами Національної поліції України інформаційних технологій регламентується Постановою Кабінету Міністрів України від 28 жовтня 2015 року № 877 «Про затвердження Положення про Національну поліцію» та Законом України «Про Національну поліцію», а саме статтями 25 «Повноваження поліції у сфері інформаційно-аналітичного забезпечення», 26 «Формування інформаційних ресурсів поліцією», 27 «Використання поліцією інформаційних ресурсів» та 40 «Застосування технічних приладів, технічних засобів та спеціалізованого програмного забезпечення» [2].

На сьогодні в Україні розповсюджена така інформаційна система яка має назву «Інформаційний портал Національної поліції України», ця система має на меті формування інформаційних баз обліку МВС України, надання оперативного доступу до інформаційно-довідкових баз даних МВС України, обробки інформації, яка утворена в процесі діяльності поліції. Діяльність та функціонування цієї системи затверджені наказом МВС № 676 від 03.08.2017 «Про затвердження Положення про інформаційно-телекомунікаційна систему «Інформаційний портал Національної поліції України» [3].

Інформаційний портал Національної поліції України не є єдиною інформаційною системою, яка застосовується в діяльності Національної поліції України. Наприклад, до складу Єдиної інформаційної системи Міністерства внутрішніх справ входять: 1) Інтегрована інформаційно-пошукова система Національної поліції; 2) Система централізованого управління нарядами патрульної поліції «ЦУНАМІ»; 3) ДБД Арсенал – відомості щодо зброї, яка перебуває на озброєнні МВС, МО, МНС, АДПС, СБУ, ДПА, ДМС, ДДПВП, УДО; 4) ІС Оріон – єдині оперативні обліки, які передбачені Законом України «Про оперативно-розшукову діяльність»; 5) ОДК – оперативно-довідкова картотека, в який розміщено відомості щодо притягнення осіб до кримінальної відповідальності та судимості осіб; 6) АДІС «ДАКТО» – автоматична дактилоскопічна інформаційна система [4, с. 109].

Отже виходячи з вищевказаних фактів ми можемо зробити висновок, що наразі використання інформаційних технологій у підрозділах Національної поліції України є досить розвиненою тенденцією станом на 2022 рік, існує багато систем та підсистем які використовуються в діяльності поліція як для зберігання інформації так і для протидії злочинності тому застосування відповідних інформаційних систем дає змогу поліції швидше реагувати та протидіяти злочинності на території нашої держави.

Список використаних джерел:

1. Рогатюк І. В. Використання інформаційних технологій у досудовому розслідуванні: сучасний стан і перспективи розвитку. Н*ауковий вісник Національної академії внутрішніх справ*. 2013. № 3. 9 с.
2. Закон України «Про Національну поліцію» – Документ 580-VIII, редакція від 15.06.2022 р. 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.
3. Наказ Міністерства внутрішніх справ України № 676 від 03.08.2017 р. – Документ z1059-17, редакція від 01.04.2022 р. z0349-22. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.
4. Вишня В. Б., Ісмайлов К. Ю., Краснобрижий І. В. Інформаційні технології: підручник. Дніпро: ДДУВС, 2021. 492 с. URL: http://er.dduvs.in.ua/handle/123456789/6820.

Криса О. Ю.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Паршин Ю. І.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

ПРОБЛЕМИ ТА ЕКОНОМІЧНЕ ВРЯДУВАННЯ УКРАЇНИ В УМОВАХ ВІЙНИ

Військове вторгнення російської федерації завдає потужного удару по економіці країни та завдає величезної шкоди інфраструктурі, промисловим об'єктам, об'єктам комунального та соціального призначення, що є спробою знищити незалежність України. Більшість підприємств і половина ВВП розташовані в 10 областях, де ведуться бойові дії.

Найбільше окупованих територій за кількістю підприємств, які не можуть працювати, є у таких регіонах, як Київ (121 572), Запорізька (15 368), Херсонська (8 116) та Донецька (9 473) області [1]. Багато логістичних ланцюгів повністю розірвані, багато підприємств фізично знищені, деякі не можуть працювати у воєнному режимі, багато працівників виїхало [2]. Проте економіка держави має працювати, перш за все, забезпечуючи як потреби Збройних Сил України під час війни з Російською Федерацією, так і щоденні потреби населення у житлі, харчах, медикаментах, одязі, тощо

Мобілізація резервів відбулася в перші тижні війни, але запаси потребуватимуть постійного поповнення, яке можна реалізувати шляхом тимчасового перенесення господарської діяльності у «безпечні» райони, залучення тимчасово переміщених осіб, а головне – зменшення дисбалансу попиту та пропозиції та можливість подальшого фінансування бюджетних видатків. Уряд вжив потужних заходів для підтримки рівня доходів населення: підтримано виплати працівникам бюджетної сфери, пенсії, здійснено виплати особам, які вимушено втратили роботу, суттєво збільшено виплати військовим збільшився та ін.

Втрата значною частиною підприємств правоздатності вимагає зовнішнього втручання в економічні процеси нашої країни. Окрім гуманітарної допомоги, Україна потребує масштабної фінансової підтримки для підтримки економіки та зусиль уряду для підтримки постраждалих українських громадян.

Також з початком війни Україна отримала нові виклики, які потребують економічного вирішення:

– зросла потреба у видатках на інформаційну сферу війни – дезінформацію, пропаганду та протидію;

– важче мобілізувати населення для бойових дій, зростає роль розподілу благ між соціальними групами;

– інвестиції, акції компаній, фінансова та платіжна системи потребують максимального збереження сприятливого клімату розвитку;

– повне імпортозаміщення стає неможливим - зростає роль запасів нових видів ресурсів, патентів, технологій, спеціалістів виробництва;

– матеріально-технічне забезпечення військових дій або стратегія оборони має враховувати значну кількість нових сфер, зокрема кіберсферу [3].

У нинішній період, в умовах воєнного часу, критично необхідно забезпечити стабільність економіки шляхом її ефективного управління, що допоможе перейти до етапу післявоєнного відновлення та майбутньої інтеграції до Європейського Союзу.

Список використаних джерел:

1. Наслідки будуть колосальними: Марченко розповів, як війна вплине на економіку України. Аналітичний портал «Слово і діло». URL: https://www.slovoidilo.ua/2022/03/14/novyna/ekonomika/naslidky-budutkolosalnymy-marchenko-rozpoviv-yak-vijna-vplyne-ekonomiku-ukrayiny.
2. Державна служба статистики України. URL: http://www.ukrstat.gov.ua.
3. Мороз В. П., Паршин Ю. І., Богуславський М. Г., Козін В. В. Громадська оцінка діяльності департаменту стратегічних розслідувань Національної поліції України. *Юридичний науковий електронний журнал*. 2022. № 7. С. 255-258. URL: http://lsej.org.ua/7_2022/59.pdf.

Кузовко В. О.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНІ ТА ПСИХОЛОГІЧНІ ОПЕРАЦІЇ

Інформаційна війна́ (англ. information warfare) – викладення інформації у спосіб, який формує у суспільстві чи групі людей потрібну точку зору, громадську думку, хід взаємодоповнюючих логічних думок, вичерпну систему поглядів щодо окремих питань на користь організатора інформаційної пропаганди [1]. Щоб зрозуміти всю серйозність і необхідність застосування, досить подивитися на стандарти НАТО планування ІО та ПО [2].

Таблиця 1

Послідовність оперативного планування воєнних операцій (ІО, ПО) НАТО

Етапи планування	Заходи, що виконуються штабом	Брифінги командира	Рішення командира	Документи, що розробляються	Результуючі директиви
І. Ініціація	Військові оцінки	-	Оцінка обстановки	Військові оцінки	Початкова директива
ІІ. Орієнтування	Аналіз місії	Брифінг з аналізу місії	Бачення командира і вказівки	Вказівки командира з планування	-
ІІІ. Розроблення концепції операції	Розроблення способу дій	Брифінг із вибору способу дії	Брифінг із вибору способу дії	Концепція операції/ Вимоги до сил і засобів	Директива з активації сил
IV. Розроблення плану операції	Розробка плану операції	Брифінг із затвердження плану операції	Затвердження плану	План операції	Директива з виконання
V. Перегляд плану операції	Перегляд і оцінка плану	-	-	-	-

Наш головний супротивник росія володіючи потужними силами психологічних операцій до яких входять: сили та засоби ПсО військових формувань сили та засоби ПсО спецслужб; цивільні державні структури, які залучені до проведення інформаційних операцій; цивільні недержавні структури (підконтрольні уряду) – які залучені до проведення інформаційних операцій; релігійні організації, які залучені до проведення інформаційних операцій. Задіювати вона їх почала від початку своїй агресії, як для створення позитивних тез агресії для внутрішніх глядачів, так і для спотворення інформації серед наших громадян. Пізніше вже с початком саме бойових дій за допомогою так званої електронної війни почали використовувати РЕБ,саме за допомогою комплексу «Леер-3», в комплект якого входять два безпілотних літальних апарата «Орлан-10», що можуть імітувати базову станцію GSM зв'язку, українським бійцям надсилаються повідомлення деморалізуючого змісту. У повідомленнях українських військових порівнюють із «німцями під Сталінградом», називають «м'ясом для своїх командирів», обіцяють «неминучу кару», «знаходження під снігом до весни» тощо. Так для нашої армії такий «удар» було завдано вперше, інцидент набрав розголосу в соціальних мережах, де вже до дискусії підключись ворожі «боти» розганяючи нормативи про зраду командирів, немов командування давно вже продали їх місце розташування, персональні дані. Звідси можна зрозуміти як комплексно росія підходить до подібних атак. Україна під час АТО також використовувала інформаційні операції, але іншого характеру, для придушення сепаративного настрою. Наприклад СБУ вела програму «На тебе чекають вдома», за допомогою плакатів, телесюжетів та навіть з використанням агітаційного снаряду з листівками.

З 24 лютого росія активно веде проти України ІО та ПО, навіть за межами двох країн. Якщо лобіюваними рф іноземні ЗМІ можуть спростувати наші закордоні дипломати, то операції які мають ціль на населення України, в більшу міру повинні «відбиватись» народом самотужки, держава лише повинна проінформувати про засоби та методи ведення цих операцій. Центр стратегічних комунікацій та інформаційної безпеки показав себе дуже дієво та оперативно. Але більша відповідальність на населенні, тому вони повинні фільтрувати свій інформаційний простір. Наприклад на фоні медіагаласу про те, що герої с Азовсталі виконали наказ Президента та здалися в полон, стрічка переповнилася репостами людей на публікації, які мали характерні прояв методу Гебельса 40 на 60, де 60 відсотків інформації про героїчний поступок бійців, та 40 про недовіру до Президента та початку мітингів, не дивлячись на пояснення та прохання Генштабу та Головного розвідувального управління, люди які опирались на емоції та хотіли показати свою активну громадську позицію, стали співучасниками операції та розігнали її по мережі.

Потрібно задавати собі питання: кому це б було вигідно? Якщо Головне командування попросило не піднімати це питання поки бійців не визволять?

Росія веде жорстку та безпрецедентну інформаційну та психологічну війну. Ми як народ України повині і на цьому полі не тільки відбивати її та відповідати тим же. В пріоритеті повинно бути фільтрування джерел інформації, а не емоції.

Список використаних джерел:

1. Вікідепія – вебсайт. URL: https://uk.m.wikipedia.org/wiki/Інформаційна_війна.
2. Заруба О. Г. Планування спеціальних інформаційних операцій. *Інформаційна безпека людини, суспільства, держави.* 2017. № 1. С. 140-154. URL: https://uk.m.wikipedia.org/wiki/Інформаційна_війна.

Курило Д. А.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ЕКОНОМІЧНА РІВНОВАГА ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

З початку повномасштабної агресії російської федерації проти України та українського народу ціни на де які товари або послуги збільшилися в декілька разів. Частіше за всього причинною цього стало або не хватка кадрів або неможливість створювання продуктів збиту. Так у літку 2022 року був частино зруйнований підприємство Артемсіль. Тоді пішла нестача солі, ціни на неї були завищені в 1,5-2 рази. З годом ця проблема вирішилась, але відбиток на економіці громадян все ж таки залишився. За декілька місяців до того був дуже сильний дефіцит топлива. Ціни також росли аж доки він зовсім не зник з заправок. Деякі громадяни зменьшили час на використання автівок а хтось підійшов до вирішення цієї проблеми більш радикальним засобом, багато автотранспорту стояло неділями та навіть місяцями, де хто їздив на роботу на велосипеді, громадським транспортом або зовсім йшли пішки. Багато хто, через не стачу топлива, навіть втратив свій заробіток. Цю проблему теж держава вирішила, але все ж таки наслідки де яких громадян переслідують по сьогодні. Багато експертів прогнозують, що це ще не конець, бо [1] у доповіді Світового банку говориться також про те, що бідність в Україні зросте вдесятеро, а станом на кінець 2022 року один з п’яти українців, за прогнозами, житиме в бідності. У документі додають, що головними чинниками є різке зростання цін на продовольство, а також переміщення мільйонів людей, які втратили свої домівки.

Аналітики наголошують, що зростання рівня бідності буде ще більшим від прогнозованого, якщо уряди та інституції в усьому світі не зможуть надати Україні достатнього фінансування для поповнення невоєнного бюджетного дефіциту України, який є великим і невпинно зростає [1].

«Україні довелося мобілізувати велику кількість власних ресурсів, включно з монетизацією, що призвело до інфляційного тиску. Тож чим більше грантового фінансування ми зможемо надати Україні, тим краще», – зазначає Віце-президент Світового банку Анна Б’єрде.

В якості висновку зазначимо, що головне не піддаватися паніці, всі проблеми, економічного або матеріального характеру держава намагається як най швидше вирішити, щоб запобігти кризи.

Список використаних джерел:

1. Салліван А., Ржеутська Л. Як війна вплинула на економіку України. DW – 12.09.2022 р. URL: https://www.dw.com/uk/ak-vijna-vplinula-na-ekonomiku-ukraini/a-63093916.

Лініченко Ю. А.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Паршин Ю. І.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

СТАН ОРГАНІЗОВАНОЇ ЗЛОЧИННОСТІ В СУЧАСНОМУ СВІТІ

Організована злочинність є продуктом суспільства та пронизує своїм негативним впливом його різні сфери та соціальні відносини. У той же час вона як самостійне цілісне явище має власні закономірності розвитку. Отже, проаналізуємо стан організованої злочинності у світі загалом та за окремими показниками у нашій країні.

За даними на 2021, 2020, 2019 та 2018 роки Україна посідала 150, 152, 154 та 156 місце відповідно зі 163 позицій згідно з міжнародним рейтингом найбезпечніших для життя країн у Глобальному індексі світу. У цьому рейтингу 2021 року Україна посіла позицію між Північною Кореєю та Суданом. Для порівняння: у 2017 р. наша держава посідала 152 місце, у 2016 р. – 144, з 2010 по 2013 рр. – 120, 2009 р. – 118 місце [1]. Можна констатувати тенденцію щодо підвищення рівня небезпеки для життя людей в Україні.

Згідно з Концепцією розвитку сфери безпеки та оборони України, поширення організованої злочинності є однією з найактуальніших загроз у середньостроковій перспективі. Основними завданнями сектору безпеки та оборони є боротьба з тероризмом, корупцією та організованою злочинністю у сфері управління та економіки. Відповідно до звіту Генеральної прокуратури України за результатами боротьби з ОГ та ЗО, у 2020 році виявлено 288 ОГ та ЗО, з них 7 з неповнолітніми, 21 з корупційними зв'язками, 10 з них в органах влади та управління, з міжрегіональними зв'язками – 41, з транснаціональними зв'язками – 7, сформованими за національною ознакою – 17, з них у бюджетній сфері – 22, у банківській системі – 7, зокрема комерційних банках – 7, у фінансово-кредитній системі (без банків) – 4, у сфері земельних правовідносин – 1, у вугільній промисловості – 4, у нафтогазовій галузі – 3, в електроенергетичному комплексі – 1, у металургійній промисловості – 2 [1].

За результатами аналізу заходів щодо протидії організованій злочинності підрозділами кримінальної поліції за січень-травень 2021 р., порівняно з цим періодом 2020 р. зареєстровано 151 ОГ та ЗО (на 13,6 % більше, ніж за аналогічний період минулого року (151 од. проти 133) у складі 566 учасників, які були викриті за скоєння 1096 правопорушень, з них 833 тяжкі та особливо тяжкі.

Однією із головних проблем у нашій країні залишається боротьба з корупційними злочинами. За 2021 рік правоохоронними органами (без урахування НАБУ) виявлено 3679 кримінальних корупційних правопорушень (2831 у 2020 році, 2175 у 2019 році, 2493 у 2018 році), і це більше, ніж у попередні роки [1-2].

Що стосується зарубіжних країн, то правоохоронні органи країн ближнього зарубіжжя нині не мають єдиної офіційної статистики організованої злочинності, хоча, за різними оцінками вчених та фахівців, на території цих країн налічується кілька сотень організованих злочинних груп, які мають великі міжнародні зв'язки [3, с. 104]. За даними МВС України, до глобальних злочинних організацій залучено понад 2000 громадян України. Вони мають міцні зв'язки із кримінальними структурами країн СНД, Балтії, США, Німеччини, Польщі, Угорщини, Туреччини та інших країн [4, с. 128].

Проте ні на науковому, ні на емпіричному рівні достовірно не відомі реальний стан та масштаби діяльності організованих злочинних груп, у тому числі в економічній сфері, а також кількість скоєних ними правопорушень.

Згідно зі статистичними звітами МВС Польщі, з 2005 р. спостерігається постійне зниження кількості злочинів, скоєних організованими групами та злочинними організаціями у державі. Їх кількість зменшилася з 7741 у 2005 р. до 4682 у 2007 р., 3670 у 2008 р., 3514 у 2009 р., 3135 у 2010 р., 3023 у 2014 р., 2128 у 2 р., 1608 – 2020 р. [5, с. 167].

На думку деяких експертів, ці статистичні дані відображають масштабну реформу правоохоронних органів європейських країн. Усього за 2005-2021 роки кількість виявлених організованих злочинних груп у Європі скоротилася більш ніж у 4 рази, а злочинів, скоєних цими групами, – у 4,8 рази з 2005 по 2021 рік [5, с. 170].

Звичайно, наведена статистика може свідчити не так про позитивні тенденції, як про посилення латентності даного виду злочинів та неефективну діяльність правоохоронних органів щодо їх розкриття.

Список використаних джерел:

1. Блажівський Є. М. Моніторинговий кримінологічний аналіз злочинності в Україні (2009-2021 роки): монографія. Київ: Національна академія прокуратури України, 2021. 484 с.
2. Про запобігання корупції: Закон України від 14.10.2014 р. № 1700-VII. URL: http://zakon3.rada.gov.ua/laws/show/1700-18/page.
3. Пятчаніна О. С. Загальні чинники міжнародно-правового співробітництва держав у протидії організованій транснаціональній злочинності. *Часопис Київського університету права.* 2016. № 9. С. 99-107.
4. Міняйло Н. Є. Організаційно-правові основи боротьби з організованою злочинністю. *Науковий вісник Чернівецького університету.* 2018. Вип. 714. Правознавство. С. 126-130.
5. Шостко О. Ю. Формування спільної європейської політики протидії організованій злочинності. *Проблеми законності*: зб. наук. праць. 2017. Вип. 89. С. 166-173.

Лукомська А. А.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Гребенюк А. М.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ОРГАНІЗАЦІЯ ВІДЕОСПОСТЕРЕЖЕННЯ ЯК НЕВІД'ЄМНА ЧАСТИНА КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ ОБ'ЄКТІВ В УМОВАХ ВОЄННОГО СТАНУ

На даний час Україна переживає бурхливе реформування, перетворення всіх своїх інститутів, як соціальних так і правових. Не виключенням є і правоохоронна система разом із законодавчою базою. В умовах науково-технічного прогресу, особливо в інформаційній сфері, представники криміногенного світу все частіше використовують в своїй злочинній діяльності передові здобутки такого розвитку. Не важливим чинником, який має суттєвий вплив на криміногенну ситуацію в країні є умови воєнного стану, у яких на сьогоднішній день перебуває наша держава. Тому правоохоронна система України вимушена змінюватись, еволюціонувати та перетворюватись з метою можливості надання адекватної відповіді злочинності.

Відеоаналітика є одним із найважливіших інструментів для досягнення поставлених цілей у боротьбі зі злочинністю. Все, що потребується від працівника воєнізованої охорони та Національної поліції – це навички у отриманні та використанні інформації із відеокамер. Це є золотим ключем до відкриття усіх «зчинених» злочинів тільки в тому випадку якщо встановлені новітні системи відеоспостереження.

Кримінальний аналіз, який останнім часом активно впроваджується в діяльність Національної поліції України, що на наше переконання є беззаперечним позитивом. Країни Європейського Союзу, США а також інші розвинені країни світу використовують можливості кримінального аналізу правоохоронними органами на постійній основі. Зміст, процедура та правила застосування детально регламентовані в законодавчій базі [1, с. 4].

Системи відеоспостереження дають змогу ефективно вирішувати значне коло питань, багато яких без застосування таких технологій складно, або взагалі неможливо вирішити. Камери відеоспостереження встановлюють: для охорони території, для контролю за виробництвом, для забезпечення особистої безпеки, для здійснення стеження, для ідентифікації осіб.

Саме Використання відеоінформації та сучасних технологій її обробки у діяльності Національної поліції сприятиме зниженню кількості правопорушень на «Укрзалізниці». Тому ми вважаємо, що особливості та проблеми, які виникають під час впровадження та реалізації відеоаналітичного забезпечення на залізничному транспорті потребують вирішення ряду технічних, організаційних та законодавчих питань.

Сьогодні розроблені сучасні методи та технології запобігання різних видів ризиків на залізних дорогах інших країн, а також створені системи прогнозування ризиків і катаклізмів. Необхідно сформувати правові та організаційно-економічні механізми зниження ризиків на залізничному транспорті за рахунок підвищення управлінського впливу на їх реалізацію.

В зв'язку з великою пропозицією різноманітних систем відеоспостереження необхідно розуміти і знати які вибрати камери та як їх встановити, які параметри вона має її чутливість і роздільну здатність, які поєднують одночасно всі переваги кольорових та монохромних (чорно-білих) камер відео спостереження.

У тих випадках, коли однією з головних умов є спостереження у кольорі та розпізнавання кольорів, використовують кольорові відеокамери. За якість одержуваного зображення відповідає роздільна здатність. А також можливість інтелектуальної обробки даних з використанням необхідного програмного забезпечення.

Чим вище роздільна здатність камери відеоспостереження, тим чіткішим буде підсумкове зображення і тим більша ймовірність розпізнавання дрібних деталей на зображенні. Дозвіл системи в цілому залежить від того компонента, який має найнижчу роздільну здатність.

Варто наголосити на тому, що залежно від типу використовуваного обладнання системи відеоспостереження ділять на аналогові та цифрові. Аналогові системи відеоспостереження використовують там, де необхідно організувати відеоспостереження в невеликій кількості приміщень та інформацію з відеокамер записувати на відеомагнітофон. Для безпеки особливо відповідальних або територіально розподілених об'єктів використовують цифрові системи відеоспостереження, які, як правило, інтегруються в комплексні системи безпеки. Такі комплекси фіксують, записують і аналізують інформацію, що надходить від відеокамер, зчитувачів системи контролю доступу, охоронних та пожежних датчиків, а також «приймають рішення» щодо захисту об'єкта, що охороняється, в автономному режимі або за вказівкою оператора системи [2].

Сьогодні цифрові технології відеоспостереження поступово «витісняють» аналогові системи за функціональними та технічними характеристиками, а за своєю ціною вже наближаються до вартості аналогових систем відеоспостереження.

Особливості зон, де мають бути встановлені відеокамери, далеко не єдиний параметр, який слід враховувати під час проектування системи відеоспостереження на залізничних об'єкті. Необхідно визначити: 1) норми освітленості; 2) наявність мертвих зон; 3) кліматичні та технологічні умови;

Ці параметри дозволять визначити кількість та тип необхідного для побудови системи відеоспостереження обладнання.

Отже, під час проектування системи відеоспостереження слід враховувати такі особливості: 1) розмір території; 2) можливість територіальної роз'єднаності об'єктів; 3) екстремальні умови роботи камер [3, с. 316].

На теперішній час одним із пріоритетів державної політики має бути рішення комплексу завдань, спрямованих на забезпечення життєдіяльності та створення умов безпеки в місцях масового скупчення людей. До таких об'єктів відносяться залізничні вокзали, та ін. Тому забезпечення безпеки при експлуатації об'єктів такого типу наукової задачі розробки або вдосконалення механізму управління ризиками полягає в визначенні комплексу заходів, спрямованих на мінімізацію або їх усунення.

Наразі замість поліції на «Укрзалізниці» працює воєнізована охорона яка не може впоратися з основними кримінальними викликами так як має недостатньо особового складу, а при отриманні інформації або виявлення незаконних дій необхідна зафіксувати акт такої дії та викликати Національну поліцію на місце злочину, що не завжди виконується.

Отже, зважаючи, що наша країна знаходиться у стані війни, і всі ресурси держави зосередженні для відбиття збройної агресії росії та забезпеченню функціонуванню критичної інфраструктури, цілком зрозумілим є дефіцит фінансування на впровадження новітніх методик боротьби зі злочинністю. Тож впровадження систем відеонагляду здійснюється недостатніми темпами та вкрай нерівномірно, хоча варто зазначити, що в останні роки цей процес значно пожвавився. Системи безпеки та відеонагляду є важливою частиною виявлення та нейтралізації небезпек. Така система забезпечує стійкість підприємства, та має можливість виконувати різні функції контролю та захисту. І потрібна як для воєнізованої охорони «Укрзалізниці» так і для працівників підрозділів Національної поліції які мають змогу отримати та проаналізувати додаткову інформацію з камер відеоспостереження.

Список використаних джерел:

1. Албул С. В. Кримінальна розвідка як функція оперативно-розшукової діяльності: Європейський досвід та Українські перспективи. *European Reforms Bulletin: international scientific peer-reviewed journal: Grand Duchy of Luxembourg*. 2015. № 2. P. 2-6.

2. Кримінальний процесуальний кодекс України, редакція від 28.11.2019 р. *Відомості Верховної Ради України*, 2013, № 9-13, ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

3. Мирошниченко В. О. Аналіз біометричних систем ідентифікації особи в умовах діяльності правоохоронних органів *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2007. Вип. 1 (32). С. 314-321.

Маляренко Д. О.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ДЕЯКІ ОСОБЛИВОСТІ ІНФОРМАЦІЙНОЇ ВІЙНИ

Інформаційна війна – викладення інформації у спосіб, який формує у суспільстві чи групі людей потрібну точку зору, громадську думку, хід взаємодоповнюючих логічних думок, вичерпну систему поглядів щодо окремих питань на користь організатора інформаційної пропаганди. Як наслідок, відбувається усвідомлення окремих фактів чи подій у потрібному для маніпулятора світлі, формування потрібного світогляду чи життєвої позиції стосовно питань, у яких раніше були протиріччя чи нерозуміння. У випадку відсутності протиріч і наявної сталої системи поглядів, завданням інформаційної війни є породження сумнівів, насівання протиріч та домислів в існуючі переконання. Розвиток людини влаштований так, що людина завжди шукає відповіді про турбуючи її питання, спірні питання, що є невід'ємною рисою безперервних процесів пізнання. У молодому віці, у мало освічених верствах суспільства, через м'яку несформовану свідомість і прогалини у знаннях, завданням інформаційної війни є заміна правдивої інформації на неправдиву, надзвичайно легку для засвоєння і на перший погляд логічну. Відповідно, із зростанням обізнаності зменшується вразливість, у такому випадку, інформаційна війна потребує більш складного підходу для породження сумнівів, використовує численні техніки перекручування інформації, наприклад, подання неправди з логічними доказами правдивості цих фактів, фальсифікованими дослідженнями та доказами у які жертва гіпотетично має повірити і прийняти їх як свої переконання.

Антидотом у інформаційній війні є комплекс заходів під спільною узагальнюючою назвою інформаційна гігієна, який розкриває механізми боротьби з інформаційною війною, пояснює механізми інформаційної війни, розробляє протидію – від створення швидкого легкозасвоюваного «інформаційного цукру» на випередження, де простими словами пояснюється суть явища, до пояснення складних механізмів перевірки джерел інформації, виявлення фальшивих новин, загальноосвітня діяльність з акцентуванням уваги на можливе перекручування окремих фактів супротивником [1].

Інформаційна війна як засіб впливу. Зважаючи на роль інформації у сучасному світі, американський дослідник Маклюен виводить цікаву тезу, яка звучить так: «Істинно тотальна війна - це війна за допомогою інформації».

Мета інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях.

Очевидно, що інформаційна війна – складова частина ідеологічної боротьби. Такі війни не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто не позбавляється їжі, даху над головою. І це породжує небезпечну безпечність у ставленні до них. Тим часом, руйнування, яких завдають інформаційні війни у суспільній психології, психології особи, за масштабами і за значенням цілком відповідні, а часом і перевищують наслідки збройних війн.

Як науковці пояснюють явище інформаційної війни в сучасному світі. У книзі Прокофьєва «Інформаційна війна і інформаційна злочинність» дано визначення: інформаційна війна – це дії, початі для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації та інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації і інформаційних системах [2].

Інформаційна складова війни. Інформаційна війна у сучасних умовах є одним з вирішальних факторів перемоги. Особливо це важливо для України, яка веде асиметричну війну проти ядерної держави з переважаючим військовим потенціалом. Від того, як за кордоном сприймають події в Україні, залежить і рівень політичної підтримки, і обсяги допомоги, і масштаби запроваджених проти агресора санкцій. Об’єктивні дані свідчать, що перший раунд інформаційного протистояння протягом 50 днів війни Україна виграла вчисту.

Відкритість, високий професійний рівень організації інформаційної кампанії Офісом президента, Міноборони, МЗС та українськими журналістами, готовність і вміння відстоювати нашу позицію у світових ЗМІ, активно працювати у соціальних мережах, – все це в українському «меню» виявилося значно «смачнішим», ніж нескінчена і відверта брехня кремлівської братії агітаторів і пропагандистів [3].

Інформаційна війна – це не тільки фейки. Фейки є найменшою одиницею такої війни. Не буду вдаватися в теоретичні дебати щодо визначень, адже їх багато й вони тривають весь час. Поясню з практичного боку, як формується смислова частина інформаційної війни Росії проти України зараз і чому нам важливо це розуміти. Інформаційний фронт у часи війни безпосередньо обслуговує бойові дії. Тобто різними інструментами країна інформаційно допомагає собі в бою. Якщо продовжити аналогію між кінетичною та інформаційними війнами, уявімо, що територію можна порівняти з увагою. Тобто воюють і завойовують в інформаційній війні увагу. Як територію,

її можна утримувати чи відвойовувати. Способів завоювання території в кінетичній війні є безліч: піти в наступ артилерією, узяти місто в кільце чи висадити десант [4].

У сучасних умовах затяжна інформаційна війна не вигідна нікому, крім журналістів і власників ЗМІ. Підприємство, яке атакують, витрачає значні кошти на те, щоб відновити свою репутацію в очах споживачів. У свою чергу, підприємство, яке здійснює атаку, ризикує надмірно захопитися боротьбою.

Список використаних джерел:

1. Учасники проектів Вікімедіа. Інформаційна війна. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Інформаційна_війна.
2. Інформаційна війна – зброя масового знищення! *Українська правда*. URL: https://www.pravda.com.ua/rus/articles/2006/04/20/4399050.
3. Корсунський С. Інформаційна складова війни: як Росія намагається послабити підтримку Заходу. *Радіо Свобода*. URL: https://www.radiosvoboda.org/a/informatsiyna-viyna-rosiyskyy-vplyv/31811302.html.
4. Ілюк К. Інформаційна війна – це не тільки фейки. URL: https://ms.detector.media/propaganda-ta-vplivi/post/29264/2022-03-31-informatsiyna-viyna-tse-ne-tilky-feyky.

Матвійчук А. О.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Економічна та інформаційна глобалізація світових відносин супроводжується створенням ефективних механізмів і засобів для інформаційного та фінансового впливу на партнерів і конкурентів на місцевому, регіональному та глобальному масштабах. Метод такої дії, як правило, полягає в розподілі реальних товарів, вироблених на користь тих, хто розробляє, застосовує відповідні технології. Починаю з того, що у країні є більше проблем з інформацією та економічною безпекою.

Українська економіка страждає від нестачі інвестицій і інновацій. Проблема значно поширилася в останні роки, оскільки результати ліберальних реформ в Україні виявилися досить суперечливими. Хоча багато планованих програм економічного зростання були прийняті, практично всі залишалися нереалізованими. Виходячи з цього дослідження економічної безпеки за допомогою інформаційних технологій є досить актуальним. У науковій літературі є певний консенсус щодо задоволення рівня екологічної безпеки, тобто такого стану економіки, для цілей забезпечення сталого зростання економічної продуктивності та ефективного задоволення економічних потреб населення, зберігається продуктивний контроль держави над використанням національних ресурсів, є захист інтересів країни на національному і міжнародному рівнях. Процес встановлення ринкових відносин в Україні виявився досить складним і ненадійним. Він супроводжувався глибоким соціальним і економічним кризом, що в свою чергу сприяло розвитку країни. Текучі проблеми економічної безпеки в нашій країні викликані такими негативними економічними явищами, як дефіцит бюджету, інфляція, безробіття і падіння рівня життя населення. Глобальна економічна криза, яка викликала низку негативних наслідків для поширення інфекційних захворювань, є додатковим фактором у поточній ситуації. У зв’язку з вищезгаданим, роль інформаційних технологій в забезпеченні безпеки України вважається важливою для загальних наукових цілей [1].

Ми спробуємо проаналізувати ситуацію щодо впливу інформаційних технологій на економічну безпеку України. Для швидкого розвитку, формування та захисту інформаційного простору та зміцнення економічної безпеки можна використовувати сучасні інформаційні технології, які зараз надаються дуже мало уваги на рівні вищих органів влади. Низький рівень інформації про безпеку призводить до зниження економічного розвитку і конкурентоспроможності світового ринку. Щоб забезпечити поліпшення ситуації, потрібні не тільки реформи інформаційної політики, але і створення сучасного інформаційного простору, а також системи захисту. Продукт IT-технологій може бути використаний в інших секторах економіки, що дозволить їм значно поліпшити свою продуктивність.

1. Споживачі Інформаційні технології можуть самостійно створювати нові продукти і отримувати більше грошей за них. існує дуже перспективна можливість створення різноманітного цифрового ринку.

2. Ідеальним середовищем для використання інформаційних технологій є сільська економіка. У структурі української економіки цей сектор є одним з провідних. На думку вчених, для забезпечення ефективної роботи відповідних суб’єктів, нові інформаційні технології повинні бути використані. Це дозволить збільшити виробництво сільськогосподарських продуктів. Інформація, надана агро-підприємствами в сучасних умовах, є значною недостатньою, що пояснюється багатьма причинами. Серед них, низька ефективність управління підприємствами з точки зору неефективного економічного впливу на процеси

створення матеріально технічних підприємств, а також відсутність розвитку інформаційної інфраструктури виробництва підприємства. Робота сучасних сільськогосподарських працівників може стати набагато більш ефективною і продуктивною в результаті збільшення технологічних навичок робітників.

3. Управління витратами в області логістики можна значно оптимізувати за допомогою використання інформаційних технологій. Автоматизація повинна бути здатна збирати і накопичувати інформацію про витрати і факти, що призвели до їх виникнення. Також можна використовувати статистичний аналіз витрат, сформульованих в різних звітах і інших процесах. Їх можна впорядкувати за допомогою IT-технологій [2].

В результаті хочеться зазначити, що процес глобалізації характеризується усіма новими сферами діяльності. Це стає актуальним в області національної безпеки, де конкретне положення про інформаційну безпеку чітко визначено. Важкості наслідків реалізації економічних загроз залежить не тільки від сил джерела загрози, які прагнуть змінити державу, але і від неподільності державних систем реагувати на ці загрози. У нинішніх нестабільних турбулентних умовах, у світлі зростаючих проблем інформаційної безпеки та економічної безпеки, дуже важливо оцінити економічні загрози інформаційної безпеки і на цій основі приймати необхідні заходи для запобігання загрозам, захисту інформації та економічних інтересів від потенційних джерел небезпеки.

Список використаних джерел:

1. Застосування інформаційно-комунікаційних технологій у забезпеченні економічної безпеки держави. Літопис Волині. URL: http://litopys.volyn.ua/index.php/litopys/article/view/179.
2. Інформаційно-економічна безпека як фактор стабільного розвитку держави. Публічне урядування. *Наукова періодика Міжрегіональної Академії управління персоналом*. URL: http://journals.maup.com.ua/index.php/public-management/article/view/152.

Москаленко Д. А.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ВДОСКОНАЛЕННЯ СИСТЕМИ ЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ НАРЯДАМИ ПОЛІЦІЇ «ЦУНАМІ»

Оперативно реагувати на правопорушення і в лічені хвилини приїжджати на місце злочину правоохоронним органам допомагає «ЦУНАМІ». Це сучасний центр управління нарядами патрульних, який створений на базі

Ситуаційних центрів ГУНП в областях. Ця система являє собою певний комплекс апаратних та програмних засобів інформування, а також персоналу, призначений для управління силами й засобами Національної поліції.

Система дозволяє відстежити, в якому квадраті кожного з районів того чи іншого міста знаходиться той чи інший екіпаж патрульної служби. Працівники можуть отримувати завдання в інших квадратах. За командою чергового патруль може переїхати з квадрата в квадрат. При цьому виїжджати за територію району патрулювання поліцейським заборонено.

Дана система забезпечує користувачів необхідними інформаційними, технічними та аналітичними ресурсами для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Система фіксує, зберігає та робить доступними для аналізу та контролю повідомлення і результати реагування на них [1]. Диспетчери використовують різні засоби зв'язку – мобільні та стаціонарні телефони, а також рації. Патрульні часто телефонують їм, щоб проконсультуватися. Сьогодні в поліції перестали скаржитися на повільність правоохоронців.

До того ж, співробітники Ситуаційних центрів регіонів стежать за використанням електронних засобів контролю, браслетів, щодо тих громадян, яким було обрано такий запобіжний захід. Тому це, насамперед, забезпечення прозорості даної діяльності [2].

На меті «ЦУНАМІ» – забезпечення користувачів ресурсами інформації для виконання функціональних обов'язків та прийняття ефективних управлінських рішень. Система розпізнає, зберігає та робить доступними для аналізу та контролю повідомлення і результати реагування на них. Тим самим програма є зручною у використанні.

Створення даної системи було обумовлене наступними проблемами. По-перше, було зрозуміло, що колишні чергові частини не відповідають сучасним вимогам, і, як результат, правоохоронці сильно програють у швидкості реагування. По-друге, збільшилася кількість звернень громадян.

На жаль, порівняльний аналіз якості роботи поліції вкрай утруднений. Це пов'язано з тим, що практично немає одного показника кримінальної статистики, які збираються та трактуються у всіх країнах однаково. Ця різноманітність організаційних форм робить майже неможливим порівняльний аналіз поліцій різних країн. Не можна зробити однозначного висновку про переваги або недоліки зонального поділу поліцейських сил, що не збігається з межами муніципалітетів.

Наприклад, у Бельгії зональний територіальний поділ виявився програшною стратегією, оскільки поліція не зуміла налагодити стосунки з муніципальною владою. У Чехії, навпаки, цей підхід був визнаний єдиною можливою стратегією, оскільки там потрібно було розірвати зв'язки між різними рівнями влади. При цьому мілітаризована, вертикально ієрархована поліцейська структура у всіх випадках виявляється більш звичним способом функціонування поліції.

Таким чином, робимо висновки, інформаційно-телекомунікаційна система «ЦУНАМІ» повинна постійно вдосконалюватись як у технологічному, так і у інформаційному плані. Це удосконалення системи дасть поштовх до нових відкриттів та оптимізації роботи усіх підсистем правоохоронних органів. Хочу додати, що дана система є однією з найкращих досягнень реформ Національної поліції України, яка значно покращила ефективність реагування на звернення громадян до поліції.

Список використаних джерел:

1. Вишня В. Б., Мирошниченко В. О., Комісаров О. Г., Прокопов С. О. Інформаційне забезпечення діяльності Національної поліції України: зб. законодавчих та нормативних документів. Дніпро: ДДУВС, 2016. 476 с. URL: http://er.dduvs.in.ua/handle/123456789/2043.
2. Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційне забезпечення професійної діяльності: навч. посібник. Дніпро: ДДУВС, 2018. 220 с. URL: http://er.dduvs.in.ua/handle/123456789/2046.

Мудровський Р. Т.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

КІБЕРВІЙНА МІЖ РОСІЄЮ ТА УКРАЇНОЮ

У 2016 році НАТО офіційно визнало кіберпростір ареною військових дій поряд з традиційними сферами – сушею, морем і повітрям. Насправді Росія стала використовувати кіберпростір для агресії понад 15 років тому. Саме російські хакери стояли за кібератаками на Естонію 2007 року та потужною DDoS-атакою на Грузію в 2008 році. Близько 10 років знадобилося світовій спільноті з метою оцінки рівня загрози російських хакерів. Часто вони працюють поза офіційними державними структурами, але глибоко інтегровані в спецслужби Росії; їхня діяльність щільно координується з іншими військовими активностями. Одним із найбільш наочних випадків під час повномасштабного вторгнення в Україну була атака на Одеську міськраду, яку здійснювали одночасно з ударом крилатими ракетами по місту.

Подібно до найманців, таких як ПВК Вагнер, яких кремль використовує для розмивання кордонів між державними та кримінальними суб'єктами, хакери є неофіційним, проте важливим елементом наступального потенціалу російської держави.

Так, як російська армія систематично ігнорує правила ведення війни, російські хакери поводяться досить безпринципно в кіберпросторі. Їхніми цілями є об'єкти критичної інфраструктури, такі як енергетичні та комунальні підприємства, лікарні та служби екстреного реагування, фінансова система, логістика, що надають допомогу організації. У період найбільшого потоку українських біженців хакери також атакували гуманітарні організації.

Сьогодні кожен український громадянин може стати жертвою кібератаки, а хакери отримати доступ до особистих даних і контактів, що надасть російським спецслужбам можливість здійснити несанкціонований доступ до систем українських установ чи організацій, ідентифікувати потенційних опонентів або підготувати спеціалізовані пропагандистські.

Очевидно, що кіберзлочинці здійснюють кібератаки в тандемі з військовими, користуючись доступом до секретних даних розвідки. Такий підхід порівняно дешевий, адже кіберзлочинці можуть фінансувати свої операції, використовуючи шахрайські схеми.

Ідея співпраці держави із злочинними елементами також не нова. Однак у цьому випадку слід зазначити, що держава, про яку ми говоримо, є досі постійним членом Ради Безпеки ООН.

Російське вторгнення в Україну продемонструвало поширення сучасних бойових дій майже на всі аспекти повсякденного життя. Розвиток інтернету та масове поширення цифрових технологій означають, що буквально все від водопостачання до банківських послуг може потрапити в руки злочинців і припинити працювати. Понад вісім місяців Україна щодня відчуває безпрецедентні кібератаки, але державі вдалося забезпечити надання базових комунальних послуг на більшості території країни.

Чому ж, незважаючи на всю міць російських хакерів, інформаційна інфраструктура України працює? Тому що в попередні роки держава працювала над посиленням кіберстійкості. Держспецзв'язку розпочала реформу системи кіберзахисту та розвиток технологічної інфраструктури захисту, розвиток кадрів та міжнародної взаємодії та обміну даними про загрози [1]. Тепер Держспецзв'язок нашої держави має набагато краще уявлення про ворога. Держспецзв'язок бачє загрозу, яку представляє ворог, і може оцінити межі його можливостей [1].

Україна отримала неоціненну підтримку низки країн-партнерів і в той же час ділиться з знаннями і досвідом. Оскільки сам інтернет не знає кордонів, найуспішніші ініціативи у сфері кіберзахисту міжнародні за своєю суттю. Також Україна має потужну внутрішню підтримку від власних фахівців, які раніше були зайняті в приватній сфері.

Щоб і далі бути стійкими, потрібно продовжувати роботу, адже залишається чимало слабких місць. По-перше, кожен повинен відповідати за свою кібербезпеку: і приватні особи, і організації. Нехтування питаннями кібербезпеки становить загрозу утворення слабких ланок у ширших системах, що може мати катастрофічні наслідки. Український бізнес не повинен повністю покладатися на державу і повинен бути готовий інвестувати у відповідні запобіжні заходи. Це вже стало обов'язком.

Російсько-українська війна – це перша в світі повномасштабна кібервійна, але аж ніяк не остання. Навпаки: всі наступні конфлікти матимуть потужний кіберкомпонент. Кібербезпека буде не менш важливою для виживання, ніж міцні збройні сили.

Тому другий аспект захисту – це протидія ворогові на міжнародному рівні. За роки росія розробляла інструменти для здійснення атак на критичну інформаційну інфраструктуру. Деякі з них російські військові хакери протестували на українських інформаційних системах. Міжнародна спільнота надто пізно розпізнала реальні наслідки цієї стратегії і тепер відчайдушно намагається надолужити втрачене. Війна в Україні наочно продемонструвала, як хакери можуть виконувати військову функцію, а кібератаки відігравати ключову роль у веденні сучасної війни. Тому обмеження доступу росії до сучасних технологій має розглядатися як один з пріоритетів міжнародної безпеки.

З гордістю (але і печаллю, адже ніхто в Україні не бажав нам такої долі) потрібно вказати, що Україна – повноцінний учасник міжнародних процесів з протистояння росії в кіберпросторі та створенні колективної системи кібербезпеки. У кінці травня українська делегація вперше взяла участь у засіданні Керівного комітету CCDCOE. Комітет об’єднує союзників з НАТО і партнерів за межами Альянсу, сприяє їх співпраці в області кіберзахисту [1].

Ми на передової кібервійни. І нам є чим поділитися зі світом. Україна і далі впроваджуватиме найкращі світові рішення у сфері кіберзахисту і готова ділитися своїм досвідом з міжнародною спільнотою для того, щоб зупинити агресора.

Але при цьому – безліч речей має бути зроблено самими українцями для власного захисту. Як рядовими людьми, які сьогодні теж є мішенню російських хакерів, так і бізнесом. Бізнес має системно інвестувати в кібербезпеку. Адже часи, коли можна було вважати, що ви можете бути комусь нецікаві, ніколи не повернуться.

Список використаних джерел:

1. Щиголь Ю. Перша у світі повномасштабна кібервійна відбувається в цей час в Україні. URL: https://www.google.com/amp/s/biz.nv.ua/amp/polnomasshtabnava-kibervovna-v-ukraine-vpervye-v-istorii-ukrspecsvyaz-50253612.html.

Петрушин О. В.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Синиціна Ю. П.,
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

OSINT ТЕХНОЛОГІЇ: АКТУАЛЬНІСТЬ, ЕТАПИ ТА ПЕРСПЕКТИВИ

Результативність боротьби зі злочинними діяннями в правоохоронній діяльності залежить від належної організації її інформаційного забезпечення, що представляє собою систему збору, оброблення, накопичення й використання інформації, що має значення для виявлення, попередження й розслідування злочинних проявів. Активні трансформаційні процеси в системі суб'єктів правоохоронної діяльності відбуваються у зв'язку з різними глобальними чинниками, зокрема інформаційними.

Диверсифікація послуг, що пропонуються в Інтернеті, що призвела до еволюції зростаючої маси цифрових даних [1]. До цих даних можна отримати доступ за допомогою інтерфейсів програмування програм (API) або різних служб, додатків тощо. Діяльність збору та співвіднесення такої інформації за допомогою інструментів називається розвідкою з відкритим джерел (OSINT) [6].

За результатами ретроспективного аналізу визначено, що основні питання інформаційно-аналітичної діяльності в правоохоронній галуззі вивчали наступні видатні вчені: Вербенський М., Антонов К., Буржинський В., Никифорчук Д. та інші.

Термін OSINT розшифровується як Open source intelligence розвідка серед доступних джерел, що охоплює будь-яку інформацію, включає пошук, аналіз і використання загальнодоступної інформації.

Правоохоронні органи: поліція використовує джерела OSINT для захисту громадян від зловживань, сексуального насильства, викрадення особистих даних та інших злочинів. Це можна зробити, відстежуючи у соціальних мережах цікаві ключові слова та фотографії, щоб запобігти злочинам до їх ескалації.

Правоохоронці використовують OSINT для дослідження даркнету. Вони сканують вебфоруми та магазини на предмет торгівлі незаконними товарами та послугами. Такі дослідження полегшують розслідування у сфері кібербезпеки, кібертероризму та кібервійн.

Крім того, OSINT використовують для розслідування злочинів. За допомогою збору інформації з відкритих джерел, слідчі можуть розрахувати всі ризики спецоперації, визначити місце, де ховається зловмисник, передбачити перешкоди тощо. Такий аналіз також є корисним у створенні профілю злочинця – щоб мати краще уявлення про спосіб життя, звички тощо.

Адвокатські фірми теж часто користуються техніками OSINT для розслідувань та підготовки справ, аналізуючи відкриті дані з соцмереж чи медіа.

До основних етапів OSINT технології відноситься:

1. Забезпеченість – OSINT Toolkit. До основного набіру інструментів OSINT технології можемо віднести:
   - доступ до традиційних джерел новин, таких як Google;
   - Google-Карти, Пошук, Зображення;
   - платформа соціального моніторингу з можливостями геозонування.
2. Систематичність;
3. Визначення геолокації;
4. Перевірка даних;
5. Конфіденційність.

Перспективність OSINT технології, як професійного напрямку роботи буде тільки зростати. Згідно з дослідженням Global Market Insights, ринок OSINT-розвідки за результатами 2020 року вже перевищив 5 млрд доларів та до 2027 року може зрости ще на 25 %. Наприклад, у Німеччині OSINT став основною технологією очищення, упорядкування та аналізу величезних обсягів даних та приніс близько 42,66 млн доларів доходу в 2020 році. Це означає, що навички, які українці сьогодні отримують для ведення «інформаційної» війни, в майбутньому стануть в пригоді і для виконання мирних задач: бізнесових, правових, журналістських тощо.

На основі проведеного дослідження було виявлено, що на даний момент OSINT є дуже популярним методом пошуку інформації. Оскільки технологія удосконалюється з кожним днем, виникає потреба у швидкому та конкретному зборі інформації, і це збільшує потребу в OSINT. Використовуючи OSINT технологію в правоохоронній діяльності, можемо отримати важливу інформацію за лічені хвилини, що можливо лише шляхом глибокого аналізу засобів масової інформації та соціальних мережах,

Для застосування OSINT технології на практиці використовуються різноманітні інструменти і підбір інструменту під кожний окремий випадок є проблемним та актуальним питанням тому, що немає єдиного підходу до підбору до вирішення різноманітних задач.

Список використаних джерел:

1. Pune M. Open Source Intelligence (OSINT). Market Research Report-Global Forecast to 2023 – Market Analysis, Scope, Stake, Progress, Trends and Forecast to 2023. Market Research Future. 2020. URL: https://www.marketresearchfuture.com/reports/open-source-intelligencemarket-4545.
2. Norton R. Guide to Open Source Intelligence. US Intell. Stud. 2011. Vol. 18, pp. 65-67. URL: https://www.afio.com/publications/Norton_Open_Source_in_AFIO_INTEL_WinterSpring2011.pdf.

Письмений Д. В.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Паршин Ю. І.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

ЗАГАЛЬНІ ТЕНДЕНЦІЇ МЕХАНІЗМУ ВІДПОВІДАЛЬНОСТІ ЗА КОРУПЦІЙНІ ПРАВОПОРУШЕННЯ ТА ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ АНТИКОРУПЦІЙНОГО ЗАКОНОДАВСТВА

Загальновідомим є той факт, що в 1991 році відбулася значна для нашого народу подія – відновлення Незалежності України. Уже в перші роки самостійного існування у світовому просторі правова система України почала наповнюватися провідними ідеями міжнародного юридичного співтовариства. В той же час, незважаючи на всі позитивні тенденції розвитку нашої вітчизни, вона також мала ряд недоліків, які пригальмовували її піднесення. Одним із таких пороків була корупція. Було проведено колосальну роботу, аби створити ефективний механізм боротьби з нею. Зокрема, прийнято ряд законів, таких як Закон України (ЗУ) «Про запобігання корупції» [1], ЗУ «Про державну службу» [2], ЗУ «Про засади державної антикорупційної політики» [3]. Також було доповнено Кримінальний кодекс України положеннями, які стосувалися відповідальності за корупційну діяльність [4]. Проте, не дивлячись на вказаний вище позитивний законотворчий результат, корупція нікуди не зникла, а навпаки почала все більше розростатися країною загалом та апаратом публічних службовців зокрема.

Для визначення загальної тенденції механізму відповідальності за корупційні правопорушення, маємо використати положення Кримінального кодексу України, і зокрема статей 191, 210, 262, 308, 312, 313, 320, 354, 364-369, 410 [5]. Проаналізувавши їх, можемо виокремити наступні закономірності:

1) Перш за все ми можемо згадати про існування взаємозв'язку між ступенем суспільної небезпечності корупційного діяння, його шкідливими наслідками для функціонування держави з однієї сторони та відповідальністю за дане правопорушення з іншої. Для прикладу візьмемо частини 2 та 3 статті 368 ККУ: ч. 2 – Прийняття пропозиції, обіцянки або одержання службовою особою неправомірної вигоди у значному розмірі карається позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років. Ч. 3 –

Прийняття пропозиції, обіцянки або одержання службовою особою неправомірної вигоди у великому розмірі карається позбавленням волі на строк від п’яти до десяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років, з конфіскацією майна. Тобто ми можемо дійти того висновку, що в чинному законодавстві, яке направлено на протидію корупції, має місце наступний взаємозв’язок: чим більшим є обсяг неправомірної вигоди (тобто чим більшою є шкода від корупційного правопорушення для держави і суспільства), тим серйознішим буде покарання за нього.

2) По-друге, досліджуючи статті 368 та 369 ККУ, ми можемо побачити, що відповідальність за вчинення корупційного правопорушення не є односторонньою, тобто покарання буде нести не лише та особа, яка вчинила корупційне правопорушення(наприклад, одержала неправомірну вигоду), а ще й та, яка запропонувала, вмотивувала особу вчинити дане правопорушення (у нашому випадку запропонувала або ж уже надала неправомірну вигоду службовій особі, наприклад, бізнесмен, що дав державному чиновнику хабар, аби той закрив очі на незаконну виробку лісу тощо).

3) По-третє, введення відповідальності за вчинення корупційних правопорушень активного та пасивного характеру, що в свою чергу блокує можливість державних службовців незаконно збагатитися внаслідок знаходження певних «шпарин» у законодавстві.

Проте, незважаючи на той факт, що з першого погляду вітчизняне антикорупційне законодавство видається досконалим, воно все ж має величезну кількість недоліків, якими й користуються нечесні на руку особи. Тому сьогодні ми запропонуємо власні варіанти щодо того, яким чином можливо ліквідувати дані «шпарини» у законодавстві.

Насамперед, ми пропонуємо взамін презумпції невинуватості, яка у наш час панує в українському законодавстві, ввести саме презумпцію винуватості стосовно корупційних правопорушень. Її зміст можна розтлумачити як той факт, що особа вважається винною у вчиненні корупційного правопорушення до того часу, поки не доведе протилежне. Даний правовий інститут існує в Японії, де досить добре себе зарекомендував. На нашу думку, перевагою даної презумпції буде також те, що чиновники змушені будуть декларувати всі свої доходи, прибутки, майно і підтверджувати законність їх набуття, інакше будуть притягнуті до кримінальної відповідальності. Це в свою чергу сприятиме збільшенню прозорості діяльності представників державного апарату.

По-друге, негативний вплив на діяльність нашої держави мають зв’язки між державними службовцями та їхніми родичами, а також інститут «кумівства». Це призводить до того, що в щорічних деклараціях, які подають наші можновладці, вони не виступають власниками якогось дуже дорогого майна, а от їхні родичі: брати, сестри, дідусі, бабусі, батьки – виступають власниками того майна, на яке вони змогли б заробити хіба що 100 років працюючи без відпустки та вихідних. Тому тут виникає питання, яким же чином можна

боротися з даною проблемою? Ми пропонуємо внести зміни до Кримінального кодексу України стосовно відповідальності тих осіб, які де-юре виступають власниками майна, одержаного корупційним шляхом. Дані нововведення міститимуть більшу кримінальну відповідальність для даних осіб у порівнянні з тими, хто такі корупційні правопорушення вчиняє. Тобто до відповідальності буде притягуватися не тільки сам хабарник, а ще й особи, які йому тим чи іншим чином допомагають цей злочин приховати.

Отже, підсумовуючи все вище викладене, можна зробити такі висновки. Загальні тенденції механізму відповідальності за корупційні правопорушення відповідають європейській теорії та практиці, які в свою чергу запозичує наша держава, аби максимально ефективно сприяти розвитку та збагаченню вітчизняного права. Проте, все ж варто говорити не лише про успіхи боротьби з корупцією в нашій державі, варто ще й згадати про певні недоліки, зокрема під час впровадження закордонного юридичного наукового доробку в нашу правову систему, досить часто не враховуються особливості національного менталітету українців (наприклад, інститут «кумівства»), тому я вважаю, що аби максимально ефективно боротися з корупцією, ми маємо не лише користуватися доробками правових систем держав Європи, а ще й певним чином їх адаптувати до умов українського сьогодення.

Список використаних джерел:

1. Закон України «Про запобігання корупції» від 14.10.2014 р. № 1700-VII. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text.
2. Закон України «Про державну службу» від 10.12.2015 р. № 889-VIII. URL: https://zakon.rada.gov.ua/laws/show/889-19#Text.
3. Закон України «Про засади державної антикорупційної політики на 2014-2017 роки» від 14.10.2014 р. № 1699-VII. URL: https://zakon.rada.gov.ua/laws/show/1699-18#Text.
4. Кримінальний кодекс України від 05.04.2001 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
5. Академічний тлумачний словник української мови. URL: http://sum.in.ua/s/tendencija.

Попко С. В.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Паршин Ю. І.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

ТЕОРЕТИЧНІ АСПЕКТИ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У сучасних умовах ефективність діяльності підприємств зумовлюється переважно станом їх фінансів, що призводить до необхідності розгляду проблем забезпечення фінансової безпеки підприємства. Топ-менеджери вітчизняних підприємств приймають управлінські рішення, коли їх господарська діяльність перебуває під загрозою впливу 216 різноманітних деструктивних факторів, що сприяють зменшенню фінансової стійкості, втраті платоспроможності чи навіть банкрутства. Конкурентна боротьба загострює ці проблеми, тому актуалізується питання забезпечення фінансової безпеки підприємств як гарантії їх стабільного функціонування. У такому контексті слід сказати, що фінансова безпека (як головна складова економічної безпеки) поєднує в собі відносини з управління фінансовими ресурсами та оптимізацію їх використання, а також фінансові інструменти, що забезпечують ефективну діяльність підприємства.

Дослідження фінансової безпеки на рівні окремого підприємства здійснювалося як вітчизняними, так і закордонними науковцями, такими як: Бланк І., Доценко А., Афанас'єва Д., Графєєва А., Розніна Н., Гукова А., Анікіна І., Чібісова І., Козак Л., Багровецька І., Пономаренко О., Горячева К., Єпіфанов А., Пластун О., Домбровський В., Журавка О., Бондаренко Є., Кудрицька Ж., Бердар М. та ін. Однак враховуючи цінність праць науковців дана тема є досить дискусійною чим обумовлено її вибір та актуальність.

У вітчизняній науковій літературі поняття «фінансова безпека» розглядається дослідниками та практиками на макрорівні в системі більш загальних категорій – «національна безпека» або «економічна безпека країни» [1]. На макрорівні під економічною безпекою розуміють такий стан національної економіки, який дає змогу зберігати стійкість до внутрішніх та зовнішніх загроз і здатний задовольняти потреби особи, сім'ї, суспільства та держави. Складовими економічної безпеки є: макроекономічна, фінансова, зовнішньоекономічна, інвестиційна, науково-технологічна, енергетична, виробнича, демографічна, соціальна, продовольча безпека.

Фінансова безпека – це такий стан бюджетної, грошово-кредитної, банківської, валютної системи та фінансових ринків, який характеризується збалансованістю, стійкістю до внутрішніх і зовнішніх негативних загроз, здатністю забезпечити ефективне функціонування національної економічної системи та економічне зростання [2, с. 135].

Науковець У. Ладичко пропонує трактувати поняття фінансової безпеки підприємства як кількісно та якісно детермінований рівень його фінансового стану, що забезпечує стабільну можливість захисту його пріоритетних, збалансованих фінансових інтересів від визначених реальних і потенційних загроз зовнішнього та внутрішнього характеру, параметри якого визначаються на основі фінансової політики підприємства [3]. У свою чергу, К. Горячева, базуючись на аналізі сутності категорії «фінансова безпека підприємства», пропонує таке визначення: фінансова безпека підприємства – це фінансовий стан, який характеризується [4, с. 66]:

– збалансованістю і якістю фінансових інструментів, технологій та послуг, котрі використовуються підприємством;

– стійкістю до внутрішніх і зовнішніх загроз;

– здатністю фінансової системи підприємства забезпечувати реалізацію власних фінансових інтересів, місії і завдань достатніми обсягами фінансових ресурсів;

– забезпечувати ефективний і сталий розвиток цієї фінансової системи [1, 3].

На нашу думку, під фінансовою безпекою підприємства слід розуміти здатність підприємства самостійно розробляти і провадити фінансову стратегію відповідно до цілей корпоративної стратегії в умовах невизначеної і конкурентного середовища.

Головна мета фінансової безпеки підприємства полягає в тому, щоб гарантувати його стабільне та максимально ефективне функціонування у даний час та високий потенціал розвитку в майбутньому. До основних функціональних цілей фінансової безпеки належать:

– забезпечення високої фінансової ефективності роботи;

– підтримка фінансової стійкості та незалежності підприємства;

– досягнення високої конкурентоздатності;

– забезпечення високої ліквідності активів;

– підтримка належного рівня ділової активності;

– забезпечення захисту інформаційного поля і комерційної таємниці;

– ефективна організація безпеки капіталу та майна підприємства, а також його комерційних інтересів [2, с. 137].

Перед фінансовою безпекою суб’єктів підприємництва виникають завдання [1]:

– ідентифікація ризиків і пов’язаних з ними потенційних небезпек і загроз;

– визначення індикаторів фінансової безпеки суб’єктів підприємництва;

– впровадження системи діагностики і моніторингу стану фінансової безпеки;

– контроль і оцінка ефективності дії системи фінансової безпеки;

– створення необхідних фінансових умов, що забезпечують стабільне зростання компанії;

– створення умов для формування оптимального обсягу фінансових ресурсів з внутрішніх і зовнішніх джерел;

– підтримка фінансової стійкості і платоспроможності фірми протягом всього періоду функціонування;

– створення умов, необхідних для забезпечення оптимального обсягу і рівня ефективності інвестицій;

– мінімізація фінансових ризиків компанії;

– своєчасне впровадження у фінансову діяльність фірми сучасних технологій управління та інструментарію їх забезпечення;

– ефективний і швидкий вихід з фінансової кризи і нейтралізація його наслідків [1].

Отже, спираючись на визначення фінансової безпеки, що пропонуються науковцями, розуміємо під даним поняттям здатність підприємства самостійно розробляти і провадити фінансову стратегію відповідно до цілей корпоративної стратегії в умовах невизначеної і конкурентного середовища. До ключових рис фінансової безпеки підприємств відносимо: забезпечення рівноважного та стійкого фінансового стану, сприяння ефективній діяльності суб'єкта підприємництва, дозволяє на ранніх стадіях визначити проблемні місця в діяльності організації, нейтралізує кризи та запобігає банкрутству.

Список використаних джерел:

1. Михаліцький А. О. Фінансова безпека підприємства: пробеми та напрями вирішення. URL: http://www.nbuv.gov.ua/e-journals/Dutp/2005-2/txts/soc/05mnjjbp.pdf.

2. Журавка О. С. Теоретичні аспекти формування системи фінансової безпеки підприємства. *Інноваційна економіка*. 2020. № 5. С.134-139.

3. Ладичко У. Б. Управління фінансовою безпекою підприємств. URL: http://libfor.com/index. php?newsid=373.

4. Горячева К. С. Фінансова безпека підприємства. Сутність та місце в системі економічної безпеки. *Економіст.* 2019. № 9. С. 65-69.

Проворова К. Д.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ «ГАРПУН»

Живучи сьогодні, можна сказати, що люди вступають у нову еру, коли інформація та знання вважаються однією з найвищих цінностей, тобто розвиток інформаційно-комунікаційних технологій у всіх сферах економічного та соціального життя є найбільш зростаючим ресурсом. Сьогодні підвищення рівня боротьби зі злочинністю є однією з найважливіших умов широкого застосування досягнень сучасного науково-технічного прогресу, а в галузі інформаційних технологій за останні роки відбулися прориви.

Ефективність реагування на правопорушення полягає в отриманні інформації з будь-якого достовірного регламентованого нормативними актами джерела. Такими джерелами може бути набір інформаційно-пошукових систем, створених і керованих правоохоронними органами. Міністерством внутрішніх справ було видано наказ від 13.06.2018 № 497 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» [1].

Патрульна поліція у Дніпропетровській області однією з перших в Україні почала ефективно використовувати інформаційну підсистему «Гарпун». Це дозволило виявляти та реагувати на транспортні засоби усіх типів та номерні знаки ТЗ, що розшукуються у рамках кримінального, виконавчого проваджень, проваджень у справах про адміністративні правопорушення, оперативно-розшукової діяльності, а також за ухвалою слідчого судді, суду. Інформаційна підсистема «Гарпун» використовує сучасні технології, комп'ютерну та телекомунікаційну техніку для об'єднання інформації про розшукувані транспортні засоби та номерні знаки в єдиний інформаційний простір. Інформаційна підсистема «Гарпун» є найнадійнішою системою, яка здатна фіксувати номерний знак у разі викрадення автомобіля, а також перевіряти відповідно запис про викрадений автомобіль чи номерний знак. Вона в автоматичному режимі надсилає диспетчеру Ситуаційного центру ГУНП в областях сигнал, за яким при спрацьовуванні камер розшукуваного

автомобіля він потрапляє в поле зору на моніторі, диспетчер може надіслати завдання конкретному патрулю для реагування, або інформація про цей транспортний засіб надходить всім найближче розташованим патрулям у автоматичному режимі

Основними завданнями ІП «Гарпун» визначено: фіксування номерних знаків – двійників та тих, які за даними ЄДР МВС знищено, забезпечення оперативного реагування посадовими особами органів поліції про розшук транспортних засобів і номерних знаків, забезпечення взаємодії з державними та приватними виконавцями під час розшуку транспортного засобу боржника у виконавчому провадженні [2].

Система «Гарпун» автоматично створить картку в інформаційно-телекомунікаційній системі ЦУНАМІ та автоматично сповістить про цю подію. Обліку в інформаційній підсистемі підлягає інформація про розшук транспортних засобів, які стали засобом або об'єктом кримінального чи адміністративного правопорушення. Ця підсистема містить детальну інформацію про транспортні засоби та події правопорушення [3, с. 195].

Виходячи з вищевикладеного, можна зробити висновок, що завдяки системі штучного інтелекту «Гарпун», при тісній співпраці муніципальних керівників та правоохоронних органів, поліція буде швидше реагувати на транспортні злочини. Інформаційна підсистема «Гарпун» значно підвищує оперативність процесу, здешевлює впровадження, підвищує ефективність роботи правоохоронців.

Список використаних джерел:

1. Наказ МВС від 13.06.2018 р. № 497 «Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України». URL: https://zakon.rada.gov.ua/laws/show/z0787-18#Text.
2. Вперше у дніпропетровській області було впроваджено систему ІП «Гарпун». Новини сайту Міністерства юстиції. URL: https://minjust.gov.ua/news/ministry/vpershe-u-dnipropetrovskiy-oblasti-bulo-vprovadjeno-sistemu-ip-garpun.
3. Вишня В. Б., Ісмайлов К. Ю., Краснобрижий І. В. Інформаційні технології: підручник. Дніпро: ДДУВС, 2021. 492 с. URL: http://er.dduvs.in.ua/handle/123456789/6820.

Рагімлі З. М.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Прокопов С. О.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРОБЛЕМА ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПОЛІЦІЇ УКРАЇНИ

Нині володіння інформаційними технологіями допомагає розвитку суспільства, держави, інформаційних процесів, дозволяє впровадити нові винаходи, досягнення, але й стає чинником збільшення чисельності комп'ютерних правопорушень та поліпшення шляхів вчинення протиправних посягань. Такий стан ускладнює запобіганню, виявленню та протидії злочинності в країні і визначає вдосконалення досягнених та опрацювання нових способів та шляхів її реалізації. Покращення інформаційного забезпечення діяльності поліції стане підвищенням ефективності їх роботи. Головною причиною низької ефективності запобіганню злочинності є незадовільна взаємодія підрозділів поліції всіх рівнів, бо відсутня ефективна інтегрована система обміну інформацією.

Науковці вважають, що однією з проблем інформаційного забезпечення діяльності поліція України є кадровий потенціал, який на низькому рівні. І. Катеринчук зазначив у своєму дослідженні те, що існують проблеми підготовки працівників поліції, які володітимуть досвідом застосування інформаційною технологією, так як у вищих навчальних закладах не приділяють увагу на набуття технічних навичок, а концентруються більш на юридичну освіту поліцейських [1, с. 377].

Інформаційна підготовка повинна формувати в курсантів вищих навчальних закладів інформаційної культури внаслідок поглинення ними напрямок професійної інформатики, набуття ними практики застосування інформаційних технологій в діяльності поліції. [2, с. 222]. На першому курсі Дніпропетровського державного університету внутрішніх справ ми вивчали дисципліну «Інформаційні технології» яка була розрахована лише на 44 навчальних годин, на другому курсі вивчаємо дисципліну «Інформаційне забезпечення професійної діяльності», яка розрахована на 38 навчальних годин, чого явно не достатньо для вивчення ефективного застосування комп'ютерної техніки та інформаційних технологій для подальшої роботи в поліції, бо не вистачає часу для більш детального вивчення таких, наприклад,

важливих тем, як «Пошук службової інформації в мережі Інтернет», «Основи аналітичної діяльності». Важливо є проведення якісної службової підготовки працівників поліції в інформаційних підрозділах і тому треба повсякчасно підвищити кваліфікацію працівникам з комп'ютерної підготовки та інформаційної культури [3, с. 2].

Ще одною проблемою вдосконалення інформаційного забезпечення поліції України є перебування в низькому рівні забезпечення усіх інформаційних підрозділів потужною комп'ютерною технікою та застарілість програмного забезпечення. Згадана проблема виникає з причин недостатнього фінансування сфери вдосконалення інформаційного забезпечення підрозділів поліції. Подолати таку проблему можна тільки за допомогою фінансової підтримки міжнародних партнерів, таких як ЄС. Ось, наприклад, заради удосконалення роботи працівників поліції, представники Консультативної місії ЄС нещодавно передали комп'ютерне обладнання на суму 98 тисяч євро ГУ Національної поліції в Харківській області [4].

Всі ці вищезгадані проблеми, на мою думку, можна вирішити детально дослідивши їх, шукаючи ефективні шляхи їхнього вирішення, наприклад, для курсантів потрібно збільшити кількість годин для навчання та набуття навичок використання інформаційних і комунікаційних технологій, застосування сучасних інформаційних технологій та роботи пошук інформації, використовуючи різноманітні ресурси. Також вирішення цих проблем можна домогтися, якщо наші працівники поліції запозичать зарубіжний досвід успішної діяльності інформаційних систем, якщо громадськість залучиться до процесу розвитку нормативно-правової бази інформаційного забезпечення, бо саме високоякісне інформаційне забезпечення діяльності поліції значно вплине на ефективність їхньої роботи і таким чином покращить стан захищеності прав і свобод людини та громадянина в Україні.

Список використаних джерел:

1. Катеринчук І. П. Актуальні проблеми інформаційного забезпечення правоохоронних органів України. *Форум права*. 2011. № 2. С. 376-380. URL: http://www.nbuv.gov.ua/e-journals/FP/2011.
2. Колісник Т. П. Особливості системи навчання інформатики курсантів у вищих навчальних закладах МВС України. *Право і Безпека.* 2009. № 4. С. 220-222. 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=Pib_2009_4_51.
3. Шорохова Г. М. Проблема вдосконалення інформаційного забезпечення діяльності правоохоронних органів України. *Economic and legal challenges*. 2016, с. 1-4.
2. Харківській поліції передали комп'ютери від ЄС на 98 тис. євро. Укрінформ. URL: http://glavnoe.ua/news/n313828-es_peredal_harkovskoj_policii_oborudovanie_na_98_tys_evro.

Радченко Д. О.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Станіна О. Д.,
доцент кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

КІБЕРЗЛОЧИННІСТЬ: МИНУЛЕ ТА СУЧАСНЕ

Поява та подальше широке розповсюдження телефонів, комп'ютерів та мережі Інтернет серед населення стало причиною виникнення нового типу злочинності – кіберзлочину. Сьогодні вже складно знайти таку людину, яка не зіткнулася з кіберзлочинністю в тому чи іншому її вигляді. За законом України «Про основні засади забезпечення кібербезпеки України», «кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [1].

І справді, під кіберзлочинністю часто розуміють онлайн-правопорушення, але в дійсності цей термін є більш загальним і до нього також можна відносити правопорушення, які є результатом втручання безпосередньо до різноманітних комп'ютерних технологій. Через «взривне» розповсюдження останніх кіберзлочинність є загрозою не тільки на національному, але й на міжнародному рівні.

Наразі кіберзлочинність має широке розповсюдження та у налічує у своїй наявності досить багато схем для застосування [2]. Вона володіє підвищеною громадською небезпекою внаслідок можливості спричинення великого збитку при мінімальних витратах й невисокому ризику.

Не полегшує ситуацію і той факт, що зараз законодавчо все ще немає чіткого розмежування таких визначень, як, наприклад, «кіберзлочинність» та «комп'ютерні злочини» [3].

Окремо слід зазначити, що не так давно спостерігалася відсутність серйозного сприйняття всього, що відбувається в кіберпросторі, відчуття, що все, так би мовити, «не насправді». А отже, в той час, коли зловмисники мали змогу розвиватися та покращувати свою навички, суспільство гаяло час дарма, не сприймаючи ситуацію за серйозну.

За останнє десятиріччя сприйняття проблеми «кібербезпеки» дійсно змінилося, і тепер ми маємо справу з великою кількістю досліджень, проведених

в даній області, але й тут не все так просто, як могло здаватися на перший погляд. Не дивлячись на зростання кількості наукових та практичних робіт, направлених на вивчення кіберзлочинності, та спроби порівняти її з традиційними формами злочинності, серйозною проблемою для досліджень насправді є або відсутність даних, або їх низька достовірність. Спричинено це тим, що кіберзлочинність характеризується високою латентністю («невидимістю»), внаслідок чого статистика правоохоронних органів не відображає достовірної картини стану кіберзлочинності як на рівні держави, так і на загальносвітовому рівні [4].

Протидія кіберзлочинності в широкому розумінні включає в себе загальнодержавні заходи економічного, політичного, виховного та іншого характеру, а також комплекс спеціальних заходів, спрямованих на безпосереднє подолання злочинності. Більш того, інтуїтивно зрозуміло, що існує цілий ряд методів боротьби зі звичайною злочинністю, які перестають працювати в сфері кіберзлочинності, а отже, ми маємо потребу у створенні нових та оновленні вже існуючих методів боротьби з правопорушниками і їх шкідливими діями в області ІТ-технологій.

Боротьба з кіберзлочинністю вимагає спільних дій різних країн, активізації міжнародного співробітництва. Зокрема, діяльність таких міжнародних інституцій, як Інтерпол та Європол, є одним з ефективних засобів протидії кіберзлочинності на міжнародному рівні [3].

Зараз світ впевнено увійшов в цифрову епоху, і разом із полегшенням повсякденного життя ми маємо справу з виникненням нового типу правопорушників – кіберзлочинців. Сьогодні з кожним днем все зрозумілішою стає серйозність ситуації та необхідність її розгляду з точки зору не тільки ІТ-сфери чи кримінальної справи, але й загалом міждисциплінарних відносин. Крім того, здається, що жодна з інших областей злочинності наразі на має такого глобального характеру, а отже, це проблема міждержавна та загальносвітова, і шляхи її вирішення можна буде відшукати саме в сфері глобальної взаємодії та взаємодопомоги.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: Закон України. Урядовий кур’єр, № 215, 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
2. Рудік Г. С., Станіна О. Д. Кібербезпека як міра соціальної свідомості. *Інформаційні технології в освіті та практиці:* матер. Всеукр. наук.-практ. конф. (м. Львів, 17 грудня 2021 р.). Львів: ЛьвДУВС, 2021. С.71-72.
3. Попко В. В., Попко Є. В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського Національного Університету.* 2021. № 66. С. 276-283.
4. Трофіменко О. Г. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2019. Т. 21 (3). С. 150-157.

Рубан І. Д.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Паршин Ю. І.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

ІНФОРМАЦІЙНА БЕЗПЕКА ПІД ЧАС ВІЙСЬКОВОГО СТАНУ

Інформаційна безпека означає, що ми використовуємо випадкові або передбачувані природні або штучні несприятливі наслідки, включаючи інформацію, яка використовується для порушення інформаційної інфраструктури, включаючи інформацію, ми розуміємо, що інформація захищена їх власниками. Захист інформації – це комплекс заходів, спрямованих на забезпечення інформаційну безпеку.

Основними організаторами інформаційної безпеки є такі категорії: надання інфраструктури та підтримка конфіденційності, цілісності та доступності інформаційних ресурсів.

Використання – це можливість отримати необхідне інформаційне обслуговування протягом певного періоду. Цілісність – це доступність інформації, захищена від руйнування та несанкціонована модифікація. Можливість змінювати інформацію має бути доступна лише тим, хто має право на участь. Ця інформація захищена від несанкціонованого доступу та може бути надана тільки для інформації.

Удосконалення інформаційного забезпечення органів внутрішніх справ на основі оснащення їх сучасними програмно-технічними комплексами та системами, а також впровадження у практичну діяльність нових та перспективних інформаційних технологій є одним із пріоритетних напрямків підвищення ефективності правоохоронної діяльності

Практика боротьби зі злочинністю свідчить, що для успішного проведення процесуально-наслідкових та оперативно-розшукових заходів правоохоронним органам необхідна ефективна інформаційна підтримка. Основним інструментом такої підтримки процесу розкриття та розслідування злочинів є оперативно-довідкові, розшукові та криміналістичні обліки, створені та які ведуть органів внутрішніх справ.

Основне завдання обліків – сприяти розкриття та розслідування злочинів. Насамперед вона реалізується шляхом відпрацювання різнопланових запитів. Звертаність до централізованих оперативно-довідкових обліків становить мільйони запитів, у тому числі за електронними, каналів МВС України. Кількість запитів зростає [1].

У побуті захист інформації в основному розглядається як захист від вірусних програм, чи вірусів. Комп'ютерний вірус – вид шкідливого програмного забезпечення Воно здатне створювати власні копії, впроваджуватись в код інших програм, завантажувальні сектори або системні області пам'яті, а також розповсюджувати власні копії з різних каналів зв'язку.

Комп'ютерний вірус недарма був названий так можна порівняти його поширення з біологічним вірусом. У нього є безліч видів: Черв'яки, Троянські програми, Поліморфні віруси та багато інших.

Кожен з цих вірусів діє по-своєму, і постійно з'являються нові і нові віруси. Однак існують і засоби протидії. Вони так і називаються – антивіруси. Антивірус – це спеціалізована програма, призначена для виявлення, усунення та запобігання появі комп'ютерні віруси. Також однією з функцій антивіруса є відновлення заражених вірусами файлів.

Отже, визнаючи потребу в існуванні інтегрованої єдиної державної інформаційної системи, ми зазначаємо щодо необхідності відображення в ній наступних основних складових, які потрібні для проведення повноцінного аналізу баз даних:

– автоматизовані банки даних, що дають можливість накопичення, подальшого пошуку та використання необхідної для повноцінного проведення аналізу інформації (картотеки МВС, бази даних реєстрації автотранспорту);

– автоматизовані системи обліку документообігу, їх систематизація, зберігання та накопичення;

– системи нормативного підтримання діяльності державних органів, суб'єктів господарювання та загальні правові інформаційні системи;

– автоматизовані системи підтримки управлінських рішень;

– спеціалізовані програми пошуку необхідної інформації;·

– забезпечення обміну інформацією [3].

Зазначимо, що інформаційно-комунікаційні технології не розвиваються ізольовано від культури та потреб людей. Зростання масштабів впровадження комп'ютерних технологій та кількості користувачів мобільних пристроїв, підключених до інтернету, одночасно зі створенням нових просторів спілкування посилює техногенні загрози та створює правовий вакуум, яким можуть користуватися зловмисники.

Список використаних джерел:

1. Концепція інформатизації Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, на 2016-2020 роки: Наказ МВС України від 14.06.2016 р. № 511.

2. Кудінов В. А. Проблеми нормативно-правового забезпечення функціонування інтегрованих інформаційно-пошукових систем Міністерства внутрішніх справ України та Національної поліції. *Протидія злочинності: теорія та практика*: матер. VII Всеукр. наук.-практ. конф. (м. Київ, 19 жовтня 2016 р.). Київ: Національна академія прокуратури України, 2016. С. 330-332.

3. Хахановський В. Г. Інтегрований банк даних: формування термінології та проблеми впровадження у правоохоронну діяльність. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2012. № 1 (27). С. 307-311.

Садовий Р. О.,
курсант
Дніпропетровського державного
університет внутрішніх справ
Науковий керівник:
Пиріг І. В.,
професор кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університет внутрішніх справ,
доктор юридичних наук, професор

ОКРЕМІ ПИТАННЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Успіх будь-якої людської діяльності, у тому числі і такої особливої, як розслідування кримінальних правопорушень безпосередньо залежить від рівня інформаційного забезпечення. Саме кваліфікований аналіз інформації про об'єкти, що мають значення для кримінального правопорушення, отриманої з різних джерел, її уміле використання лежать в основі швидкого та ефективного розслідування кримінальних правопорушень.

Необхідність накопичення й обрання інформації ініціювала появу великої кількості інформаційних систем у різних галузях людської діяльності. Сьогодні підґрунтям удосконалення основ інформаційного забезпечення розслідування є інформатизація суспільства, зростання значення інформації в управління та вирішенні найрізноманітніших завдань. Завдяки інтеграції різних за змістом і формою відображень даних з масивів інформації створюються інформаційні системи, що включають велику кількість баз даних з можливістю доступу до інформації з будь-якої віддаленої точки доступу через ядро інтегрованої бази даних.

Сучасні автоматизовані інформаційні системи завдяки програмному забезпеченню здійснюють аналіз інформації в автоматичному режимі. Основою діяльності Національної поліції України є інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України», що являє собою сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності поліції та її інформаційно-аналітичного забезпечення [1]. У сучасних умовах, ключове значення також відіграє кримінальний аналіз, що виступає специфічним видом інформаційно-аналітичної діяльності, яка полягає в ідентифікації та визначенні внутрішніх зв'язків між різними видами інформації, що стосуються кримінального правопорушення, і будь-якими іншими даними, отриманими з різноманітних джерел, їх використанні під час слідчої та оперативно-розшукової діяльності, їх аналітичної підтримки [2, с. 9-10].

Вся діяльність слідчого, починаючи від моменту реєстрації інформації про кримінальне правопорушення у ЄРДР, обирання організаційних заходів та шляхів їх вирішення, планування та проведення слідчих (розшукових) та негласних слідчих (розшукових) дій, здійснюється у інформаційному просторі. Перш за все, необхідно зазначити, що за характером інформація повинна мати відношення до події злочину, тобто мова йде про криміналістично значиму інформацію.

При цьому, В. Тіщенко, зазначає, що джерелами або носіями інформації є об'єкти, що містять у собі криміналістично значущу інформацію, яка використовується з метою доказування й прийняття обґрунтованих процесуальних і тактичних рішень. Однак джерело інформації міститься й зберігається в її носії як у формі, що містить у собі її зміст. Зусилля слідчого спрямовані на розшук і розшифровку носіїв (потенційних джерел) інформації, одержання відомостей, що містяться в них, а також процесуальне закріплення, після чого носії інформації стають джерелами доказової інформації [3, с. 148].

Якщо розглядати розслідування як взаємопов'язану діяльність уповноважених осіб: слідчого, працівників оперативних підрозділів, експертів, спеціалістів тощо, можна зазначити, що всі вони таким чи іншим чином приймають участь у інформаційному забезпеченні розслідування. Ми поділяємо точку зору Пирога І., який вважає, що інформаційне забезпечення розслідування складається з двох різних за змістом видами діяльності: 1) отримання інформації з певних джерел; 2) накопичення та систематизації отриманої інформації [4, с. 350]. Оскільки кримінальне правопорушення є подією минулого, яку учасники розслідування безпосередньо не сприймали, його пізнання здійснюється опосередковано, через виявлення та дослідження відображень його елементів, як системи слідів та об'єктів, що несуть інформацію про подію правопорушення. Існують декілька шляхів отримання інформації, основними з яких є виявлення та дослідження матеріальних об'єктів, що несуть на собі інформацію щодо правопорушення, інший – отримання необхідної інформації від людей, які володіють інформацією про злочин у вербальній формі. Слідчий (дізнавач) та оперуповноважений можуть отримувати інформацію обома шляхами, експерти та спеціалісти – шляхом виявлення та дослідження матеріальних об'єктів.

Список використаних джерел:

1. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: Наказ МВС України від 03.08.2017 р. № 676. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text

2. Основи кримінального аналізу: навч. посібник. Львів: ЛьвДУВС, 2021. 288 с.

3. Бірюков В. В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів: монографія. Луганськ: ЛДУВС ім. Е. О. Дідоренка, 2009. 664 с.

4. Пиріг І. В. Теоретико-прикладні проблеми експертного забезпечення досудового розслідування: монографія. Дніпропетровськ: ДДУВС; Ліра ЛТД, 2014. 366 с.

Свистонюк В. А.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Паршин Ю. І.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

ВИЩИЙ АНТИКОРУПЦІЙНИЙ СУД УКРАЇНИ В СИСТЕМІ ДЕРЖАВНОЇ АНТИКОРУПЦІЙНОЇ ПОЛІТИКИ

Утвердження України як правової держави, зміцнення національних політичних і владних інститутів конче потребує здійснення системної та послідовної державної антикорупційної політики. Вказане твердження ґрунтується на визнаному в академічному середовищі та суспільством загалом постулаті, що «корупція становить загрозу для національної безпеки та державності, її політичного, соціального й економічного розвитку, утвердження і забезпечення принципів демократії, верховенства права, прав і свобод людини та громадянина» [1, с. 43].

Відзначимо, що спеціальні дослідження засвідчують: корупція залишається однією з найактуальніших і найбільш гострих проблем в Україні. Зокрема, дослідження, проведене навесні 2021 року за Методикою стандартного опитування щодо рівня корупції в Україні, засвідчило, що 91,2 % населення України вважає проблему корупції «дуже серйозною» (69 %) або «скоріше серйозною» (22,2 %) [2]. Отож актуальність ефективної антикорупційної політики для України надзвичайна.

Необхідно відзначити, що «Україна як Держава-учасниця Конвенції ООН проти корупції зобов'язана на виконання її вимог розробляти й здійснювати (проводити) ефективну скоординовану політику протидії корупції, яка сприяє участі суспільства і яка відображає принципи правопорядку, належного управління державними справами й державним майном, чесності й непідкупності, прозорості й відповідальності» [3].

При цьому антикорупційну політику обґрунтовано визначити як специфічну діяльність спрямовану на протидію корупції, що передбачає наявність спеціальних засобів (нормативно-правових та організаційно-правових) та методів для реалізації відповідних цілей і завдань. З вказаного визначення походить, що однією з запорук успіху антикорупційної політики є наявність спеціальних інституцій, серед яких особливе місце в реаліях України займає Вищий антикорупційний суд (ВАКС).

Ще до самого моменту свого створення ВАКС став приводом для дискусій. Все це пов'язане з його правовим статусом. В цьому випадку люди поділилися на два табори: перший, який вважає його не конституційним та другий, який впевнений в правомірності створення Вищого спеціалізованого суду, а також запевняє, що перший табір просто не правильно тлумачить закон в цій ситуації.

Ми поділяємо позицію, що поява ВАКС відповідає нормам конституції й спеціального законодавства щодо створення саме спеціалізованих судів [4, с. 3]. ВАКС не є особливим судом, він входить до загальної системи судів України. Натомість, супротив чинять державні службовці, які бояться відчути на собі результат роботи ВАКС, оскільки конституційність створення, наприклад, подібного Вищого спеціалізованого суду щодо питань інтелектуальної власності мало хто обговорює з тих, хто обговорює ВАКС. Безперечно вказана ситуація не може позитивно впливати на роботу суду, оскільки це можна навіть вважати тиском на Суд. Така позиція суголосна з позицією Європейського суду з прав людини (далі – ЄСПЛ), який у своїх рішеннях обґрунтував позицію, «що п. 1 ст. 6 Конвенції про захист прав людини і основоположних свобод щодо права на справедливий розгляд справи незалежним і неупередженим судом, встановленим законом, не може розглядатися як заборона створення спеціальних/спеціалізованих кримінальних судів, якщо вони мають правову основу» [1, с. 46]. Крім того ЄСПЛ обґрунтував розмежування «спеціалізованих судів» від «надзвичайних судів».

Говорячи про місце та роль Вищого антикорупційного суду в системі державної антикорупційної політики, передусім відзначимо, що його завданням є здійснення правосуддя відповідно до визначених законом засад і процедур судочинства з метою захисту особи, суспільства й держави від корупційних і пов'язаних із ними злочинів та судового контролю за досудовим розслідуванням цих злочинів, дотриманням прав, свобод та інтересів осіб у кримінальному провадженні, а також вирішення питання про визнання необґрунтованими активів та їх стягнення в дохід держави у випадках, передбачених законом, у порядку цивільного судочинства [5]. Як визнають експерти, «основними аргументами на користь створення ВАКС були потреба в підвищенні ефективності судочинства, доброчесності та незалежності під час розгляду справ про корупцію, особливо тих, які стосуються політичних еліт, а також очевидна нездатність звичайних судів забезпечити швидкий та безсторонній розгляд таких справ» [6, с. 3].

Діяльність Вищого антикорупційного суду за своїм змістом фактично фіналізує діяльність НАБУ, НАЗК та САП. Саме на суддів ВАКС покладено місію заохочення довіри до національної антикорупційної політики й відповідних заходів. Натомість, як наголошує координатор проектів ОБСЄ в Україні Генрик Віладсен, брак довіри до антикорупційних заходів сприяє поновленню корупції.

У підсумку відзначимо, що поява у структурі судової влади України Вищого антикорупційного суду можна вважати одним з вагомих результатів

антикорупційної реформи, що в Україні була розпочата у 2014 році після Революції Гідності. Нині ВАКС працює у тісній взаємодії з іншими суб'єктами національної антикорупційної політики – НАБУ, НАЗК та САП. Будучі за статусом незалежними органами, вони потребують постійного контролю з боку суспільства, що виступає запорукою ефективності антикорупційної політики. Водночас, необхідно визнати, що ВАКС є наймолодшим суб'єктом такої політики і нині переживає етап інституціонального становлення. Втім це саме той час коли, законодавці й громадяни мають особливо ретельно й критично ставитися до його діяльності. Власне сама Голова ВАКС Олена Танасевич визнає, що на антикорупційному фронті попереду ще багато роботи [7].

Список використаних джерел:

1. Подорожня Т., Худик А. Вищий антикорупційний суд як вищий спеціалізований суд в Україні: проблема конституційно-правового статусу. *Український часопис конституційного права*. 2021. № 2. С. 42–54.
2. Пояснювальна записка до проекту Закону України «Про засади державної антикорупційної політики на 2020-2024 роки». Верховна Рада України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70007.
3. Антикорупційна політика. Офіційний веб-сайт Національного агентства з питань запобігання корупції. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=70007.
4. Косиця О. О. Організаційно-правові підстави створення антикорупційного суду в Україні. *Судова та слідча практика в Україні*. 2017. Вип. 4. С. 6-10.
5. Про Вищий антикорупційний суд: Закон України від 07.06.2018 р. № 2447-VIII. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2447-19#Text.
6. Кузь І., Стівенсон М. Вищий антикорупційний суд України. *U4 Brief*. 2020. № 5. URL: https://www.u4.no/publications/ukraines-high-anti-corruption-court-ukranian.pdf.
7. Сильні антикорупційні органи, політична воля та контроль суспільства – складові ефективної боротьби з корупцією. НАБУ, 09.12.2021. URL: https://nabu.gov.ua/novyny/sylni-antykorupciyni-organypolitychna-volya-ta-kontrol-suspilstva-skladovi-efektyvnoyi.

Сімашкевич П. Р.,
здобувач вищої освіти
Університету митної справи та фінансів
Бутов Д. А.,
здобувач вищої освіти
Університету митної справи та фінансів
Науковий керівник:
Чупілко Т. А.,
доцент кафедри комп'ютерних наук
та інженерії програмного забезпечення
Університету митної справи та фінансів,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЛОГІСТИЦІ ЯК СКЛАДОВІЙ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Сучасна логістика є одною зі складових економічної безпеки. Організація роботи доставки, координація між цехами виробництва, обмін інформацією між відділами та філіями, швидке реагування на надзвичайні ситуації, аналіз споживання продукту та рівень продажів засновані на сучасних інформаційних технологіях.

Інформаційні системи і технології у сучасній логістиці – це комплекс програмно-технічних засобів і методів виробництва, передачі, обробки та споживання інформації в товаропродажних системах, що забезпечуються. ІТ у сучасній логістиці спрямована на інтеграцію інформаційних потоків на основі сучасних методів обробки та передачі даних.

З логістикою тісно пов'язана телематика, яка охоплює телекомунікації, транспортні технології, що надаються за допомогою комунікаційних мереж. У зв'язку з телематикою можна виділити кілька системних рівнів [1]:

- технічне забезпечення (обладнання, програмне забезпечення);
- комунікаційні можливості (типи інформації, режими взаємодії);
- загальні служби (електронна пошта, конференції);
- прикладні задачі (наприклад, робота проектних груп, ділові ігри).

Інформаційні потоки циркулюють всередині логістичної системи або між логістичною системою та зовнішнім середовищем.

Використання в логістиці технології автоматичної ідентифікації штрихових кодів дозволяє суттєво покращити управління матеріальними потоками на всіх етапах логістичного процесу. Автоматичне отримання інформації з допомогою штрих-кодів може здійснюватися завдяки використанню декількох видів кодів [1]:

- код з прямокутним контуром – ITF-14 – може друкуватися не тільки на гладких поверхнях, використовується переважно для кодування товарних партій;
- код 128 – використовується паралельно з іншими кодами для кодування додаткової інформації (номер партії, дата виготовлення, термін реалізації тощо);

– код EAN – найчастіше використовується на товарах масового вжитку, складається з чотирьох частин, на основі яких можна визначити країну виробника, підприємства виробника, найменування товару а також проконтролювати правильність формування коду.

З допомогою спеціального обладнання та програмного забезпечення зчитування кодів при придбанні чи реалізації товарів дозволяє відстежувати оперативні зміни розмірів запасів на складах, в оптовій чи роздрібній сітці.

Інформаційні потоки розрізняються за [2]:

– відношенням до логістичної системи та її ланок – внутрішніх та зовнішніх, горизонтальних та вертикальних, вхідних та вихідних;

– видами носіїв інформації – паперових, магнітних, електронних;

– періодичністю надання інформації – регулярної, періодичної, оперативної;

– призначенням інформації – директивні, нормативно-довідкові, обліково-аналітичні, допоміжні;

– ступеню відкритості – відкриті, закриті, секретні;

– способом надання – кур'єрські, поштові, телеграфні, телефонні, факсові, радіотелевізійні, електронна пошта, телекомунікаційні, інтернетівські.

Логістичні операції – це сукупність дій, спрямованих на перетворення речовинного, енергетичного або інформаційного потоку. Деякі логістичні операції є продовженням технологічного виробничого процесу, наприклад розфасовки. Ці операції змінюють споживчі властивості товару, які можуть здійснюватися як у сфері виробництва, так і в сфері обігу.

Логістичні операції такі, як постачання сировини на підприємство або збут готової продукції, виконувані в процесі «спілкування логістичної системи із зовнішнім світом», відносять до категорії зовнішніх логістичних операцій. Логістичні операції, що виконуються всередині логістичної системи, називають внутрішніми. Інформаційна логістика розвивається завдяки значній ролі інформації у господарському процесі та інноваційним технологіям, матеріальною базою яких є:

– електронно-обчислювальна техніка;

– персональні комп'ютери і сервери;

– засоби комунікації;

– автоматизоване устаткування.

Використання інформаційних технологій стає більш актуальним через збільшення обсягу інформації, яку потрібно обробити і подати у потрібному вигляді. Швидкість обробки інформації впливає на ефективність управління, фінансові успіхи, кількість клієнтів. Сучасні інформаційні технології, побудовані на основі використання концепцій інформаційних сховищ та інтелектуальної обробки даних, сприяють суттєвому підвищенню продуктивності в розв'язанні задач логістики.

Список використаних джерел:

1. Інформаційна логістика. Інформаційні технології в логістиці. URL: https://stud.com.ua/1912/logistika/informatsiyna_logistika.

2. Цілі, завдання та функції інформаційної логістики. URL: https://stud.com.ua/23017/logistika/logistika_informatsiyne_zabezpechennya_protsesiv.

Стоєва Т. І.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Коренев А. О.,
доцент кафедри
загальноправових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Сьогодні суспільний розвиток та обізнаність українців характеризується формуванням інформаційної сфери держави. Зокрема, інформаційна сфера є фундаментальним чинником життя суспільства, ефективно впливає на стан розвитку політичної, економічної, військової та інших складових інформаційної безпеки. Головну роль в ефективності забезпечення інформаційної безпеки відіграє адміністративне право, яке забезпечує реалізацію механізму забезпечення інформаційної безпеки. У зв'язку з цим адміністративно-правове забезпечення інформаційної безпеки набуває все більшої значущості в загальній системі інформаційного права держави. Саме тому одним із пріоритетних завдань України, як правової демократичної держави, є прагнення розвитку інформаційної сфери. В умовах сучасних глобальних та регіональних змін значно змінюється ситуація в інформаційній сфері, істотно трансформуються її окремі складові, але в цілому проблема забезпечення інформаційної безпеки залишається актуальною, оскільки наразі спостерігається кібервійна та посягання на інформаційний простір України. Тобто сьогодні функціонуванні інформаційної безпеки України залишаються невирішеними проблеми щодо створення ефективної системи захисту національного інформаційного простору, подолання колізій та прогалин у чинному інформаційному законодавстві, попередження порушення інформаційних прав і свобод людини та громадянина. Тому особливе місце у державному та суспільному просторі займає проблема адміністративно-правового забезпечення інформаційної безпеки. Метою роботи є аналіз сучасного стану адміністративно-правового забезпечення інформаційної безпеки в Україні.

Тож проблематика інформаційної безпеки складна і багатоаспектна, що потребує необхідність вивчення й узагальнення наукових праць представників різних галузей юридичної науки. Зацікавленість викликає робота таких дослідників як Дані-льян О., Дзьобань О., Панов М., які у своєму навчальному посібнику «Національна безпека України: сутність, структура та напрямки

реалізації», визначають інформаційну безпеку як безпеку об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією та нерозголошення даних про той чи інший об'єкт, що є державною таємницею [1]. Цікавим є визначення Кормича Б., який зазначає, що інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави [2, с. 142]. Отже, визначаючи поняття інформаційної безпеки, можна виокремити декілька підходів окреслення сутності цього феномену. Зокрема, під поняттям інформаційна безпека розуміють комплекс заходів щодо запобігання несанкціонованому доступу та використання інформації, тобто процес захищеності інформаційного простору шляхом встановлення законодавством нормативно-правових актів, за якими відбуваються інформаційні процеси в державі. А специфіка забезпечення інформаційної безпеки відображена в Законі України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про захист персональних даних».

Особливого значення серед нормативно-правових актів набуває адміністративно-правове забезпечення інформаційної безпеки. Тож адміністративно-правове регулювання має засоби щодо забезпечення інформаційної безпеки, які виступають невід'ємною складовою сучасної системи захисту інформаційного простору. Найбільш актуальним серед адміністративно-правових засобів забезпечення інформаційної безпеки можна вважати метод колегіальності контролю за додержанням режиму секретності. Так, наприклад, О. Олійник стверджує, що застосування названого методу передбачає проведення колегіальних (комісійних) перевірок додержання режиму секретності (конфіденційності): внутрішньо об'єктових, тобто в центральних апаратах державних органів, на підприємствах, установах і організаціях – у строки, визначені нормативними документами; галузевих, відомчих, загально-державних (здійснюються спеціально уповноваженим органом державної влади у сфері охорони державної таємниці) – у строки, визначені відповідними керівниками [3, с. 107]

Не менш важливу роль серед адміністративно-правових засобів забезпечення інформаційної безпеки України і, як один із методів державного управління, виступає реєстраційний метод. У чинній системі виконавчої влади функції з реєстрації віднесені до контрольно-наглядових. Реєстрація засобів масової інформації являє собою необхідну умова діяльності щодо виробництва й випуску засобів масової інформації. Так, з урахуванням вимог статті 4 Закону України «Про друковані засоби масової інформації (пресу) в Україні», вказано, що друковані засоби масової інформації в Україні видаються державною мовою, а також іншими мовами реєстрації засобу масової інформації [4].

Отже, інформаційний простір відіграє важливу роль у державотворчому процесі, розвитку економічної, політичної й суспільної сфер та відстоюванні інтересів держави на міжнародному рівні. Одним із пріоритетних завдань

України, як правової демократичної держави, є прагнення розвитку інформаційної сфери. В умовах динамічного розвитку інформаційної сфери питання інформаційної безпеки має вагоме значення для національної безпеки України. Наведені вище підходи до визначення поняття інформаційної безпеки дають змогу розглядати дану проблематику більш комплексно і системно. Тобто під поняттям інформаційної безпеки України слід розуміти процес захищеності інформаційного простору, закріплений на законодавчому рівні за якими відбуваються. Важливе місце у забезпеченні інформаційної безпеки посідає методи адміністративно-правового регулювання. Методи адміністративно-правового регулювання є своєрідним специфічним інструментом правового регулювання. Таким чином здійснення методів адміністративно-правового забезпечення покликані на забезпечення протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захист держави та суспільства від негативного інформаційного впливу.

Список використаних джерел:

1. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: сутність, структура та напрямки реалізації. Харків: «ФОЛІО», 2002. 296 с.
2. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: Юридична література, 2003. 472 с.
3. Олійник О. В. Методологічні засади забезпечення системи інформаційної безпеки та її складової – захисту інформаційних ресурсів. *Право і безпека*, 2014. С. 103-109.
4. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 р. *Відомості Верховної Ради України (*ВВР), 1993.

Стоєва Т. І.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Грицай І. О.,
професор кафедри
загальноправових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
доктор юридичних наук, професор

РОЛЬ ЖІНКИ-ВІЙСЬКОВОСЛУЖБОВЦЯ В УКРАЇНІ В УМОВАХ ВОЄННОГО СТАНУ

Завдання держави щодо забезпечення гендерного балансу у військовій сфері набуває особливого значення в умовах воєнного стану. На сьогодні гендерна рівність є одним з основоположних напрямів законодавчої та

політичної діяльності держави. Цілі, які визначила для себе Україна щодо забезпечення гендерної рівності полягають у подоланні обмежень прав та можливостях самореалізації у військовій сфері, як на законодавчому рівні, так і в реальному житті, особливо в умовах дії воєнного стану, коли нормальне функціонування сфер життєдіяльності суспільства і самої держави стає неможливим. Дотримання державою гендерного паритету в усіх сферах її діяльності дає особам обох статей рівні умови для реалізації прав людини, для участі в національному, політичному, економічному, соціальному та культурному розвитку держави. Наразі гендерна політика України у військовій сфері загалом відповідає світовим досягненням, це пов'язано з ти, що Збройні Сили України йдуть шляхом трансформації щодо питання гендерної рівності. Тому зараз українське суспільство відходить від стереотипу «армія – не для жінок».

Тож рівень гендерної рівності у військовому інституті базується, насамперед, на суттєвих позитивних змінах у політико-правовому аспекті українського суспільства та законодавстві держави. Це зростання є об'єктивним показником подальшої правової обізнаності й демократизації сучасного суспільства на шляху до встановлення відповідної гендерної рівності. Питання рівних прав і можливостей жінок і чоловіків в українському суспільстві втілюється, передусім, на державному рівні та регулюються Конституцією і іншими спеціальними нормативно-правовими актами. Так відповідно до частини третьої статті 24 Конституції України: «Громадяни мають рівні конституційні права і свободи та є рівними перед законом. Рівність прав жінки і чоловіка забезпечується: наданням жінкам рівних з чоловіками можливостей у громадсько-політичній і культурній діяльності, у здобутті освіти і професійній підготовці, у праці та винагороді за неї» [1]. Конституція України є основним нормативно-правовим актом, який спрямований на реалізацію жінками і чоловіками своїх рівних прав і можливостей, і закріплює рівність прав жінки і чоловіка. Права людини належать кожному індивіду, незалежно від статті особи. Тобто, частина третя статті 24 Конституції України безпосередньо присвячена подоланню дискримінації стосовно жінок в Україні та наголошує на тому, що рівність прав жінок та чоловіків забезпечується наданням жінкам рівних з чоловіками можливостей.

Аналізуючи нормативно-правові акти слід констатувати той факт, що Збройні Сили України зазнають певної трансформації, тому фізична сила, яку традиційно вважають чоловічою особливістю, втрачає свою цінність і все частіше й ефективніше застосовуються інтелектуальні тактики, підвищується вимога до особового складу і в рівні освіти, з інтелектуально-психологічних якостей, і зі спеціальної підготовки. Саме тому, фізична сила та агресія притаманна чоловікам відходить на другий план і все частіше вдаються до розумових якостей. Таким чином, прийнятий Закон України «Про військовий обов'язок і військову службу» є підтвердженням значущості жінки, як військовослужбовця [2]. Роль жінки-військовослужбовця набуває особливого значення, адже тепер фізична сила та витривалість – це не тільки особливості,

які притаманні чоловікам. Тож сьогодні, в умовах воєнного стану, жінки, як парамедики, артилеристки, снайперки, розвідниці, командирки рот і взводів виконують свій військовий обов'язок на передовій та в тилу нарівні з чоловіками.

Зважаючи на викладене, можна зробити висновок, що рівноправність чоловіків і жінок є невід'ємною частиною прав людини. Україна, як соціальна, правова та демократична держава забезпечує гендерну рівність в усіх сферах життєдіяльності суспільства, зокрема і у військовій сфері. Об'єктивним аспектом у досягненні гендерної рівності є наділення жінок повноваженнями і більш широкими можливостями в різних сферах розвитку суспільства [3]. Такий рівень гендерної рівності у військовому інституті ґрунтується, насамперед, на суттєвих позитивних змінах у політико-правовому аспекті держави. Жінок у збройних силах буде все більше та більше, це об'єктивний та соціальний процес, тому питання ролі та місце жінки-військовослужбовця в Збройних Силах України залишається актуальним явищем. Роль жінки-військовослужбовця набуває особливого значення, адже зараз армія стає більш інформаційним та інтелектуальним інститутом, що потребує реалізації не тільки в фізичній силі та агресії, а насамперед інтелектуального і досвідченого потенціалу військовослужбовців. Для України надто важливим аспектом є якість війська, тому Збройні Сили України на сьогоднішній день не зважають на стать, а в першу чергу важливою ознакою є професіоналізм. Саме тому, сьогодні в умовах воєнного стану в Україні роль жінки-військовослужбовця набуває особливого значення, що пов'язано не тільки з рівнем демократичності держави, але і з дотриманням гендерного паритету у військовій сфері.

Список використаних джерел:

1. Конституція України: Закон України від 28.06.1996 р. № 254к/96. (зі змін. і доп.). *Відомості Верховної Ради України.* 2019, № 38, ст.160.
2. Про військовий обов'язок і військову службу: Закон України від 25.03.1992 р. *Відомості Верховної Ради України* (ВВР), 1992, № 27, ст. 385 URL: https://zakon.rada.gov.ua/laws/show/2232-12#Text.
3. У лавах ЗСУ служать понад 50 тисяч жінок: Львівський портал. Новини Львова. URL: https://portal.lviv.ua/news/2022/07/26/u-lavakh-zsu-sluzhat-ponad-50-tysiach-zhinok#:~:text.

Сумцов А. Ю.,
курсант
Харківського національного
університету внутрішніх справ
Науковий керівник:
Світличний В. А.,
доцент кафедри
протидії кіберзлочинності
Харківського національного
університету внутрішніх справ,
кандидат технічних наук, доцент

ДЖЕРЕЛА ІНФОРМАЦІЇ В СИСТЕМІ СУБ'ЄКТНО-ОБ'ЄКТНИХ ВІДНОСИН ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ. ТИПОЛОГІЯ ТА КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ

Згідно із Законом України «Про інформацію» «джерелами інформації є передбачені або встановлені Законом носії інформації: документи та інші носії інформації, які являють собою матеріальні об'єкти, що зберігають інформацію, а також повідомлення засобів масової інформації, публічні виступи». У свою чергу, документ – це передбачена Законом матеріальна форма одержання, зберігання, використання і поширення інформації шляхом фіксації її на папері, магнітній, кіно-, відео-, фотоплівці або на іншому носієві [1]. З поняттями «джерело інформації» та «документ» пов'язаний термін «носій інформації (даних)», який в науковій літературі визначається як матеріальний об'єкт, призначений для зберігання даних.

Таким чином, у системі суб'єктно-об'єктних відносин інформаційної діяльності джерелом інформації є будь-який об'єкт, де нагромаджуються повідомлення, дані, що в подальшому використовуються суб'єктами інформаційних відносин (державними організаціями, посадовими та юридичними особами, громадянами), впливають на їхню поведінку.

Джерела інформації поділяються на друковані та недруковані або змішані та електронні. До друкованих належать: неперіодичні видання, довідково- енциклопедичні, наукові видання, інші видання (брошури, рекламні буклети), періодичні видання. До недрукованих належать: спеціальні рукописні матеріали та науково-технічна документація, реклама, виставки, конференції, консультаційні послуги, статистична інформація, чутки, компромат, приватні бесіди, інші джерела інформації. До електронних належать: радіо, телебачення, телефон, Інтернет тощо [2].

Типологія та класифікація інформації. Види інформації, які використовуються в управлінні, класифікуються за наступними ознаками:

- змістом – політична, директивна, правова, науково-технічна, економічна, планова, адміністративна, виробнича, бізнесова, нормативно-довідкова, обліково-бухгалтерська, статистична;

- напрямом руху – вхідна, вихідна;
- характером фіксації – фіксована, нефіксована;
- способом фіксації – документована, звукова, аудивізуальна;
- відношенням до суб'єкта управління – зовнішня, внутрішня;
- ступенем обробки – первинна, довільна, підсумкова;
- ступенем постійності – постійна, перемінна;
- формі надання – літерна, цифрова, кодована;
- можливості обробки – піддається і не піддається обробці;
- насиченості – достатня, недостатня, збиткова;
- правдивості – достовірна, недостовірна [1-2].

Інформація з обмеженим доступом, у свою чергу, поділяється на таємну і конфіденційну. До таємної належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі [3]. Конфіденційна – інформація, що містить відомості, які знаходяться у володінні, користуванні або розпорядженні юридичних та фізичних осіб і поширюється за їхнім бажанням згідно з передбаченими умовами (ст. 30 Закону України «Про інформацію»).

Відкрита – інформація, якою дозволено користуватися широкому загалу. Існує певний зв'язок між реальною доступністю інформації та режимом доступу до неї. Він проявляється у праві на інформацію та його реалізації. Адже не всяка відкрита інформація доступна певному суб'єктові і навпаки.

За своєю генезою інформація (дані) поділяється на первинну і вторинну. Первинна – це інформація (дані), зібрана вперше для розв'язання якого-небудь завдання. А вторинна – та, яка вже була зібрана раніше для інших цілей. Поширене трактування вторинної інформації як продукту переробки первинних даних висхідного повідомлення.

За своєю суб'єктною належністю інформація поділяється на внутрішню і зовнішню. Наприклад, інформація, що обертається в межах підприємства, є його внутрішньою інформацією. А та, що надходить з оточуючого середовища, – зовнішньою.

Інформація виникає і змінюється разом з її матеріальної структурою в єдиному русі, як результат порівняння властивостей об'єктів у процесі їх взаємодії. Це відбувається скрізь і постійно, і в живому, і в неживому.

Список використаних джерел:

1. Про інформацію. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
2. Учасники проектів Вікімедіа. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Інформація.
3. Поняття та види інформації з обмеженим доступом. *Електронна бібліотека онлайн MegaLib.* URL: http://megalib.com.ua/content/148_42Ponyattya_ta_vidi_informacii_z _obmejenim_dostypom.html.

Тараніна М. В.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Рибальченко Л. В.,
завідувач кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ПРОТИДІЯ ГЕНДЕРНИМ СТЕРЕОТИПАМ ТА ГЕНДЕРНІЙ НЕРІВНОСТІ: МІЖНАРОДНИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД

Питання гендерної рівності в Україні є одним із актуальних на рівні з економічними та політичними. Захист прав та свобод є запорукою успішної держави з міцною підтримкою на суспільство, бо в будь-якому демократичному суспільстві кінцеві результати тих чи інших дій залежать від суспільства. Дослідження міжнародного досвіду по правовому забезпеченню гендерної рівності має вагоме значення для народу не тільки у вигляді виконання міжнародних норм та стандартів, дотримання та виконання прав і свобод людей, а й також внесення змін у сучасне законодавство України по забезпеченню прав задля формування ефективних заходів застосування їх на практиці.

Гендерна рівність є основним елементом соціальної відповідальності і для розширення прав жінок та чоловіків. Процес становлення рівних прав та свобод знаходиться на стадії стрімкого розвитку. Більшість країн Європи прискореними темпами запроваджують у практику раніше задекларовані положення про рівність можливостей жінок та чоловіків у всіх сферах життя суспільства, що є одним із основних факторів економічного та соціального розвитку. У деяких країнах Європи на чолі уряду стоять жінки та здобуто паритетне представництво чоловіків і жінок у парламенті [1].

Одночасно у багатьох країнах Світу відбувається маніфестація маргіналізації цих питань, щодо до їх внесення у порядок денний вищих органів державної влади. Завдяки впливу та тиску міжнародних організацій ці питання стають частиною політичного порядку денного залишаючись певним реверансом у бік міжнародного співтовариства. Це відбувається тому, що творці та адепти гендерної теорії та політики не завжди можуть знайти правильні шляхи впровадження ідей гендерної рівності, зіштовхуючись с такими проблемами як непорозуміння з суспільством, також труднощами у пристосуванні теоретичних положень до сучасного стану суспільного розвитку.

Зараз у сучасному суспільстві, проблеми гендерної рівності, гендерних стереотипів та політики сприймаються суспільством доволі сумнівно.

Наразі не всі люди готові йти в ногу з часом та змінювати своє життя відповідно до нових трендів та нововведень.

Якщо в одних країнах жінки живуть на рівних правах з чоловіками, то в інших – дівчата систематично потерпають від принижень, дискримінації стосовно ґендерної ознаки та сексуальному насиллю. Так, в Афганістані 87 % жінок потерпають від домашнього насильства. Для сучасного суспільства це є занадто шокуючим і неприпустимим. Згідно конституції Афганістана, яка була прийнята в 2004 році, жінки та чоловіки «мають рівні права та можливості перед законом» та «праця є правом кожного афганця», але на практиці дівчатам не можна з'являтися на очі перед чоловіками з 8 років, крім своїх рідних. Навіть навчатися в школі дівчата не мають можливостей, тому й рівень грамотності складає лише 28 %. В усьому світу ще існує велика кількість нерівних прав жінок та чоловіків. Так, наприклад, у світі жінки виконують 66 % усієї роботи, виробляють 50 % їжі але заробляють 10 % від доходу і володіють 1 % власності [3]. До інших ознак нерівності прав між чоловіками та жінками можна віднести *заборону доступу жінок до багатьох професій, оплата праці жінок є меншою, ніж у чоловіків, переваги у вихованні дітей та виконання домашньої роботи припадають здебільше на жінок та багато іншого.*

В основі гендерних стереотипів можуть бути народні вірування, традиційні у відповідності до певного регіону. Уявлення про зовнішність жінки народів Африки суттєво відрізняється від європейських.

Отже, міжнародні стандарти забезпечення прав і свобод людини мають бути основоположними принципами в правовій сфері та відповідати вимогам демократичного, громадянського суспільства. Розвиток цього напрямку має полягати у застосуванні міжнародних стандартів, які забезпечували б функціонування суспільних відносин у різних сферах життєдіяльності на засадах непорушності конституційних прав і свобод людини та громадяни [3]. Згідно рейтингу країн світу за рівнем гендерної нерівності, найвищу правову захищеність має суспільство Швейцарії, а найбільша незахищеність у Ємені [3].

З часом відбуваються позитивні зміни в суспільстві, коли в родині народжується дитина, а у декретну відпустку йде мати. Так, відповідно до законодавства України, чоловіки тепер мають право на декретну відпустку.

В *Законі* України «Про *забезпечення рівних прав* та *можливостей жінок* і *чоловіків*» зазначено основні напрямки державної політики щодо забезпечення рівних прав та можливостей жінок і чоловіків [2].

Таким чином, двадцять перше сторіччя стало періодом становлення гендерної рівності – соціальної рівності чоловіків і жінок. Міжнародний досвід показує, що велика кількість людей зацікавлена у змінах свого життя на краще. Міжнародні стандарти прав та свобод людини були створені, використовуються та будуть удосконалюватися надалі для підвищення рівня життя населення. Процес розвитку гендерного законодавства продовжується за сприянням Уряду та органів виконавчої влади для забезпечення гендерної рівності в українському суспільстві.

Список використаних джерел:

1. Рибальченко Л. В. Правові відносини забезпечення гендерної рівності у сфері праці: матер. VI Міжнар. наук.-практ. конф. (м. Дніпро, 11 березня 2022 р.). Дніпро: ДДУВС, 2022. С. 98-100.
2. Про забезпечення рівних прав *та* можливостей жінок і чоловіків: Закон України від 08.09.2005 р. № 2866-VI (із змін. та доп. № 2229-VIII від 07.01.2018 р.).
3. Рейтинг країн світу за рівнем гендерної нерівності. URL: https://gtmarket.ru/ratings/gender-inequality-index.

Тараніна М. В.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Рибальченко Л. В.,
завідувач кафедри
інформаційних технологій
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ВДОСКОНАЛЕННЯ ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ЛЮДИНИ І ГРОМАДЯНИНА НА ШЛЯХУ ІНТЕГРАЦІЇ УКРАЇНИ В ЄВРОПЕЙСЬКИЙ СОЮЗ

Тема результативного забезпечення прав та свобод людей і громадян займає одне із першочергових місць будь-якої країни, яка визначає себе як демократичною, правовою, соціальною державою. Виняткової сучасності у дослідженні питань щодо забезпечення механізму захисту прав та свобод людей і громадян в Україні набуває через велике прагнення нашої країни здійснити долучення до європейської спільноти, а окремо у рамках реалізації Угоди про асоціацію між Україною та ЄС.

Пошановування прав та свобод людини є ключовим принципом, що полягає в основі діяльності ЄС. Однією з першочергових цілей щодо європейської інтеграції було визначено запобігання повторення жахливих наслідків Другої світової війни, і якраз тому в першій Європейській Конвенції 1957 року є положення, що є присвячені правам людини, а саме такі: заборона дискримінації, свобода пересування та право на гідну винагороду [1]. Одночасно вкрай доцільно розуміти саме рух європейської інтеграції як процес підвищення значення прав людей і громадян в Європейському правовому порядку: крім того, права та свободи людини набувають всякчас ще більшої вагомості у процесі розширення Союзу. Історія доводила багато разів: хоча права людини

не побутували у початкових договорах, але все ж таки вони безпремінно набули вагомого значення з кінця 1960-х років [2]. Даний рух останнім часом, навіть прискорився. Найбільш виразним доказом можна зазначити рішення Європейської ради на саміті, що відбувся у м. Кельні про те, що для Європейського Союзу повинна бути розроблена Хартія прав людини, тому що «захист основних прав є основоположним принципом Союзу і необхідною умовою для його легітимності» [3]. Наразі ЄС є спільнотою, в котрій держави про себе заявляють як демократичних та європейських держав, котрі прагнуть до зміцнення миру і процвітання [1]. Так, у відповідності до ст. 2 Договору про Європейський Союз (далі – Договір про ЄС) Союз, що є заснований на таких цінностях як: повага до людської гідності, свобода, демократія, рівність, верховенство права, повага до прав людей і громадян, включаючи права осіб, котрі належать до меншин. Ці цінності визнаються спільними для держав-членів в суспільстві, в якому превалюють плюралізм, недискримінація, рівність між жінками і чоловікам толерантність, справедливість, солідарність. Союз визначає права, свободи і принципи, що є зазначені в Хартії основних прав Європейського союзу від 7 грудня 2000 року, адаптованої в Страсбурзі 12 грудня 2007 року, яка буде мати ту ж юридичну цінність в якості договорів. Союз зробив приєднання до Європейської конвенції про захист прав людини і основних свобод. Основоположні права, котрі є гарантовані Європейською конвенцією про захист прав людини і основних свобод та як вони випливають із загальних конституційних традицій держав-членів, становлять загальні принципи права Союзу (стаття 6 Договору про ЄС) [4].

Україна вже достатньо твердо стала на шлях щодо розвитку тісніших зв’язків з Європейським Союзом та його державами-членами. Україна вже давно та доволі плідно інтегрувалася в Європу. Окрім узгодження своїх власних інтересів економічної сфери з ЄС, Україна вже є членом таких організацій як: Рада Європи (1995), ОБСЄ(1992), Енергетичне співтовариство (2011) і визнає юрисдикцію Європейського суду з прав людини, у зв’язку з підписанням Європейської конвенції з прав людини у 1997 році. Ратифікація 16 вересня 2014 р. Верховною Радою України та Європейським Парламентом Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (далі – Угода про асоціацію, Угода) стала вагомим етапом на шляху вдосконалення механізму захисту прав та свобод людей і громадянин в Україні. Статтею 2 Угоди про асоціацію сказано, що повага до демократичних принципів, прав людини та основоположних свобод, а також повага до принципу верховенства права повинні формувати основу внутрішньої та зовнішньої політики Сторін і є основними елементами цієї Угоди.

Згідно до ст. 4 Угоди у всіх сферах, що являє собою обопільний інтерес, між сторонами повинен як розвиватися так і зміцнюватися політичний діалог. Цілями подібного діалогу визначають є зміцнення поваги до демократичних принципів, верховенства права та доброго врядування, прав людини та основоположних свобод, також і прав осіб, котрі належать до нацменшин, не дискримінації осіб, котрі мають свою приналежність до меншин, і поваги до різноманітності, а ще й внесок у консолідацію внутрішніх політичних реформ [5].

Таким чином, варто зробити акцент, що для подальшого забезпечування плідного механізму захисту прав та свобод людей і громадян в Україні, процес європейскої інтеграції має важливе стратегічне значення. Серед нечималої кількості тих викликів, що стоять перед українською народом, котра обрала європейський вектор розвитку, щонайголовнішого значення являють собою такі питання як наближення законодавства України у сфері захисту прав людини до європейських стандартів, котрі вже є загальновизнаними. Зокрема багатообіцяючими, на наш погляд, в контексті європейської інтеграції можна виокремити такі напрямки реформування законодавства у сфері захисту прав людини і громадянина, як: покращення законодавчої бази України у частині забезпечення принципу рівності та недискримінації; модернізування функціонування таких правозахисних інститутів, як Уповноважений Верховної Ради України з прав людини, суду, прокуратури; поліпшення механізму захисту прав.

Відштовхуючись від вищезазначеного дослідження, можна стверджувати, що вдосконалення забезпечення прав і свобод людини і громадянина на шляху інтеграції України в Європейський Союз, має нечималі перешкоди, але як влада так і суспільство здійснює плідну спільну співпрацю щодо вступу України до ЄС. Наша країна вже приклала велику кількість зусиль для досягнення суспільної мети, але попереду не менш важкий етап, щоб нарешті отримати бажане.

Список використаних джерел:

1. Icelandic Human Rights Centre. The Role of the European Union (EU). URL: http://www.humanrights.is/en/human-rights-education-project/human-rights-concepts-ideas-and-fora/human-rights-actors/the-role-of-the-european-union-eu.
2. Cassese C. W. Human Rights and the European Community. Human Rights and the European Community: the Substantive Law. Vol. 3. Baden-Baden, 1991.
3. Bogdandy A. The European Union as a Human Rights Organization? Human Rights and the Core of the European Union. *Common Market Law Review.* 2000. Vol. 37, pp. 1307-1338.
4. Consolidated version of the Treaty on European Union – 26.10.2012. P. 13-390.
5. Association Agreement between the European Union and its Member States of the one part, and Ukraine, of the other part (29.05.2014). P. 2133-2137.

Тишков В. Р.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Паршин Ю. І.,
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

НАПРЯМИ ПОБУДОВИ ПРОЦЕДУР АНТИВІДМИВЧОГО РЕГУЛЮВАННЯ В УКРАЇНІ

Україна, як центральноєвропейська держава, займає важливе геополітичне становище. Відповідний стан зумовлює великий інтерес у зарубіжних злочинних угрупувань та організацій поширювати свій вплив на території України. Крім того, сучасний стан антикорупційного законодавства в державі створює всі необхідні умови для успішного відмивання коштів та їх тінізації. Відповідні обставини зумовлюють необхідність вдосконалення процедур антивідмивчого регулювання.

Важливо аби напрями побудови процедур антивідмивчого регулювання базувалися і на досвіді міжнародних організацій. Гарним прикладом може бути Група з протидії відмиванню брудних грошей (FATF). Вона допомагає країнам створювати підрозділи фінансової розвідки (ПФР), задача яких – керувати потоком інформації між своїми установами та правоохоронними органами. Законодавство зарубіжних країн виводять відповідні фінансові установи на перший рівень боротьби з відмиванням грошей. Вони попереджають правоохоронні органи про підозрілі операції, які можуть мати злочинний характер. Про відповідну діяльність вони складають так звані звіти про підозрілі операції (STR) та звіти про підозрілу діяльність (SAR), які потім направляють до відповідних правоохоронних органів [1].

Для успішної боротьби з відмиванням брудних грошей багато зарубіжних країн створюють спеціальні нормативні акти, схожі на ті, що розроблялися Держфінмоніторингом в Україні. Прикладом такого спеціального законодавства можуть бути:

– США: Патріотичний акт США, Закон про банківську таємницю;

– ЄС: Четверта Директива ЄС щодо боротьби з відмиванням грошей (4AMLD);

– Канада: Закон про доходи від злочинів (відмивання грошей) та фінансування тероризму (PCMLTFA);

– Австралія: Закон про боротьбу з відмиванням грошей та фінансуванням тероризму 2006 року [1].

В різних країнах вимоги відповідних нормативно-правових актів залежать саме від юрисдикції фінансових установ, що здійснюють боротьбу з відмиванням брудних грошей. Проте, загалом вони вимагають проведення відповідних процедур: програма ідентифікації клієнта або «Знай свого клієнта» (KYC), звітність про великі операції в іноземній валюті, моніторинг підозрілої діяльності та звітування, дотримання санкцій.

Сучасний стан антикорупційного законодавства в Україні потребує удосконалення та актуалізації під тенденції сьогодення. Для цього необхідно переймати досвід зарубіжних країн в яких рівень відмивання коштів та їх тінізації такий, що не створює проблем для нормальної життєдіяльності суспільства.

Список використаних джерел:

1. Боротьба з відмиванням грошей: що таке БВГ і чому це важливо. URL: https://www.sas.com/ru_ua/insights/fraud/anti-money-laundering.html.

Устименко В. А.,
здобувач вищої освіти
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Рижкова С. А.,
старший викладач кафедри
адміністративного права, процесу
та адміністративної діяльності
Дніпропетровського державного
університету внутрішніх справ,
майор поліції

ОСНОВНІ АСПЕКТИ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Вивчаючи питання кібербезпеки, слід враховувати, що кібербезпека є невід'ємною частиною інформаційних технологій. Завдання дослідження кібербезпеки України полягає у визначенні адміністративної складової забезпечення кібербезпеки в державі, принципу системності в електронній сфері, структурування рівнів впливу інформаційного середовища на адміністративне регулювання України й вироблення універсального алгоритму захисту суспільства, особи та держави від інформаційних небезпек в адміністративному середовищі. В Україні політика щодо кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Службу безпеки України, Національну поліцію України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України [1, с. 71].

Зауважимо, кібертероризм як головна складова кіберзлочинності посідає не останнє місце й серед низки загроз національній безпеці та інтересам України. За даними соціологічних опитувань на його поширення нині активно впливають: високий потенціал і професійний рівень українських програмістів, здатність молоді швидко опановувати технічні новинки, про які ще вчора вони не мали жодного уявлення, а також темпи комп'ютеризації.

На сьогодні усі громадяни, юридичні особи та державні установи України мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів [2, с. 17].

Одним з найважливіших питань в умовах воєнного стану це протидія у інформаційній війні, яка виявляється у пропаганді – наприклад, розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору, збір інформації – злом приватних сторінок, втручання в роботу обладнання – атаки на комп'ютери або сервери. З початку війни по всій Україні працюють розрізнені групи, люди можуть підключатися до слабо захищених або публічних мереж і таким чином передавати дані зловмисникам. Хакери-злочинці можуть отримати інформацію з пристрою за лічені секунди. Найкраще використовувати мобільний інтернет, який за необхідності можна роздавати на підключений ноутбук. Не рекомендується надсилати або зберігати особливо конфіденційну інформацію в загальній папці на комп'ютері [3, с. 60].

Виходячи з вищевикладеного, найбільш ефективним засобом зниження ймовірності успішності кібератак, це переглянути ключові набори контролів кібербезпеки зокрема тих, які допомагають захиститися від загроз від держави-агресора або організованих угруповань, які активізували свою діяльність під час війни. Основи законодавчих механізмів для ефективного кіберзахисту в умовах воєнного стану закладені. Завдання кожного – при виявленні кібератаки якнайшвидше запустити цей механізм, щоб у майбутньому подібних атак та збитків від них ставало дедалі менше.

Список використаних джерел:

1. Кібергігієна. Кібербезпека. *Безпека держави:* матер. наук. семінарів (м. Київ, 27 листопада 2020 р.). Київ: КНТЕУ, 2020. 101 с.
2. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. Київ: Видавничий дім «Кондор», 2019. 272 с.
3. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ: ДУТ, 2015. 288 с.

Чукалов К. Е.,
курсант
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Калякін С. В.,
викладач кафедри
протидії кіберзлочинності
Дніпропетровського державного
університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ЗАХИСТУ WEB-ДОДАТКІВ ВІД АТАК ТИПУ XSS

SQL ін'єкція — один з поширених способів злому сайтів та програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду. Впровадження SQL, залежно від типу СКБД та умов впровадження, може дати можливість атакуючому виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та/або запису локальних файлів та виконання довільних команд на сервері. Атака типу впровадження SQL може бути можлива за некоректної обробки вхідних даних, що використовуються в SQL-запитах. Розробник застосунків, що працюють з базами даних, повинен знати про таку уразливість і вживати заходів протидії впровадженню SQL [1].

На даний момент однією з найуразливіших систем є web-додатки. Наявність величезного масиву робочих і часом конфіденційних даних створює необхідність захисту від атак ззовні. Розглянемо таку атаку web-сервер як SQL injection, (XSS англ. Cross Site Scripting — «міжсайтовий скріптинг» [1]) – тип вразливості інтерактивних інформаційних систем у вебі. XSS виникає, коли на сторінки, які були згенеровані сервером, з якоїсь причини потрапляють користувацькі скріпти. Специфіка подібних атак полягає в тому, що замість безпосередньої атаки сервера зловмисники використовують вразливий сервер для атаки на користувача. Довгий час програмісти не приділяли їм належної уваги, вважаючи їх безпечними. Однак ця думка помилкова: на сторінці або в HTTP-Cookie можуть бути досить вразливі дані (наприклад, ідентифікатор сесії адміністратора). На популярному сайті скрипт може влаштувати DoS-атаку. На початковому етапі розвитку web-додатків, кожна з них містила величезну кількість уразливостей. З розвитком технологій більшість із них були усунені, через що зломщики розробляли нові види атак. Одним з таких видів атаки був виділений у окремий клас атак під назвою CSRF.

CSRF (англ. Cross Site Request Forgery – «Підробка міжсайтових запитів) – вид атак на відвідувачів веб-сайтів, що використовує недоліки протоколу HTTP. Суть цієї атаки в тому, що заходячи на сайт зловмисника,

від імені «жертви» надсилається запит на інший сервер, з метою здійснення іншої операції (наприклад, переказ грошей). Складність реалізації атаки полягала у необхідності мети злому бути авторизованою на сервер, на якому проводиться атака, і запит не повинен вимагати будь-яких підтвердження з боку користувача.

Небезпека CSRF в тому, що ця поведінка браузерів і всього протоколу HTTP є нормальним. Наприклад, адже нормально те, що сайт може на своїх сторінках утримувати зображення з іншого сайту. А браузеру невідомо заздалегідь, що саме намагаються змусити його завантажити, дійсно картинку, або під виглядом даного завантаження буде виконано якась дія на цільовому сайті. Ця атака стала прабатьком XSS, бо і там, і там потрібно змусити

Для захисту від XSS-атаки необхідно виконати певні правила під час написання веб-додатків. Не можна довіряти даним вступникам від користувача або від будь-якого стороннього джерела. Дані повинні проходити перевірку до біта [2]. По-перше, необхідно перевірити достовірність даних, що означає, якщо очікується на вхід число, то скрипт повинен відсіювати будь-яку іншу інформацію. По-друге, має проводитися санітарна обробка даних, суть якої в тому, щоб переконається у відсутності небажаних бітів [2]. Наприклад, видалення будь-якої HTML-розмітки з рядка, в якому її не повинно бути. Третє, має використовуватися стандартна функція secureInnerData, яка дозволяє захистити від атак типу SQL injection та XSS. Алгоритм роботи цієї функції простий [3]:

1. видаляються прогалини на початку рядка;
2. перетворюються спеціальні символи в HTML аналоги;
3. очищені дані повертаються.

Підсумком роботи можна зробити висновок, що була проведена класифікація web-уразливостей і докладно розглянута вразливість типу XSS, а також попередня вразливість CSRF.Також були сформульовані основні принципи захисту власного ресурсу від злому і на підставі цих принципів необхідно намагатися будувати захист. Для того, щоб убезпечити свій ресурс необхідно подивитися на слабкі місця web-додатка та оцінити, з точки зору зловмисника, які є недоліки в системі:

1. Чи є можливість перейти на іншу сторінку зі шкідливим кодом.
2. Відсутність будь-якого захисту.
3. Користувач не повинен мати можливості підтвердити дію, які б міг хотіти зробити зловмисник.
4. Під час проведення атаки користувач має бути авторизовано у систему.

Список використаних джерел:

1. Аналіз і методи захисту web-додатків від атак типу XSS. URL: https://cyberleninka.ru/article/n/analiz-i-metody-zaschity-web-prilozheniya-ot-atak-tipa-xss.
2. Positive Research 2022. Positive Technologies – vulnerability assessment, compliance management and threat analysis solutions. URL: https://www.ptsecurity.com/ru-ru/research/analytics/positive-research-2022/
3. Welcome to Eprints Repo – Eprints Repo. URL: http://eprints.library.odeku.edu.ua/id/eprint/7040/1/Grosu_doslidzhennya_metodiv_zabezpechennya.pdf.

Шаблиста О. О.,
ад'юнкт
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Гребенюк А. М.,
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

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. Основним регулюючими правовими актами у галузі інформаційних ресурсів є Закони України «Про інформацію» та «Про державну таємницю». Разом із тим існують більше 150 нормативних правових актів різного рівня, що регламентують питання забезпечення збереження державної і службової таємниці. Враховуючи, що кримінально-правові норми, що діють у цій сфері, є бланкетними, то на практиці виникають певні труднощі щодо їх правильного розуміння та застосування.

Сама система 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 володіння відповідними знаннями та навичками у галузі провідних інформаційних технологій [3].

Таким чином, потрібне подальше вдосконалення інформаційних технологій для захисту інформації у роботі співробітників Національної поліції України.

Список використаних джерел:

1. Вишня В. Б. Інформаційне забезпечення юридичної діяльності: підручник. Дніпро: ДДУВС, 2019. 228 с.
2. Державна інформаційна політика. URL: http://merega.org.ua/law/projects/derzhpolityka.
3. Краснобрижий І. В., Прокопов С. О., Рижков Е. В. Інформаційне забезпечення професійної діяльності: навч. посібник. Дніпро: ДДУВС, 2018. 220 с.

Навчальне видання

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Матеріали Всеукраїнського науково-практичного семінару

10 листопада 2022 року

Редактори, оригінал-макет – *Є. В. Коваленко-Марченкова, А. В. Самотуга*

Підп. до друку 08.02.2023. Формат 60х84/16. Друк – трафаретний, цифровий.
Гарнітура – Times. Ум.-друк. арк. 11,9. Обл.-вид. арк. 12,75.

Надруковано у Дніпропетровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Гагаріна, 26, rvv_vonr@dduvs.in.ua