Міністерство внутрішніх справ України
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
НАВЧАЛЬНО-НАУКОВОГО ІНСТИТУТУ ПРАВА ТА ПІДГОТОВКИ
ФАХІВЦІВ ДЛЯ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

СУЧАСНІ ПРІОРИТЕТИ РОЗВИТКУ УКРАЇНИ: ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Матеріали
Всеукраїнської науково-практичної конференції
(м. Дніпро, 10 жовтня 2023 р.)

Дніпро
2024

УДК 33+004
С 89

Рекомендовано до друку науково-методичною радою Дніпропетровського державного університету внутрішніх справ (протокол № 7 від 21.02.2024 р.)

С 89 Сучасні пріоритети розвитку України:економічна та інформаційна безпека : матеріали Всеукр. науково-практ. конф. (м. Дніпро, 10 жовтня 2023 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2024. 132 с.

ISBN 978-617-8035-92-1

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

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

Матеріали подано в редакції авторів тез.
Оргкомітет не несе відповідальності
за їхній зміст та автентичність

ISBN 978-617-8035-92-1

ЗМІСТ

Баранник Лілія Борисівна
професор кафедри
соціального забезпечення та
податкової політики
Університету митної справи та фінансів,
доктор економічних наук, професор

ПИТАННЯ ПРОТИДІЇ КОРУПЦІЇ В УКРАЇНІ В КОНТЕКСТІ ПОСИЛЕННЯ СОЦІАЛЬНОЇ БЕЗПЕКИ

В умовах післявоєнного відродження країни, її економіки, першочергове значення набуває питання протидії корупції. Це має декілька значень. І одне з них – це посилення соціальної безпеки, встановлення в українському суспільстві соціальної злагоди як підґрунтя його подальшого розвитку.

Треба визнати, що наразі корупція стала не просто тією подією, яка «бруднить» мундир того чи іншого чиновника, вона перетворилася на політичну систему, яка пронизує вже всі сфери суспільства й, на жаль, освітню також. Сумно і злочинно те, що під час війни корупція не щезла, а навіть посилилася. Нещодавно опублікований Transparency International індекс сприйняття корупції (ІСК) за 2022 р. показує, що Україна сприймається як найкорумпованіша країна Європи і посідає 33-ю позицію у світі [1]. І справа навіть не в геополітичній «позиції», хоча за державу прикро та соромно. Корупція залишається основною причиною глибокого соціального конфлікту, який роз'їдає суспільство й веде до фінансової бідності та духовного зубожіння. Корупція знижує громадську довіру до держави, провокуючи дедалі більш важкий контроль загроз соціальній безпеці. Потурання й бездіяльність держави створюють можливості для корупції та підриває зусилля правоохоронних органів щодо її припинення. Країни з високими показниками ІСК є загрозою для глобальної безпеки, бо впродовж десятиліть вітали брудні гроші з-за кордону, дозволяючи клептократам збільшувати своє багатство, владу та руйнівні геополітичні амбіції. Треба визнати, що «довоєнний» від'їзд робочої сили, у тому числі висококваліфікованої, з України до інших країн у пошуку заробітку, є певною відповіддю на ситуацію, яка склалася в нашій країні. Молодь міркує так: «В Україні забезпечено живе лише та частина суспільства, яка бере хабарі, не сплачує податки, займається сумнівними махінаціями з публічними фінансами, тому треба від'їжджати…». І якщо нам здається, що ця частина молоді не знайде за кордоном собі певне заняття, то ми дуже помиляємося. «За даними державних реєстрів, за десять місяців 2021 р. із України виїхала рекордна кількість громадян – понад 660 тис., які не повернулися додому – це найбільший показник, починаючи з 2014 р. (560 тис.). До 2014 року із України щороку виїжджало 400–500 тисяч громадян. Винятком був 2020 рік, коли через пандемію в Україну більше повернулося громадян, аніж виїхало» [2]. Не треба нехтувати і тим, що сьогодні за межами України перебуває понад сім

мільйонів біженців, які в більшості своїй є працездатними людьми й в них зацікавлені європейські країни, в яких відбувається старіння населення.

Корупція є також аномальною морально-етичною проблемою, що нівелює патріотичні та громадські інтереси. «Декілька українських президентів, колишніх урядовців, політиків, олігархів та кілька маловідомих в Україні осіб, з'явилися на сайті Архіву клептократії – безкоштовної онлайнової бази даних інституту імені Гадсона (США). Мета сайту – продемонструвати, наскільки руйнівною може бути клептократія для держав, які не приділяють достатньо уваги для боротьби з нею» [3].

Велика проблема, яка створюється через корупцію – це та, що кошти не потрапляють до бюджету, осідаючи у нечисленних кишенях, або вивозяться в офшорні зони, і отже, не дозволять вирішувати нагальні проблеми. За даними «Комерсант-Україна» із посиланням на неурядову організацію Tax Justice Network, за роки незалежності з України в офшори вивели $167 млрд. Заявлена сума виведених з України коштів перевищує обсяг ВВП 2011 р. ($165,2 млрд), крім того, вона більше ніж удвічі більша за обсяг державного боргу на кінець червня – $60 млрд [4]. «Це цілком правдоподібні розрахунки», – визнає директор Інституту економіки та прогнозування НАНУ Валерій Геєць. За його словами, частина цих коштів повернулася у вигляді іноземних інвестицій та кредитів, а також фінансування виборчих проєктів [5]. Домогтися повернення капіталу практично неможливо. Отже, населення стає позбавленим певної частки ресурсів. Згадаємо, наскільки неспроможною виявилася система охорони здоров'я України у протидії пандемії COVID-19, що обернулося численними жертвами серед населення та втратами для економіки.

Корупція – це проблема колективних дій, її викорінення в інтересах всього суспільства. Методи боротьби з корупцією можна поділити на превентивні (що застосовуються для запобігання її) та каральні (застосовувані вже після скоєння корупційного правопорушення з метою попередження наступних). Кожна з країн світу вибирає свої методи, які будуть ефективними саме тут. «Наприклад, у Нідерландах роблять такі кроки для боротьби з корупцією: 1) звітність міністра внутрішніх справ щодо питань виявлення корупції; 2) система моніторингу джерел виникнення корупції; 3) основна форма покарання – заборона працювати в органах державної влади та втрата соціальних гарантій; 4) реєстрація випадків корупції, вчинених чиновниками; 5) проведення розслідувань ЗМІ. У Німеччині створено реєстр корумпованих фірм, яким не надаються державні замовлення. У Сінгапурі створено бюро розслідування випадків корупції, тут використовуються: 1) щорічна звітність урядовців; 2) жорсткі покарання (мали місце розслідування, ініційовані навіть щодо близьких родичів прем'єр-міністра Сінгапуру); 3) міністрам і суддям встановлено плату у 100 тис. дол. США на місяць» [6].

---

1. Індекс сприйняття корупції. URL: https://www.transparency.org/en/ /2022
2. Виїхало понад 600 тисяч громадян. URL: https://m.day.kyiv.ua/article/den-ukrayiny/vyyikhalo-ponad-600-tysyach-hromadyan
3. Яневський О. Експерти: США повинні триматися осторонь брудних грошей з України та Росії. URL: https://voa.pangea-cms.com/preview/uk-UA/a/ kleptocracy-archive

4. Україну назвали одним із лідерів із виведення грошей в офшори. URL: https://www.rbc.ua/rus/news/za-gody-nezavisimosti-iz-ukrainy-bylo-vyvedeno-v-offshory-24072012113800

5. За роки незалежності з України було виведено в офшори 167 млрд дол. URL: https://www.rbc.ua/rus/news/za-gody-nezavisimosti-iz-ukrainy-bylo-vyvedeno-v-offshory-24072012113800

6. Як виховується чесність чиновників, як працюють механізми контролю та чому транспарантність зведена в абсолют? URL: https://ru.sweden.se/lyudi-i-obschestvo/demokratiya/kak-v-shvetsii-boryutsya-s-korruptsiej-10-principov

Воліков Тарас Анатолійович
кандидат юридичних наук
докторант кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університету внутрішніх справ

ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ПРОТИ ВЛАСНОСТІ

В умовах становлення незалежної держави, реформування її соціально-економічної та політичної сфер, євроінтеграції України до країн Європейського співтовариства спостерігається зростання злочинності. Кількісні й якісні зміни у структурі злочинності характеризуються удосконаленням існуючих, застосуванням новітніх способів учинення кримінальних правопорушень, форм та способів протидії досудовому розслідуванню. Дедалі спостерігається входження до злочинних угруповань як колишніх, так і діючих працівників правоохоронних органів, представників органів влади й управління. На сьогодні технологія злочинної діяльності значно ускладнилася, що зумовлено використанням новітніх технічних засобів, складними й витонченими способами підготовки й приховування кримінальних правопорушень, які традиційними методами виявляти досить складно. Низька якість розкриття й розслідування, недостатність кваліфікованих кадрів у правоохоронних органах, відсутність системи попередження і профілактики кримінальних правопорушень, створили підґрунтя до збільшення їх кількості, які дедалі набувають усе більш загрозливих форм.

Під час збройної агресії з боку росії, здійснення так званої «спеціальної операції», проведення активних бойових дій у багатьох регіонах України спостерігається масова міграція населення країни в центральні та західні її регіони. Громадяни України вимушені покидати власні домівки та переміщуватися зі значними матеріальними коштами. Разом із населенням у

ці регіони прибуває і кримінальний контингент, який намагається швидко відновити злочинні схеми. Внаслідок цього спостерігається значне зростання кількості учинення кримінальних правопорушень, особливо проти власності. Зважаючи на це, вагомого значення набуває швидке розкриття та розслідування кримінальних правопорушень зазначеної категорії та профілактична діяльність з метою запобігання кримінальним проявам. Важливою складовою розслідування кримінальних правопорушень проти власності є застосування спеціальних знань. Завдяки цьому можливе ефективне забезпечення використання тактичних прийомів (комбінацій) під час проведення окремих слідчих (розшукових) дій.

У кримінальних провадженнях вказаної категорії важливе значення має залучення до проведення окремих слідчих (розшукових) дій спеціаліста. Спеціаліст здебільшого залучається до проведення огляду (100 %), призначення експертизи (100 %), тимчасового доступу до речей й документів (34 %), обшуку (45 %), допиту (17 %) та одночасного допиту двох раніше допитаних осіб (8 %).

Відповідно до ч. 7 ст. 237 КПК України, «при огляді слідчий, прокурор або за їх дорученням залучений спеціаліст має право проводити вимірювання, фотографування, звуко- чи відеозапис, складати плани і схеми, виготовляти графічні зображення оглянутого місця чи окремих речей, виготовляти відбитки та зліпки, оглядати і вилучати речі і документи, які мають значення для кримінального провадження.

Згідно з п. 2.2 Інструкції про участь працівників Експертної служби МВС України у кримінальному провадженні як спеціалістів, прибувши для участі в огляді, спеціаліст отримує від слідчого, прокурора необхідну інформацію про обставини справи, дії учасників огляду, здійснені до його прибуття, завдання, які необхідно вирішити, та надалі виконує доручення слідчого, прокурора, які стосуються використання його спеціальних знань.

При розслідуванні кримінальних правопорушень проти власності спеціалісти до проведення окремих слідчих (розшукових) дій залучаються у випадках: необхідності виявлення, фіксації та вилучення слідів злочинної діяльності; відсутності спеціальних знань та практичних навичок у слідчого; необхідності з етичних або тактичних точок зору доручити здійснення визначених дій саме спеціалістові; одночасного застосування низки науково-технічних заходів; необхідності виконати значний обсяг роботи, що вимагає спеціальних знань та навичок [1, с. 126–127]. Реалізація техніко-криміналістичного забезпечення стосується різних питань, пов’язаних із залученням спеціальних знань, участю спеціалістів (зокрема, інспекторів-криміналістів, судових експертів) при проведенні окремих слідчих (розшукових) дій, вилученням речових доказів, наступним проведенням судових експертиз. Судово-експертна діяльність є предметом дослідження за змістом багатьох наукових робіт, заслуговує особливої уваги у структурі техніко-криміналістичного забезпечення, а згідно з іншого погляду – як

самостійна складова криміналістичного забезпечення. Зважаючи на це, основний зміст техніко-криміналістичного забезпечення розслідування кримінальних правопорушень становлять відповідні спеціальні знання і технічні засоби, а також суспільні відносини, що виникають у процесі їх застосування. Розвиток суспільних відносин, вплив науково-технічного прогресу, удосконалення засобів та методів злочинної діяльності вимагають постійної уваги до вказаних питань [2, с. 221].

При розслідуванні кримінальних правопорушень проти власності спеціальні знання використовують переважно у таких формах: безпосереднє використання спеціальних знань слідчим, прокурором (у тому числі криміналістом) при виконанні своїх процесуальних функцій щодо збирання, дослідження та оцінки доказів; участь спеціалістів при провадженні окремих слідчих (розшукових) та процесуальних дій; призначення і провадження судових експертиз.

Проведення слідчих (розшукових) дій без залучення відповідних спеціалістів або поверхневе використання спеціальних знань переважно призводить до того, що переважна кількість кримінальних правопорушень проти влас**н**ос**т**і залишаютьс**я** не розкритими, а злочинці продовжують (відновлюють) свою протиправну діяльність.

1. Костиря О. М. Криміналістична характеристика та особливості розслідування грабежів і розбоїв, учинених раніше засудженими особами : дис. … канд. юрид. наук : 12.00.09 / Дніпропетровський державний університет внутрішніх справ. Дніпро, 2019. 212 с.

2. Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів: наукові засади та напрями реалізації. *Сучасні тенденції розвитку криміналістики та кримінального процесу* : тези доп. Міжнар. науково-практ. конф. до 100-річчя від дня народження проф. М. В. Салтевського (м. Харків, 8 листоп. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2017. С. 220–222.

Єфімов Микола Миколайович
професор кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університету внутрішніх справ,
доктор юридичних наук, професор

ДО ПИТАННЯ РЕАЛІЗАЦІЇ ПРОФІЛАКТИЧНИХ ЗАХОДІВ ПРИ РОЗСЛІДУВАННІ ШАХРАЙСТВ У МЕРЕЖІ «ІНТЕРНЕТ» ПІД ЧАС ВІЙСЬКОВОГО СТАНУ В УКРАЇНІ

Кіберзлочинність під час дії військового стану в Україні наразі продовжує розвиватися. Це зумовлено різними факторами. По-перше, це й військова агресія нашого східного «сусіда», по-друге, безперервний розвиток

комп'ютерної техніки, по-третє, постійне удосконалення хакерами своїх професійних навичок. Серед найбільш поширених протиправних діянь, які вчиняються кіберзлочинцями різного рівня, безумовно треба виокремити шахрайство у мережі «Інтернет». Вказане кримінальне правопорушення може вчинюватися багатоманітними способами та за допомогою різноманітних засобів. Треба наголосити на тому, що одним із важливих напрямів діяльності правоохоронних органів є профілактика кримінальних правопорушень. Реалізація профілактичних заходів при розслідуванні шахрайств у мережі «Інтернет» також наявна з-поміж інших.

Щодо загальних засад та характеристик профілактики правопорушень ми підтримуємо судження О. М. Макаренка, який визначив її як «… методологічно складне суспільне явище, що пояснюється таким. По-перше, профілактика правопорушень – багаторівнева система заходів, що проводяться державними, недержавними органами та установами, громадськими формуваннями та окремими громадянами для мінімізації дії або нейтралізації причин, що породжують правопорушення або сприяють їх вчиненню. По-друге, профілактика правопорушень – це особливий вид соціального управління, що має за мету зниження інтенсивності процесів детермінації правопорушень, нейтралізацію дії її причин та умов для обмеження правопорушень до соціально прийнятного рівня. По-третє, профілактика правопорушень – це різноманітна за формами діяльність, яка спрямована на пошук шляхів, засобів та інших можливостей ефективного впливу на правопорушення» [1, с. 119].

У розрізі досліджуваного питання необхідно згадати й про Департамент кіберполіції Національної поліції України, на який покладено обов'язки як з розслідування кіберзлочинів, так і з їх попередження. Наприклад, серед обов'язків працівників вказаного підрозділу визначено розслідування правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, а також правопорушень, які вчиняються за допомогою комп'ютерних технологій [2]. Інакше кажучи, до цієї категорії протиправних діянь можна віднести і шахрайство, передбачене ч. 3 ст. 190 КК України, та заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку [3, с. 134].

С. В. Самойлов обґрунтовує думку про те, що ефективність профілактики шахрайств, учинених із використанням мережі «Інтернет», можна значно підвищити лише за комплексного підходу до означеної проблеми із залученням не лише можливостей правоохоронних органів, а й інших суб'єктів впливу. Дослідник впорядкував профілактичні заходи в такій структурі: «…заходи, що використовуються державою на законодавчому рівні (розробка, апробація та прийняття законів та підзаконних актів, які врегульовують відносини в мережі «Інтернет» та сприяють створенню таких умов, за яких вчинення аналізованих шахрайств буде унеможливлено або дуже ускладнено); заходи, що застосовуються постачальниками послуг (у межах їх

власної ініціативи); заходи, що використовуються правоохоронними органами (заходи роз'яснювального та запобіжного характеру); заходи, що застосовуються користувачами мережі (активна позиція пересічного користувача мережі «Інтернет», що полягає у: правомірній поведінці безпосередньо в мережі; відстоюванні своїх прав та законних інтересів через установлені законодавством механізми); заходи, що використовуються спільними зусиллями різних суб'єктів» [4, с. 11–12].

Також ми підтримуємо позицію А. Е. Жиліна, який серед профілактичних заходів, які необхідно здійснювати уповноваженим особам правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів, виділив такі: «… повідомлення громадянам через засоби масової інформації про юридичну відповідальність за шахрайську діяльність в сфері використання банківських електронних платежів; виявлення осіб, схильних до антисуспільної поведінки в сфері комп'ютерної діяльності (хакери, фішери) та подальша їх постановка на облік у підрозділах Кіберполіції; інформування населення через засоби масової інформації, месенджери та соціальні мережі про випадки вчинення шахрайських дій у сфері використання банківських електронних платежів (фішинг, кардинг, сніфферінг)» [5, с. 214].

Підсумовуючи, зазначимо, що реалізація профілактичних заходів при розслідуванні шахрайств у мережі «Інтернет» під час військового стану в Україні є досить важливим аспектом в діяльності правоохоронних органів. Адже без ефективної профілактики протиправних діянь кількість випадків їх вчинення лише буде збільшуватись.

1. Макаренко О. М. Щодо з'ясування терміну «профілактика правопорушень» та суміжних з ним понять. *Право і безпека*. 2004. № 3. Ч. 1. С. 118–120.

2. Кіберполіція. Кібербезпека України. URL: https:// wiki.legalaid.gov.ua/index.php/Кіберполіція._Кібербезпека_України (дата звернення: 12.09.2023).

3. Єфімов М. М., Павлова Н. В., Чучко С. В. Методика розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу Інтернет: теоретичні та праксеологічні засади : монографія. Одеса : Видавничий дім «Гельветика», 2022. 200 с.

4. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : автореф. дис. … канд. юрид. наук : 12.00.09. Донецький юридичний інститут. Донецьк, 2014. 18 с.

5. Жилін А. Е. Актуальні питання реалізації профілактичних заходів працівниками правоохоронних органів при розслідуванні шахрайства у сфері використання банківських електронних платежів. *Юридична наука*. 2020. № 2. Т. 2. С. 209–215.

Кривопуск Олександр Григорович
викладач кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університету внутрішніх справ

ЩОДО ЗНАЧЕННЯ ВІРТУАЛЬНИХ (ІНФОРМАЦІЙНИХ) СЛІДІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ ЗЛІСНОГО НЕВИКОНАННЯ ОБОВ'ЯЗКІВ ПО ДОГЛЯДУ ЗА ДИТИНОЮ АБО ОСОБОЮ, ЩОДО ЯКОЇ ВСТАНОВЛЕНА ОПІКА ЧИ ПІКЛУВАННЯ

Слідова картина будь-якого злочину є одним з ключових елементів криміналістичної характеристики. Кожне злочинне діяння характеризується змінами навколишнього середовища, що є результатом вчинення дій з підготовки, вчинення та приховування слідів злочинної діяльності.

У криміналістиці класично прийнятою вважається двокомпонентна структура слідової картини, яка охоплює матеріальні та ідеальні сліди. Проте останнім часом все частіше, крім ідеальних та матеріальних слідів, вчені криміналісти виділяють окрему групу слідів, під назвою віртуальні, або інформаційні, які залишаються внаслідок використання комп'ютерного обладнання або телекомунікаційних систем.

Переходячи до розгляду віртуальних слідів, які зберігають інформацію про вчинення злочину, передбаченого ст. 166 КК України, необхідно зауважити, що на сьогодні відсутній єдиний підхід щодо визначення поняття віртуальних (комп'ютерних) слідів. На думку Я. Найдьон, віртуальні сліди – це цифровий образ, електронні сигнали, що залишаються в пам'яті електронних і подібних до них пристроїв, що передаються за допомогою заданого алгоритму і мають кримінально-релевантне значення [1, с. 306].

В умовах стрімкого технологічного розвитку, який відбувається в нашій державі, відмічається тенденція зміни суспільних відносин, через що змінюється і злочинність, а це призводить до зростання кількості віртуальних (комп'ютерних) слідів, які залишають по собі злочинні діяння. Відносно нещодавно категорія віртуальних слідів розглядалась науковцями здебільшого в контексті вчинення окремих видів злочинів у сфері використання комп'ютерів та комп'ютерних мереж, виготовлення та розповсюдження порнографічної продукції, вчинення шахрайств за допомогою мережі «Інтернет» тощо. Проте на сьогодні практично кожне злочинне діяння може залишати інформаційні сліди, не є винятком вчинення злісного невиконання обов'язків по догляду за дитиною або особою, щодо якої встановлена опіка чи піклування.

З огляду на аналіз матеріалів кримінальних проваджень за ст. 166 КК

України, згідно з яким до основних джерел віртуальних (комп'ютерних) слідів можна віднести інформацію (фотознімки, відеозаписи із зображеннями потерпілого), що міститься на мобільних телефонах або смартфонах злочинця, потерпілого або свідків. Це твердження знаходить своє відображення у судових рішеннях, наприклад фрагмент Вироку Орджонікідзевського районного суду м. Запоріжжя від 10.06.2022: «… Коли приходив дільничний педіатр, їх не було вдома, і тому очно лікар дитину не оглядав. Вона (обвинувачена) спілкувалась телефоном із медичною сестрою, відправляла їй фотографії дитини…» [2].

Крім того, до типових віртуальних слідів, характерних також злісному невиконанню обов'язків по догляду за дитиною або особою, щодо якої встановлена опіка чи піклування, доречно віднести: сліди листування за допомогою електронної пошти в мережі «Інтернет» з лікарями або іншими третіми особами, які містяться в комп'ютерах, ноутбуках чи смартфонах злочинця, потерпілого або свідка; сліди листування за допомогою різних месенджерів, використовуючи при цьому комп'ютерну техніку та/або смартфони; сліди, які зберігаються на цифрових записах камер відеоспостереження громадських місць, місць масового відпочинку, де може міститись інформація про подію кримінального правопорушення, або дії потерпілого, підозрюваного чи інших учасників ні місці події. Істотного значення набуває інформація, яка міститься в розпорядженні операторів мобільного зв'язку, а саме інформація про розміщення пристроїв мобільного зв'язку на певних ділянках місцевості, що дозволяє висунути версії вчиненого кримінального правопорушення, встановити можливих свідків та осіб, які можуть бути причетними до вчинення злочину.

До окремої групи віртуальних слідів, характерних здебільшого злісному невиконанню обов'язків по догляду за дитиною або особою, щодо якої встановлена опіка чи піклування, пропонуємо відносити інформацію стосовно: подання заяв до органів влади або місцевого самоврядування, за допомогою електронних сервісів про реєстрацію новонародженої дитини (видачу свідоцтва про народження тощо), надання допомоги про народження дитини; електронних звернень до закладів МОЗ та отримання рецептів.

Підсумовуючи викладене, можна сказати, що з розвитком технологій все більшого значення для досудового розслідування набувають сліди відображені та які зберігаються на цифрових носіях інформації. Слідова інформація, що зберігається на комп'ютерних носіях, дозволяє більш глибоко зрозуміти механізм вчинення злочину цієї категорії, висунути версії щодо способу, обстановки та умов вчиненого злочину, особи злочинця, що допоможе ухвалити необхідні процесуальні рішення, ініціювати проведення слідчих (розшукових) дій, призначити необхідні судові експертизи та вибрати оптимальні шляхи досудового розслідування.

1. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право.* 2019. № 5. С. 304–307.

2. Вирок Орджонікідзевського районного суду м. Запоріжжя від 10 червня 2022 року URL: https://reyestr.court.gov.ua/Review/86407270 (дата звернення: 19.12.2022).

Лазарєв Владислав Олександрович
директор Навчально-наукового інституту
права та підготовки фахівців для
підрозділів Національної поліції,
кандидат юридичних наук,
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

КІБЕРЗЛОЧИННІСТЬ ТА ЕКОНОМІЧНІ ЗЛОЧИНИ В МЕРЕЖІ DARK WEB В УМОВАХ ВОЄННОГО СТАНУ

Стрімкий розвиток інформаційних технологій в Україні та світі, який ми спостерігаємо останнє десятиріччя, невблаганно супроводжується динамічним розвитком злочинів у цій сфері. Масова комп'ютеризація та стрімкий розвиток цифрових технологій, які значно спростили життя людині, не стали винятком. Кіберзлочини є найдинамічнішою групою суспільно небезпечних діянь, адже з кожним роком кіберзлочини стають дедалі масовими й небезпечними.

Кіберзлочинність та економічні злочини в мережі Dark Web є серйозною загрозою для безпеки та фінансової стабільності.

Dark Web – це частина Інтернету, яка є прихованою та недоступною для пошуку за допомогою звичайних пошукових систем. Вона працює на основі технології невидимих мереж (наприклад, Tor), що приховують інформацію про сервери та користувачів. Це робить Dark Web ідеальним простором для злочинних дій.

Умовно Інтернет можна поділити на три прошарки. На поверхні – всім відомий Surface Web, або ж «поверхневий веб», який індексується стандартними пошуковими системами, такими як Google тощо [1].

«Глибинний інтернет» Deep Web, який містить у собі контент внутрішніх мереж корпорацій та університетів, або ж комерційні бази даних, до яких не може отримати доступ будь-хто та може бути у 400–500 разів більшим, ніж відомий нам Surface Web.

«Темний інтернет» Dark Web, контент якого прихований навмисно.

Потрапити туди можна за допомогою спеціальних програм, таких як Tor, Tails, Maltego, OnionScan чи I2P тощо. Tor, наприклад, дозволяє користувачам дістатися вебсайтів через серію віртуальних каналів замість прямого зв'язку, таким чином дозволяючи як організаціям, так і людям ділитися інформацією через публічні мережі без загрози їхній приватності [2, 5].

Більшість сайтів, які знаходяться в «темній мережі», використовують інструмент шифрування Tor. Власне Tor став відомим як технологія, яка дозволяє користувачам зберігати свою анонімність в Інтернеті.

Кіберзлочинність в мережі Dark Web містить такі види злочинів, як крадіжка особистих даних (зокрема, логінів, паролів та фінансової інформації), розповсюдження шкідливих програм, крадіжка ідентифікаторів, злам рахунків та мережевих систем, шахрайство в Інтернеті, атаки на компанії та державні установи, кібершантаж тощо.

Економічні злочини в мережі Dark Web містять торгівлю наркотиками, зброєю, контрабандою товарів та послуг, відмивання грошей, фальшивомонетництво, крадіжку ідентифікаторів, кредитних карток та фінансових даних, організацію фінансових пірамід тощо. Торгівля зброєю та наркотиками активізувалася внаслідок збройної агресії нашого сусіда.

Dark Web дозволяє злочинцям залишатися анонімними, що робить викриття та притягнення їх до відповідальності складними завданнями для правоохоронних органів.

Для розрахунку на чорних маркетплейсах використовуються віртуальні валюти, більшість злочинців у даркнеті торгують біткойнами. Більшість цін на ринках вказані в біткойнах, і без них було б важко торгувати кримінальними матеріалами. Оскільки біткойн децентралізований, немає обмежень щодо того, де можна налаштувати обліковий запис біткойна. Дедалі складніша інфраструктура обмінників, міксерів і альтернативних віртуальних валют (наприклад, Monero, Ethereum).

Основні поради для захисту від кіберзлочинності – використання стійких паролів, оновлення програмного забезпечення, обережність при натисканні на посилання та завантаження файлів, використання антивірусного програмного забезпечення та технологій шифрування, а також вміння розпізнавати шахраїв та шахраїв.

Кіберзлочинність та економічні злочини в мережі Dark Web є серйозною проблемою, яка потребує спільних зусиль правоохоронних органів, урядів, технологічних компаній та користувачів Інтернету для боротьби з цією загрозою і забезпечення безпеки в онлайн-середовищі.

При розслідуванні злочинів там, де ринок даркнету підтримує тисячі користувачів, може бути неможливо ідентифікувати діяльність правоохоронних органів з інших країн. Та може вплинути на численні розслідування проти окремих постачальників або порушити онлайн-розслідування.

Нобхідно обов'язково співпрацювати з організаціями, які створені для

кординації та більш єфективної боротьби з кіберзлочинами і єкономічними злочинами.

У Європі можна здійснювати через Європол. ЄС3 (Європейський центр боротьби з кіберзлочинністю) і робота під керівництвом координаційного центру (FP) CYBORG може підтримувати конкретні запити, щоб допомогти обмежити дублювання, забезпечує основу для взаємної співпраці між державами-членами ЄС, а також підтримує оперативні угоди з деякими країнами, що не входять до ЄС (наприклад, Канада, Швейцарія та Сполучені Штати) [3, 4].

У США працює IOC2 (Міжнародний центр розвідки та операцій із боротьби з організованою злочинністю), щоб допомогти впоратися з можливими проблемами. IOC2 є частиною відділу комп'ютерних злочинів та інтелектуальної власності (CCIPS) Міністерства юстиції. IOC2 — це багатовідомча структура, яка підтримує різноманітні міжнародні ініціативи, якщо це стосується США.

Мета полягає в тому, щоб надати всім країнам спосіб співпраці щодо міжнародних розслідувань правоохоронних органів і обміну розвідувальною інформацією в Європі.

Важливо зазначити, що боротьба з економічною злочинністю в темній мережі є складним і тривалим процесом, який вимагає сукупності заходів, спрямованих на виявлення, перекриття та запобігання таким діям. Необхідно співпрацювати з міжнародними організаціями, розвивати нові технології для виявлення та запобігання кіберзлочинності, а також змінювати законодавство для належного реагування на такі злочини. Тому бажано поєднувати спільні зусилля з міжнародними партнерами виробити стратегію для досягнення максимального ефекту забезпечення безпеки та стабільність у цифровому просторі, навіть під час найскладніших воєнних конфліктів.

1. Васильєв А. А. Особливості кваліфікації кіберзлочинів проти власності. *Проблеми правознавства та правоохоронної діяльності*. 2016. № 4 (58). С. 136–143.

2. Драгоненко А. О., Ніколенко М. І. Проблеми кваліфікації шахрайства з використанням електронно-обчислюваних машин. *Порівняльно-аналітичне право*. Ужгородський національний університет. 2018. № 1. С. 256–259.

3. Карчевський М. В. Особливості кваліфікації шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки. *Науковий вісник Львівського державного університету внутрішніх справ*. Серія : Юридична. 2014. Вип. 1. С. 272–281.

4. Карчевський М. В. Перспективи правового регулювання в контексті гіпотези розвитку технологій трансгуманізму. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2019. С. 115–127.

5. What Are The Trending Cryptocurrencies On CoinMarketCap? URL: https://coinmarketcap.com/trending-cryptocurrencies/

Неклеса Олександр Вікторович
викладач кафедри кримінального
процесу та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ

ЕФЕКТИВНІСТЬ ТА ВИКЛИКИ ОПЕРАТИВНОЇ РОБОТИ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ В СУЧАСНИХ УМОВАХ

У сучасних умовах оперативна робота підрозділів Національної поліції стикається з низкою викликів, зокрема з швидкозмінною кримінальною обстановкою, розвитком технологій та кіберзлочинністю, необхідністю забезпечення громадської довіри та збалансованого впливу на правопорушників, що вимагає постійного вдосконалення стратегій, технічних засобів та співпраці з іншими правоохоронними органами та громадськістю. Оперативна робота підрозділів Національної поліції в сучасних умовах має на меті ефективне запобігання злочинності, затримання злочинців та забезпечення безпеки громадян [1]. Однак є низка викликів, з якими стикаються поліцейські у своїй роботі. По-перше, швидкозмінна кримінальна обстановка вимагає оперативного реагування на нові види злочинності та змінювані моделі поведінки злочинців. Підрозділи національної поліції повинні постійно оновлювати свої методи, засоби та аналітичні підходи для виявлення та припинення нових форм злочинності. По-друге, розвиток технологій спричиняє появу кіберзлочинності, яка стала серйозною загрозою для суспільства. Поліцейські повинні мати не лише підготовку щодо традиційних видів злочинів, але й компетенції в галузі кібербезпеки та цифрового слідства, щоб ефективно реагувати на цю загрозу. По-третє, забезпечення громадської довіри є важливою складовою операційної діяльності поліції. Підрозділи Національної поліції повинні прагнути до прозорості, відкритості та взаємодії з громадою, а також здійснювати свою роботу з повагою до прав та гідності кожного громадянина [2].

Для подолання цих викликів підрозділи Національної поліції повинні постійно підвищувати професійну підготовку своїх працівників, використовувати сучасні технонології та інструменти для збору, аналізу та обробки інформації, сприяти співпраці з іншими правоохоронними органами та міжнародними партнерами. Поліцейські повинні бути готовими до швидкого реагування, але водночас діяти в межах закону та з дотриманням прав людини. Забезпечення ефективної співпраці між підрозділами та взаємодія з іншими суб’єктами правоохоронної діяльності є ключовими факторами для досягнення успіху в оперативній роботі. Крім того, оперативна робота підрозділів Національної поліції в сучасних умовах також стикається з

інформаційною перенасиченістю та потоком даних. Ефективна аналітика та використання розвинених технологій обробки даних стають необхідними для виявлення злочинців та вирішення кримінальних справ. Зокрема, глобалізація та зростання транскордонного злочинницького активізму створюють потребу в зміцненні міжнародного співробітництва. Загалом успішна оперативна робота підрозділів Національної поліції в сучасних умовах залежить від постійного професійного розвитку, використання передових технологій, ефективного обміну інформацією та співпраці з іншими правоохоронними органами та громадськістю. Поліцейські повинні мати не тільки високий рівень фахової підготовки, але й розвинуті навички комунікації, переговорів та вирішення конфліктів. Додатковим викликом для оперативної роботи є необхідність забезпечення особистої безпеки поліцейських у небезпечних ситуаціях. Вони повинні бути готовими до протидії злочинності, а іноді (у разі потреби) до використання фізичної сили або спеціальних засобів, щоб захистити себе та інших громадян. У підсумку, ефективна оперативна робота підрозділів Національної поліції в сучасних умовах вимагає комплексного підходу, що містить професійну підготовку, використання сучасних технологій, співпрацю з іншими органами правоохоронної системи та громадськістю, забезпечення безпеки поліцейських та дотримання принципів правової держави. Тільки шляхом постійного вдосконалення, адаптації до певних викликів в роботі і використання передових методів та інструментів підрозділи Національної поліції можуть досягти ефективної оперативної роботи, забезпечити безпеку громадян і зберегти довіру громадськості [3].

1. Користін О. Є., Пефтієв Д. О., Пеньков С. В., Некрасов В. А. Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою: ILP : навч. посіб. за заг. ред. М. Г. Вербенського. Київ : «Видавництво Людмила», 2019.

2. Кримінальний процесуальний кодекс України. Науково-практичний коментар / за заг. ред. проф. В. Г. Гончаренка, В. Т. Нора, М. С. Шумила. Київ : Юстініан, 2012.

3. Керевич О. В. Організація взаємодії слідчого з оперативними підрозділами в діяльності щодо розкриття та розслідування кримінальних правопорушень. 2012.

Ohrimenco Serghei
DSC, Professor Laboratory of Information Security
Academy of Economic Studies of Moldova
Spinachi Vitalie
Magistrate, Laboratory of Information Security
Academy of Economic Studies of Moldova
Nikulin Egor
Student TI222, Laboratory of Information Security
Academy of Economic Studies of Moldova

CYBER POWER IN THE CYBER CONFLICTS

In the context of the digital transformation of society, cybersecurity problems are increasing manifold. And this is caused by objective factors, both the micro and macro levels. Cyber threats have become one of the most acute problems facing national security and critical infrastructure protection. Under these conditions, the system of risk assessment at the appropriate levels of critical infrastructure management requires additional interdisciplinary research.

The importance of this topic is confirmed by the desire of each state to ensure the protection of national interests in the field of cyber security, in the face of cyber conflicts and cyber sanctions [1, 2].

For these purposes, consider a set of cybersecurity indices developed for selected countries:

1. Cyber Maturity in Asia and the Pacific, developed by the Australian Strategic Policy Institute (https://www.aspi.org.au/report/cyber-maturity-asia-pacific-region-2017).
2. National Cybersecurity Index developed by the Estonian Academy of Electronic Governance (https://ega.ee/project/national-cyber-security-index/).
3. Global Cybersecurity Index developed by the International Telecommunication Union (ITU) (https://www.itu.int).
4. The Kaspersky Lab Cybersecurity Index (https://www.kaspersky.com/about/press-releases/2016_21-29-60-kaspersky-lab-presents-the-first-cybersecurity-index).
5. Asia-Pacific Cybersecurity Dashboard developed by the Business Software Alliance (BSA) (https://www.bsa.org/news-events/news/new-bsa-study-shows-how-apac-markets-can-bolster-national-cybersecurity-strategies).
6. Cyber Readiness Index developed by the Potomac Institute for Policy Studies (which includes existing capabilities) (https://www.potomacinstitute.org/academic-centers/cyber-readiness-index).
7. Cyber Green Index, which focuses on technical threats (https://cybergreen.net).

We should note the rationality of using a set of specific indicators in such

studies, including Cyber Power (National Cyber Power Index 2022) [3], Indexing Equation for Cyber Power [4], Future Conflict Assessment, Perceived Cyber Power [6], Composite Index of National Capabilities and others [7].

Of interest to us is the deterrence calculation formula index for estimating future conflict, in which the net benefit or cost is equal to the ratio of the sum of the benefits and harms to the victim to the sum of the costs and harms expected from the victim [5].

Where: AA - net benefit or cost;

Ba - the benefits the attacker receives;

Ca - the harm the attacker inflicts on the victim (i.e., the relative benefit to the attacker);

Hv - the harm the attacker expects the victim to suffer in retaliation.

In turn, the formula used to measure perceived cyberpower is as follows:

Perceived Cyberpower=(C+E+M+I) *(S+W) + Interrelations (C, E, M, I) (2)

Where: C is the critical mass, which includes the size and age of the population and the level of cyber awareness of the population;

E - economic component, which includes cyberinfrastructure, technology and the development of and access to critical information infrastructure;

M - military component, includes the use of cybernetics in the armed forces;

I - information component, includes communication and information flows between systems and technologies;

S - strategic component, includes implementation of national cyber strategy;

W - influence of people on responsible use of cyber security rules (awareness) and prevention of cybercrime.

---

1. Ohrimenco Serghei, Cernei Valeriu (2023). Organizing a Cyber Blockade. The 8th International Conference "Management Strategies and Policies in the Contemporary Economy. ASEM, Chisinau, 24-25 martie 2023. ISBN 978-9975-147-99-6 DOI: https://doi.org/10.53486/icspm2023.51

2. Ohrimenco Serghei., Borta Grigire., Cernei Valeriu. (2021). Estimation of the Key Segments of the Cyber Crime Economics. 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PICS&T). ISBN:978-1-6654-0682-6 DOI: 10.1109/PICST54195.2021.9772165

3. Julia Voo, Irfan Hemani, Daniel Cassidy (2022). National Cyber Power Index 2022. Report September 2022. (access date 07.09.23)

4. Aaron Franklin Brantly (2016). The Decision to Attack Military and Intelligence Cyber Decision- Making. University of Georgia Press. ISBN 9780820349190

5. Lucas Kello (2017). The Virtual Weapon and International Order. Yale University Press. ISBN 9780300220230

6. Jansen van Vuuren, J.C., Leenen, L. (2018). A Model For Measuring Perceived Cyberpower. Proceedings of the 13th International Conference on Cyber Warfare and Security, National Defence University, 8-9 March 2018, Washington D.C., pp. 320-327 ISBN 978-1-5108-5963-0 http://hdl.handle.net/10204/10361 (access date 07.09.23)

7. Composite Index of National Capability. https://www.wikiwand.com/en/ Composite_Index_of_National_Capability (access date 07.09.23)

Прокопович-Ткаченко Дмитро Ігорович
т.в.о. завідувача кафедри кібербезпеки
та інформаційних технологій
Університету митної справи
та фінансів,
кандидат технічних наук, доцент
Хрушков Борис Сергійович
здобувач вищої освіти Університету
митної справи та фінансів

ПРОГРАМНО-АПАРАТНЕ ТЕСТУВАННЯ, ЕЛЕМЕНТ IoT, АКТУАТОР, ДАВАЧ, НАДІЙНІСТЬ СИСТЕМИ, КРИТИЧНО ВАЖЛИВИЙ ЕЛЕМЕНТ IoT, ПРОМИСЛОВИЙ IoT

Основною характеристикою систем є неоднорідність їхніх компонентів і технологій. Величезна кількість різноманітних незалежних пристроїв, таких як вбудовані об'єкти, приводи та датчики, постійно підключені, що призводить до величезного масштабу компонентів [1]. Такі системи зазвичай містять рівень генератора даних, який агрегує дані з усіх підключених пристроїв. Потім через мережевий рівень різні протоколи та шлюзи використовуються для передачі даних для застосування аналітичних процесів, надаючи відповідні послуги додаткам цільового користувача [2]. Тестування потрібно на всіх етапах, коли все підключено, а дані передаються по мережах [3]. Проблеми та загрози виникають все частіше, особливо це пов'язано з найбільш небезпечними програмно апаратними елементами.

Тож різко зростає кількість досліджень щодо тестування систем на основі IoT, у яких зміни в таких великих системах нескінченні. Безперервна регресія під час виконання та інтеграційне тестування неодноразово потрібні для частої динамічної інтеграції компонентів IoT, а також запитів на зміну системи [5]. З часом зазвичай створюється величезна кількість тестів (TCs), які можуть бути релевантними чи нерелевантними для конкретної нової інтеграції чи запиту на зміну. Отже, потреба в мінімізації кількості виконаних ТС експоненціальне зростає, щоб зменшити витрати на тестування та максимізувати ефективність.

Системи промислового Інтернету речей швидко розвиваються на основі всіх апробованих елементів загального Інтернету речей (IoT) у різних сферах життя людини. Для реалізації телекомунікаційних можливостей для зв'язку між багаточисельними програмно апаратними пристроями через усі рівні системи IoT, що спричиняє багато проблем із безпекою та продуктивністю та напрацюванням на відмову.

Найбільш поширеними методиками тестування Інтернету речей є регресійне та інтеграційне тестування вони мають багаторазове використання але це призводить до величезних масивів тестів, які не мають єдиної номенклатури, що перешкоджає адекватному тестуванню таких систем. Ця

низка проблем вимагає зосередитися на вивченні інноваційних підходів до масштабованого тестування для великих наборів тестів у системах на основі Інтернету речей, особливо промисловому Інтернету речей.

Пропонується масштабована структура комплексного тестування для безперервної інтеграції та регресійного тестування в системах на основі промислового Інтернету речей, заснована на критеріях, пов'язаних з відокремленням найбільш техногенно небезпечних програмно апаратних елементів, для приотерізації, класифікації, фіксації-документування та вибору тестових випадків.

Комплексний підхід тестування багатоелементного масиву програмно апаратних засобів використовує методи, засновані на пошуку хибних елементів, щоб забезпечити оптимізований пріоритетний набір тестових випадків для індикації та штучного прийняття рішень, що в цілому підвищує інтегральну надійність всієї системи.

Вибір ґрунтується на децентралізованій моделі прогнозування для стандартних компонентів IoT з використанням керованих алгоритмів глибокого навчання за допомогою штучного інтелекту для постійного забезпечення загальної надійності систем промислового Інтернету речей. Експериментальні результати перевірки поліпшення вірогідносних показників надійності досягли точності визначення пріоритетів до 90 % і 92 % для регресійного тестування та інтеграційного тестування відповідно. Це забезпечує розширену та ефективну структуру для безперервного тестування систем на основі Інтернету речей відповідно до критеріїв, пов'язаних з Інтернетом речей, для встановлення пріоритетів і вибору.

Було досліджено багато обмежень для тестування систем IoT, таких як нездатність впоратися з динамічністю підключених компонентів, різноманітність мережевих протоколів і технологій, складність у реальному часі та масштабованість систем, які керують своїм підключенням [6; 7; 8]. Крім того, треба часто перевіряти сумісність систем. Розглянемо процеси тестування промислового інтернету речей як структуру яка складається з різноманітних алгоритмів тестування, що забезпечує функціонування системи IoT.

Рис. 1. Впорядкована структура процесів тестування промислового IoT

З огляду на зображену на рис. 1 структуру можно побачити, що всі недоліки тестування промислового Інтернету речей поширюється на кожний структурний елемент комплексного тестування.

1. Bart Preneel. Analysis and Design of Cryptographic Hash Functions. URL: Internet: homes.esat.kuleuven.be/~preneel/phd_preneel_feb1993.pdf

2. Carlet C. Vectorial Boolean functions for Cryptography. Cambridge Univ. Press, Cambridge. 2010. 95 s.

3. Carlet C. Boolean functions for cryptography and error correcting codes. Cambridge Univ. Press, Cambridge. 2007. 148 s.

4. Zhuo Zepeng, Zhang Weiguo. On correlation properties of Boolean functions" Chinese Journal of Electronics. 2011. Vol. 20. № 1. S. 143–146.

5. L. O'Connor. An analysis of a class of algorithms for S-box construction. J. Cryptology, 1994. S. 133–151.

6. Clark J. A., Jacob J. L., Stepney S. The Design of S-Boxes by Simulated Annealing. New Generation Computing, 2005. 23(3). S. 219–231.

7. Courtois N., Meier W. Algebraic Attacks on Stream Ciphers with Linear Feedback. Eurocrypt 2003. LNCS 2656. S. 345–359.

8. Meier W., Pasalic E., Carlet C. Algebraic Attacks and Decomposition of Boolean Functions. Eurocrypt 2004. LNCS 3027. S. 474–491.

Плетенець Віктор Миколайович
професор кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університету внутрішніх справ
доктор юридичних наук, професор

ОСОБЛИВОСТІ УБЕЗПЕЧЕННЯ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО НЕЇ В УМОВАХ ВОЄННОГО СТАНУ

Інформаційні технології знаходять все більшого відображення у всіх сферах нашого життя, в тому числі і в діяльності правоохоронних органів. Боротьба зі злочинністю, з одного боку, зумовлена необхідністю збору та систематизації даних, які в подальшому можуть стати доказовою базою в кримінальному провадженні, з іншого – убезпеченням наявної доказової інформації від стороннього доступу.

Треба наголосити, що Закон України «Про інформацію» містить визначення інформації, згідно з яким інформацією є будь-які відомості та / або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. У цьому ж Законі визначені основні види інформації: 1) інформація про фізичну особу; 2) інформація довідково-енциклопедичного характеру; 3) інформація про стан довкілля (екологічна інформація);

4) інформація про товар (роботу, послугу); 5) науково-технічна інформація; 6) податкова інформація; 7) правова інформація; 8) статистична інформація; 9) соціологічна інформація; 10) інші види інформації [1].

Потребують уваги й думки науковців, які надають своє бачення терміна інформація. Зокрема, під інформацією розуміють повідомлення відомостей, даних тощо [2, с. 19–22]. Аналіз наведених джерел демонструє розуміння інформації з позиції даних, отриманих із зовнішнього світу.

Також наявні різні погляди на визначення поняття інформація в різних науках, зокрема: соціології, математиці, біології, економіці тощо. Це зумовлено різними науковими поглядами на цю категорію, що ускладнює надання єдиного визначення.

Проте в математиці та кібернетиці є окремий розділ «Теорія інформації», де досліджуються процеси зберігання, перетворення і передачі інформації. Теорія інформації ґрунтується на теорії ймовірностей і математичній статистиці [3, с. 8]. Треба наголосити, що основи теорії інформації закладено американським вченим Клодом Шенноном [4]. І на цей час вона є основою отримання, передачі, обробки даних з використанням комп'ютерної техніки.

Без неї немає оформлення більшості постанов, запитів, протоколів слідчих (розшукових) дій та їх збереження в електронному вигляді на відповідних носіях. Проте варто враховувати й наміри незацікавлених в розслідуванні осіб в здійсненні доступу до даних, що зберігаються в електронному вигляді для їх коригування чи знищення.

Особливої актуальності це набуло в умовах збройної агресії рф проти України, коли країною агресором вживаються заходи доступу до зібраних за цими фактами відомостей. Тож за її інформацією, кіберзлочинці намагалися викрасти матеріали слідства у справі про катастрофу пасажирського лайнера Malaysia Airlines на сході України [5]. Подібні до наведеного прикладу випадки є непоодинокими. Це зумовлює потребу вжиття заходів, спрямованих на убезпечення зібраної за відповідними фактами інформації від стороннього доступу.

Отже, можемо наголосити, що одержання, застосування, збереження, поширення інформації є невід'ємними складовими діяльності уповноважених осіб. Відповідно й вжиттю заходів щодо убезпечення від стороннього доступу до інформації, що міститься на електронних носіях, з боку уповноважених осіб повинно бути належне ставлення. Це зменшить можливість впливу на зібрану інформацію за кримінальними провадженнями, зокрема й за фактами збройної агресії рф проти України для подальшої правової оцінки в судових інституціях.

---

1. Про інформацію : Закон України від 02.10.1992 р. URL: http://zakon4.rada.gov.ua/laws/show/1906-15

2. Калюжний Р. А., Швець М. Я., Цимбалюк В. С., Гавловський В. Д. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики / за ред. Р. А. Калюжного, В. О. Шамрая; Академія державної

податкової служби України. Київ : Видавництво «КВІЦ», 2002. 296 с.

3. Коваленко А. Є. Теорія інформації і кодування: курс лекцій : навч. посіб. для здобувачів ступеня бакалавра за спеціальністю 124 «Системний аналіз» / КПІ ім. Ігоря Сікорського; уклад.: А. Є.Коваленко. Електронні текстові дані (1файл: 5,758 Мбайт). Київ : КПІ ім. Ігоря Сікорського, 2020. 248 с.

4. Хто такий Клод Шеннон і чим йому завдячує програмування? URL: https://robotdreams.cc/uk/blog/239-kto-takoy-klod-shennon-i-chem-emu-obyazano-programmirovanie

5. Російські хакери намагалися викрасти матеріали розслідування у справі MH17. URL: https://wz.lviv.ua/news/145932-rosiiski-khakery-namahalysia-vykrasty-materialy-rozsliduvannia-u-spravi-mh17

Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ЗАПОБІГАННЯ ЕКОНОМІЧНІЙ ЗЛОЧИННОСТІ В УКРАЇНІ

Загрози економічній безпеці держави та будь-які порушення щодо безпеки діяльності в економіці призводять до зниження рівня ефективності країни за багатьма складовими економічної та національної безпеки держави.

Економічна злочинність має значний негативний вплив на усі сфери життєдіяльності країни, особливо на рівень національної безпеки. Не залишаються при цьому осторонь правоохоронна та соціальна сфери, інформаційна та міжнародна сфери, соціальна та політична сфери. Значний вплив на забезпечення економічної безпеки держави має створення усіх необхідних умов щодо запобігання та подолання економічної злочинності. Для цього необхідно сформувати відповідні заходи усунення тих причин, через які створюються економічні злочини та на законодавчому рівні створити ефективну базу протидії злочинності та гарантування економічної безпеки держави. Економічна злочинність являє собою загрозу національній безпеці країни.

Саме розробка комплексної державної політики щодо протидії різним проявам економічної злочинності в країні сприятиме гарантованій безпеці в багатьох сферах безпекової ситуації в державі.

Зростання рівня тіньової економіки знижує рівень національної безпеки.

Особливої уваги заслуговує це питання в умовах війни та виведення економіки України з тіні. Саме зростання рівня тінізації економіки відбувається у періоди кризи, а війна є одним з таких періодів процвітання тіні. Тіньова економіка в Україні становить близько третини валового

внутрішнього продукту. Тіньова економіка є прихованою від оподаткування та будь-якого контролю із боку держави, вона має широкий спектр діяльності.

У багатьох країнах світу є тіньова економіка, але її наслідки різні. Фахівці визнають, що безпечним вважається рівень менше 15 %. За дослідженнями Кельнського інституту економіки, в 2021 році рівень тіньової економіки у США був на рівні 7,4 %, у Швейцарії – 8,2 %, Канаді – 12,8 %, Франції – 12,9 %, Німеччині – 14,3 %, Італії – 23,4 %, Польщі – 26,6 %, Туреччині – 30,4 %, Болгарії – 34,2 %. За розрахунками Мінекономіки, рівень тіньової економіки в Україні становить 30 % від офіційного ВВП.

Під час зростання рівня тінізації економіки відбувається нестабільність у соціальній складовій національної безпеки.

Найбільшими видами економічних злочинів в Україні є шахрайство, кіберзлочини, незаконне привласнення майна, хабарництво, корупція, шахрайство у сфері закупівель, фінансові збитки підприємств від злочинної діяльності, професійне шахрайство тощо.

Важливе місце в процесі забезпечення безпеки підприємства посідає формування концепції забезпечення економічної безпеки підприємства, яка містить засоби та принципи забезпечення економічної безпеки підприємств, інструменти та чинники впливу на економічну безпеку підприємств, основні елементи економічної безпеки підприємств та завдання економічної безпеки підприємств [1].

Суттєвими питаннями, які саме і мають негативний вплив на економічну безпеку держави, є загрози від тероризму, відсутність сталого розвитку економіки у довготривалому періоді, фінансова криза, військовий стан в країні, зниження рівня надходжень до державного бюджета, високий рівень недовіри до державних інституцій, низький рівень правової відповідальності за злочинну діяльність та інше.

Тому питання державної політики щодо створення відповідних управлінських рішень для виявлення, подолання та протидії можливим проявам в сфері економічних злочинів із застосуванням комплексних методів, підходів, впровадження моніторингу дослідження самих причин та їх наслідків, які мають бути вирішені для гарантування економічної безпеки держави.

Застосування системного підходу запобігання економічної злочинності може бути вирішено лише у комплексі із такими сферами суспільного життя, як соціальна, політична, економічна, інформаційна, правоохоронна, судова, міжнародна та інші. Важливим є створення реформ у правоохоронній системі для підвищення заходів протидії економічним злочинам та удосконалення законодавства з питань протидії злочинності у сфері економіки.

Щорічний розвиток цифрових технологій стає привабливим для економічної злочинності, постають найважливішими питання надійності та забезпечення безпеки у глобальному кіберпросторі.

Вирішення організаційних, технічних та юридичних питань стає дедалі

найважливішим та актуальнішим. Ці питання є стратегічними не лише для країн, в яких рівень кібербезпеки є найбільшим чи високим, а й країн, що розвиваються, та найбільше стосується країн, які відчувають саме зараз найбільші кібератаки на просторі свої країни, до яких саме належить Україна [2].

Тож державна політика щодо запобігання економічній злочинності має забезпечити високий рівень її ефективності, приносити економічну, соціальну та безпекову користь для суспільства та забезпечити гарантування економічної безпеки держави.

Для боротьби із економічними злочинами необхідно брати до уваги міжнародний досвід країн із низьким рівнем економічної злочинності, враховувати рівень якості життя населення, який формує рівень розвитку країни і є основою для економічної та національної безпеки.

_____--

1. Rybalchenko L., Kosychenko A. Ensuring economic security of enterprises taking into account the peculiarities of information security. Scientific journal «Philosophy, Economics and Law Review». 2022. 2 (1). S. 96–107.

2. Rybalchenko L. Cybercrime in the global space. *Науковий вісник ДДУВС*. 2022. Спец. вип. № 2. С. 524–530.

Рижков Едуард Володимирович
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ФОРМУВАННЯ СТРАТЕГІЇ КІБЕРЗАХИСТУ В УМОВАХ ВОЄННОГО СТАНУ

Державницькі зусилля щодо формування стратегії кіберзахисту в Україні мають свою історію й етапи. Але критерієм їх ефективності має бути не історичний опис, а конкретний результат здатності уповноважених суб'єктів протистояти посяганням на кіберпростір держави, а також їх відповідність ступеню та характеру небезпеки з урахуванням динаміки та складності існуючих загроз.

Безумовно, система наявних кіберсуб'єктів за останні 20 років набула сталих ознак та розвитку. Проте вона не задовольняла потреби нашого суспільства з огляду на загрози, що їх принесла із собою російська воєнна агресія. Основною проблемою стала недосконала координація дій вже наявних суб'єктів протидії кіберінцидентам з огляду на необхідність оперативного супроводу основного суб'єкту захисту держави в умовах воєнного стану – Збройних Сил України. Ситуація унеможливлювала ефективну реалізацію з

боку Збройних Сил України операцій протидії ворогові із використанням кіберсередовища. Тому в умовах, коли об'єктивно всі ознаки вказують на реальну кібервійну за участі України, виникла потреба у створенні такого нового суб'єкта, як кібервійська в структурі Збройних Сил України з наступною потребою їх кадрового забезпечення.

З боку керівництва держави було вжито певних заходів. Протягом 2021 року видана низка нормативних актів. Серед них Указ Президента України 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, 2].

Зазначеними нормативними актами було продекларовано створення в Україні кібервійськ. Рекрутування фахівців у сфері ІТ було розпочато у різних формах: від ананімного через спеціалізовані чат-боти до централізованого анкетування з формуванням відповідної бази фахівців [3]. Хоча і передбачається, що після ухвалення відповідного закону кібервійська будуть частиною Міноборони, наразі майбутніх кібербійців планується розподілити між різними структурами, що вже відповідають за кібербезпеку: Службою безпеки України, Державним спеціальним зв'язком, кіберполіцією, Радою національної безпеки та оборони, Національним банком України, Міністерством цифрофої трансформації, Міністерством оборони, Збройними Силами України та розвідкою.

Треба наголосити, що серед основних причин, які зумовили реалізацію ініціативи фахівців у створенні в Україні кібервіськ, є безумовно агресія росіян у кіберпросторі по відношенню до нашої держави, а також поступова та неухильна інтеграція країни до альянсу з НАТО та Європейської спільноти. Проте, доцільно зазначити що створення кібервійськ в державі та забезпечення їх ефективного функціонування – то справа не на місяці, а на роки. Зокрема, 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 [4]. Тобто підготовчий період офіційної появи зайняв термін, який Україна, враховуючи реалії військової ситуації, не може собі дозволити. Наразі у США у кібервійську 9 тисяч військовослужбовців, у Великобританії приблизно дві тисячі, у росії також десь тисяча.

На старті 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 дуже актуальною.

До сьогодні немає закону про кібервійська. Є лише законопроєкт. Тому цифровізація ЗСУ відбувається за іншим сценарієм. Новітнє західне озброєння, волонтерська допомога, новаторські рішення на рівні програмного

забезпечення поступово призвели до розуміння необхідності та поступового втілення цифри у фронтові реалії. І на сьогодні «КРОПИВА», як приклад прикладного програмного забезпечення у військах, є звичною та незамінною.

Поступово в ЗСУ без спеціалізованого закону формується відповідна кіберінфраструктура та на теоретичному рівні вимальовується перспективна структура Кіберкомандування кіберсил ЗСУ [4].

В умовах військової мобілізації до лав Збройних Сил України потрапляє певна кількість фахівців у сфері інформаційних технологій, для яких з огляду на державницький інтерес комп'ютер більш раціональна зброя, ніж будь-яка інша. Механізм виявлення та залучення таких фахівців до кібервійськ чи його резерву повинен працювати на випередження їх можливої втрати на полі бою.

Треба зазначити, що положення офіційної Стратегії кіберзахисту доповнюються законодавчими ініціативами, що здатні суттєво змінити баланс пріоритетів створення та функціонування уповноважених суб'єктів кіберзахисту та послабити роль кіберпідрозділів ЗСУ.

У 2023 р. Верховна Рада України ухвалила у першому читанні за основу проєкт Закону про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури (реєстр. № 8087).

У проєкті пропонується внести зміни до низки законів України,

спрямовані на нормативне забезпечення захищеності від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, на створення належної правової основи для здійснення заходів з попередження, виявлення і припинення актів агресії у кіберпросторі в умовах війни російської федерації проти України, а також на загальне удосконалення нормативно-правової бази у сфері кібербезпеки та захисту інформації задля посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам.

Зокрема, запропоновані зміни до законів України «Про Державну службу спеціального зв'язку та захисту інформації України» та «Про основні засади забезпечення кібербезпеки України» передбачають створення та забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози та визначення Державної служби спеціального зв'язку та захисту інформації України уповноваженим органом, що здійснює забезпечення функціонування цієї системи.

Серед іншого пропонується: створити в органах державної влади, що є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, підрозділи із кіберзахисту; призначати у вищевказаних органах офіцерів із кіберзахисту, яким безпосередньо підпорядковуються підрозділи із кіберзахисту; надати право Держспецзв'язку визначати функції, повноваження, загальні вимоги до підрозділів із кіберзахисту та їх співробітників, а також особливості правового статусу та загальні вимоги до офіцерів із кіберзахисту [5].

У березні 2023 р. Держспецзв'язку заявило, що в кіберармії України перебувають 400 тисяч людей, які самі організувалися для боротьби з росією. Нехай повноцінні війська зібрати так і не встигли, але оборонний потенціал у кіберпросторі українці мають [6].

Проте по факту маємо ситуацію, в якій залучено до співпраці лише десятки фахівців з тисяч. Виникає питання, чому склалася така ситуація? Чому у глухому «резерві» вже протягом року перебувають дуже 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, або мета анкетування була зовсім не та, що продекларована? Картинка налагодження співпраці з представниками населення є, але результат зовсім не той, що очікували [7, с. 58].

Така протилежність оцінок ситуації та різна спрямованість державницьких зусиль зумовлена зволіканням законотворців та інших суб'єктів, які так і не реалізували до цього часу положення офіційної Стратегії кіберзахисту України в частині ухвалення Закону «Про кібервійська України», що є неприпустимим з огляду на сучасні загрози нашій державності. Збройні

Сили України, їх кіберпідрозділи, а у найближчий час і кібервійська повинні бути основним пріоритетом державницької політики щодо розвитку суб'єктів кіберзахисту в період воєнного протистояння з російським ворогом.

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про невідкладні заходи з кібероборони держави» : Указ Президента України від 26 серпня 2021 року № 446/2021. URL: https://www.president.gov.ua/documents/4462021-40009

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://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. Леднєй Вадим: «Метою діяльності кіберсил ЗСУ є захист суверенітету держави та відсіч збройної агресії в кіберпросторі». URL: https://lb.ua/news/2023/01/31/544318_vadim_liedniey_metoyu_diyalnosti.html

5. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури : проєкт закону. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40553

6. В Україні досі немає кібервійськ: експерт розповів, коли вони з'являться і навіщо потрібні. URL: https://focus.ua/uk/digital/518279-v-ukraine-do-sih-por-net-kibervoysk-ekspert-rasskazal-kogda-oni-poyavyatsya-i-zachem-nuzhny

7. Ryzhkov E. Problematic issues of staffing cyber troops of Ukraine under martial law. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2022. Special Issue. № 1 (120). S. 55–60. URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/04/S1/NV_DDUVS_spec_1_2022-55-60.pdf

Сеник Володимир Васильович
доцент кафедри обчислювальної математики та програмування, доцент кафедри міжнародної інформації Національного університету «Львівська політехніка», кандидат технічних наук, доцент

Магеровська Тетяна Валеріївна
доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат фізико-математичних наук, доцент

ЦИФРОВІЗАЦІЯ ОСВІТИ: ВИКЛИКИ ПРОЦЕСАМ ЗАПРОВАДЖЕНННЯ ЕЛЕМЕНТІВ ДИСТАНЦІЙНОГО НАВЧАННЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Дистанційна форма навчання з використанням цифрових технологій у цей час є одним із елементів досягнення програмних результатів навчання під час підготовки фахівців різних галузей знань. Дослідженню ефективності використання такої форми навчання присвячено багато наукових праць. Уже повною мірою визначено: основні переваги та недоліки дистанційної форми навчання; психологічні аспекти, які виникають внаслідок її застосування; проаналізовані платформи для проведення занять у формі онлайн; досліджено особливості організації освітнього процесу під час підготовки фахівців за окремими галузями знань; особливості проведення занять за окремими компонентами (дисциплінами) тощо. Водночас набутий досвід організації навчального процесу в онлайн-форматі, який отримали науково-педагогічні працівники внаслідок вимушеного переходу на дистанційну форму навчання під час пандемії Covid-19 та внаслідок широкомасштабного вторгнення російських військ на територію суверенної України, у низцувипадків показав доцільність використання елементів цієї форми навчання у подальшому, навіть під час організації освітнього процесу в очному форматі. У будь-якому разі розвиток цифровізації різних галузей як в Україні, так і у світі скоріше чи пізніше призвів би до запровадження цифровізації освіти в Україні, яка обіцяє зробити навчання доступнішим, інноваційнішим та ефективнішим. Covid-19

та війна лише пришвидшили ці процеси. Головне, що базове розуміння цих процесів є в керівництва МОН України [1]. Тому набутий за останні чотири роки досвід проведення занять онлайн потребує досконалішого вивчення та використання.

З метою дослідження думок здобувачів вищої освіти щодо використання елементів дистанційного навчання з використанням інформаційних технологій у Львівському державному університеті внутрішніх справ проведено репрезентативне опитування студентів спеціальності 126 «Інформаційні системи та технології». Це опитування анонсувалось нами на одній з попередніх конференцій, а сьогодні ми наводимо його основні, найцікавіші результати [2]. В опитуванні взяло участь 92 % здобувачів вищої освіти, що навчаються за вказаною спеціальністю.

На запитання «Яка з форм проведення навчання, на вашу думку, не впливає або сприяє якості навчання (засвоєння знань, отримання необхідних компетентностей)?» 60,5 % респондентів відповіли – «змішана форма», очна – 21,1 %, дистанційна – 18,4 %.

Відповідаючи на запитання «Як впливає дистанційне навчання на засвоєння знань порівняноз очним навчанням?» 41,2 % зазнчили, що знання засвоюються аналогічно з очним навчанням, і лише 10,5 % вважають, що знання не засвоюються зовсім.

На запитання: «Як впливає дистанційне навчання на ваш розпорядок дня (пов’язаний з навчанням)?» основна частка (73,6 %) відповіла, що приділяє більше або ж стільки часу на вивчення навчальних дисциплін; 15,8 % відмітили, що додатково приділяють більше уваги вивченню навчальних дисциплін професійного напряму; менше часу вивченню дисциплін приділяє лише 7,9 % респондентів.

На запитання: «Чи доцільно поділити навчальні дисципліни на такі, які можна засвоювати використовуючи лише дистанційну форму навчання і на такі, які треба проводити лише в очному форматі?» лише 26,3 % відповіли «ні», що відповідає приблизно кількості респондентів, які вважають, що лише очна форма навчання здатна забезпечити засвоєння знань на необхідному рівні.

На наступні три запитання відповідали респонденти, які підтримували проведення навчання у дистанційній чи змішаній формі. Ім пропонувалося вибрати навчальні дисципліни, які треба викладати лише в очному, дистанційному чи змішаному форматі. Результати опитування подано на рис. 1–3 [3].

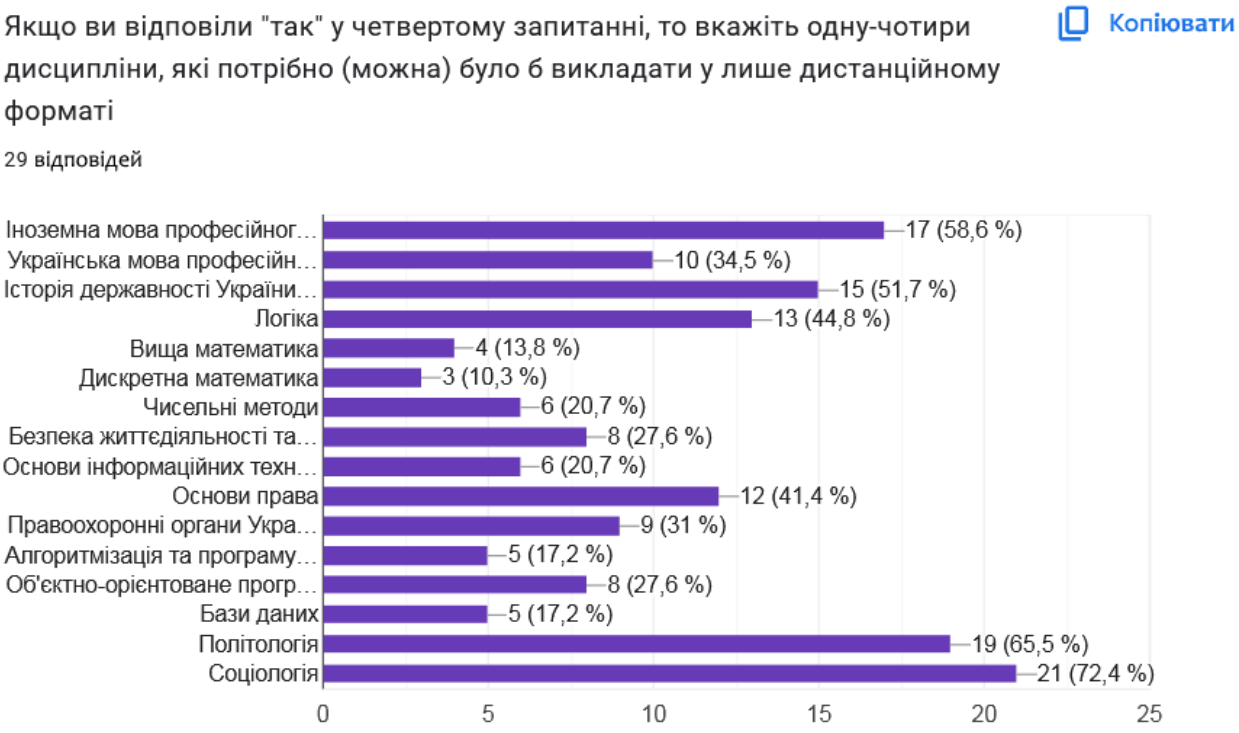

Рис. 1. Результати опитування щодо дисциплін, які треба викладати лише в дистанційній формі

Рис. 2. Результати опитування щодо дисциплін, які треба викладати лише у очній формі

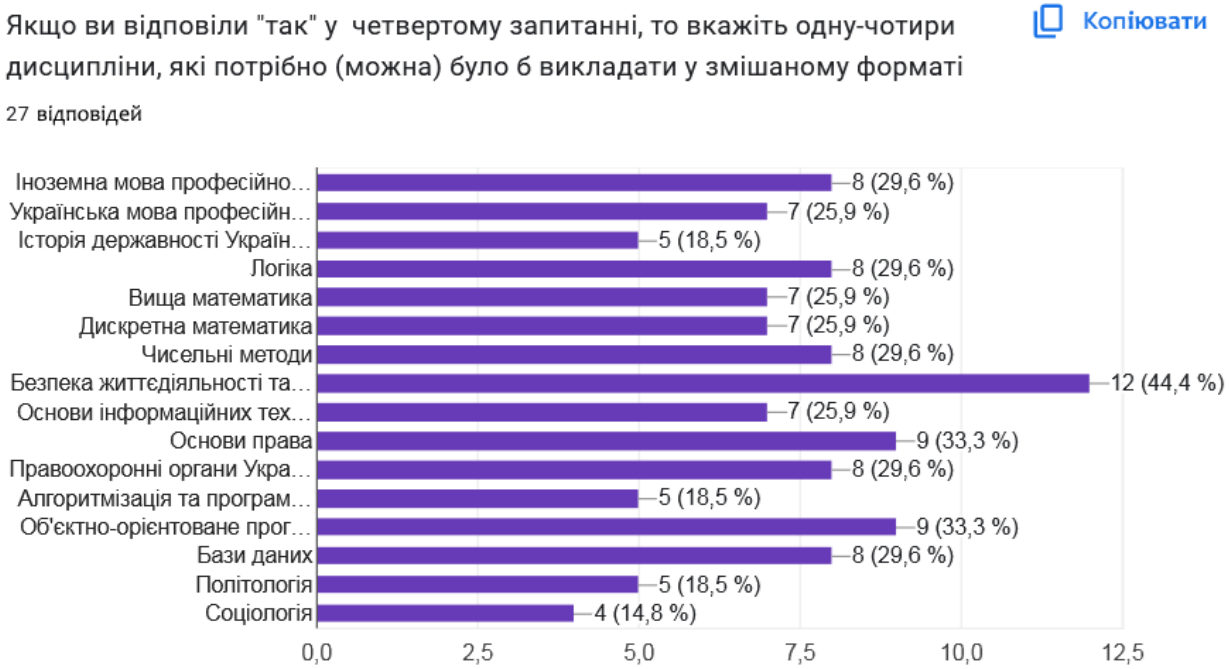

Рис. 3. Результати опитування щодо дисциплін, я
кі треба викладати у змішаному форматі

Стало несподіванкою те, що всі навчальні дисципліни згадані респондентами як такі, що можуть викладатися лише очно, або лише дистанційно. Однак гістограма (рис. 3) вказує на те, що всі навчальні компоненти можна викладати з використанням змішаної форми навчання. Водночас результати опитування (рис. 2, 3) констатують той факт, що дисциплінам фахового спрямування (вищій математиці, об'єктно-орієнтованому програмуванню, базам даних, алгоритмізації та програмуванню) більшу частку навчального часу необхідно відводити очному формату. Щодо гуманітарних дисциплін (соціологія, політологія, основи права), то більше часу треба виділити для дистанційної форми навчання.

На запитання «Чи задоволені ви платформами, за допомогою яких проводяться дистанційне навчання?» відповідь була очевидною внаслідок специфіки спеціальності, на основі якої проводилось опитування. Жоден з респондентів не відповів «Ні». Лише 10,5 % не змогли ствердно відповісти на поставлене запитання, вибравши відповідь «Не можу відповісти».

Наступні два запитання спрямовані на визначення переваг та недоліків застосування елементів дистанційної форми навчання саме під час підготовки фахівців з інформаційних технологій. Респондентами визначено, що основними перевагами дистанційного навчання є: можливість визначити для себе час та його тривалість на виконання практичних завдань; економія накладних витрат, пов'язаних із транспортом і проживанням; можливість створення власної, зручної, спокійної побутової обстановки для навчання. 57,9 % респондентів не вбачає особливих недоліків у дистанційній формі проведення занять. Найбільшим недоліком дистанційної форми навчання під

час підготовки фахівців у галузі інформаційних технологій є те, що така форма навчання позбавляє можливості навчатися командної роботи та комунікабельності.

Тому можемо констатувати: проведене анкетування показало, що дистанційне навчання, як один з елементів цифровізації освітньої діяльності та форми організації освітнього процесу, має низку позитивних елементів і може застосовуватися з метою підвищення ефективності формування компетентностей фахівців різних галузей знань.

Однак є потреба у проведенні подальших досліджень, які полягають у визначенні для кожної окремої освітньої компоненти часток часу, які виділятимуться для онлайн-освіти і очних занять. При цьому ці частки можуть (і мають) бути різними для кожної окремо визначеної галузі знань. Також однією із основних проблем, які треба вирішити, є внесення відповідних змін у нормативно-правове забезпечення освітнього процесу. А такі проблеми, як внесення змін до освітньо-професійних програм, до навчально-методичного забезпечення фахівці (гаранти, науково-педагогічні працівники), можуть вирішити у дуже короткий час.

1. Про деякі питання організації роботи закладів фахової передвищої, вищої освіти на час воєнного стану : наказ Міністерства освіти і науки України від 07.03.2022 № 235. URL: ttps://zakon.rada.gov.ua/rada/show/v0235729-22#Text

2. Сеник В. В. Аналіз застосування дистанційної форми навчання під час її застосування у 2021-2022, 2022-2023 навчальних роках у Львівському Державному університеті внутрішніх справ. *Інформаційні технології в освіті та практиці* : матеріали науково-практ. конф. (Львів, 16 грудня 2022) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2023. С. 63–64.

3. Сеник В. В., Магеровська Т. В., Магеровський Д. В. Особливості застосування систем дистанційного навчання у формуванні компетентностей під час підготовки фахівців з інформаційних технологій. *Науковий вісник НЛТУ України* : зб. науково-тех. пр. 2023. Т. 33. № 3. С. 77–82.

Синиціна Юлія Петрівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського
державного університету
внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ

Інформаційне суспільство є одним із типів суспільств, які розвиваються внаслідок соціального прогресу. Сьогодні ми можемо спостерігати активну фазу переходу суспільства від індустріального до інформаційного простору. Можливості глобальної мережі, що активно використовуються у всіх сферах суспільного життя, засновані на інформаційних ресурсах і являють собою сукупність даних, які організовані в інформаційних системах для отримання достовірних відомостей у різних сферах знань та практичної діяльності. Однак одночасно зі збільшенням ролі інформації підвищується і важливість її захисту за допомогою інструментів інформаційної безпеки. Актуальності це питання набуває в особливий правовий режим – воєнний стан, що діє на території нашої країни починаючи з 24 лютого 2022 року у зв'язку з активною фазою вторгнення російської федерації. У сучасних воєнних реаліях важко та навіть недоречно заперечувати роль інформації як інструменту протистояння, фактично – зброї. Інформація дозволяє вигравати у війні не зробивши жодного пострілу, шляхом формування і розпалювання внутрішніх суперечностей. Така тактика є характерною для війн нового формату – гібридних, де безпосередньо військовий фактор є лише однією зі складових цілого [1].

Відповідно до законодавства України, поняття «інформаційна безпека» має таке визначення: «Стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди державі через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [2].

Інформаційна безпека містить:

- стан захищеності інформаційного простору, завдяки якому забезпечується його формування та розвиток на користь держави, громадян та організацій;
- стан інформації, що унеможливлює або значно впливає на порушення таких її властивостей, як цілісність, конфіденційність та доступність;

- стан інфраструктури, що дозволяє використовувати інформацію суворо за призначенням та без негативного впливу на систему;
- економічну складову, що містить телекомунікаційні та інформаційні системи та структури управління, такі як системи збору, кумуляції та обробки даних, загальноекономічного аналізу та прогнозування господарського розвитку управління, координування та ухвалення рішень;
- фінансову складову, що охоплює інформаційні мережі та бази даних, системи фінансових розрахунків та обміну.

Варто зазначити, що інформаційна боротьба стає тим чинником, що вплине на саму війну, її початок, процес і результат. Це підтверджується агресією росії проти України. На початку 2021 року ухвалена нова Стратегія інформаційної безпеки, що передбачає комплексну взаємодію на основі Конституції України, законів України, Стратегії національної безпеки України, Стратегії кібербезпеки України, а також міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України [2]. У змісті Стратегії інформаційної безпеки конкретизуються потенційні інформаційні загрози: «інформаційна політика російської федерації – загроза не лише для України, але й для інших демократичних держав» [1].

Ключовою характеристикою сутності інформаційної безпеки під час військового стану є властивість захищеності, що містить два різновиди захисту: активний та пасивний.

Активний – захист спрямований на попередження несанкціонованого доступу до інформації. Пріоритетами цього захисту є: захист особистих даних, тобто соціальних цінностей та інших конфіденційних відомостей громадян та держави в цілому; експлуатація засобів інформаційної безпеки; експлуатація та захист об'єктів критичної інфраструктури; міжнародні інтереси.

Пасивний – захист поширюється на суспільство та економічний розвиток. Пріоритетними напрямами пасивного захисту можна визначити: розвиток культури; розвиток онлайн-демократії; розвиток економіки; розвиток ІТ-сектору; міжнародне співробітництво.

Якщо говорити про «забезпечення інформаційної безпеки», то потрібно розуміння основних принципів «забезпечення інформаційної безпеки»: [3]:

1. Принцип системності. Відповідно до нього, захисні заходи повинні бути спрямовані на запобігання інформаційним атакам з боку зовнішніх та внутрішніх джерел. Засоби захисту повинні використовуватись адекватно ймовірним видам загроз та функціонувати у вигляді комплексної системи захисту.
2. Принцип міцності. Встановлює, що правила забезпечення інформаційної безпеки повинні охоплювати всі зони безпеки, мати рівну надійність захисту та дозволяти визначати ймовірні загрози.
3. Принцип багаторівневого захисту. Орієнтований створенням кордонів захисту інформаційної системи, що складається з послідовно розташованих зон безпеки, ключова з яких розташовується всередині всієї

системи.

4. Принцип безперебійності. Відповідно до нього функціонування системи інформаційної безпеки має бути безперервним та безперебійним.

5. Принцип розсудливості. Виражається в розумності застосування захисних заходів із необхідним ступенем безпеки. В основі цього принципу лежить доцільність високих матеріальних витрат та раціональність, їх подальшого використання.

Сутність інформаційної безпеки під час військового стану час полягає у формуванні активного захисту щодо пріоритетних інтересів, пов'язаних з використанням інформаційних ресурсів, у спрямованості на створення умов нормального розвитку нашого суспільства та економіки. Забезпечення інформаційної безпеки є комплексним завдання, що обумовлено складністю та багатоплановістю інформаційного середовища. Вирішення проблеми із забезпечення інформаційної безпеки вимагає застосування організаційних, законодавчих та програмно-технічних заходів, які мають бути задіяні в сукупності, оскільки у разі нехтування хоча б одним з цих аспектів підвищується ймовірність втрати інформації, роль якої в сучасному житті суспільства набуває все більшого значення.

Отож в період особливого воєнного стану саме інформація є тією зброєю «масового ураження». Здійснення інформаційної безпеки в умовах воєнного стану є комплексною діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини. У сьогоднішніх реаліях інформаційна безпека відіграє важливу роль в житті суспільства і людини, тому захист інформаційної безпеки в нашій державі повинен мати та має пріоритетний напрям.

---

1. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. Вип. 1. С. 150–155.

2. Стратегія інформаційної безпеки : Указ Президента України від 28 грудня 2021 року № 685/202. URL: http://surl.li/lospu

3. Milov O., Hrebeniuk A., Nalyvaiko A., Pasko I., Rzayev Kh., Salii A., Soloviova O., Synytsina U. Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system Eastern-European Journal of Enterprise Technologies, № 6/2 (108), ISSN ISSN 1729-3774 Scopus, DOI: 10.15587/1729-4061.2020.218660, 2020. S. 30–52. URL: http://surl.li/lotwp

Синиціна Юлія Петрівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ
кандидат технічних наук, доцент

МОДЕЛЮВАННЯ ЕКОНОМІЧНОЇ ДИНАМІКИ НАЦІОНАЛЬНОЇ ПРОМИСЛОВОСТІ ТА БІЗНЕС-ПРОЦЕСІВ ПІДПРИЄМСТВА

Е сучасних умовах розвитку національної промисловості однією з основних умов ефективного функціонування підприємств є управління їх процесами. У наукових працях більшості сучасних вчених управління процесами підприємства неможливе без використання процесного підходу, який, зі свого боку, базується на моделюванні процесів підприємства.

Моделювання бізнес-процесів підприємства присвячено наукові праці видатних вчених, як-от: Ф. Тейлор, М. Хаммер и Д. Чампи, П. Фингар тощо. Трактуванню значення поняття «бізнес-процеси», їх класифікації та розробленню методів їх моделювання присвячена значна кількість досліджень, виконаних українськими та іноземними науковцями, серед яких: Е.Ойхман; М. Робсон, Ф. Уллах; М. Хаммер та Д. Чампі; А. Шеєр; В. Демінг та інші [1].

Незважаючи на значні досягнення в теорії та практиці, питання, пов'язані з методами моделювання бізнес-процесів та їх використанням для впровадження процесного підходу на промислових підприємствах України, залишаються недостатньо вивченими.

Управління процесами є інформацією, необхідною для забезпечення управління, і спрямоване на підтримку стабільного та повторюваного процесу шляхом виявлення та усунення причин відхилень. Процеси розвитку орієнтовані на постійні, цільові зміни процесу на основі цілей, які встановлено керівним органом управління. Побудова бізнес-процесу, формування та вивчення моделі називаються моделюванням.

Моделювання ґрунтується на математичній теорії подібності, згідно з якою модель повинна достатньо точно відображати функціонування змодельованої системи. Термін «моделювання бізнес-процесів» визначається за допомогою термінології кількох галузей знань і містить у собі такі категорії, як моделювання і бізнес-процес. Моделювання базується на математичній теорії подібності, згідно з якою модель повинна достатньо точно відображати функціонування змоделюваної системи. З погляду бізнес-процесу термін «моделювання» має два основних значення. По-перше, під моделюванням розуміють процес створення моделі як певного образу (оригіналу), що відображає найважливіші його риси та властивості. Якщо модель процесів вже

є, то моделювання – це процес дослідження функціонування системи. Метою моделювання бізнес-процесів є опис етапів та принципів функціонування моделі бізнес-процесів. Найважливішим елементом процесної моделі будь-якого підприємства є система класифікації бізнес-процесів. Модель бізнес-процесів – це текстовий, графічний, табличний або символьний опис, який відображає реальну або передбачувану діяльність організації.

Модель повинна містити такі відомості про бізнес-процес, як:

- перелік складових процесів (підпроцесів), які формують загальний процес;
- алгоритм виконання процесів;
- механізми контролю та управління в межах бізнес-процесу;
- чітке визначення відповідальних за виконання процесів;
- регламентація та документування входу та виходу процесу;
- перелік необхідних ресурсів для виконання кожного процесу;
- параметри, що характеризують результативність виконання кожного окремого процесу та бізнес-процесу в цілому.

Моделювання бізнес-процесу повинно здійснюватися поетапно. Текстова модель бізнес-процесів ґрунтується на принципах процесного підходу і містить такі етапи:

- ідентифікація наявних процесів;
- опис виконання кожного процесу;
- визначення відповідальних за координацію процесу;
- визначення ресурсозабезпечуючих компонентів процесу;
- поетапне проектування мережі процесів та створення процесної моделі;
- регламентація управління бізнес-процесами;
- оптимізація організаційної структури на основі створеної моделі.
- формування системи контрольних показників.

Отже, моделювання побудови системи бізнес-процесів на підприємстві є завданням, яке треба вирішувати комплексно. Усі вказані етапи моделювання бізнес-процесу мають описовий характер, на основі яких можна створити графічне, символьне і табличне відображення бізнес-процесу будь-якого підприємства. На нашу думку, моделювання бізнес-процесів українських підприємств повинно здійснюватися шляхом координації окремих галузей, як складових елементів розвитку національної промисловості.

---

1. Мельник О. Г., Мукан О. В., Злотнік М. Л. Особливості моделювання бізнес-процесів підприємства та їх оптимізування в контексті здійснення міжнародної діяльності. *Менеджмент та підприємництво в Україні: етапи становлення та проблеми розвитку*. 2019. Вип. 2 С. 43–52.

Тютченко Світлана Миколаївна
кандидат економічних наук, доцент,
доцент кафедри прикладної економіки,
підприємництва та публічного управління
Національного технічного університету
«Дніпровська політехніка»

РИЗИКИ ТА НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ВІЙНИ

Економічна безпека держави – це стан, в якому економічні системи та ресурси країни захищені від зовнішніх та внутрішніх загроз, що можуть створити негативний вплив на стійкість економіки та добробут громадян. Економічна безпека має кілька ключових аспектів, а саме:

1. Захист економічних ресурсів. Це означає забезпечення стійкості та безпеки економічних ресурсів, таких як сировинні матеріали, енергетичні ресурси, технології, та інші активи, які є критичними для функціонування національної економіки.

2. Захист фінансової стійкості. Це містить у собі управління фінансовими ризиками, збереження стабільності валюти, контроль інфляції, та забезпечення фінансової стійкості системи банківського сектору.

3. Захист виробництва та економічної інфраструктури. Містить у собі захист від терористичних атак, кібератак, природних катастроф, та інших подій, які можуть завдати шкоди економіці.

4. Захист торговельних інтересів. Держава має використовувати торговельні політики та міжнародні договори для забезпечення захисту власних торговельних інтересів та зменшення негативного впливу міжнародної конкуренції.

5. Захист працівників та соціального добробуту. Забезпечення економічної безпеки також містить у собі захист прав працівників, забезпечення соціального захисту та добробуту населення.

Забезпечення економічної безпеки держави вимагає вдосконалення політики, законодавства, стратегій і механізмів, щоб запобігти можливим загрозам та забезпечити стійкість національної економіки в умовах змін і небезпек.

Забезпечення економічної безпеки держави в умовах війни є важливим завданням, оскільки війна призводить до серйозних загроз економіці та фінансовому становищу країни. Важливі ризики та напрями забезпечення економічної безпеки в умовах війни становлять таке:

Ризики:

1. Економічні збитки. Війна призводить до значних економічних збитків через руйнування інфраструктури, знищення виробництва та інших сфер

економіки.

2. Зменшення інвестицій. Війна спричиняє відсутність інвестицій та зменшення довіри іноземних інвесторів, що може вплинути на розвиток економіки.

3. Збільшення державних видатків. Держава змушена виділяти значні кошти на оборону та військові операції, що може призвести до дефіциту бюджету та збільшення боргу.

4. Зниження рівня життя населення. Війна може призвести до зменшення рівня життя населення через зростання цін, втрату робочих місць та інфляцію.

Напрями забезпечення економічної безпеки в умовах війни:

1. Резерви та резервні фонди. Держава повинна мати достатні резерви та фонди, які можуть використовуватися для покриття витрат на військові операції та відновлення після війни.

2. Диверсифікація економіки. Розвиток різних галузей економіки допомагає зменшити залежність від окремих галузей, що може забезпечити більшу стійкість в умовах війни.

3. Забезпечення продовольчої та енергетичної безпеки. Держава повинна мати достатні запаси продовольства та енергоресурсів, щоб забезпечити населення в умовах війни.

4. Розвиток внутрішнього ринку. Збільшення внутрішнього споживання та підтримка вітчизняних виробників може допомогти зменшити залежність від зовнішнього ринку.

5. Моніторинг та аналіз. Постійний моніторинг економічних та фінансових показників дозволяє реагувати на зміни та приймати необхідні заходи для забезпечення економічної безпеки.

Отже, забезпечення економічної безпеки в умовах війни вимагає комплексного підходу та вчасних заходів для запобігання серйозним наслідкам для економіки та населення держави.

---

1. Тютченко С. М. Групування методів оцінки економічної безпеки підприємства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2019. № 1(98). С. 21–25. URL:http://er.dduvs.in.ua/bitstream/123456789/3490/1/6.pdf

2. Ханова І. М., Гільмутдінова Р. А. Фінансове прогнозування як елемент управління ризиками в умовах забезпечення економічної безпеки підприємства. *Економічна безпека: стан і перспективи* : матеріали Міжнар. наукової конф. 2018. С. 365–368.

Антропов Богдан Олегович
студент магістратури ННІ права
та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
Ділігул Аліна Сергіївна
доцент кафедри
цивільного права та процесу
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ФІНАНСОВИЙ АСПЕКТ БЕЗПЕКИ УКРАЇНИ У СУЧАСНОМУ ФОРМУВАННІ ДЕРЖАВНОСТІ

Особливістю сьогодення є постійна увага до забезпечення захисту держави та суспільства від різних видів загроз, а також їх відвернення. Однією із загроз сучасного світу для держави є неконкурентоспроможності національного виробництва, недотримання торговельних переваг, незабезпечення переваг національної економіки на світових ринках, тобто чинники небезпеки фінансового або економічного стану. Тому фінансова або економічна безпека України є важливим аспектом у сучасному формуванні державності.

Тож на сьогодні точного та єдиного тлумачення фінансової або економічної безпеки України немає. Однак є гарні приклади наукових діячів, з якими ми можем погодитись. Наприклад, О. Власюк вважає, що економічна безпека України базується на творчому поєднанні ресурсів стабільності, керованості та дозованого економічного ризику в тих сферах господарювання, де можна отримати максимальну соціально-економічну поточну ефективність, а також створити сприятливі умови для перспективних інноваційних проєктів [1, с. 17]. Однак Н. Попадинець вважає, що економічна безпека – це сукупність умов, що забезпечують незалежність національної економіки, її стабільність і стійкість, здатність до постійного відновлення і самовдосконалення, здатність економіки забезпечувати ефективне задоволення ендогенних та екзогенних суспільних потреб [2, с. 21].

Проаналізувавши вище зазначене, можна виокремити, що економічна або фінансова безпека – це сформований з часом комплекс захисних заходів або засобів, які спрямовані на утримання, зберігання та формування фінансового забезпечення держави на її потреби.

Щодо фінансових аспектів безпеки, на нашу думку, їх можна виокремити у дві групи: ті, які є державними і формуються в середині держави (бюджети, фонди, збори, внутрішній ринок), і ті, які надходять від інших

держав (інвестиції, разові фінансові виплати, позики, кредити). Ці аспекти можуть забезпечити фінансування державних апаратів та всіх інших соціальних верств. Зокрема, вище вказані фінансові аспекти безпеки забезпечують наповнення бюджету держави для уникнення кризових ситуацій.

Однак на сьогодні Україна зазнає низку змін у державності і варто звернути увагу на економічну або фінансову безпеку, оскільки на цей час держава, яка не має свого фінансово-стійкого бюджету, може програвати у багатьох позиціях у світі. Також наявні різні погляди щодо чинників, які є потенційною загрозою економічній безпеці. Зокрема, висловлюється позиція Я. Б. Базилюка та С. В. Давиденко, що до найбільш небезпечних загроз економічної безпеки України треба віднести: неефективність державного регулювання та керованості соціально-економічними процесами; зростання «тіньової» економіки, посилення її криміналізації; свідомі чи несвідомі дії представників вищих органів державної влади та управління, спрямовані на шкоду державі та національним інтересам; соціальна незахищеність значної частини населення, зростання бідності; непослідовність і безсистемність у здійсненні економічних реформ, відсутність власної моделі реформ та їх ідеологічного забезпечення; деформована структура виробництва, відсутність науковообґрунтованої структурної перебудови економіки; неефективність податкової системи, масове ухилення від сплати податків; неефективне управління державним сектором економіки; високий рівень матеріало- та енергомісткості виробництва; корупція в управлінській сфері; недосконалість національного законодавства, пов’язаного з регулюванням економічних процесів; домінування видобувних і базових галузей з низьким ступенем переробки сировини; незадовільна орієнтація на виробництво продукції кінцевого споживання; застарілі технології у більшості галузей виробництва [3, с. 38].

У зв’язку із вище вказаним, можна дійти висновку, що однозначно сьогодні Україна переживає період великих перетворень та проблем, зокрема проблематику фінансового аспекту. На цьому етапі перетворень та проблем дуже важливо, щоб, ухвалюючи економічні та політичні рішення, уповноважені представники керувалися виключно національними інтересами, дбали про добробут народу та держави, розвивали ефективну співпрацю з іноземними партнерами, а також забезпечували належну економічну та національну безпеку.

Вважаємо за доцільне подбати про фінансову та економічну безпеку України та активувати не лише фінансові аспекти безпеки інших країн (інвестиції, разові фінансові виплати, позики, кредити), а розвивати власний ВВП (бюджети, фонди, збори, внутрішній ринок зі змогою експорту продукції до інших країни). Зокрема, не зупинятись на досягнутому та проводити подальше дослідження стану економічної безпеки в Україні, а також створювати прогнози та перспективу її захисту від зовнішніх та внутрішніх загроз.

1. Власюк О. С. Теорія і практика економічної безпеки в системі науки про економіку. 48 с.

2. Попадинець Н. М. Основні чинники забезпечення економічної безпеки України. URL: http://ird.gov.ua/sep/sep20162(118)/sep20162(118)_020_PopadynetsNM.pdf

3. Базилюк Я. Б., Давиденко С. В. Економічна безпека України в умовах гібридної агресії. Київ : НІСД, 2017. 84 с.

Білієнко Єлисей Геннадійович
студент магістратури ННІ права
та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
Рижков Едуард Володимирович
професор кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОСНОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Захищаючи свої інформаційні інтереси, кожна держава має дбати про свою інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України формується як складова частина її соціально-економічної політики, зважаючи на пріоритетність національних інтересів та загрози національній безпеці країни. Із правової позиції вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно із чинним законодавством. В Україні назріла об'єктивна потреба у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу та рівню розвитку інформаційних технологій, нормам міжнародного права, але водночас ефективно захищала б власні українські національні інтереси. Відносини, пов'язані із забезпеченням інформаційної безпеки, як найважливіші сьогодні для суспільства та держави вимагають найшвидшого законодавчого регулювання.

Проведення вдалої інформаційної політики може суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних та військових конфліктів. Інформаційна безпека є однією із суттєвих складових частин національної безпеки країни, її забезпечення завдяки послідовній реалізації грамотно сформульованої національної інформаційної стратегії в значній мірі

сприяло б забезпеченню досягнення успіху при вирішенні завдань у політичній, соціальній, економічній та інших сферах державної діяльності.

Вивченням ролі держави у формуванні інформаційного суспільства займаються такі вчені як Арістова І., Почепцов Г. [1; 2] та ін. Низка публіцистів Супрун В., Ярочкін В. розробили основні принципи забезпечення інформаційної безпеки [3; 4]. Водночас окремого дослідження вимагають структурно-функціональні аспекти процесу гарантування інформаційної безпеки.

Метою дослідження є виявлення та аналіз основних напрямів державної інформаційної політики з метою захисту національного інформаційного простору та гарантування інформаційної безпеки.

Результати дослідження. У ст. 17. Конституції України зазначено: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [5]. Інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз [6]. Ця безпека повинна містити ефективну протидію сукупності інформаційних загроз. Необхідність гарантування інформаційної безпеки зумовлюється, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей. Завдання інформаційної безпеки – створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави [7]. У разі виникнення криз, загострення конфліктів інформаційна боротьба може перерости в інформаційну війну, яка здійснюється за допомогою інформаційної зброї. Показниками є цілеспрямованість, масштабність та комплексність дій тощо.

З огляду на вищевказане зазначимо, що державна інформаційна політика повинна відбивати нагальні питання, що склалися у міжнародній сфері та сфері інформаційної безпеки тощо. Необхідним є забезпечення законодавчого захисту прав та інтересів всіх суб’єктів інформаційних відносин. Найскладнішими тут є такі завдання, що передбачають гармонійне забезпечення інформаційної безпеки держави, особи і суспільства з одночасним виокремленням нагальних пріоритетів, до яких треба віднести створення/відновлення основних точок захисту системи національної безпеки в інформаційній сфері, практичну реалізацію наведеної вище схеми створення ефективної системи інформаційної безпеки держави, перегляд списку нових інформаційних загроз, усунення наявних із визначенням ступеня можливих наслідків та рівнів їх інтенсивності. Основні акценти державної інформаційної політики повинні базуватись на забезпеченні права на достовірну, повну та

своєчасну інформацію, свободу слова та інформаційну діяльність, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно до Конституції України; збереженні та вдосконаленні вітчизняного національного інформаційного продукту та технологій, забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантуванні державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій.

1. Арістова І. В. Діяльність органів внутрішніх справ щодо реалізації державної інформаційної політики : монографія. Харків : Нац. ун-т внутр. справ, 2016. 354 с.

2. Почепцов Г. Інформаційна політика : навч. посіб. Київ : Знання, 2018. 663 с.

3. Супрун В. М. Інформаційний суверенітет як один з елементів інформаційної безпеки держави: теоретико-правовий аспект. URL: http://www.nbuv.gov.ua/portal/natural/vkhnu/Pravo/2019.

4. Ярочкін В. Система безпеки фірми. URL: http://www.nbuv.gov.ua.

5. Про інформацію : Закон України. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12.

6. Боднар І. Р. Сучасні реалії інформаційного суспільства: проблеми становлення та перспективи розвитку : монографія. Львів : Видавництво Львівської комерційної академії, 2021. 320 с.

7. Бондаренко В. Інформаційна безпека сучасної держави: концептуальні роздуми. URL: http://www.crime-research.iatp.org.ua/library/strateg.htm.

Бразалук Вадим Павлович
студент магістратури ННІ права
та підготовки фахівців
для підрозділів Національної поліції
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ У ВСЕСВІТНІЙ МЕРЕЖІ «ІНТЕРНЕТ» ТА ВПРОВАДЖЕННЯ МЕТОДІВ БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ В ІНТЕРНЕТ-СЕРЕДОВИЩІ

Сьогодні жоден із сучасних людей не може уявити своє існування без системи Інтернет, яка відкриває широкий спектр різноманітних можливостей для спілкування та обміну будь-якою інформацією. Саме тому є ціла система суспільних відносин в інтернет-просторі, які чітко відслідковуються у всіх сферах життєдіяльності, наприклад: економіці, державному управлінні, науці

та навіть мистецтві. Але, на жаль, разом із позитивними здобутками, які привносить Інтернет у наше життя, є ціла низка негативних явищ криміногенного характеру, що відбуваються в інтернет-середовищі, зокрема: порушення авторських прав, розповсюдження і збут наркотичних засобів, психотропних речовин, їх аналогів та прекурсорів, а також інших заборонених речовин, вимагання, шахрайство через Інтернет та інші види як традиційних, так і власне комп'ютерних злочинів. Процес розслідування злочинів, скоєних із використанням мережі «Інтернет», набагато складніший за процес розслідування такої ж категорії злочинів, вчинених у звичайних умовах, саме тому потребує в постійному створенні та впровадженні новітніх методів боротьби з інтернет-злочинцями. Зазначеним треба пояснювати необхідність вивчення методичних і практичних питань розслідування злочинної діяльності в Інтернеті.

Практична цінність результатів криміналістичних наукових досліджень залежить насамперед від того, наскільки глибоко і повно науці вдається проникнути в механізм злочину, показати порядок і шляхи інформації про нього, добування інформації та розшифрування її.

Механізм злочину виражає функціональну сторону злочинної діяльності, без аналізу змісту якої, послідовності етапів злочинної діяльності не можна усвідомити кореляційний зв'язок, зіставити наявні про конкретний злочин дані з системою узагальнених відомостей про раніше розслідувані злочини вказаного виду.

Зважаючи на природу електронного середовища, на практиці наявна проблема юрисдикції мережі, каналами якої, наприклад, протиправно пересилають об'єкти авторського права. Саме цим варто пояснювати транснаціональний (екстериторіальний) характер технології вчинення злочинів у мережі «Інтернет».

Типовою нині можна вважати ситуацію, коли правопорушник-громадянин однієї держави є власником вебсайту, зареєстрованого на території іншої держави, а цільова аудиторія цього інформаційного ресурсу мешкає на території третьої держави.

Треба звернути увагу на тому, що однією з особливостей функціонування Інтернету є те, що провайдери як головні суб'єкти глобальної мережі, які забезпечують доступ до інформації та надають відповідні послуги, не в змозі контролювати весь обсяг розміщеної в Інтернеті інформації, оскільки фактично вона може бути на комп'ютері – www-сервері, розташованому в будь-якій частині світу [1]. Відповідно, обмін інформацією в електронній цифровій формі характеризується легкістю й оперативністю її створення, поширення, модифікації або знищення. Все це призводить до виникнення проблем у частині забезпечення доказування й, відповідно, викликає необхідність у розробленні нових та вдосконаленні наявних техніко-криміналістичних і тактичних засобів збирання доказів в інтернет-середовищі.

Отже, з метою подальшого розроблення методики розслідування

злочинів, учинених у мережі «Інтернет», виділяють такі напрями роботи. По-перше, ототожнення механізму вчинення таких злочинів безпосередньо залежить від змісту послуг або угод, наданих чи укладених суб'єктами, що постраждали від злочинних дій, та виду інформаційно-комунікаційних технологій, через які така подія сталася в мережі «Інтернет». По-друге, окремі тактичні засади розроблюваної методики обов'язково повинні враховувати інтернаціональний характер технології такої злочинної діяльності. По-третє, в методиці необхідно запропонувати нові та вдосконалити наявні тактичні засоби збирання доказів електронного походження, що містяться в мережі «Інтернет».

1. Левковець О. М. Інноваційна безпека України: проблеми забезпечення в глобалізованому світі. URL: http://www.rusnauka.com/31_PRNT_2010/Economics/73679.doc.htm.

2. Шлемко В. Т. Економічна безпека України. Київ : НІСД, 1997. 144 с. URL: http://old.niss.gov.ua/book/rozdil/binko.htm

Годзенко Олександр Олександрович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ШАХРАЙСТВО В УМОВАХ ДІЇ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ

Зазначимо, що в усьому світі зростає кількість кримінальних правопорушень економічної спрямованості, що завдають шкоди людям, організаціям і навіть країнам в цілому. Розслідування таких кримінальних правопорушень стає все дедалі складнішим, це пов'язано, зокрема, і з впровадженням воєнного стану на всю територію України, адже шахрайство та економічна злочинність активно поширюються та постійно набувають нових форм. Тож з початком бойових дій на території нашої держави виникли нові види шахрайських способів заволодіння грошовими коштами громадян України, організацій тощо. Саме тому доцільним є розглянути нові схеми шахрайських дій та можливі напрями протидії з ними.

Зазначимо той факт, що будь-які види шахрайства (незалежно від

розміру матеріальної шкоди потерпілій особі) несуть за собою кримінальну відповідальність, яка відображається в змісті статті 190 Кримінального кодексу України. Крім того, нещодавно були внесені зміни до вказаної статті і тепер частиною 3 статті 190 передбачається вчинення шахрайства в умовах воєнного стану, що завдало значної шкоди потерпілому [1].

Звернемо увагу на те, що заходи щодо запобігання шахрайству все ж таки працюють. Аналіз даних про здійснення економічного шахрайства з 2018 року свідчить, що частка організацій (людей), які постраждали від економічної злочинності, стабільна і потрохи зменшувалася з року в рік (2018 рік – 49 %, 2020 рік – 47 %, 2022 рік – 46 %), хоча технологічний розвиток не тільки розширив можливості здійснення шахрайства, але дав поштовх розвитку інструментів його попередження та виявлення [2, с. 162].

Доцільним є зауважити, що кількість шахрайства в умовах війни невпинно зростає, а способів та засобів цих протиправних дій стає все більше. З початку повномасштабної війни, а саме приблизно перший рік (враховуючи і зазначене вище), кількість злочинів, пов'язаних із шахрайськими діями, було набагато менше, ніж за 2023 рік. Цей факт може пояснюватися тим, що часто люди з різних причин не звертаються до правоохоронних органів, ставши жертвами вчинення таких злочинів, що відповідно не дає змоги врахувати такі злочини під час обліку вчинення шахрайств. Також досить складно напрацювати ефективний механізм протидії злочинам, про які не було повідомлено в органи досудового розслідування [3, с. 202–203]. Однак вже з початку 2023 року велика кількість людей масово почали звертатися з відповідними заяви до правоохоронних органів і тому вже на сьогодні вдалося розробити певний механізм розслідування та протидії таким кримінальним правопорушенням.

Нижче розглянемо найпоширеніші способи вчинення шахрайства. Перший спосіб має умовну назву «банківські шахрайства». Він полягає в тому, що зловмисники телефонують особам та представляються працівниками банків, а також можуть використовувати такі словосполучення для отримання конфіденційних даних від осіб: «ваша картка заблокована», «з вашого рахунку намагаються списати грошові кошти», «чи робите ви зараз конвертацію грошових коштів в іншу валюту» тощо. Так шахраї просять надати номер картки, пін-код, тризначний номер на звороті картки, термін її дії або ввести пароль, який надійшов на їх мобільний телефон через смс-повідомлення.

Наступним, не менш поширеним способом, є використання оголошень на сайтах, зокрема OLX. У цьому випадку це стосується оголошень, які викладають саме потенційні потерпілі особи. Ця схема діє так, що в особисті повідомлення пишуть особи (зловмисники) про те, що зацікавились оголошенням і пропонують оформити доставку саме через платформу OLX та надсилають посилання, на яке переходить потерпіла особа та вводить дані своєї банківської картки, після чого з неї знімають грошові кошти.

Вказані нами кримінальні правопорушення стоять на контролі

Департаменту кіберполіії Національної поліції України, який забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність у зазначеній сфері. Стратегічними завданнями цього підрозділу визнають формування та забезпечення реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, що вчиняються за допомогою електронно-обчислювальної техніки, шляхом вивчення механізму їх підготовки, вчинення або приховування, а також участь у попередженні, виявленні та припиненні кримінальних правопорушень іншими підрозділами національної поліції, що не мають навичок у протидії кіберзлочинності, однак у провадження яких перебувають кримінальні провадження зі згаданим способом вчинення [4]. Вказані підрозділі в подальшому направляють матеріали про виявлені ознаки шахрайства до відповідних слідчих підрозділів та в подальшому супроводжують їх під час досудового розслідування кримінальних проваджень.

Отже, можна зробити висновок, що в умовах війни кримінальні правопорушення, які пов’язані з викраденням грошових коштів шахрайським способом, зросли та їх дослідження набуває все більшої актуальності. Завдяки інформаційному розвитку правопорушники розробили нові схеми шахрайства та застосовують їх все частіше, бо багато людей просто не знають про можливість використання їх на практиці. Тому потрібно постійно інформувати населення про можливі способи та засоби застосування шахрайства щодо них.

---

1. Кримінальний Кодекс України від 05.04.2001 року №2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 24.09.2023).

2. Нежива М. О., Мисюк В. О. Протидія шахрайству в умовах війни. *БізнесІнформ*. 2023. № 1. С. 160–166.

3. Балановський Р. А. Запобігання кібершахрайству в контексті кібервійни між росією та Україною. *Актуальні проблеми протидії злочинності та корупції* : зб. матеріалів Всеукр. науково-практ. конф. Харків, 2023. С. 202–206.

4. Про підрозділ. Кіберполіція: Національна поліція України. URL: https://cyberpolice.gov.ua/contacts/ (дата звернення: 24.09.2023).

Гутнік Максим Олексійович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Сучасна суспільна дійсність характеризується стрімким розвитком інформаційних технологій, які відіграють ключову роль у всіх аспектах життя суспільства. Національна поліція України не є винятком і активно використовує інформаційні технології для вирішення різноманітних завдань та полішення якості своєї діяльності.

Національна поліція України зосереджує свої зусилля на забезпеченні громадської безпеки та боротьбі зі злочинністю. Інформаційні технології відіграють важливу роль у досягненні цієї мети. Зокрема, впровадження систем відеоспостереження та розпізнавання обличчя допомагає виявляти злочини та швидко реагувати на них. За допомогою інформаційних баз даних поліцейські можуть ефективно вести слідство та ідентифікувати злочинців. Інформаційні технології також дозволяють поліції вести моніторинг громадської думки та реагувати на громадські події. Декілька ключових аспектів в інформаційній діяльності правоохоронців. Системи моніторингу і виявлення:

● Сучасні системи відеоспостереження, радари та супутникові технології надають можливість нагляду за великими територіями та вчасному виявленню потенційних загроз.

● Системи штучного інтелекту (ШІ) можуть аналізувати великі обсяги даних і виявляти незвичайні патерни, що можуть свідчити про можливі загрози.

Кібербезпека:

● Запити на цифрові дані стали невід’ємною частиною боротьби з кіберзлочинністю та кібертероризмом.

● Інформаційні технології допомагають виявляти, блокувати та слідкувати за кібератаками.

Комунікації та обмін інформацією:

● Сучасні засоби зв'язку, зокрема мобільний зв'язок та Інтернет, дозволяють оперативно обмінюватися інформацією між службами громадської безпеки та реагувати на надзвичайні ситуації.

Аналітика та прогнозування:

● Системи аналітики даних допомагають урядовим органам прогнозувати потенційні загрози на основі зібраних даних і розробляти стратегії для їх запобігання.

Оперативність та реагування на надзвичайні ситуації є важливою частиною діяльності Національної поліції України. Інформаційні технології допомагають поліцейським швидко обмінюватися інформацією, координувати дії та забезпечувати безпеку громадян. Інтеграція технологій в роботу правоохоронних органів відкриває безліч можливостей для підвищення оперативності поліції та поліпшення загального рівня безпеки суспільства. Використання спеціальних програм та мобільних додатків дозволяє поліції оперативно реагувати на події та вести облік кримінальних злочинів.

Однією з основних функцій поліції є збір і аналіз інформації про можливі порушення закону та злочини. Сучасні інформаційні технології дозволяють збирати, зберігати та обробляти величезний обсяг даних швидко і ефективно. Аналітичні системи можуть ідентифікувати зв'язки та залежності між різними видами злочинів, що допомагає поліції у попередженні та розкритті злочинів. Інформаційні технології також сприяють поліпшенню комунікації між різними підрозділами поліції та між правоохоронними органами різних рівнів влади. Впровадження систем обміну даними дозволяє швидко обмінюватися важливою інформацією про кримінальні події та оперативно реагувати на них. Поліція також повинна захищати себе від кіберзлочинців. Інформаційні технології використовуються для збереження важливої інформації та захисту її від несанкціонованого доступу. Кіберполіція відіграє важливу роль у виявленні та припиненні кіберзлочинів. Важливо продовжувати інвестувати в розвиток інформаційних технологій для поліції та забезпечувати навчання персоналу для максимального використання їх можливостей. Тільки так можна забезпечити безпеку та порядок у сучасному світі.

З огляду на важливість особистої інформації та право на приватність, Національна поліція України зобов'язана забезпечувати захист особистих даних громадян. Захист особистих даних є фундаментальним правом кожної людини. Усе більше інформації про громадян збирається і обробляється різними установами, у тому числі поліцією, для забезпечення громадської безпеки і боротьби зі злочинністю. Проте цей процес повинен бути суворо регульований, адже незаконний доступ до особистої інформації може призвести до порушення приватності, дискримінації й інших негативних наслідків. У цьому контексті важливою є роль правового регулювання та механізмів контролю за збором і використанням особистих даних поліцією.

Прозорість у діяльності поліції також має вирішальне значення для

довіри громадян до правоохоронних органів. Громадяни повинні бути достатньо інформованими про роботу поліції, її завдання та методи, що використовуються для досягнення цих завдань. Такий підхід сприяє більшому взаєморозумінню між громадянами і поліцією і допомагає у підвищенні віри в правоохоронні органи. Прозорість також містить у собі розкриття інформації про випадки порушення прав і свобод громадян поліцією, що є важливим кроком у підтримці відповідальності за дії правоохоронців.

Для досягнення балансу між захистом особистих даних та прозорістю в діяльності поліції необхідно впроваджувати сучасні технології та вдосконалювати правові межі. Одним із способів є регулювання збору і використання особистих даних поліцією, забезпечуючи конфіденційність, цілісність і доступність даних. Також важливо створювати механізми для незалежного контролю за діяльністю поліції, зокрема організацію аудитів і регулярну публікацію інформації про роботу поліції та її досягнення.

Крім того, освіта громадян щодо їхніх прав та можливостей звернутися за захистом є важливим аспектом прозорості та забезпечення їхньої активної участі в контролі діяльності поліції.

Інформаційні технології стали необхідною складовою в діяльності Національної поліції України, допомагаючи вирішувати завдання забезпечення громадської безпеки, підвищення оперативності та захисту особистих даних громадян. Впровадження нових інформаційних рішень та технологій сприяє поліпшенню роботи поліції та збільшенню її ефективності.

1. Звіт Національної поліції України про результати роботи у 2022 році (2023). URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2022/Zvit_polic_2022.pdf

2. Голіна В. В. Зменшення можливостей вчинення злочинів: стратегічний підхід : монографія. URL: https://ivpz.kh.ua/wp-content/uploads/2021/09/моно_Стратегія-зменшення-можливостей.pdf

3. Стратегія громадської безпеки та цивільного захисту України (29.06.2021). URL: https://mvs.gov.ua/uk/ministry/normativna-baza-mvs/proekti-normativnix-aktiv/strategiya-gromadskoyi-bezpeki-ta-civilnogo-zaxistu-ukrayini-zatverdzeno-vid-29062021

4. Про захист персональних даних : Закон України від 01.06.2010. URL: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17#Text

Дрозд Андрій Олександрович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ В БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ ПІД ЧАС ВОЄННОГО СТАНУ В УКРАЇНІ

У сучасному Українському суспільстві, де кожна активна особистість використовує мобільні пристрої та користується Інтернетом, велика частина сфер діяльності, зокрема державні органи, банківський сектор, залізниця, авіатранспорт, і великі підприємства, засновані на стабільності кіберпростору, з яким вони взаємодіють, спирається на електронні засоби зв'язку. Ця цифрова трансформація відкриває нові можливості для розвитку суспільних відносин, але також створює умови для зростання кіберзлочинності.

За офіційною статистикою Офісу Генерального прокурора України, протягом останніх 8 років кількість виявлених кіберзлочинів зросла майже в 7,5 разів, і це без включення класичних правопорушень, пов'язаних із використанням комп'ютерної техніки. Інформаційна революція відкрила нові можливості для злочинців, а тому злодії вже не обов'язково є холоднокровними зловмисниками зі зброєю в руках [3]. Тепер злодієм може бути будь-яка особа, яка має доступ до комп'ютера та Інтернету.

У складних умовах повномасштабної війни рф проти України злочинці можуть стати дієвими бойовими одиницями, а їхнім основним інструментом стають кібератаки та взломи. Злодії можуть використовувати цей хаос для здійснення атак не лише від імені ворога, який намагається завдати шкоди обороноздатності України, але й від імені тих, хто готовий скористатися ситуацією, коли правоохоронні органи перенапружені, для свого особистого збагачення за рахунок грошей громадян.

Заради забезпечення стабільності в Україні під час воєнного конфлікту правоохоронні органи, зокрема поліція, працюють в посиленому режимі, не припиняючи свою діяльність. Зібрана інформація з різних джерел обробляється і узагальнюється цілодобово. З огляду на стрімкий ріст кіберзлочинності, Верховна Рада України ухвалила низку законодавчих змін,

спрямованих на оптимізацію кримінального та кримінально-процесуального законодавства для боротьби з цією загрозою. Зміни в законодавстві дозволили поліпшити підстави та процедури притягнення кіберзлочинців до кримінальної відповідальності [1].

Однією з ключових складових боротьби з кіберзагрозами є моніторинг та аналіз ситуації. Використання сучасних технологій, таких як системи штучного інтелекту та машинного навчання, дозволяє виявляти потенційні загрози у реальному часі та надавати швидку реакцію на них.

Крім того, створення централізованих систем виявлення та реагування на кібератаки є надзвичайно важливим аспектом. Ці системи дозволяють оперативно контролювати інциденти та приймати необхідні заходи для їх припинення. Автоматизовані рішення можуть значно полегшити цей процес.

Ще однією важливою сферою є захист даних. Використання сучасних методів шифрування допомагає зберігати конфіденційну інформацію від доступу несанкціонованих осіб. Важливо враховувати, що в умовах війни доступ до важливих даних може бути критично важливим завданням [2, с. 18].

Освітня робота серед громадян також має велике значення. Грамотність у сфері кібербезпеки допомагає уникнути фішингових атак, шахрайства та інших кіберзагроз. Інформаційні кампанії та освітні заходи можуть значно підвищити рівень обізнаності громадян.

Важливо також надавати пріоритет міжнародній співпраці та обміну інформацією щодо кіберзагроз. Умови війни можуть сприяти зростанню кібератак, і лише спільні зусилля країн та міжнародних партнерів можуть забезпечити ефективний захист.

Отже, застосування сучасних технологій в боротьбі з кіберзлочинністю в умовах війни є необхідним завданням для забезпечення національної безпеки та захисту інформаційних ресурсів країни. Сполучення технічних і організаційних заходів, а також співпраця різних секторів суспільності та міжнародних партнерів є ключовими чинниками успіху в цій сфері.

---

1. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text

2. Сащенко М. І. Проблемні аспекти запобігання кіберзлочинності в Україні. *Young Scientist*. 2022. №1 (101). С. 17–20.

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

Дроздовська Юлія Олегівна
слухач магістратури ННІ права
та підготовки фахівців для підрозділів
Національної поліції
Науковий керівник:
Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ПЕРСПЕКТИВИ ТА НАСЛІДКИ РОЗПОВСЮДЖЕННЯ НЕЛЕГАЛЬНОЇ ВОГНЕПАЛЬНОЇ ЗБРОЇ У ПОВОЄННИЙ ПЕРІОД В УКРАЇНІ

Аналіз стану обігу зброї дозволяє зрозуміти важливі процеси, що відбуваються в соціально-політичній сфері країни, та слугує важливим показником національної, громадської та військової безпеки. Усі три сфери є надзвичайно важливими для України в контексті збройного конфлікту, що триває на території нашої країни. Необхідність аналізу переспектив та наслідків розповсюдження нелегальної вогнепальної зброї в Україні в повоєнний період і становить актуальність нашого дослідження.

Треба зазначити, що право на захист свого життя й життя рідних, як відомо, належить до переліку прав та свобод людини й громадянина як критерії міжнародно-нормативного підходу. Саме питання самозахисту наших громадян, а також невизначеність правового характеру у сфері контролю над володінням зброєю спричинили значне розповсюдження нелегальної вогнепальної зброї ще у довоєнний час [1].

Наразі ж, коли на території України ведеться повномасштабна війна, не можемо не відзначити, що сучасна безпека громадян, користування і контроль над зброєю також є нагальними питаннями. Прикро визнавати цей факт, однак очевидним є те, що після закінчення війни проблема поширення нелегальної вогнепальної зброї набуде неабиякого масштабу. Вже станом на сьогодні спостерігається значний приріст кількості кримінальних правопорушень, що вчиняються з використанням вогнепальної зброї.

Треба відмітити, що «чорний ринок» вогнепальної зброї вже зараз, під час війни, став більш відкритим, і тепер зброю можна придбати в Інтернеті, а діапазон її застосування справді вражає. Зброя та вибухівка використовуються у побутових конфліктах та політичних суперечках, а гранати все частіше кидають у натовп. Тож відсутність регульованого обігу зброї в країні у

повоєнний період може мати непередбачувані наслідки. Особливо враховуючи те, що зброю знаходять в аеропортах, мостах, водопроводах тощо, а отже, на території критичної інфраструктури міст.

Аналізуючи перспективи розповсюдження вогнепальної зброї після війни, згадаймо 2014 рік, коли показники незаконного обігу зброї в державі були надвисокими. В той час на Донбасі постійно змінювалася лінія зіткнення, постійно відбувалася ротація військових частин та добровольчих формувань, а система фільтраційних заходів лише починала налагоджуватися на місці виходу із зони АТО. Важко й уявити масштаби поширення нелегальної вогнепальної зброї, які можуть виникнути на території Україні після перемоги у повномасштабній війні.

Вважаємо за потрібне зазначити, що значну роль у розповсюдженні вогнепальної зброї на території України відіграє посттравматичний стресовий розлад у військовослужбовців Збройних Сил України, адже після побачених трагічних подій на фронті та участі у відбитті збройної агресії ворога психоемоційний стан військових не може залишитися стібальним. Чимало військових потребуватимуть психологічної реабілітації. Вже сьогодні ми спостерігаємо непоодинокі випадки, коли військовослужбовці з нестабільною психікою привозять як трофеї вогнепальну зброю із зони бойових дій, яка у майбутньому цілком ймовірно може стати предметом вчинення кримінального правопорушення. До того ж такий безконтрольний вивіз зброї з прифронтових територій зумовлений недостатньо якісними перевірками осіб на блокпостах. Тимчасом як на блокпостах повинні перевірятися документи всіх, хто перебуває в автомобілі, особисті речі, сам транспортний засіб, багаж та вантаж, вказані дії щодо військовослужбовців нерідко не здійснюються. Щодо цивільних осіб, то нерідко їх «перевірка» на блокпостах обмежується тільки запитом паролю.

Зважаючи на вищевикладене, вважаємо необхідним посилити кримінальну відповідальність за використання зброї незаконослухняними громадянами України, адже лише за роки війни на Сході України кількість зброї в незаконному обігу практично неможливо перерахувати. Бойові дії на Донбасі переконливо довели, що в населення наявна в незаконній власності й зберігається досить велика кількість різноманітної зброї, яку можна використовувати як бойову. Не можемо також оминути увагою той факт, що надмірне поширення вогнепальної зброї серед населення може негативно позначитися на роботі органів досудового розслідування, адже ймовірне підвищення рівня злочинності призведе до збільшення навантаження на слідчих територіальних підрозділів.

Цікавим є факт, що за результатами проведеного опитування громадян України було встановлено, що значна частина опитуваних (64 %) схиляються до думки, що після закінчення війни є реальна загроза нелегального обігу вогнепальної зброї, для 35 % громадян можливість існування такої загрози є незначною і лише 3 % не бачать загроз. Вказне опитування показує, що з

початку повномасштабної війни в Україні населення занепокоєно питанням безпеки і вважає розповсюдження вогнепальної зброї достатньо небезпечним фактором [2].

Підсумовуючи вищезазначене, вважаємо за потрібне сказати, що ефективна державна політика сфері запобігання розповсюдженню нелегальної вонепальної зброї дозволить встановити контроль за її обігом, вивести з тіні зброю, яка вже на сьогодні є в громадян. Такі заходи, як свідчить практика, не лише не призведуть до збільшення злочинності, а навпаки, з часом стимулюватимуть зниження її рівня.

1. Діденко С., Грінь А. Попов С. Особливості адміністративно-правового регулювання обігу вогнепальної зброї в Україні: реалії сьогодення та перспективи. *Науковий вісник Ужгородського національного університету*. Серія : Право 69 (2022): 266-271.

2. Перше опитування в Дії від МВС і одразу рекорд. *Департамент комунікації МВС України*. URL: https://mvs.gov.ua/uk/news/perse-opituvannya-v-diyi-vid-mvs-i-odrazu-rekord

Жданова Катерина Володимирівна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В РЕАЛІЯХ ВІЙНИ

Е цей складний для всіх українців час, через збройну агресію Росії, коли постійно лунають повітряні тривоги, та є висока вірогідність ракетних ударів по місцях скупчення людей, компанії масово переводять персонал на дистанційний режим роботи. Під час таких подій виникають складнощі, пов’язані не тільки з реалізацією онлайн-роботи по частині інформаційних технологій, але й як основне – забезпечення інформаційної безпеки віддалених підключень та збереження конфіденційної інформації.

Ні для кого не буде секретом, що онлайн працюють дуже багато компаній у різних сферах, в тому числі дистанційно можуть надавати послуги

волонтерські організації. Діяльність українських волонтерів є одним із напрямів, за якими працюють російські кіберзлочинці, наприклад, викрадення грошей з електронних гаманців, отримання даних про військових, місця зустрічей волонтерів, місця складів з гуманітарною допомогою.

Не можна не зазначити, що й військові користуються у своїх службових потребах онлайн-зв'язком чи певними додатками.

Для своєї користі як отримання певних конфіденційних даних росія неодноразово застосовувала трояни та інші засоби для виконання своїх цілей. Наприклад, нещодавно виявлена програма Infamous Chisel, якою користувалось кіберугрупування, кероване кремлівськими спецслужбами. Вірусна програма контролювала додатки для прицілювання та картографування, які використовуються українськими військовими на війні. Infamous Chisel, найімовірніше, використовували для викрадення конфіденційної військової інформації. Розробку шкідливого застосунку в британському оборонному відомстві приписують спеціалістам головного центру спеціальних технологій гру генерального штабу рф.

Переходячи до базових методів забезпечення інформаційної безпеки, як основне, зазначимо певні правила в роботі онлайн:

- дотримуватись правил «цифрової гігієни» при роботі з комп'ютером або смартфоном, а саме використовувати режим «інкогніто» у браузерах, приховувати реальну ір-адресу, регулярно очищати історію перегляду та файли кукі;
- використовувати тільки передбачені виробником програмне забезпечення, додатки, сервіси оновлення і безпеки;
- уникати використання піратського програмного забезпечення;
- не завантажувати з мережі «Інтернет» файли та додатки з низьким рівнем довіри або підозрілі;
- користуватися антивірусним захистом, бажано їх платними версіями;
- не використовувати в роботі версії операційної системи, підтримку яких вже припинено (наприклад, Windows XP);
- регулярно оновлювати прошивки мережевого обладнання (wifi-роутери);
- не надавати доступ до інформації третім особам (включно з друзями та членами сім'ї);
- перед опрацюванням корпоративної інформації на особистому комп'ютері в дистанційному режимі переконатися, що на ньому відсутнє шкідливе програмне забезпечення (просканувати комп'ютер наявною системою антивірусного захисту);
- не тримати постійно (тобто без нагальної потреби) активними сесії месенджерів, соціальних мереж тощо – виходити з особистих кабінетів і не зберігати робочі дані авторизації в браузері без нагальної потреби);
- не відкривати підозрілі посилання і файли, що надійшли до вас електронною поштою чи від малознайомих людей у месенджерах.

Отже, онлайн робота і спілкування не є повністю безпечними, і російські кіберзлочинці й далі будуть намагатися здійснювати атаки, красти інформацію й інше. У роботі зазначені певні загрози кібербезпеки в Україні, а також базові правила безпечного користування смартфонами чи комп'ютерами.

Заікін Даніїл Анатолійович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ПРІОРИТЕТ ТА НАПРЯМИ РОЗВИТКУ УКРАЇНИ ПІСЛЯ ПЕРЕМОГИ

Наразі в Україні йде війна. Війна – річ не з дешевих. Україна щомісяця витрачає приблизно 130 млрд грн, тоді як місячний дохід дорівнює 80 млрд грн. Розвиток економіки в таких умовах майже неможливий. Різні експерти дають різні терміни кінця війни, їх показання різняться від місяця до дванадцяти років. Від результатів війни буде залежати подальший розподіл сфер впливу не тільки в Європі, а й у світі. Але очевидно, що результат війни буде тільки перемога України.

Після перемоги Україні треба буде відновлювати економіку. Зазирнувши в підручник історії, можна розглянути післявоєнну відбудову різних Європейських країн, таких як Великобританія, Франція, Німеччина, Італія тощо. Фактор, який суттєво вплинув на відновлення, це план Маршалла (фінансова допомога США, що була на 20 % з дешевих кредитів і на 80 % з безоплатної фінансової допомоги, насамперед цей план мав на меті відновлення промисловості). Найбільш вірогідно, що Україна може розраховувати на схожий план, який значно полегшить відбудову після перемоги.

Росія заподіяла надзвичайно великих збитків, за підрахунками KSE (Kyiv School of Economics) сума збитків сягає понад 151 млрд доларів. Відновлення інфраструктури, логістики, розмінування на територіях, які були анексовані (за офіційними джерелами, Україна замінована на 30–40 % території). На відбудову і розмінування можуть піти десятиліття і сотні млрд

доларів.

За підрахунками, на кінець серпня 2022 року збитки, завдані інфраструктурі через російські обстріли, оцінюються в 113,5 млрд доларів. Це стосується доріг залізничних колій, генерації енергії, складських потужностей, іригаційних систем тощо. Зважаючи на це, треба запроваджувати програми з відновлення інфраструктури та розробку ефективних правових процедур відшкодування втраченого або знищеного майна через повномасштабне вторгнення.

Серйозне питання щодо демографії та робочої сили. Більше 5 млн людей покинули країну (половина з них діти та молодь, решта переважно економічно активні люди). Проведені опитування показують, що вважливо провести модернізацію законодавства про працю, а також активне проведення програм про працевлаштування допоможе реінтегрувати українців, які повернуться на ринок праці.

Також важливо не забувати про бізнес. До повномасштабного вторгнення в Україні було приблизно 500 великих та 400 тис. малих та середніх підприємств. Важливими факторами для бізнесу є ринкове стимулювання та реформи. Приблизно 70 % підприємств за мету беруть на 2022–2023 роки розширення. Сумарні потреби малих і середніх підприємств оцінюються в 73 млрд доларів, вирішенням цієї проблеми є розширення програми «Доступні кредити 5–7–9 %» або ПІІ (Прямі іноземні інвестиції), найкращим кандидатом підійде ЄС.

Підтримка ЄС у формі фондів спільного інвестування та гарантій. Однією з причин недостатнього фінансування для бізнесу є те, що вони не можуть отримати страхування від воєнних ризиків. Зараз відсутність страхування не тільки гальмує розвиток українського бізнесу, але є однією з основних перешкод для іноземних інвестицій в країну. Підприємства виграють від зменшення податкових ставок та спрощеного податкового адміністрування. Але зараз це не видається можливим, оскільки це призведе до значних втрат бюджету. Приблизно 93 % представників бізнесу вважають, що влада повинна провести ефективну судову реформу та викорінити корупцію.

Емпіричні дослідження вказують на необхідність торгівлі для збільшення ВВП. Збільшення експорту дуже добре вплине на економіку України в майбутньому, важливо щоб відбувся перехід від експорту сировини та напівфабрикатів до продукції з високою доданою вартістю.

З огляду на деякі країни, які успішно застосували цю стратегію і досягли значного прогресу в економічному розвитку своєї країни, для нас це може стати рушієм зростання. Ще одним засобом є інвестиції в інноваційні високотехнічні галузі, сприяння дослідженням та розробкам, а також перекваліфікації робочих.

Так звані «Азійські тигри»: головними їхніми фокусами у другій половині XX століття були експорт та жорстка політика у сфері розвитку та

інвестиції в інновації. Варто зазначити, що головна увага була зосереджена на експорті продукції з високою доданою вартістю (такі товари, як: електричне устаткування, обладнання та запчастини, прилади для відтворення та запису телевізійного звуку та зображення, а також аксесуари та запчастини до таких виробів). Пріоритезація експорту разом з іншими програмами сприяння розвитку допомогла «Азійським тиграм» досягти приблизного зростання реального ВВП у 8 % на рік впродовж декількох десятиліть (з середини 1960-х років до 2000 року).

Нові можливості відкриває вступ до ЄС. Співпраця з експортно-кредитними агенціями європейських країн допоможе залучити інвесторів для підготовки українських підприємств до роботи за правилами ЄС.

Україна стикається зі складним завданням відновлення економіки після війни з росією. Від відбудови і реінтеграції втрачених територій до забезпечення працевлаштування для повернутих емігрантів і підтримки бізнесу, країна потребує комплексної стратегії. Співпраця з міжнародними партнерами, включно з ЄС і фінансовою підтримкою, буде важливими факторами у відновленні та розвитку України після війни. Експорт товарів з високою доданою вартістю, інвестиції в інновації та розвиток ефективних правових процедур також відіграють ключову роль у стабільному економічному зростанні країни.

1. Журнал Forbes Україна 2023. URL: https://forbes.ua/money/yak-pisslya-viyni-ukraina-mae-vidnovlyuvati-ekonomiku-ta-biznes-velike-doslidzhennya-deloitte-15122022-10501

2. Україна – найбільш замінована країна світу: скільки української території забруднено мінами. URL: https://www.slovoidilo.ua/2023/03/02/infografika/bezpeka/ukrayina-najbilsh-zaminovana-krayina-svitu-skilky-ukrayinskoyi-terytoriyi-zabrudneno-minamy

3. 5 історій економічного успіху після війни: світовий досвід для України. URL: https://lb.ua/economics/2022/04/13/513199_5_istoriy_ekonomichnogo_uspihu_pislya.html

4. Дячкіна А. Росія завдала українській інфраструктурі збитків на понад 151 мільярд доларів – KSE. URL: https://www.epravda.com.ua/news/2023/10/4/705100

Здор Дарія Олександрівна
студентка НТУ «Дніпровська політехніка»
Науковий керівник:
Тютченко Світлана Миколаївна
кандидат економічних наук, доцент,
доцент кафедри прикладної економіки,
підприємництва та публічного управління
Національного технічного університету
«Дніпровська політехніка»

ЕКОНОМІЧНА ЗЛОЧИННІСТЬ ТА ЇЇ ВПЛИВ НА РОЗВИТОК ДЕРЖАВИ

На сьогодні питання економічної злочинності в Україні залишається дуже актуальним. За оцінками, які дають фахівці з різних куточків світу, в Україні фактично склались дві економіки: легальна, яка є контрольована державою, та нелегальна, тобто тіньова. Криміналізація економіки України гальмує розвиток підприємництва, становлення реального ринкового середовища [1].

Економіка є фундаментом в існуванні та стабільному розвитку будь-якої сучасної держави. Саме тому формування ефективної системи економічних відносин, стійкої до негативних зовнішніх впливів та водночас інтегрованої до міжнародного економічного простору, є одним із найважливіших завдань національної політики держави. Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 р. № 287/2015, визнала забезпечення економічної безпеки одним з основних напрямів державної політики України [2].

Ефективність протидії злочинності безпосередньо залежить від отримання повної та достовірної інформації щодо кількісних і якісних показників певного виду злочинів та визначення тенденцій розвитку досліджуваного феномену. Однією з проблем протидії економічній злочинності в Україні є труднощі у визначенні її кількісних та якісних показників. З одного боку, це пов’язано зі внесенням значних змін до Кримінального кодексу України (далі – КК України) щодо відповідальності за економічні злочини, з іншого – з відсутністю єдиної статистичної звітності щодо вчинених економічних злочинів.

Фахівці зазначають, що зменшення кількості зареєстрованих злочинів у сфері господарської діяльності свідчить про значне зниження активності правоохоронців у виявленні економічних злочинів. Щодо географії економічної злочинності по регіонах України, то спостерігається тенденція її поширення переважно в найбільш економічно розвинутих областях, а саме в Дніпропетровській, Одеській, Харківській, Запорізькій, Львівській та

Вінницькій областях і в м. Києві.

Серед економічних факторів аналізованого виду злочинності найбільш вагоме місце посідає низький рівень доходів населення в країні, що безпосередньо впливає на формування корисливої мотивації. За оцінками ООН на 2017 р., 80 % населення України живе за межею бідності. Крім того, фактичний прожитковий мінімум більше ніж удвічі перевищує офіційний.

Суттєвим чинником економічної злочинності в Україні залишається й високий рівень безробіття населення. За даними Державної служби зайнятості, рівень безробіття у 2016 р. становив 9,1 %, у 2017 р. – 9,9 %, а у 2018 р. – вже 10,1 % [3]. Через тривалий спад виробництва, що відбувається в багатьох галузях, постійно зростає кількість людей, які лише числяться на виробництві, а на практиці перебувають у неоплачуваних відпустках. Останні є фактично «тимчасовими» безробітними – резервом безробіття реального.

Аналіз поточних кількісних і якісних показників економічної злочинності та порівняння з відповідними даними за попередні роки загалом засвідчують наявність низки негативних тенденцій у поширенні економічних злочинів в Україні. Хоча відповідно до офіційної статистики частка економічних злочинів у структурі злочинності в нашій державі становить лише 6 %, прямі та непрямі збитки від них становлять мільярди гривень щорічно. Значні прогалини в регулюванні економічних відносин, неефективність контролю за сферою державних закупівель, лобіювання інтересів конкретних виробників, низька ефективність ужитих державою антикорупційних заходів і відсутність комплексної нормативно-правової бази протидії економічній злочинності призводять до неефективності спорадичних антикриміногенних заходів у вказаній сфері. Окрім того, негативні тенденції економічної злочинності в України значно посилюються завдяки впливу низки економічних, соціальних і політичних детермінант, безпосередньо пов’язаних із наявністю збройного конфлікту на сході України. Убачається, що встановлені тенденції економічної злочинності мають бути враховані під час розробки комплексної стратегії протидії цьому виду злочинності як важливого інструменту забезпечення економічної безпеки держави та поліпшення добробуту її громадян.

1. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: http://zakon.rada.gov.ua /laws

2. Кримінальний кодекс України. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131. URL: http://zakon.rada.gov.ua/laws

3. Глущенко В. В. Економічна злочинність , прийоми приховування і методи ії виявлення. *Вісті Кримінологічної асоціації України*. 2004. Вип 1. Харків : В-во Харк. нац. ун-ту внутр. справ. С. 173–175.

Івоніна Анна Анатоліївна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ОСНОВНІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ВОЄННОГО СТАНУ

Сьогоднішній час є переломним і випробовує стійкість України, яка потрапила у війну, що розпочалася 24 лютого 2022 року. Ця війна має не лише фізичний фронт на полі бою, але й віртуальний фронт в інформаційному просторі Інтернету. Втрати, пов'язані із загибеллю близьких, втрата домівок, безперервного заняття роботою та введення режиму воєнного стану суттєво вплинули на свідомість і поведінку населення, часто ведучи його до антиправових дій.

Однією з найактуальніших проблем є активізація інтернет-шахраїв, які використовують вразливість населення України і зацікавлених іноземців для власної користі. Ця проблема вимагає негайного втручання правоохоронних органів нашої держави. Наслідком цього стало поширення кількості кіберзлочинів, зокрема шахрайства в Інтернеті, що стало особливо актуальним у цей період.

В умовах війни і кризи важливо підтримувати правопорядок та боротьбу з кіберзлочинами, щоб захистити вразливих громадян і забезпечити стабільність в інформаційному просторі. Наша держава повинна приділити особливу увагу цій проблемі та вжити необхідні заходи для боротьби з інтернет-шахраями та кіберзлочинами, які загрожують безпеці нації [3].

Відгукуючись на стрімке зростання кіберзлочинності, Український парламент – Верховна Рада, вжила активні заходи щодо перегляду та вдосконалення кримінального та кримінально-процесуального законодавства з метою поліпшення правопорядку та збільшення ефективності переслідування злочинців, які здійснюють кіберзлочини.

Отже, внесені зміни до відповідних законодавчих актів, зокрема Закон України «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в

умовах дії воєнного стану» та Закон України «Про електронні комунікації» спрямовані на підвищення ефективності проведення переддосудового розслідування «за гарячими слідами», на посилення боротьби з кібератаками. Ці важливі зміни в законодавстві були затверджені в законах № 2137-IX від 15 березня 2022 року та № 2149-IX від 24 березня 2022 року, під час роботи в умовах введеного воєнного стану [1].

Ці дії Верховної Ради свідчать про серйозний підхід до проблеми кіберзлочинності та відображають прагнення підвищити ефективність боротьби з цими злочинами в період важливих подій для держави. Реформи в правовій сфері розкривають намір України забезпечити безпеку в інформаційному просторі та захистити цифрову інфраструктуру в умовах сучасних викликів.

Отож, підвищення ефективності протидії кіберзлочинам під час періоду війни і збільшення відповідальності за ці порушення є необхідним та давно очікуваним кроком. Новий закон розширює повноваження правоохоронних органів у справах щодо розслідування кіберзлочинів, які визначені в статтях 361 та 361-1 Кримінального кодексу України. Введення більш суворих санкцій і додаткова криміналізація окремих дій можуть відлякувати потенційних злочинців від вчинення нових злочинів [2].

Раціональним вважається також впровадження відповідальності за кіберзлочини, які вчинені під час воєнного конфлікту. Суворі покарання за такі дії відображають складні обставини в країні, оскільки особа, яка завдає шкоди національним інтересам України або громадянам в кіберпросторі, фактично сприяє агресору в цьому конфлікті і не може уникнути відповідальності, яка була б менш важкою, ніж для військових злочинців.

Сфера кіберпростору вже раніше потребувала змін та посиленого захисту. Відкрите вторгнення росії викликало необхідність у вдосконаленні чинного законодавства та забезпеченні безпеки в сучасному інформаційному середовищі. Такі дії є обґрунтованими та важливими для збереження національної безпеки в умовах цифрової війни.

---

1. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 26.09.2023).

2. Боротьба з кіберзлочинністю в умовах дії воєнного стану. 2022. URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 26.09.2023).

3. Левківська Я. І. Вплив воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні. URL: http://dspace.onua. edu.ua/handle/11300/19993 (дата звернення: 26.09.2023).

Кадірова Аріна Олександрівна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Синиціна Юлія Петрівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ПОТРЕБА ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

У сучасному світі, де технологічний прогрес швидко розвивається, інформаційні технології стають невід'ємною частиною різних сфер життя, включно з правоохоронною сферою.

Застосування інформаційних технологій у Національній поліції України є критично важливим кроком для підвищення ефективності та гласності поліцейської діяльності. Також можна додати, що дані технології забезпечують оперативність, швидкість та повноту роботи правоохоронних органів.

Інформаційна потреба – це певний стан суб'єкта службової діяльності, який виникає у зв'язку з необхідністю отримання відомостей, що забезпечують вирішення службових завдань. При цьому проблема виявлення, опису та вимірювання інформаційних потреб поліцейських стає однією з основних у комплексі проблем інформаційного забезпечення НПУ. Тільки на основі її рішення можна формулювати вимоги до інформаційно-аналітичного забезпечення. Інформаційні потреби визначають мету інформаційного забезпечення НПУ, яка полягає в наданні поліцейським інформації необхідної якості у відповідні терміни і в межах чинної технічної та організаційної структур, правового регулювання та фінансування [1].

Також можна виокремлювати основні причини, які підтримують потребу в застосуванні інформаційних технологій у поліції:

1. Поліпшення комунікації. Застосування інформаційних технологій дозволяє поліцейським швидко та ефективно обмінюватися інформацією між різними відділами та підрозділами. Це допомагає забезпечити швидку реакцію (прийняття відповідного рішення) на події та злочини.

2. Збереження та аналіз даних. Інформаційні технології дозволяють збирати, зберігати та аналізувати великі обсяги даних, що допомагає виявляти законодавчі тенденції, розробляти стратегії протидії злочинності та

забезпечувати ефективність розслідування.

3. Електронна документація. Застосування інформаційних технологій дозволяє поліцейським замінити традиційну паперову документацію на електронну форму. Це спрощує та оптимізує процес обробки та збереження інформації (створення відповідних баз даних), а також полегшує доступ до необхідної інформації [2].

4. Моніторинг та відстеження. Застосування інформаційних технологій дозволяє поліцейським вести моніторинг та відстеження злочинності, включно з використанням систем відеоспостереження, GPS- трекерів та інших технологій, а також здійснювати моніторинг змін у нормативно-правовій документації.

5. Комп'ютеризоване навчання. Застосування інформаційних технологій дозволяє поліцейським отримувати доступ до онлайн-курсів та навчальних матеріалів, що сприяє постійному професійному розвитку та підвищенню кваліфікації.

Загалом заснування інформаційних технологій у Національній поліції України допомагає поліпшити оперативну діяльність, ефективність розслідування злочинів, забезпечити ефективну взаємодію між структурами поліції, спростити процеси роботи та забезпечити безпеку громадян. Інформаційне забезпечення правоохоронної діяльності відкриває нові можливості для попередження злочинності та сприяють ефективному і точному прийняттю рішень з метою розкриття злочинів. Беззаперечно, що використання інформаційних технологій може стати чи не головним чинником зміцнення законності, забезпечення обороноздатності країни, соціально-політичної стабільності та розвитку демократичних засад в управлінні державою [3].

---

1. Іванов І. Є. Інформаційні технології в діяльності національної поліції України. *Юридична наука* 6 (108) (2020): 91-98.

2. Курс «Інформаційні та комунікаційні технології». *Дніпропетровський державний університет внутрішніх справ*. URL: https://osvita.dduvs.in.ua/md/course/view.php?id=1409 (дата звернення: 26.09.2023).

3. Лекція з дисципліни «Інформаційні системи та інформаційне забезпечення правоохоронної діяльності». *Дніпропетровський державний університет внутрішніх справ*. URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/lectures/2020/eib/N/z004.docx (дата звернення: 26.09.2023).

Капелюшний Олександр Євгенович
курсант 4-го курсу Навчально-наукового
інституту права та підготовки фахівців
для підрозділів Національної поліції
Дніпропетровський державний
університет внутрішніх справ
Науковий керівник:
Рибальченко Людмила Володимирівна
доцент кафедри економічної та
інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ

Україна переживає надзвичайно складний період своєї історії, будучи у стані війни, яка почалася 24 лютого 2022 року. У такому контексті роль інформаційної безпеки набуває важливості безпрецедентного рівня.

Інформаційна безпека стала невід'ємною складовою сучасного світу, який піддався радикальним змінам завдяки розвитку технологій та глобалізації. Україна, як суверенна держава, не є винятком і відчуває вплив інформаційних процесів на свою національну безпеку. Роль інформаційної безпеки в забезпеченні національної безпеки України набуває все більшої важливості у сучасних умовах.

Завдяки великій кількості інформації, яка тепер легко доступна завдяки Інтернету та медіа, інформаційна безпека стає ключовою складовою стратегічного управління та прийняття рішень на різних рівнях українського суспільства. Від цілісності державних секретів до захисту особистих даних громадян, від захисту критично важливої інфраструктури до боротьби з дезінформацією та кіберзагрозами, інформаційна безпека визначає успіх та стійкість України перед внутрішніми та зовнішніми загрозами [1, с. 49].

У даному контексті вивчення ролі інформаційної безпеки в забезпеченні національної безпеки України є важливим завданням для нашої країни. Це означає розуміння впливу інформаційних факторів на стан безпеки, розвиток відповідних стратегій, законодавства та технічних засобів, які дозволять зберегти національний суверенітет та захистити інтереси громадян.

За останні десятиліття концепція національної безпеки суттєво еволюціонувала і містить у собі інформаційний вимір. Інформаційна безпека стала необхідною складовою захисту суверенітету та інтересів країни в сучасному інформаційному суспільстві. У контексті війни інформаційна безпека має такі ключові аспекти. Захист інформаційних систем, мереж і даних

від кібератак і хакерських атак стає надзвичайно важливим завданням. Захист критично важливої інфраструктури, такої як енергетика та транспорт, від кіберзагроз визначає можливість функціонування країни в умовах війни.

Умови війни створюють ідеальні передумови для проведення інформаційних операцій, які можуть мати глибокий вплив на суспільство та національну безпеку. Ця характеристика відображає ключову роль боротьби з дезінформацією та фейковими новинами в умовах війни:

– *Маніпуляція громадською думкою*. Інформаційні операції можуть спрямовувати громадську думку у відповідному напрямі, створюючи сприятливу атмосферу для політичних чи військових цілей. Зміна громадської думки може впливати на стратегічні рішення, голосування та підтримку конкретних дій у війні.

– *Роз'єднання суспільства*. Дезінформація може створювати конфлікти внутрішнього характеру, роз'єднуючи суспільство за політичними, етнічними або релігійними лініями. Це може призвести до внутрішнього розколу та послаблення національної єдності.

– *Мобілізація суспільства*. З іншого боку, боротьба з дезінформацією є важливою для мобілізації суспільства на захист національної безпеки. Правильна інформація і об'єктивна оцінка ситуації сприяють підтримці урядових заходів, розумінню загроз та активної участі громадян в патріотичних зусиллях.

– *Захист від дезінформації*. Боротьба з дезінформацією вимагає розвитку інформаційної грамотності серед населення, вдосконалення медійного простору та підтримки незалежних журналістів і редакцій. Також важливою є співпраця з міжнародними партнерами для виявлення та припинення інформаційних атак [2, с. 164].

Загалом боротьба з дезінформацією та інформаційними операціями стає критично важливою частиною стратегії забезпечення національної безпеки України в умовах війни, яка вимагає комплексного та добре організованого підходу для збереження національної єдності та мобілізації суспільства на захист країни.

Також зазначимо, що забезпечення ефективної контррозвідки і розвідувальних операцій стає важливою частиною інформаційної безпеки в умовах війни. Виявлення інформаційних загроз та забезпечення захисту від них є критичним завданням [3, с. 97].

Україна має враховувати інформаційний аспект під час розробки стратегічних документів та ухваленні рішень в умовах війни. Інформаційна безпека повинна бути інтегрованою частиною національної безпеки та оборони. Створення інформаційних координаційних центрів, розвиток кіберзахисту, підвищення інформаційної грамотності суспільства – це лише декілька напрямів, які треба розглядати в контексті інформаційної безпеки.

Отже, умови війни, яка триває в Україні з 2022 року, висувають перед нашою країною особливі вимоги щодо забезпечення національної безпеки,

зокрема у сфері інформаційної безпеки. Роль інформаційної безпеки стає критичною у збереженні суверенітету та стійкості України. Інтеграція інформаційної безпеки в стратегічне планування та ухвалення рішень, а також розвиток відповідних заходів інформаційного захисту, стануть запорукою національної безпеки в умовах війни.

1. Інформаційна безпека : підручник / під ред. В. В. Остроухова. Київ : Вид-во Ліра-К, 2021. 412 с.

2. Лизанчук В. В. Інформаційна безпека України: теорія і практика : підручник. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.

3. Кавун С. В., Носов В. В., Манжай О. В. Інформаційна безпека : навч. посіб. : у 2 ч. Харків : Вид. ХНЕУ, 2018. Ч. 2. 196 с.

Карелін Єгор Віталійович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Хашев Вадим Георгійович
доцент кафедри
кримінального права та кримінології
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ДЕЯКІ АСПЕКТИ ФОРМУВАННЯ СТРАТЕГІЇ КРИМІНАЛЬНО-ВИКОНАВЧОЇ ПОЛІТИКИ У ПІСЛЯВОЄННИЙ ЧАС В УКРАЇНІ

Одним з найбільш важливих завдань сучасної кримінально-виконавчої політики є забезпечення повного нагляду за виконанням вимог чинного законодавства та рішень парламенту і уряду органами і установами виконання кримінальних покарань та їх посадовцями.

Це робиться за допомогою судових і прокурорських інстанцій, а також органів державної виконавчої влади, місцевого самоврядування, громадських об’єднань та окремих громадян, які мають відповідні повноваження згідно із законом.

Підтримка та розвиток громадської ініціативи є іншим актуальним завданням, особливо на державному рівні, де сприяють формуванню громадських об’єднань, які мають на меті поліпшення роботи кримінально-виконавчої системи України і надають їй допомогу та підтримку [1, с. 88].

Важливо також ретельно та всебічно інформувати громадськість через засоби масової інформації про роль кримінально-виконавчої системи в житті

суспільства та держави, зокрема у забезпеченні громадської безпеки та морального відродження українського суспільства.

На сьогодні після того, як Міністерство юстиції України представило свою презентацію «Реформи в пенітенціарній системі», було визначено основні проблеми в системі, визначені пріоритети реформи, а також сформульовані цілі та ключові завдання.

Різні експерти мають різні погляди щодо досягнення результатів цих років. Офіційна думка, яка підтримується численними міжнародними організаціями, стверджує, що система виконання покарань стала більш гуманною та відкритою для громадянського суспільства. Більшість вчених, які вивчають пенітенціарні проблеми, поділяють цю оцінку.

Але важливо врахувати, що реформа кримінально-виконавчої служби не має системного підходу, не враховує перспективи, ігнорує наявні проблеми, такі як окуповані території та проведення бойових дій, і не має чіткого плану реалізації поставлених завдань у цих умовах.

Серед основних недоліків реформи Міністерства юстиції України є неможливість здійснення демілітаризації та введення нового персоналу при збереженні старого, відмову від ротацій та скорочень на рівнях СІЗО та УВП, повільний процес розробки нового законодавства, відсутність належного фінансування.

Одним із способів оптимізації діяльності слідчих ізоляторів, установ виконання покарань та підприємств установ виконання покарань є розроблений Порядок оптимізації, затверджений постановою Кабінету Міністрів України від 7 червня 2017 року [2].

Важливо, щоб кримінально-виконавча політика відповідала міжнародним стандартам поводження із засудженими та реалізувала принципи прав людини.

До найважливіших завдань цієї політики належить забезпечення всебічного контролю за дотриманням персоналом УВП вимог чинного законодавства, стимулювання формування громадських об’єднань, інформування громадськості через засоби масової інформації про роль кримінально-виконавчої системи в житті суспільства та створення громадських фондів для підтримки УВП [3, с. 34].

Отже, визначення успіхів та недоліків у реалізації цілей та завдань кримінально-виконавчої політики базується на відповідності їхнього змісту гуманістичним цінностям, правовим нормам, врахуванні потреб громадян, суспільства та держави, а також на забезпеченні системної реформи кримінально-виконавчої політики в післявоєнний час у цій сфері.

---

1. Кернякевич-Танасійчук Ю. В. Кримінально-виконавча політика України : монографія. Івано-Франківськ : Прикарпат. нац. ун-т ім. Василя Стефаника, 2019. 336 с.

2. Про порядок оптимізації діяльності слідчих ізоляторів, установ виконання покарань та підприємств установ виконання покарань : Постанова Кабінету Міністрів України від 07.06.2017 р. № 396. URL: http://zakon2.rada.gov.ua/laws/show/396-2017-п

3. Кримінально-виконавча система України та її роль у розбудові правової і соціальної держави : матеріали IX заочної Всеукр. науково-практ. конф. (м. Чернігів, 17 червня 2022 р.) / гол. ред. О. М. Тогочинський; Академія Державної пенітенціарної служби. Чернігів : Академія ДПтС, 2022. 148 с.

Киричок Владислав Едуардович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

У сучасному світі, де інформаційні технології є неодмінною складовою нашого повсякденного життя, кіберзлочинність стала серйозною загрозою для суспільства. Треба констатувати, що відбулося різке набуття кримінального професіоналізму, збільшується кількість зухвалих за задумом і кваліфікованих за виконанням злочинів [2]. Кіберзлочинці використовують сучасні технології для злочинних дій, таких як шахрайство, крадіжка особистих даних, кібершантаж, дестабілізація політичних систем і багато іншого. Однак, на щастя, так само як кіберзлочинці використовують технології для своїх цілей, так і сучасні технології можуть бути застосовані для боротьби з кіберзлочинністю.

Насамперед одним з найважливіших аспектів боротьби з кіберзлочинністю є розробка сучасних кіберзахисних технологій. Компанії, урядові організації та приватні особи повинні використовувати передові системи захисту, такі як антивіруси, файрволи, системи виявлення вторгнень та інші. Ці технології допомагають виявляти та блокувати шкідливі програми та хакерські атаки, забезпечуючи безпеку інформації і мереж.

Другим важливим аспектом боротьби з кіберзлочинністю є розвиток кіберполіції та кіберслужб безпеки. Урядові органи повинні мати спеціалізовані підрозділи, які займаються розслідуванням кіберзлочинності та наданням допомоги жертвам. Крім того, співпраця між країнами є необхідною, оскільки кіберзлочинці можуть діяти з будь-якої точки світу. Спільні розслідування та обмін інформацією допомагають виявляти та притягати до відповідальності злочинців.

Третім аспектом, який необхідно враховувати, є популяризація кібербезпеки серед користувачів. Інформаційні кампанії та освітні програми повинні надавати людям необхідні знання про захист своїх пристроїв та особистих даних. Люди повинні бути усвідомлені про ризики, пов'язані з небезпечними посиланнями, ненадійними паролями та публікацією особистої інформації в мережі.

Також не треба забувати, що більшість кіберзлочинів вчиняється з корисливих мотивів, завдання держави – створити такі умови для спеціалістів, аби останні працювали на громадянське суспільство, а не проти нього. Водночас необхідно розуміти, що на кожного комп'ютерного «генія» знайдеться більш розумний, а тому викрити кіберзлочинця можна, для цього лише потрібний більш кваліфікований фахівець [1]. Міжнародні комп'ютерні мережі, такі як Інтернет, є відкритим середовищем, що дає користувачам можливості чинити певні дії за межами кордонів держав, у яких вони перебувають. Тимчасом як оперативні або слідчі дії правоохоронних органів повинні обмежуватися територією власної держави. Це означає, що боротьбу зі злочинністю у відкритих комп'ютерних мережах не можна здійснювати без належного міжнародного співробітництва [2].

Отже, застосування сучасних технологій у боротьбі з кіберзлочинністю є надзвичайно важливим завданням. Розробка кіберзахисних технологій, розвиток кіберполіції та кіберслужб безпеки, а також популяризація кібербезпеки серед користувачів – це ключові напрями, які допоможуть зменшити кіберзлочинність і забезпечити безпеку в інформаційному суспільстві.

---

1. Кіберзлочинність:: актуальна судова практика. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika

2. Боротьба з кіберзлочинністю та регулювання інтернет-відносин у країнах Європи. URL: https://referatss.com.ua/work/borotba-z-kiberzlochinnistju-ta-reguljuvannja-internet-vidnosin-u-krainah-ievropi/

Кисельова Єлизавета Юріївна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Синиціна Юлія Петрівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

НАПРЯМИ РОЗВИТКУ УКРАЇНИ ПІСЛЯ ПЕРЕМОГИ

Україна, яка переживає складний період політичних та економічних змін, демонструє важливість свого суверенітету та внутрішньої стабільності під час численних випробувань. Майбутня перемога в повномасштабній війні з російською федерацією та збереження територіальної цілісності стануть ключовими досягненнями, що дасть Україні змогу рухатися вперед у процесі розвитку. Стратегічні напрями розвитку України після перемоги повинні враховувати різноманітні аспекти, включно з економікою, політикою, соціальною сферою, освітою та міжнародними відносинами.

Після перемоги України економічний розвиток стане однією з основних пріоритетних справ. Реформування податкової системи, поліпшення інвестиційного клімату та сприяння розвитку малого та середнього бізнесу є ключовими компонентами стратегії економічного зростання [1].

Згідно з дослідженнями Світового банку та Міжнародного валютного фонду, Україна повинна продовжувати вдосконалювати адміністративні процедури для бізнесу, зменшувати корупцію та залучати іноземних інвесторів для створення нових робочих місць і підтримки сталого економічного зростання [2]. Забезпечення демократичних стандартів, підвищення прозорості та участі громадян в ухваленні рішень є важливими аспектами політичних реформ після перемоги. Наявність дієвої системи поділу влади, реформа судової системи та боротьба з корупцією є ключовими завданнями.

Україна повинна продовжити робити кроки в напрямі підвищення рівня демократії та правової держави – головна та специфічна умова для України. Не всі країни, які зробили економічний стрибок після війни, були демократіями. Свого часу Японія, Південна Корея були автократіями. Специфікою ситуації в Україні є те, що середній клас виріс ще до того, як ми підходимо до євроінтеграції та економічного стрибка. Середній клас в Україні є єдиною соціальною групою, яка створює запит на демократію. Було б дуже легко вбити цей середній клас, негайно запровадивши європейські правила, наприклад, скасувавши податкову

систему, яка сьогодні існує для ІТ-індустрії [3].

Забезпечення соціального захисту та розвитку людського капіталу є іншими важливими напрямками розвитку. Поліпшення доступу до якісної медичної допомоги, освіти та соціальних послуг, а також боротьба з бідністю та безробіттям є невід'ємними складовими розвитку суспільства.

Розвиток освіти та науки є ключовими для забезпечення конкурентоспроможності України в глобальному світі. Збільшення інвестицій у науку, створення сприятливих умов для наукових досліджень та підтримка інноваційних проектів можуть сприяти зростанню національного потенціалу [4].

За даними дослідницького центру «Разом для майбутнього», Україна має зосередити увагу на поліпшенні якості освіти, забезпеченні доступності медичних послуг та створенні сприятливих умов для розвитку дітей та молоді [2].

Українське суспільство навряд чи прийме етнічних українців, які живуть у росії. Відповідно буде потрібна велика міграція: люди іншої раси, культури, мови, релігії будуть приїжджати на постійне місце мешкання, на територію України. Враховуючи вище зазначений факт, Україні потрібні дуже потужна мова та культура, щоб дати цим людям можливість асимілюватися. Зі свого боку, в Україні виникнуть нові поняття, такі як: інклюзивність української ідентичності, суспільства, а також готовність прийняти нових людей – афроукраїнців, арабоукраїнців, узбекоукраїнців, якщо вони будуть готові стати новими українцями. Наразі не факт, що суспільство готове на це. Але дослідження відновлення української економіки показують, що саме збереження демократії та готовність прийняти нових людей є ключовими для розвитку [3].

Отже, Україна стоїть перед низкою важливих завдань після перемоги в гібридній війні, включно з економічним розвитком, політичними реформами, підвищенням якості життя громадян, підтримкою освіти та науки. Поєднання зусиль у цих напрямах допоможе Україні зміцнити своє місце у світовому співтоваристві та забезпечити сталий і процвітаючий розвиток. Реалізація цих стратегічних завдань вимагатиме від влади, громадян та міжнародних партнерів спільних зусиль та впровадження комплексних заходів.

---

1. Шпаргалка О. Вплив освітньої політики на інноваційний розвиток України. *Науковий вісник Українського державного університету фізичної культури*. 2020. № 2(49). С. 208–215; Діагностика соціально-економічного розвитку України. URL: https://together-ukraine.org/ua/diagnostics/ (дата звернення: 25.09.2023).

2. Відбудова України після перемоги: що маємо робити вже зараз. URL: https://mind.ua/publications/amp/20258907-vidbudova-ukrayini-pislya-peremogi-shcho-maemo-robiti-vzhe-zaraz (дата звернення: 25.09.2023).

3. Стратегія розвитку освіти та науки в Україні на 2021–2030 роки. URL: https://mon.gov.ua/ua/osvita/osvita-v-ukrajini/strategiya-rozvitku-osviti-ta-nauki-v-ukrajini-na-2021-2030-roki (дата звернення: 25.09.2023).

Кислиця Світлана Андріївна
студентка групи М-ЕК-221
Науковий керівник:
Синиціна Юлія Петрівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

РОЗРОБКА МОДЕЛІ ДЛЯ КОРЕЛЯЦІЙНО-РЕГРЕСІЙНОГО АНАЛІЗУ ЗАЛЕЖНОСТІ ОБСЯГУ ПРОДАЖІВ ПРОДУКЦІЇ

На основі аналізу літератури з питань оптимізації товарного асортименту підприємств можна сказати, що загальною особливістю існуючих практичних підходів є відсутність використання наукових методів формування і управління асортиментною політикою підприємства, а в окремих випадках – відсутність економічного обґрунтування доцільності ухвалених управлінських рішень.

З цих позицій, на нашу думку, певні підстави має спроба побудови економіко-математичної моделі системи формування асортименту на сучасному підприємстві. Певною мірою за допомогою подібної теоретичної побудови можливо припустити найбільш значущі змінні фактори, що впливають на цей процес. Практичне застосування подібної моделі можливе і в галузі прогнозування стану асортименту, оцінки результативності маркетингових заходів тощо.

Економічна наука давно користується моделями. Однією з перших була модель відтворення, розроблена французьким вченим Ф. Кене ще у XVIII ст. А в XX ст. перша загальна модель економіки, що розвивається, була сконструйована Дж. фон Нейманом. Значний досвід побудови Е.-М. накопичений вітчизняними вченими, які застосовували їх для аналізу економічних процесів, прогнозування і планування в усіх ланках і на всіх рівнях економіки, аж до планування розвитку народного господарства країни в цілому, особливо перспективного.

Прийнято поділяти економіко-математичні моделі на дві великі групи:

– моделі, що відображають переважно виробничий аспект економіки;

– моделі, що відображають переважно соціальні аспекти економіки.

Під економетричною моделлю розуміють рівняння регресії, яке встановлює кількісне співвідношення між обсягом реалізованної продукції промисловим підприємством та надійністю цієї продукції, а також і витрат на формування асортименту (на рекламу, брошури і тощо). Аналіз процесу формування асортименту за допомогою економетричних методів містить:

– з'ясування факторів, які можуть впливати на формування асортименту;

– формування масиву статистичної інформації;

– знаходження регресійних залежностей (побудова регресійних моделей);

– оцінка адекватності моделей, їх економічна інтерпретація і практичне використання.

Методика аналізу включає визначення двох типів залежності, а саме:

– зв'язок між конкретним видом продукції та обсягами її реалізації;

– зв'язок між ціною одного виду товарів та обсягом її реалізації.

Наявні різні способи оцінки параметрів регресії. Найбільш універсальним є метод найменших квадратів.

Регресійна модель у загальному вигляді може бути записана так:

$$Y = a + b_1 * x_1 + b_2 * x_2 , \quad (5.3)$$

де: Y – Обсяг продажів конкретного виду продукції, грн;

- a, b_1, b_2– параметри;
- x_1 – ціна на конкретний вид продукції, грн;
- x_2 – головна характеристика.

Наступним етапом визначається існування мультиколінеарності між ціною на конкретний вид товару і її головною характеристикою.

Наступним етапом за допомогою метода найменших квадратів для моделі лінійної форми знайдемо параметри a і b_1 і b_2. Системи рівнянь такого виду розглядаються за методом Крамера. Метод Крамера – спосіб розв'язання квадратних систем лінійних алгебраїчних рівнянь з ненульовим показником основної матриці.

Наступним етапом знайдемо тісноту зв'язку. Тіснота зв'язку вимірюється з допомогою індексу кореляції. Визначаємо, наскільки значним є вплив змінної *x* на *y.* Якщо зв'язок тісний, визначаємо коефіцієнт детермінації та адекватність моделі. Розрахуємо значущість індексу кореляції. Визначимо значущість параметрів a та b_1, b_2. Перевіримо модель на наявність автокореляції залишків. На основі отриманих даних знаходимо коефіцієнт *d* статистики Дарбіна-Уотсона та з використанням таблиці Дарбіна-Уотсона з обраним рівнем значущості (0,05) та n і k знаходимо значення d_L, d_U, а також визначаємо зону автокореляційного зв'язку. Розраховуються оптимістичний і песимістичний прогнози середнього обсягу реалізації при зміні однієї з незалежних змінних і незмінної другої змінної. За допомогою описаної методики моделювання оцінюється прогноз на реалізацію конкретного виду продукції на ринок.

У сучасних ринкових умовах зусилля підприємств зосереджено на забезпеченні ефективної діяльності, а також найбільш повному задоволенні попиту покупців, який значною мірою залежить від правильного формування

асортиментної політики. Формування оптимального асортименту, що сприяє оптимізації прибутку, збереження бажаного прибутку на довгостроковий період дуже актуально для підприємств, які намагаються сьогодні бути конкурентоспроможними.

1. Синиціна Ю. П., Гунько Д. Ф. Моделювання системи асортиментної політики промислового підприємства. *Ефективна економіка*. 2014. № 5.

Клименко Дмитро Олександрович
курсант 406 навчального взводу
факультету № 1
Донецького державного університету
внутрішніх справ
Габорець Ольга Андріївна
доцент кафедри
оперативно-розшукової діяльності
та інформаційної безпеки
факультету № 3 Донецького
державного університету
внутрішніх справ, доктор філософії

КРИМІНАЛЬНИЙ АНАЛІЗ І ВИЯВЛЕННЯ ЗАКОННОСТІ ДІЙ У СПРАВАХ ПРО КОРУПЦІЮ

У сучасному світі, де виклики корупції є однією з найбільших загроз для стабільності, розвитку та довіри до владних структур, проведення кримінального аналізу та виявлення законності дій у справах про корупцію стають надзвичайно важливим завданням. Корупція, незалежно від своєї форми та розміру, підриває принципи справедливості, порушує права громадян і підриває довіру до системи правосуддя та правопорядку.

Кримінальний аналіз і виявлення законності дій у справах про корупцію стали невід'ємною частиною боротьби з цим явищем у багатьох країнах світу, у тому числі й в Україні. Завдяки ретельному дослідженню фактів, об'єктивному аналізу доказів та високому професіоналізму правоохоронців, злочини, пов'язані з корупцією, можуть бути розкриті, а винуватці притягнуті до відповідальності перед законом. Корупційні правопорушення – це поширений приклад предикатних злочинів. Тому аналіз фінансових дій окремих суб'єктів працівниками правоохоронних органів дозволяє в подальшому встановити ознаки корупційних злочинів, серед яких: привласнення, розтрата майна, незаконне заволодіння майном шляхом зловживання службовим становищем, легалізація доходів, одержаних злочинним шляхом, одержання неправомірної вигоди службовою особою.

Працівники правоохоронних органів зосереджені на виявленні корупційних схем та створенні матеріалів, які можуть стати основою для подальших розслідувань.

Основними методами, якими здійснюється кримінальний аналіз, є:

1. Аналіз даних – перевірка внутрішніх документів, які зберігаються в базах даних державних органів, комерційні бази даних тощо.

2. Аналіз злочинних схем – під час розгляду злочинних схем встановлюється невідповідність між обсягом операцій і доходами учасників, виявляються нелогічні або невигідні операції, а також розглядається наявність компрометуючої інформації.

Для ефективного виконання кримінального аналізу програмне забезпечення відіграє важливу роль для працівників правоохоронних органів. У цьому контексті важливою є можливість використовувати спеціальні програмні пакети, такі як Orion Leads, розроблені компанією Orion Scientific Systems, і Watson Powercase, що пропонується компанією Hanalys. Загальними характеристиками цих програм є можливість ідентифікувати злочинні мережі [1, с. 95].

Ці програми допомагають аналізувати великі обсяги даних та виявляти зв'язки і взаємозв'язки між різними суб'єктами, що може бути корисним під час розслідування складних кримінальних справ та ідентифікації злочинних мереж.

Спеціальне програмне забезпечення goPRS та goTRACE, розроблене та запроваджене Управлінням ООН, має на меті виявлення підозрілих дій і аналізу моделей поведінки з метою запобігання можливим випадкам шахрайства та корупції у сфері державних закупівель. Ці програми допомагають забезпечити безпечне та оперативне порівняння конфіденційних даних, що зберігаються в різних базах даних однієї або декількох установ, і визначити їх взаємний збіг [2, с. 142].

Програмне забезпечення такого типу може виявляти аномалії, аналізувати дані та надавати важливу інформацію для ухвалення рішень і реагування на потенційні загрози корупції та шахрайства в закупівельних процедурах.

YouControl – це відмінний приклад вітчизняного аналітичного програмного пакету, який дає змогу отримати актуальну інформацію про компанії або фізичних осіб-підприємців з понад 30 державних реєстрів.

YouControl дає змогу отримувати дані про фінансовий стан компаній, їхню історію та структуру власності, а також інформацію про фізичних осіб-підприємців.

Успішність проведення кримінального аналізу для виявлення корупційних злочинів зумовлена здатністю аналізувати фінансові документи та розглядати злочинні стратегії, спрямовані на приховання походження доходів, одержаних шляхом злочинної діяльності.

Ми вважаємо, що запровадження програмного забезпечення в діяльність

правоохоронних органів поліпшило діяльність аналітичних підрозділів та надало більше можливостей для протидії корупційним злочинам.

1. Вільямс Ф. Мережі і мережні війни: майбутнє терору, злочинності та бойових дій / пер. з англ. А. Іщенко; за ред. Дж. Арквілли, Д. Ронфельдта. Київ : Києво-Могил. акад., 2005. 352 с.

2. Міжнародні та національні правові положення системи захисту засобів фінансової допомоги Європейського Союзу та іноземних донорів в Україні : зб. норм.-прав. актів / упоряд.: І. Кржечковськис, В. В. Тацієнко, С. С. Чернявський та ін.; за ред. В. В. Чернєя. Київ : Нац. акад. внутр. справ, 2016. 260 с.

Крипович Сергій Ігорович
слухач магістратури ННІ права
та підготовки фахівців для підрозділів
Національної поліції
Дніпропетровського державного
університету внутрішніх справ
Науковий керівник:
Ділігул Аліна Сергіївна
доцент кафедри
цивільного права та процесу,
кандидат юридичних наук

РОЛЬ ІННОВАЦІЙ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

На сьогодні в економіці нашої країни відбуваються складні процеси глобалзації. Щороку виникає досить багато великих можливостей для економічного розвитку, але якщо поглянути на це з іншого боку, то посилюються існуючі та виникають нові загрози економічній безпеці як державі, так і окремих суб'єктів господарювання. Це, як вважають вчені, є об'єктивною закономірністю активної інтеграції національної економіки у світову економічну систему і, як наслідок, її все більшої відкритості для закордонних суб'єктів економічної діяльності. У цей час дуже складно спрогнозувати, коли і які з'являться нові, та як трансформуються існуючі загрози економічної безпеки суб'єктів господарської діяльності.

Метою вивчення цього питання є інноваційні чинники в підвищенні економічної безпеки національної економіки, проаналізовано відмінності технологічної структури економіки України від технологічної структури економік інших країн світу, що дозволило встановити в Україні домінування відтворення виробництва 3-го технологічного укладу. Зазначене дозволило зробити висновок щодо значного технологічного відставання національної економіки, яке становить загрозу її економічній безпеці. Встановлено, що

інновації є основою забезпечення конкурентоспроможності на різних ієрархічних рівнях господарської системи, яка, стає чинником забезпечення економічної безпеки господарської системи.

На сьогодні немає єдиного визначення терміна «економічна безпека». Аналіз дефініцій економічної безпеки свідчить, що серед вітчизняних та закордонних вчених немає однозначного підходу до її визначення. Водночас всі поняття при всій своїй несхожості між собою мають подібні ознаки.

Під економічною безпекою підприємства розуміємо збалансованість внутрішньої структури підприємства як відкритої соціально-економічної системи, за якої воно стабільно функціонує, відтворюється і розвивається, а також підприємства гармонійно взаємодіють із зовнішнім середовищем [1].

Проблематика забезпечення економічної безпеки щороку набуває все більшого значення. Так, на думку американського психолога, засновника гуманістичної психології А. Маслоу, безпека – це одна з основоположних базових потреб людини, основна передумова виживання людства. Розвиток теорії безпеки став закономірним наслідком розвитку суспільства. Сьогодні «безпека» є міждисциплінарною категорією, що дозволяє тлумачити її дуже широко.

Також можна продемонструвати інноваційну систему у забезпеченні економічної безпеки підприємництва, яку науковець Т. Г. Васильців проілювстрував у своїй монографії.

Європейська економічна інтеграція дає нову змогу для України та її регіонів, включно із суб'єктами економічної діяльності (тільки приблизно 2 % від загальної кількості опитаних в Україні підприємців проти вступу країни до будь-яких економічних та/чи торгових об'єднань). Проте інтеграція України у глобальний та європейський економічний простір може спричинити істотні негативні соціально-економічні наслідки для держави та тих її регіонів, які не виробили власної стратегії економічної безпеки, системотворчим елементом якої є економічна безпека підприємництва, а також не забезпечили формування відповідної суспільної ідеології. Особливо важливим це завдання є в умовах відкритої міжнародної конкуренції, впливу наддержавних систем багатостороннього регулювання, зокрема СОТ, застосування єдиних для всіх суб'єктів конкурентної боротьби принципів, правил і норм [2].

На основі проведеного аналізу зроблено висновок, що економіка України потерпає від відсутності інновацій, а це знижує рівень економічної безпеки країни. Впровадження різноманітних інновацій на основі відповідної інноваційної стратегії розвитку може змінити ситуацію на краще, підвищити темпи зростання економіки країни та життєвого рівня населення. Водночас деякі інновації, що імплементуються в окремі технологічні процеси промислового виробництва та інші галузі, можуть мати негативний екологічний ефект, а також мати додаткові загрози, пов'язані з можливістю відмови технологічних вузлів. Це може призводити до техногенних катастроф і знижувати економічну безпеку країни.

У 2023 р. стан економічної безпеки України залишається складним. Водночас стосовно попереднього періоду (весна 2022 р.) у поточному оцінюванні ризики реалізації загроз економічній безпеці були нижчими. Це можна пояснити тим, що експерти оцінювали результати спостережень щодо оперативно застосованих державою та бізнесом зусиль та управлінських рішень, які дозволили диверсифікувати діяльність та адаптувати бізнес-моделі до умов воєнного стану, а також відновити (там, де це можливо) економічну діяльність, і, хоча би частково, компенсувати збитки у пріоритетних сферах для забезпечення економічної безпеки держави [3].

1. Янковець Т. М. Взаємозв'язок потенціалу, економічної безпеки та розвитку економічних систем. Актуальні проблеми економіки. 2015. № 9(171). С. 66–73.

2. Васильців Т. Г., Волошин В. І., Бойкевич О. Р., Каркавчук В. В. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : монографія / за ред. Т. Г. Васильціва. Львів : ЛКА, 2012. 237 с.

3. Актуальні виклики та загрози економічній безпеці України в умовах воєнного стану. URL: https://niss.gov.ua/sites/default/files/2023-05/executive-1.pdf

Крисько Вікторія Андріївна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ДЕРЖАВНА ПОЛІТИКА ЩОДО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ В ІНФОРМАЦІЙНИХ СФЕРАХ

Інформаційна безпека стала невід'ємною частиною національної безпеки багатьох країн. Зміни в технологічному середовищі, зростання кількості кіберзагроз, поширення фейків і дезінформації роблять інформаційний простір уразливим перед ворогами, які можуть використовувати цю слабкість для досягнення своїх цілей. Тому державна політика щодо захисту національних інтересів в інформаційних сферах стала пріоритетною задачею для багатьох урядів.

Інформаційна безпека – це стан захищеності основних інтересів особи, суспільства і держави у сфері інформації, включаючи інформаційну й телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі

як повнота, об’єктивність, доступність і конфіденційність. Інформаційна безпека є складовою національної безпеки, але особливістю інформаційної безпеки є те, що вона, як невід’ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо [1, с.10].

Державна політика щодо забезпечення захисту національних інтересів в інформаційних сферах під час воєнного стану має високий пріоритет, оскільки інформаційні ресурси можуть бути важливою складовою ведення військових дій і впливати на рішення та публічну думку. Ось деякі аспекти такої політики:

1. Цензура та контроль над інформацією. Під час воєнного стану держава може ввести певний рівень цензури та контролю над інформацією, щоб запобігти поширенню дезінформації та інформації, що може загрожувати національній безпеці.

2. Захист критичної інфраструктури. Держава повинна приділяти увагу захисту інформаційної інфраструктури, такої як електронні системи керування, комунікаційні мережі та інші важливі об'єкти, від можливих кібератак.

3. Кібербезпека. Зміцнення кіберзаходів для захисту від кіберзагроз, включно з кібератаками та кібершпигунством.

4. Інформаційна операційна діяльність. Здійснення інформаційної операційної діяльності для підтримки національних інтересів та протидії дезінформації.

5. Захист особистих даних. Збереження приватності громадян та захист їхніх особистих даних в умовах воєнного стану.

6. Співпраця з іншими країнами та міжнародними організаціями. Держави можуть співпрацювати з іншими країнами і міжнародними організаціями для обміну інформацією та ресурсами для захисту від кіберзагроз і дезінформації.

7. Розвиток кадрів. Навчання та підготовка фахівців з кібербезпеки та інформаційної безпеки для забезпечення національної безпеки.

8. Інформаційна освіта та свідомість громадян. Забезпечення того, щоб громадяни мали доступ до надійної та достовірної інформації та були свідомі ризиків дезінформації.

Ця політика повинна бути розроблена з урахуванням специфічних потреб та загроз, які існують у конкретному контексті воєнного стану. Крім того, вона повинна дотримуватися норм міжнародного права та прав людини, забезпечуючи баланс між захистом національної безпеки та збереженням основних прав та свобод громадян.

Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є: здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних

настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні [2].

Державна система забезпечення інформаційної безпеки країни являє собою організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система становить найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави в правовій державі [3, с. 209].

Для забезпечення захисту національних інтересів в інформаційних сферах держави використовують різні підходи і інструменти. Основні принципи цих заходів містять:

– Кіберзахист. Створення і розвиток кіберзахисту стає ключовим завданням для багатьох країн. Це містить у собі розробку сучасних кіберзахисних технологій, вдосконалення законодавства щодо кібербезпеки, а також співпрацю з іншими країнами у сфері кіберзахисту.

– Захист від дезінформації. Фейки та дезінформація можуть значною мірою впливати на суспільство та політичну ситуацію в країні. Для їх запобігання важливо розвивати медіаграмотність суспільства, сприяти роботі незалежних журналістів, і здійснювати моніторинг та аналіз інформаційного простору.

– Захист від кібершпигунства. Кібершпигунство може завдати серйозної шкоди національним інтересам, особливо у сфері економіки та оборони. Держави розвивають власні програми кіберзахисту для запобігання кібершпигунству та захисту важливої інформації.

Забезпечення інформаційної безпеки є ключовим завданням для будь-якої держави у сучасному світі. Зростаюча роль інформації в житті суспільства, економіці та політиці вимагає від держав усеосяжних заходів для захисту національних інтересів в інформаційних сферах. Для досягнення цієї мети держави повинні розробляти комплексні стратегії, співпрацювати міжнародно та використовувати сучасні технології, забезпечуючи таким чином стійку та ефективну інформаційну безпеку.

1. Гур'єв В. І., Мехед Д. Б., Ткач Ю. М., Фірсова І. В. Інформаційна безпека держави : навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека». Ніжин : ФОП Лук'яненко В. В. ТПК «Орхідея», 2018. 166 с. URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ.%20безпека%20держ.%20New%20booklet%201.pdf?sequence=1&isAllowed=y

2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374

3. Горник В. Г., Кравченко С. О. Механізми забезпечення інформаційної безпеки підримницької діяльності як складника інформаційної безпеки держави. *Вчені записки ТНУ імені В.І. Вернадського*. Серія : Державне управління. 2020. Т. 31 (70). № 2. С. 206–212.

Лещенко Максим Михайлович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ІНФОРМАЦІЙНА ВІЙНА ТА ВПЛИВ ЇЇ НАСЛІДКІВ НА ПОЛІТИЧНУ, ЕКОНОМІЧНУ, СОЦІАЛЬНУ, ОБОРОННУ ТА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

З 24 лютого 2023 року Україна та кожен українець відчув нові правила життя у зв'язку з воєнними діями. Вбивство мирних громадян, катування, знищення цивільної інфраструктури відбилося на кожному з нас. Однак тема «Інформаційна війна» постає перед нами частіше, військові боронять на фронті мирних людей від окупантів, так само кіберполіція боронить нашу інформаційну безпеку в інформаційному просторі. Але науковці досліджують те, як вона вплине на політичну, економічну, соціальну, оборонну та національну безпеку України в майбутньому.

У широкому розумінні інформаційна війна – це форма боротьби між державами, організаціями чи індивідуумами, яка здійснюється за допомогою інформаційних технологій та мережі «Інтернет».

Згідно з доктриною, в переліку першочергових інформаційних операцій були визначені такі основні елементи:

– дублювання розвідувальної інформації;

– дезінформація;

– психологічні операції;

– фізичне руйнування інформаційних ресурсів противника;

– напади (фізичні, електронні) на його інформаційну структуру;

– зараження комп'ютерними вірусами обчислювальних мереж, проникнення в інформаційні мереж.

Україна вперше втратила вплив на міжнародній арені та позбавилася свого ядерного статусу через поширення негативної інформації та спотворення фактів, що призвело до добровільного відмовлення від ядерної зброї.

Розвиток інформаційно-комунікаційних технологій має помітний вплив

на політичну систему. Він впливає на способи політичної комунікації, оптимізує роботу урядових інститутів, забезпечує більшу прозорість управління та можливість громадських інститутів контролювати ресурси. Проте інформаційно-комунікаційні технології також можуть створювати негативні виклики для політичного життя, включно із загрозами для особистої приватності та демократії, функціонування державних структур і політичних лідерів і партій.

Національна безпека є важливою складовою суверенітету держави, і особливу увагу потрібно приділяти функціонуванню системи забезпечення інформаційно-воєнної безпеки України. Це охоплює не лише зовнішньополітичні аспекти, а й всі сфери, які гарантують нормальне функціонування держави. Крім захисту нашого інформаційного простору, нашою метою є відстояння військової протидії агресору, в чому Україна має вже значний досвід.

В інформаційній війні з росією ключовим чинником є вплив на різні верстви населення за допомогою інформаційно-психологічних методів. Зараз інформаційна війна набула гібридний характер і полягає в застосуванні інформаційних технологій на практиці. Орієнтири у воєнній стратегії все більше переміщуються в бік практичної реалізації інформаційних технологій. При цьому інформаційно-психологічні операції, дії та акції набувають все більшого значення в досягненні політичних і воєнних цілей.

Інформаційна війна може мати значний вплив на економіку держави. Вона полягає в маніпуляції та поширенні дезінформації, фейкових новин та іншої змістовної інформації з метою впливу на суспільство, політику, економіку та інші аспекти життя. Ось деякі з можливих способів, як інформаційна війна може вплинути на економіку держави:

Вплив на інвестиції. Інформаційна війна може створювати нестабільність і невизначеність на фінансових ринках, що може призвести до зменшення інвестицій та зниження вартості активів.

Втрата довіри. Дезінформація та фейкові новини можуть підірвати довіру громадськості до уряду, фінансових установ та інших ключових інституцій. Це може призвести до зменшення споживчої довіри, що вплине на витрати споживачів і підприємств.

Вплив на кібербезпеку. Інформаційна війна може сприяти кібератакам на підприємства та урядові системи. Це може призвести до фінансових втрат, витрат на відновлення інфраструктури та втрати даних.

Зміна економічних стратегій. Уряди можуть бути змушені витрачати більше коштів на контрзаходи для боротьби з інформаційною війною, що може призвести до перерозподілу бюджетних ресурсів та зміни економічних стратегій.

Вплив на міжнародні відносини. Інформаційна війна може погіршити відносини між країнами, що може призвести до введення санкцій та обмежень на міжнародну торгівлю, що вплине на економіку.

Втрата репутації підприємств. Фейкові новини та дезінформація можуть шкодити репутації підприємств, особливо якщо вони пов'язані з інцидентами, які використовуються в інформаційній війні.

Зменшення споживчого попиту: нестабільність та невизначеність, які супроводжують інформаційну війну, можуть призвести до зменшення споживчого попиту, що вплине на обсяги продажів та прибуток підприємств.

Отже, інформаційна війна може мати серйозний вплив на економіку держави, який варіюється залежно від тривалості, інтенсивності та масштабу такої війни. Для зменшення впливу інформаційної війни на економіку важливо вдосконалювати кібербезпеку, сприяти медійній грамотності громадян та розробляти стратегії відповіді на дезінформацію.

1. Кравчук О. Ю. Інформаційна війна проти країни як індикатор рівня забезпечення політичної безпеки. 2020.

2. Сасин Г. В. Інформаційна війна: сутність, засоби реалізації, результати та можливості протидії (на прикладі російської експансії в український простір). 2019.

3. Баглікова М. Інформаційні війни і Україна. Науковий вісник Ужгородського університету. Серія : Політологія, Соціологія, Філософія. 2018. Вип. 14. С. 158–161.

4. Нові правила: інформаційна безпека під час війни. URL: http://odnb.odessa.ua/view_post.php?id=4286.

Лісовик Ангеліна Олександрівна
слухач магістратури ННІ права
та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
Прокопов Сергій Олександрович
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРОТИДІЯ КОРУПЦІЇ В УМОВАХ ВІЙНИ В УКРАЇНІ

Корупція – це загроза суспільству і державі, це явище, яке завдає шкоди повному і всебічному розвитку будь-якого суспільства. У законодавстві України під корупцією розуміється зловживання службовим становищем, дача хабаря, отримання хабаря, зловживання повноваженнями, комерційний підкуп або інше незаконне використання фізичною особою свого службового становища всупереч законним інтересам суспільства і держави з метою отримання вигоди у вигляді грошей, цінностей, іншого майна або послуг майнового характеру, інших майнових прав для себе або для третіх осіб або

незаконне надання такої вигоди зазначеній особі іншими фізичними особами [2].

Корупція підриває авторитет державної служби і боротьба з цим явищем є на сьогодні однією з найактуальніших напрямів діяльності держави [1].

І далі констатують, що сьогодні ситуація зі стимулюванням державних і муніципальних службовців йде ще гірше, ніж навіть в радянські часи. Зарплата відповідальних посадових осіб вищого рівня незрівнянна навіть з оплатою дрібних службовців комерційних банків і приватних фінансово-господарських структур. У підсумку, наприклад, міністр на свою зарплату не може за сформованими ринковими цінами щодня обідати в ресторані, купити престижну машину і квартиру, побудувати дачу, провести відпустку із сім'єю за кордоном, оплатити навчання своїх дітей в приватній школі або на платному відділенні ЗВО [3].

На порядку денному – створення та ефективне використання системи антикорупційних заходів, які повинні містити:

• послідовне застосування адміністративних регламентів у службовій діяльності службовців органів державної влади та управління;

• оптимальне визначення прав, обов'язків, а також режиму юридичного відповідальності органів публічної влади, а також їхніх службовців;

• запровадження чітких процедур ухвалення адміністративних рішень;

• використання методики аналізу правових актів щодо корупціогенності;

• глибоке та широке роз'яснення антисоціального характеру корупції та її негативних наслідків для суспільства, держави та громадян [4].

Треба зазначити, що набір коштів, спрямованих на попередження та припинення корупційних проявів у діяльності службовців органів державної влади та управління, може бути досить різноманітним. У зв'язку з цим необхідно:

• досягти засвоєння всіма службовцями своїх прав та обов'язків та їх правильного використання;

• домогтися дотримання правил службової поведінки з боку державних та муніципальних службовців;

• суворо оцінювати діяльність та поведінку службовців з антикорупційної точки зору під час прийому на роботу (призначення, конкурсів, виборів, просування по службі), а також під час проведення періодичної атестації кадрів;

• забезпечити дотримання заборони заміщати після звільнення з державної та муніципальної служби протягом двох років посади та виконувати роботи в організаціях, якщо раніше до функцій службовця належав контроль за ними [2].

Дійсно, як показують сучасні наукові дослідження в галузі психології, подвійний моральний стандарт є важливою особливістю соціально-психологічного клімату в суспільстві. З одного боку, корупція, особливо у вищих ешелонах влади, вважається суспільно-неприйнятною [4]. Це всіляко

підтримується і повсякденною мораллю, і засобами масової комунікації, і політичною практикою, яка експлуатує антикорупційну тематику в особистих або групових (корпоративних) цілях [2].

З іншого боку, корупція, особливо низова (а точніше, «побутова»), є прийнятною частиною побуту нашого суспільства і пояснюється деякими вітчизняними фахівцями «культурними» традиціями або склалися соціальними стереотипами поведінки. У побутовій сфері життєдіяльності такий підхід до корупційного поведінки суспільством і окремими особами виправдовується сформованими традиціями в органах і установах, які обслуговують більшість населення [4].

Вихідці з таких органів і установ, проникаючи в федеральні і регіональні владні структури, приносять з собою в політичну сферу життя суспільства корупційну психологію і «культуру колективів цих органів і установ, яку в подальшому намагаються «прищеплювати» (поширювати або впроваджувати) і в органах державної влади і місцевого самоврядування, і в підконтрольних (підзвітних) установах, підприємствах, організаціях, і в політичних громадських організаціях, перетворюючи отриману владу в економічний капітал, а державну чи муніципальну посаду в джерело отримання постійного нелегального доходу.

---

1. Білецький А. В. Корупція у приватному секторі та роль громадськості у її запобіганні. Проблеми законності : зб. наук. пр. / відп. ред. В. Я. Тацій. Харків : Нац. юрид. ун-т імені Ярослава Мудрого. 2016. С. 157–166.

2. Згідно з дослідженнями EY, керівникам не вдається ефективно формувати принципи ділової етики. URL: https://utka.su/vWSB1

3. Index of economic freedom. URL: https://www.heritage.org/index/ranking/; Опитування Американської торгової палати показало ставлення українських бізнесменів до боротьби з корупцією. URL: http://tyzhden.ua/News/161979

4. Дослідження Національного агентства з питань запобігання корупції. URL: https://nazk.gov.ua/sites/default/ffles/docs/mzk_files/ doslidzhennya/8.pdf

Лукомська Аліна Андріївна
слухач магістратури ННІ права
та підготовки фахівців для підрозділів
Національної поліції
Науковий керівник:
Гребенюк Андрій Миколайович
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ РОЗКРИТТЯ ЗЛОЧИНІВ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Розкриття будь-якого кримінального правопорушення неможливе без роботи з різними видами слідів. Як відомо, робота зі слідами містить декілька етапів, а саме: виявлення, фіксація, вилучення, дослідження, оцінка та використання. Відповідний процес відбувається не швидко, а тому займає достатню кількість часу. Адже без правильної роботи на перших трьох, тобто без грамотного, процесуально правильного збирання слідів, неможливе повне дослідження та використання у процесі доведення.

Сліди біологічного походження у цьому сенсі дуже специфічні та робота з ними має низку особливостей. Складність роботи зі слідами біологічного походження полягає в тому, що вони можуть дуже швидко змінюватися, зазнаючи деструктивних змін, що унеможливлює їх використання і для вирішення ідентифікаційних завдань. Сліди біологічного походження можуть бути утворені кров'ю, спермою, слиною тощо. До них належать також волосся, органи та тканини людського організму, кістки та їх фрагменти. Джерелом слідів біологічного походження є тіло людини, її органи. Але до цього моменту ніхто з науковців-криміналістів у своїх численних працях та наукових дослідженнях не розкривав можливість використання новітніх технологій для перенесення інформації, яка знаходиться у пам'яті померлого (жертви, очевидця) способом оцифровування мозку та перенесення відповідної інформації у цифровому вигляді на диск, де він зберігатиметься до застосування комп'ютерних програм аналізу оцифрованих зрізів мозку для детального відтворення ситуації та подальшого з'ясування обставин з метою розкриття злочину, а отже знаходження та покарання винного. Цей варіант став би справжнім проривом у криміналістичній науці, а також гарною можливістю швидкісного розкриття злочинів зі стовідсотковим визначенням винного без

довготривалого знаходження очевидців, допитів свідків та проведенням численних експертиз.

Варто зазначити, що на сьогодні науково-технічний прогрес набув настільки величезного розмаху, що передумови щодо змін в природі людського життя не змушують себе чекати. Адже мозок людини і обчислювальних машин деякою мірою схожі між собою. Тому й думки про можливість їх об'єднання виникають все частіше.

Можемо стверджувати, що перенесення свідомості теоретично можливе, але лише вже з мертвого мозку, оскільки об'ємна і заплутана архітектура мозку не дозволяє проникнути будь-якому томографу до ділянок пам'яті мозку, що не складно зробити вже з мертвим мозком, але з архітектурою синаптичних зв'язків, що зберігається у ньому, яку вдається зберегти при швидкій його заморозці.

Процес завантаження свідомості (англ. Mind uploading) є гіпотетичною технологією сканування і мапування головного мозку людини, що дозволить перенести свідомість і підсвідомість людини в іншу систему, на якийсь інший носій, можливо, цифровий (наприклад, комп'ютер зі штучною нейронною мережею) [1].

Мозок людини містить приблизно 86 мільярдів нейронів. Як вже зазначалося раніше, кожен нейрон окремо пов'язаний з іншими нейронами через з'єднувачі, а саме аксони і дендрити. Сигнали в моменти (синапси) з'єднання передаються шляхом виявлення хімічних речовин, відомих як нейромедіатори. Встановлений нейрофізіологічний консенсус полягає в тому, що людський розум являє собою емерджентність обробки інформації даної нейронної мережі [2].

Видатні вчені-програмісти і неврологи передбачили, що спеціально запрограмовані комп'ютери будуть здатні мислити і навіть зможуть досягти свідомості. Незважаючи на те, що завантаження впливає на загальні можливості, воно концептуально відрізняється від загальних форм в тому, що є результатом динамічної реанімації інформації, яка була одержана від конкретного людського розуму, так що розум зберігає почуття історичної самобутності. Перенесена і відновлена інформація стане формою штучного інтелекту.

Багато теоретиків представили моделі мозку і встановили діапазон оцінок обсягу обчислювальних потужностей, необхідних для часткової і повної симуляції. Використовуючи ці моделі, вчені підрахували, що завантаження свідомості може стати можливим протягом десятиліть, якщо такі спостереження, як Закон Мура, будуть проводитися і надалі.

У теорії, якщо інформацію і процеси розуму можна відокремити від біологічного тіла, вони більше не будуть прив'язані до окремих меж і тривалості служби цього органу. Крім того, інформація в мозку можу бути частково або повністю скопійована або передана одному або кільком іншим субстратам (у тому числі для цифрового зберігання), тим самим, з механічного

погляду, відбудеться зниження або усунення «ризику смертності» такої інформації.

Проте цей процес повинен обов'язково відповідати деяким особливостям. Адже після смерті свідомості пам'ять зберігається в мозку приблизно 12 годин при кімнатній температурі у вигляді певної щільності рецепторів на синапсах нейронів. Рецептори при житті мозку реагують на нейромедіатор глутамат у його різних концентраціях, де зміни всього в 1 рецептор, на площі в 1 мікрон на мембранах дендритів нейронів вже змінює характеристики пам'яті, що зберігається всередині нейрона.

Пам'ять нейрона з ділянок із сірою речовиною мозку – це нейромедіаторна постсинаптична відповідь певної концентрації глутамату до сусідніх нейронів, що виникає при внутрішньойронній синхронізації візикул на відгук, що надходить від рецепторів цього нейрона, який відгукується на нейромедіатор передсинаптичних нейронних зв'язків. Пам'ять нейрона здатна змінюватися, якщо нейрон зазнає змін у щільності глії, що оточує нейрон, при одночасному повторенні величини передсинаптичного сигналу, якому піддається цей нейрон [3, с. 124].

Тож пам'ять з оцифрованого мозку можна перенести спочатку лише в цифровому вигляді на диск, де він зберігатиметься до появи комп'ютерних програм аналізу оцифрованих зрізів мозку, тому що комп'ютер не здатний у принципі на повноцінне аналітичне мислення, як людський мозок, а лише на обробку інформації за заздалегідь створеним програмістами алгоритмом. Ідея полягає в тому, що після сканування мікроскопом мікронних зрізах шарів мозку, отриманих нарізанням мозку на мікронні шари, створюється карта мозку з повним описом на ній щільності рецепторів на дендритах.

Труднощі сканування мозку на цей час полягає в тому, що неможливо швидко здійснити аналіз нейронних мереж, використовуючи сучасні комп'ютерні програми, бо сучасні, навіть гібридні штучні нейронні мережі, не здатні працювати з великим обсягом даних, а сама карта мозку складається протягом 6 років. Тому без тимчасової заморозки мозку при процедурі завантаження свідомості не обійтися, але можна не складати комп'ютерну карту мозку, а обійтися фотографіювання зрізів з мозку. Зберігання об'ємних фотографій зрізів з мозку, отриманих при фотографуваннях цих зрізів під різним кутом, дало змогу зберегти пам'ять мозку в хмарному сховищі або на компакт-диску.

Необхідні мікроскопи, що спеціалізуються лише на вивченні мозку, потрібні програми, які вміють відділяти рецептори в цій каші глії та нейронів і співвідносити їх з іншими зрізами, формуючи загальну картину розташування нейронів, аксонів, дендритів і тип нейронів, до яких належать рецептори. Тип рецептора відокремлювати особливої потреби немає, головне знати який тип нейронів.

Узагальнюючи усе вищевикладене, варто наголосити на тому, що точна комп'ютерна симуляція людського мозку дозволить вченим краще зрозуміти

принципи, за якими він діє, і розібратися в механізмах розвитку психічних розладів серійних убивць для подальшого запобігання вчинення злочинів. Крім того, штучний аналог стане ідеальним об'єктом для випробувань нових методів розслідування злочинів. Оскільки повне зчитування пам'яті в мозку жертви дасть працівникам правоохоронних органів змогу дуже швидко розкрити те чи інше кримінальне провадження. Вважаємо, що наше дослідження може стати підґрунтям для подальшого розвитку відповідної проблематики у галузі криміналістики. Ми впевнені, що з розвитком новітніх технологій у кожній криміналістичний лабораторії працівники зможуть з легкістю зчитувати усю необхідну інформацію з мозку жертви за короткий період часу, без потреби збирати та досліджувати неабияку кількість слідів, що значно полегшить та прискорить процес виявлення винного, а отже, забезпечить запобігання нових смертей, що є дуже важливим, адже життя людини є найвищою соціальною цінністю.

1. Завантаження свідомості. *Вікіпедія.* URL: https://cutt.ly/mwDuTcAS (дата звернення: 05.10.2023).

2. Головний мозок людини. *Вікіпедія*. URL: https://cutt.ly/MwDuYuQD (дата звернення: 05.10.2023).

13. Галян І. М. Психодіагностика : навч. посіб. Київ : «Академвидав», 2009. 463 с.

Мінченко Олександра Вікторівна
слухач магістратури ННІ права
та підготовки фахівців для підрозділів
Національної поліції
Науковий керівник:
Прокопов Сергій Олександрович
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

ПРОБЛЕМНІ ПИТАННЯ РЕАЛІЗАЦІЇ МЕХАНІЗМУ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ

Сьогодні у світі велика увага приділяється дослідженню проблеми кіберзлочинності через об'єктивні процеси розвитку інформаційно-телекомунікаційних технологій. Останніми роками держави всього світу дедалі більше розглядають кіберпростір як один з найважливіших аспектів безпеки, оскільки захист інформації стає ключовим фактором для розвитку економіки, соціальних сфер, військової безпеки та інших секторів. Кіберзлочинність стала однією з п'яти найпоширеніших форм економічних

злочинів в Україні. Зараз боротьба з кіберзлочинністю є однією з актуальних і глобальних проблем. Постійне удосконалення інформаційних технологій стає фактором, який відкриває нові можливості для здійснення таких злочинів, і, відповідно, вони створюють загрозу для глобальних мереж та суспільства в цілому.

Проте для ефективної кібероборони, яка активно формується, потрібна побудова відповідної системи правового регулювання. Подолання правопорушень у кіберпросторі та активна кібероборона під час воєнного стану потребують нових підходів і методів, вдосконалення чинного законодавства у цій галузі та вивчення проблемних аспектів роботи правоохоронних органів у сфері розслідування кіберзлочинів і протидії кібероперaціям держави-агресора [1, с. 109].

Після відкритої агресії рф у 2022 році виникли нові виклики, пов'язані з кібервійною. Треба зауважити, що активна фаза гібридної війни в інформаційному просторі України почалася ще під час анексії Криму. Після 2014 року почалися кібератаки на об'єкти критичної інфраструктури України, які були здійснювані різними кібергрупами, що мали підтримку урядових структур держави-агресора. Серед таких об'єктів можна вказати ЦВК, Закарпаттяобленерго, Бориспільський аеропорт, Укрзалізниця, банківські установи та інші. Але науковці вказують, що справжні військові кібероперації відбувалися перед початком та під час військових дій рф. У звіті Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України «Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» вказано, що «протягом 2022 року Державним центром кіберзахисту було зафіксовано в 2,8 рази більше кіберінцидентів, ніж у 2021 році» [2].

Важливо зазначити, що основні труднощі у національній політиці щодо протидії кіберзлочинності в Україні, які уповільнюють та обмежують її ефективність, пов'язані із законодавчою базою. Зокрема, це стосується недостатньої чіткості або відсутності визначення термінів, пов'язаних з кібербезпекою, що призводить до складнощів у регулюванні таких злочинів в юридичному вимірі. Крім того, важливою проблемою є відсутність прогресу у розвитку кіберзахисту з боку держави у кіберпросторі, а також відсутність ефективної співпраці між державою та приватним сектором у цій сфері. Іншим аспектом відсутності прогресивного розвитку є відсутність ініціативи з боку держави у створенні висококваліфікованих кадрів у галузі інформаційних технологій. Освіта в цій сфері надається за плату, що може призвести до відтоку кваліфікованих спеціалістів за кордон. Вирішення цих проблем визначає перспективи подальшого розвитку кібербезпеки в Україні. Якщо всі вищеописані труднощі будуть вирішені, то перспективи кібербезпеки в Україні будуть високими. Роль міжнародного співтовариства у протидії кіберзлочинності регулюється законами України та в межах її компетенції [3].

Отже, законодавча основа для системи механізмів, спрямованих на

ефективну боротьбу з кіберзлочинністю в умовах воєнного стану в нашій державі, вже є. Тому сьогодні головною метою всіх державних органів і громадян повинна стати реалізація цих механізмів. Шляхи подолання інформаційної війни, яку рф веде проти України, містять у собі створення потужної системи кіберзахисту на рівні держави та у всіх секторах суспільства, починаючи з урядових органів і закінчуючи приватним бізнесом та населенням.

1. Гуцалюк М. В. Особливості протидії кіберзлочинності під час воєнного стану. *Інформація і право*. 2023. № 3 (46). URL: http://il.ippi.org.ua/article/view/287212 (дата звернення: 26.09.2023).

2. У 2022 році кількість зареєстрованих кіберінцидентів виросла майже втричі: звіт. URL: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtr ichi-zvit (дата звернення: 26.09.2023).

3. Лавник А. М., Мороз А. С. Державна політика протидії кіберзлочинності в умовах інформаційної війни рф проти України. URL: https://dspace.nau.edu.ua/bitstream/NAU/60360/1/%d0%9b%d0%b0%d0%b2%d0%bd%d0%b8%d0%ba%20%d0%b4%d0%b8%d0%bf%d0%bb%d0%be%d0%bc.pdf (дата звернення: 26.09.2023).

Морозова Яна Олександрівна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Неклеса Олександр Вікторович
старший викладач кафедри
кримінального процесу та
стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ

ПРОЗОРІ ЗАКУПКИ: МІЦНА ЛАНКА В ЛАНЦЮГУ БОРОТЬБИ З ЕКОНОМІЧНОЮ ЗЛОЧИННІСТЮ

Економічна злочинність завжди становила серйозну загрозу для суспільства та національної економіки. Особливо актуальною ця проблема стає під час військових конфліктів, коли зростає ризик корупції та незаконних фінансових операцій. Однак є інструменти, які можуть допомогти запобігти економічній злочинності та забезпечити прозорість і ефективність державних витрат. Ми розглянемо важливість прозорих закупівель як потужної ланки в ланцюзі боротьби з економічною злочинністю. Прозорі закупки – це законодавчі та адміністративні заходи, спрямовані на забезпечення відкритості та доступності інформації про всі процедури закупівель, від

планування до укладення договору. Це означає, що громадяни, журналісти, аудитори та інші зацікавлені сторони можуть відстежувати та перевіряти кожен етап закупівельного процесу. Такий відкритий підхід допомагає запобігти корупції, оскільки він ускладнює можливість відмивання грошей та незаконного збагачення.

Однією з головних переваг прозорих закупок є те, що громадяни можуть брати участь у моніторингу витрат державних коштів. Громадяни та громадські організації можуть вносити пропозиції, аналізувати процедури закупівель, а також виявляти порушення та незаконні дії. Це створює додатковий тиск на учасників процедур закупівель та зменшує ймовірність корупційних схем. Прозорі закупки також сприяють розвитку підприємництва та конкуренції. Коли всі учасники ринку мають рівний доступ до інформації про закупівлі, це стимулює конкуренцію, допомагає знижувати ціни та підвищувати якість товарів і послуг. Зі свого боку, бізнес може брати участь у відкритих тендерах замість того, щоб покладатися на закриті домовленості.

Прозорі закупки допомагають забезпечити ефективне використання бюджетних коштів. Коли процес закупівель є відкритим та прозорим, замовникам легше визначити найкращі пропозиції та вибрати найвигіднішого постачальника. Це робить можливим отримання кращої вартості предмета закупівлі за державні кошти та забезпечує оптимальне використання обмежених ресурсів. Економічна стабільність великої країни часто залежить від того, наскільки добре управляються публічні фінанси. Прозорі закупки є важливою складовою такого управління. Вони допомагають запобігти витратам та втратам, пов’язаним з некоректними закупками, і сприяють збереженню економічної стабільності.

З вище зазначеного можна зробити висновок, що прозорі закупки є міцною ланкою в ланцюгу боротьби з економічною злочинністю. Вони частково допомагають запобігти корупції, залучати громадян до контролю цієї сфери та розвивати підприємництво. Варто наголосити, що запровадження такої системи потребує державних реформ та волі до зміни законодавства. Проте результати, яких можна досягти, зроблять суспільство більш стійким до економічної злочинності та корупції, особливо в умовах військового конфлікту.

1. Василинчук В. І. Удосконалення кримінальної відповідальності за злочини у сфері державних закупівель. *Науковий вісник НАВС*.

2. Про публічні закупівлі : Закон України від 25.12.2015 № 922-VIII. URL: https://zakon.rada.gov.ua (дата звернення: 21.09.2023).

3. Кубецька О. М., Лазарєв В. О., Неклеса О. В., Палешко Я. С., Санакоєв Д. Б. Дії працівників поліції у разі виявлення економічних злочинів : метод. рек. Дніпро : ДДУВС, 2020. 76 с.

Нагорна Дарія Андріївна
курсант ННІ права та підготовки фахівців
для підрозділів Національної поліції
Неклеса Олександр Вікторович
старший викладач кафедри
кримінального процесу та
стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ

ОСОБЛИВОСТІ ПІСЛЯВОЄННОГО ВІДНОВЛЕННЯ ЕКОНОМІКИ УКРАЇНИ

З урахуванням воєнних дій, що відбуваються на території України, довелося провести серйозну реструктуризацію національної економічної системи. Необхідно наголосити, що активні бойові дії не просто обмежують функціонування певних галузей, а швидше призводять до неможливості нормальної роботи цих секторів. Війна негативно впливає на потенціал країни.

Сьогодні, в умовах активних глобалізаційних процесів, наша країна втрачає різні ресурси та інфраструктуру, втрачає людський капітал, фінансові можливості і рівень конкурентоспроможності. Однак варто зазначити, що війна також відкриває перед Україною певні можливості, зокрема в контексті перенаправлення на нові ринки, пошуку надійних союзників та торговельних партнерів у глобальному економічному просторі і зменшення залежності від країни-агресора.

Після завершення воєнного конфлікту Україна може розпочати широкомасштабне відновлення своєї економіки. Вчені, що досліджують питання економічного відновлення країн після конфліктів, загалом вказують на те, що кожна спроба реконструкції є унікальною [1, с. 42]. Це відновлення повинно базуватися на Плані, розробленому урядом України та підтримуваному міжнародними донорами. Очевидно, що сталий економічний розвиток можливий лише за наявності міцного фундаменту у сфері безпеки. Забезпечення безпеки є суспільним завданням, яке повинно бути здійснюване як державою, так і міжнародною спільнотою. Забезпечення безпеки вимагатиме комплексного підходу і спрямування безпосередньо у таких напрямах, як зміцнення правопорядку, реконструкцію і відновлення територій, а також міжнародну підтримку.

Отже, можна виділити Міжнародні інституції, які стануть джерелами фінансування (переважно кредитів) та здатні будуть брати участь у реконструкції України. До них можна віднести: Європейський інвестиційний банк (ЄІБ), Європейський банк реконструкції та розвитку (ЄБРР), Світовий банк (СБ), а з боку гуманітарної підтримки – Організація об’єднаних націй

(ООН) та організації, такі як «Лікарі без кордонів», можуть надавати необхідну допомогу. Міжнародний валютний фонд (МВФ) може надавати короткострокове фінансування, щоб забезпечити доступ до іноземної валюти та покрити тимчасовий фіскальний дисбаланс [2].

Відновлення України відіграє важливу роль у забезпеченні стабільності і миру в Європі. Аналізуючи міжнародний досвід у відновленні країн після конфліктів, можна зазначити, що етап післявоєнної реконструкції повинен бути максимально ефективним і надійним як для національного суспільства, так і для міжнародних донорів. Це особливо важливо, з урахуванням бажання України вступити до Європейського Союзу і дотримуватися зеленого шляху розвитку.

1. Покровська Н. М. Концептуальні засади післявоєнного відновлення України, економічні аспекти. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2022. № 4 (274). С. 41–47.

2. The United Nations. URL: http://www.un.org.

Наумов Георгій Едуардович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

БОРОТЬБА З ШАХРАЙСТВОМ ПІД ЧАС ВІЙСЬКОВОГО СТАНУ В УКРАЇНІ

В Україні з 24 лютого 2022 року йде не тільки війна з агресором, а й посилена боротьба з кіберзлочинністю, зокрема інтернет-шахраями, які з 24 лютого активізували свою діяльність і користуються довірою громадян та небайдужими іноземцями. Це велика проблема, з якою зараз веде боротьбу наша правоохоронна система.

Відповідно до ч. 1 ст. 190 Кримінального Кодексу України шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою [1]. Шахрайство – це кримінально карне діяння, відповідальність за яке в Україні передбачена Кримінальним кодексом [2, с. 547].

Серед найпоширеніших схем шахрайства у військовий час можна

відокремити: оголошення про уявне чи вже займане житло для осіб, які вимушені покинути власні будинки, фейкові перевезення та квитки для в'їзду в місто, недійсні талони на паливо, маніпуляції з продажу затребуваних під час війни товарів, надання недостовірної інформації про родичів, полонених військових, різні збори в соціальних мережах на допомогу військовим, постраждалим особам [3]. Також можна виділити такі види шахрайства, які прямо пов'язані з військовими діями: евакуаційні перевезення з прифронтових територій, компенсаційні гроші від держави, грошова допомога від ООН, де потрібно сплачувати державне мито для отримання коштів тощо.

Для ефективної боротьби з кіберзлочинністю в Україні, за прикладом іноземних держав, потрібно: створити політичний фундамент (концептуальний рівень), вдосконалити законодавчу систему (законодавчий рівень), створити систему органів, основні функції яких полягають у забезпеченні захисту України від кіберзлочинності [4, с. 54]. У 2016 році було зроблено перші кроки до розробки політичної основи та тематичної системи забезпечення кібербезпеки. Зокрема, на концептуальному та інституційному рівні у березні 2016 року Уряд України затвердив Стратегію кібербезпеки України, її метою було створення національної системи кібербезпеки; у червні 2016 року Президент України підписав Указ про створення Національного координаційного центру з кібербезпеки. Першим етапом його роботи був аналіз і розробка галузевих індикаторів стану кібербезпеки; у вересні 2016 року Верховна Рада України ухвалила в першому читанні Закон «Про Основи забезпечення кібербезпеки України» [5, с. 124].

У процесі реагування на швидке зростання рівня кіберзлочинності Верховна Рада України провела оптимізацію кримінального та кримінально-процесуального законодавства, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності кіберзлочинців. Було внесено зміни до відповідних законів: «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» з питання підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15 березня 2022 року № 2137-IX та «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 року № 2149-IX [6; 7].

Зважаючи на вище вказане, робимо висновок, що через воєнний стан в Україні інтернет-шахраї активізували свою діяльність і, на жаль, від цього потерпають наші вразливі верстви населення: пенсіонери та підлітки. У більшій своїй частці не тому, що не обізнані про шахраїв, а тому, що кожен день виникають нові методи обдурення людей та введення їх в оману. Наша правоохоронна система кожен день активно з цим бориться, але в умовах воєнного стану це дуже складно, а іноді навіть неможливо.

1. Кримінальний Кодекс України в редакції Закону № 3233-IX від 13.07.2023. URL:

https://zakon.rada.gov.ua/laws/show/2341-14#Text(дата звернення: 25.09.2023).

2. Поняття та види шахрайства. URL: https://uk.wikipedia.org/wiki/Шахрайство (дата звернення: 25.09.2023).

3. Діброва Т. А., Пісенко Д. О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. URL: https://doi.org/10.32782/2524-0374/2022-11/132

4. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. Київ : КИТ, 2010. 148 с.

5. Голубєв В. О. Розслідування комп'ютерних злочинів : монографія. Запоріжжя : Гуманітарний університет «ІДМУ», 2003. 296 с.

6. 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 : Закон України від 15.03.2022 № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 25.09.2023).

7. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 25.09.2023).

Паншин Володимир Олегович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Синиціна Юлія Петрівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

РИЗИКИ ТА НАПРЯМИ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ В УМОВАХ ВІЙНИ

Умови війни завжди становлять суттєвий виклик для економічної безпеки держави. Військові конфлікти та загрози війною можуть миттєво та серйозно підірвати стабільність економіки та соціальної сфери. Ця наукова теза розглядає ризики, які супроводжують економіку держави в умовах війни, пропонує напрями забезпечення її економічної безпеки. Метою дослідження є аналіз і оцінка впливу військових конфліктів на економічну сферу держави, ідентифікація ключових ризиків та визначення напрямів стратегії, які можуть допомогти державі забезпечити економічну безпеку в умовах війни.

Найвагомішими загрозами економічній безпеці під час війни є ті, які найчутливіші до руйнівних наслідків війни. До таких факторів можна віднести:

– зменшення трудового потенціалу;

– фізична або фінансова нестача найбільш важливих ресурсів матеріально-технічного забезпечення.

До наступної групи загроз можна віднести такі, які стосуються спроможності швидкого відновлення та можливості оперативного послаблення, накопичених у період війни, дисбалансів.

Також до загроз можна віднести фактори невизначеності, які формуються внаслідок перебігу повномасштабного вторгнення, а саме:

– унеможливлення здійснення економічної діяльності на значних територіях;

– небезпеки та невизначеності у функціонуванні логістичних маршрутів;

– різного потенціалу диверсифікації виробничих та господарських процесів унаслідок географії ведення бойових дій; тощо.

Ризики для економічної безпеки держави під час війни можна поділити на такі категорії:

– втрати виробництва та інфраструктури;
– фінансові втрати та інфляція;
– зовнішньоекономічні відносини та міжнародна торгівля;
– втрати робочої сили та соціальні проблеми.

До основних напрямів стратегії забезпечення економічної безпеки в умовах війни можна віднести такі:

1. Роль влади та державних інституцій (в реалізації стратегії економічної безпеки в умовах війни влада та державні інституції відіграють критичну роль).

2. Мобілізація ресурсів та резервів (для фінансування військових операцій та відновлення економіки в умовах війни держава може мобілізувати фінансові ресурси. Це містить у собі видання державних облігацій, збільшення податків, використання золотовалютних резервів та залучення іноземних інвестицій. Також для забезпечення стабільного постачання енергії, включно з нафтою, газом та електроенергією, є критичним. Держави можуть активувати стратегічні резерви та регулювати енергетичний сектор для забезпечення безперебійного постачання).

3. Внутрішні та зовнішні інвестиції. Внутрішні інвестиції:

– забезпечення військових потреб: держава може інвестувати у виробництво військового обладнання та матеріалів для потреб оборони;

– реконструкція та відновлення, а саме інвестиції у відновлення зруйнованої інфраструктури, зокрема будівництво доріг, мостів, шкіл та лікарень, можуть бути критичними для відновлення нормального життя та функціонування економіки.

Зовнішні інвестиції:

– зовнішні фінансові ресурси, а саме держава може залучати іноземні інвестиції та фінансову допомогу для фінансування військових операцій та

відновлення;

– технологічні інвестиції, а саме іноземні технологічні компанії можуть інвестувати в дослідження та розвиток для підвищення військової та економічної потужності країни;

– торгівельні відносини, а саме збереження та розвиток зовнішньої торгівлі є важливим аспектом економічної безпеки.

4. Створення системи соціального захисту:

– соціальні виплати, а саме забезпечення грошової допомоги та підтримки для людей, які постраждали внаслідок війни, включно з військовослужбовцями, внутрішньо переміщеними особами та родичами загиблих або поранених;

– медична допомога, а саме забезпечення доступу до медичної допомоги та лікування для поранених та хворих осіб;

– соціальні послуги, а саме надання соціальних послуг для вразливих категорій населення, таких як діти, літні громадяни, люди з інвалідністю та ін.;

– психологічна підтримка, а саме надання психологічної підтримки для тих, хто пережив воєнні події та травматичні досвіди.

Якщо розглядати практичні приклади та аналіз впливу відомих війн на економічну безпеку країни, то потрібно відмітити таке: вплив Першої та Другої світових війн (обидві війни призвели до значного зруйнування інфраструктури, включно з містами, дорогами, заводами та іншими об'єктами. Це створило великі втрати і вимагало масштабних зусиль для відновлення. Війни спричинили спад виробництва в багатьох країнах через перерозподіл ресурсів на військові потреби та економічну нестабільність та інфляцію).

Зважаючи на історичний досвід та аналізуючи сучасні світові конфлікти (Україна, Сирія, тощо), можна визначити основні економічні ризики:

– велика кількість біженців та внутрішньо переміщених осіб може створити гуманітарну кризу, яка потребує фінансових та людських ресурсів для надання допомоги;

– для фінансування військових операцій та гуманітарної допомоги держави можуть взяти позики або видати облігації, що призводить до збільшення державного боргу;

– нестабільність та небезпека в конфліктних регіонах можуть відлякувати інвесторів, що призводить до втрати можливостей для економічного розвитку.

Отже, аналіз ризиків та визначення напрямів забезпечення економічної безпеки держави в умовах війни є критично важливим завданням для будь-якої держави.

---

1. Гнатенко В. Основні складові економічної безпеки держави *Науковий вісник : Державне управління*. 2021. №1 (7). С. 66–82.

2. Методичні рекомендації щодо розрахунку рівня економічної безпеки України: наказ Міністерства економічного розвитку і торгівлі України від 29.10.2013 № 1277. URL: https://zakon.rada.gov.ua/rada/show/v1277731-13#Text (дата звернення: 24.09.2023).

Петрушин Олексій Вікторович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Синиціна Юлія Петрівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ: СУТНІСТЬ ПОНЯТТЯ

Бурхливий розвиток інформаційно-аналітичної діяльності (ІАД) у вітчизняних державних і комерційних установах набув ознак однієї з істотних тенденцій останнього часу. Його реалізація зумовлена певними об'єктивними чинниками: з одного боку, це демократизація суспільного життя, розвиток ринкових відносин, легітимність, стрімкий розвиток підприємницької діяльності, а з іншого – пов'язане з цим підвищення значення інтелектуальної складової в ухваленні рішень в управлінні та в інших сферах суспільного життя, а також зростаючий потік інформації, необхідної для ухвалення управлінських рішень та здійснення інших видів соціальної діяльності.

У сучасних умовах інформаційна аналітика стає ключовим елементом процесу управління знаннями для застосування її в практичній діяльності у будь-якій сфері.

Особливе місце в структурі інформаційної діяльності займає її специфічна різноманітність. Аналітична складова пронизує всі види інформаційної діяльності, оскільки жоден інформаційний процес неможливий без елементарного аналізу інформації. Але в аналізі інформації як самостійному виді діяльності ступінь аналітичності та системності є найвищою.

Основною рисою, яка відрізняє інформаційну аналітику від інших видів інформаційної діяльності, є те, що вона не тільки інформує споживача, але й створює нові знання. Ядром інформаційної аналітики є системний аналіз.

Багато хто вважає що ІА – це продукт людської спільноти, що сформувався внаслідок процесів глобалізації та інформатизації, тобто поняття виключно сучасне. Але насправді початок інформаційної аналітики можна знайти в глибокій давнині, коли людина намагалася отримати нові знання про навколишній світ на основі вже відомої інформації про нього і робила це за допомогою логічного мислення. До тих часів належить поява перших

аналітиків-професіоналів (Арістотель – перший теоретик інформаційної аналітики, Геродот – перший аналітик-практик).

У науковій літературі є безліч визначень поняття, оскільки ця сфера є достатньо молодою, її понятійно-категоріальний апарат на стадії формування. Найпоширеніші з них:

– Кривобокова А. Н. «Інформаційна аналітика – особлива галузь людської діяльності, покликана забезпечити інформаційні потреби суспільства за допомогою аналітичних технологій шляхом переробки вихідної інформації та отримання якісно нового знання».

– Кузнецов І. Н. «Інформаційна аналітика – це процес семантичної обробки даних, в результаті якої розрізнені дані переварюються на закінчену інформаційну продукцію – аналітичний документ».

Аналізуючи наведені визначення, можна відмітити, що вони фокусуються на основних загальних моментах:

1) створення нового знання;
2) семантична переробка наявної інформації;
3) оптимізація ухвалення рішень.

Для інформаційно-аналітичної діяльності особливої ваги набуває систематичність визначення кола питань, що виникають у процесі базової діяльності споживача інформації, їх аналіз та прогнозування тенденцій розвитку. Саме спрямованість на прогнозування, розпізнавання тенденцій розвитку ситуації зумовлює переважне використання різноманітних аналітичних методів обробки інформації: аналізу інформації, аналізу джерел, аналізу ситуації, аналізу контенту тощо. Прогнозування розвитку ситуації вимагає узагальнення інформації та її оцінку, тобто використання методів узагальнення, абстрагування та моделювання. Для створення інформаційних документів у цьому напрямі іноді потрібні незалежні соціологічні, статистичні та маркетингові дослідження.

Тож ми завжди аналізуємо, коли порівнюємо інформацію, відзначаємо закономірності та зв’язки між об’єктами та явищами, отримуємо нову інформацію. На відміну від цього «професійна аналітика» займається отриманням нової похідної інформації шляхом інтелектуальної обробки наявної інформації для чітко визначеної конкретної мети, зокрема від імені клієнта, зацікавленого в нових знаннях. Цю роботу виконують професійні аналітики і в цьому разі такий професійний аналіз називається «інформаційно-аналітична діяльність». Вона завжди має чітку мету та орієнтована на ухвалення рішення.

---

1. Захарова І. В., Філіпова Л. Я. Основи інформаційно-аналітичної діяльності : навч. пос. Київ : Вид. «Центр учбової літератури», 2013. 335 с.

2. Коваль Р. А. Інформаційно-аналітичне забезпечення діяльності органів державної влади. *Теорія та практика державного управління* : зб. наук. пр. Харків : Вид-во ХарРІ НАДУ «Магістр», 2006. № 1 (113). С. 223–226.

Пристинський Богдан Олександрович
курсант ННІ права та підготовки фахівців
для підрозділів Національної поліції
Науковий керівник:
Логінова Марина Вікторівна
викладач кафедри
цивільного права та процесу
Дніпропетровського державного
університету внутрішніх справ,

ПРАВОВЕ ЗНАЧЕННЯ ЕЛЕКТРОННИХ КОРУПЦІЙНИХ РЕЄСТРІВ В АСПЕКТІ БОРОТЬБИ З НЕПРАВОМІРНОЮ ВИГОДОЮ

Корупція як соціально-економічне явище є наслідком недосконалості чи неефективності обслуговуючих суспільство у різних сферах життя державних інституцій [1, с. 215]. Повномасштабне вторгнення російської федерації в Україну вимагає від влади та суспільства підвищеної активності у сфері боротьби з корупційними правопорушеннями. Неправомірна вигода завжди негативно впливає на розвиток держави, у випадку України це виявляється в таких явищах, як: вповільнення темпів постачання озброєння країнами-партнерами, ухилення громадян від мобілізації та зниження економічного потенціалу держави. Нещодавно Національне агентство з питань запобігання корупції запустило Єдиний державний реєстр осіб, які вчинили корупційні чи пов'язані з корупцією правопорушення. У контексті вищевказаних проблем ми вважаємо необхідним проаналізувати правове значення цього реєстру, як інструмента боротьби з неправомірною вигодою.

По-перше, реєстр осіб, які вчинили корупційні правопорушення, робить облік і ідентифікацію людей з корупційним минулим доступним для кожного. Реєстр містить інформацію про осіб, які були визнані винними у корупційних діях або мають інші, пов'язані з корупцією, правопорушення. Це сприяє гласності діяльності влади перед суспільством та підвищенню рівня його довіри до державних органів.

По-друге, на підставі інформації з реєстру можуть застосовуватися обмеження щодо обіймання посад, які можуть бути сполучені з можливістю вчинення корупційних дій, або зловживанням службовим становищем. Будь-який роботодавець перед прийняттям людини на роботу зможе подивитися, чи притягувався кандидат до відповідальності за корупційні правопорушення, і для цього буде достатньо просто написати відповідне прізвище, ім'я та по-батькові в пошуку. Це сприяє очищенню органів державної влади від осіб, які не зацікавлені у сумлінному виконанні своїх посадових обов'язків.

По-третє, реєстр є доступним для громадськості, це забезпечує громадський контроль над діяльністю осіб, які вчинили корупційні

правопорушення, і сприяє виявленню корупційних схем. Наприклад, аналітика у період з 4 лютого 2019 року по 5 вересня 2023 року, показала що Львівська область займає перше місце за кількістю корупційних кримінальних правопорушень [2]. Така аналітика дає можливість звернути увагу суспільства на найбільш проблемні регіони, та зосередити діяльність громадських організацій саме там. Це прямо впливає на розвиток демократії в України, бо сприяє участі громадян в управлінні державою, взаємодії з правоохоронними органами.

Також відкриття реєстру має кримінально-правове значення в аспекті спрощення доказування кваліфікації правопорушень. Стороні обвинувачення більше не доведеться шукати кримінальне провадження щодо особи, яка раніше вчинила корупційне правопорушення, строки судимості щодо якого не погашені, щоб довести вчинення нею рецедиву [3]. Тепер слідчому або прокурору буде достатньо просто доєднати до кримінального провадження довідку про відповідну особу з реєстру НАЗК. Це пришвидшує роботу правоохоронців, знижує навантаження на органи виконавчої влади.

Отже, підсумувавши всі наведені вище факти, ми можемо сказати, що створення реєстру осіб, які вчинили корупційні чи пов’язані з корупцією правопорушення загалом має позитивний вплив на розвиток держави у сфері її протидії неправомірній вигоді. Реєстр значно спрощує роботу правоохоронних органів, а також сприяє швидкій перевірці кандидатів на роботу у державному чи приватному секторі праці. Перспективним напрямом у роботі з даними реєстру НАЗК є відсотковий аналіз правопорушень за мапою, оскільки він дає змогу ліквідувати саму причину, а не наслідок проблеми. Центральне аналітичне управління таких органів, як НАБУ, САП, ДБР та СБУ повинно виконати дослідження, чому показник корупційних правопорушень серед певних регіонів значно перевищує відсоток інших. Звісно, така робота потребує дослідження дуже великого обсягу інформації. Проте ми впевнені, що, використовуючи автоматизовані системи підрахунку та штучний інтелект, органи влади матимуть значні зрушення у цьому напрямі.

1. Кишинська І. О. Корупція як негативний чинник розвитку суспільства та держави. *Протидія організованій злочинності: проблеми теорії та практики* : матеріали регіон. науково-практ. семінару (м. Дніпро, 03 грудня 2021 р.). Дніпро : ДДУВС, 2021. С. 213–215. URL: https://er.dduvs.in.ua/bitstream/123456789/8926/1/53.pdf

2. Єдиний державний реєстр осіб, які вчинили корупційні чи пов’язані з корупцією правопорушення. URL: https://corruptinfo.nazk.gov.ua/reference/map

3. Кримінальний процесуальний кодекс України : Закон України від 24.08.2023 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

Риндич Анастасія Володимирівна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Синиціна Юлія Петрівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК КЛЮЧОВА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ: ВИКЛИКИ І СТРАТЕГІЇ ЗАХИСТУ

Аналіз проблеми забезпечення інформаційної безпеки в Україні та захисту національного інформаційного простору від негативного впливу пропаганди та маніпуляційної інформації є актуальним питанням сьогодення. У процесі ретроспективного аналізу досліджено різні теоретичні підходи до визначення сутності інформаційної безпеки і розглянуто різновиди актуальних та потенційних інформаційних загроз для медіапростору України, а також надано характеристику специфіці експансивної політики російської федерації щодо України.

Інформаційна безпека є необхідною складовою національної безпеки і розглядається як пріоритетна функція держави. Вона містить у собі забезпечення громадян якісною та доступною інформацією, а також захист від дезінформації та інформаційних загроз, що можуть підірвати цілісність суспільства і інформаційний суверенітет країни. Вирішення цієї складної проблеми інформаційної безпеки сприятиме захисту інтересів суспільства і держави, а також гарантуванню прав громадян на об’єктивну та якісну інформацію [1].

Визначення мети та принципів забезпечення інформаційної безпеки сприяє формуванню відповідної інформаційної системи і вирішенню з нею пов’язаних проблем. Інформаційна безпека часто є важливим зв’язком між політикою національної безпеки та інформаційною політикою країни. Небезпека в інформаційній сфері виникає внаслідок незбалансованості інтересів суб’єктів суспільних відносин. Це, насамперед, зумовлено недостатньою увагою державних інститутів до підвищення рівня інформаційної безпеки України [2].

Розуміння інформаційної безпеки в контексті національної безпеки можна розглядати за двома підходами, а саме: самостійний елемент

національної безпеки країни або як інтегровану складову інших видів безпеки, таких як військова, економічна чи політична. Один із найповніших визначень інформаційної безпеки містить у собі захист життєво важливих інтересів особистості, суспільства і держави. Цей захист досягається шляхом мінімізації ризиків, пов'язаних з неповнотою, невчасністю та недостовірністю інформації, негативним інформаційним впливом, наслідками функціонування інформаційних технологій та несанкціонованим поширенням інформації. Це визначення найбільш оптимально враховує всі аспекти взаємодії у сфері інформаційних відносин [2].

Україна стала об'єктом інформаційно-психологічних впливів, операцій і війн, що загрожує її інформаційній безпеці.

До основних актуальних стратегічних напрямів інформаційної безпеки можна віднести таке:

1. Український інформаційний простір недостатньо захищений від зовнішніх негативних пропагандистсько-маніпулятивних впливів і став об'єктом інформаційної експансії.

2. У світовому медіапросторі відсутній національний український інформаційний продукт, який би поширював об'єктивну, неупереджену та актуальну інформацію про події в Україні. Це призводить до відчутного дефіциту інформації у світовій громадськості або отримання неякісної інформації з інших джерел, що можуть бути дезінформуючими.

3. Діяльність вітчизняних медійних інститутів (ЗМІ) у сфері об'єктивного та систематичного висвітлення подій є недостатньою та позбавленою стратегічного планування. Інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та вдосконалення.

Отже, національний інформаційний простір України стикається із серйозними загрозами, які можуть нашкодити функціонуванню держави, її політичному та економічному розвитку та інтеграції в європейські та євроатлантичні структури. Ці загрози для національної безпеки України у сфері інформації містять у собі умови та чинники, що можуть вплинути негативно на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру.

---

1. Захист інформаційної безпеки як функція держави. URL: http://www.mego.info/матеріал/23 захист-інформаційноїбезпеки- як-функція держави (дата звернення: 26.09.2023).

2. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. URL: http://www.visnyk.academy. gov.ua.wpcontent/uploads/2015/04/20.pdf

Савенко Ганна Богданівна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Рижков Едуард Володимирович
професор кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, професор

ВПЛИВ ІНФОРМАЦІЙНОЇ ВІЙНИ НА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

Інформаційна війна (іноді також називається гібридною війною) – це форма конфлікту, в якій інформація використовується як засіб досягнення стратегічних цілей. Ця війна може містити у собі використання різних інформаційних засобів та технологій для маніпуляції громадською думкою, впливу на рішення тих, хто їх ухвалює, дестабілізації суспільства та інших цілей, що спрямовані на слабкість або падіння противника.

На сьогодні термін «інформаційна війна» використовується в двох площинах: у широкому розумінні – для визначення протиборства в інформаційній сфері, в засобах масової інформації для досягнення різних політичних цілей; у вузькому розумінні – для визначення воєнного протиборства, у військовій інформаційній сфері для досягнення односторонніх переваг в отриманні, зборі, обробці та використанні інформації на полі бою. [1, с. 11].

Вперше термін «інформаційна війна» було вжито Т. Роном у звіті «Системи зброї і інформаційна війна», підготовленому ним в 1976 р [2, с. 45].

У сучасних вітчизняних та закордонних дослідженнях окремі теоретичні аспекти інформаційних війн та їх вплив на національну безпеку розглядали А. В. Авраменко, Г. С. Лазарев, М. П. Хріпков, З. Бжезинський, Р. Арон, О. Тофлер. Вивченню сутності інформаційних війн з точки зору політології, теорії держави і права, теорії управління та безпекознавства присвячені праці І. Н. Панаріна, Г. Г. Почепцова, В. С. Цимбалюка тощо. У більшості наукових працях поняття інформаційна війна трактується як чинник, що несе загрозу інформаційній безпеці громадянам держави та національній безпеці держави.

Інформаційна війна має значний вплив на національну безпеку України, особливо у контексті геополітичних подій та з повномасштабного вторгнення російської федерації.

Інформаційна війна складається з декількох складових, що в комбінації

можуть завдавати шкоди нормальному ритму життя громадянам країни.

За майже 18 місяців повномасштабної війни на території України найчастіше противник звертався до такої складової ведення інформаційної війни, як дезінформація та пропаганда з метою впливати на громадську думку та формувати негативний образ України, роблячи це шляхом поширення певної інформації (переважно стосовно воєнних дій) через різні медіа-канали, як наслідок, відбувається розпалювання міжетнічних конфліктів, підняття антиукраїнських настроїв та дестабілізація ситуації в країні.

Значних збитків національній безпеці можуть завдати інформаційні атаки (або як їх ще називають кібератаки) на українські інфраструктури та урядові системи. Кібератаки містять у собі спроби зламати комунікаційні системи, енергетичні мережі та інші критичні інфраструктури.

Загальний вплив інформаційної війни на національну безпеку України є значущим, оскільки зазвичай важко визначити джерело інформаційних атак і ефективно захищатися від них, також ефективна реакція на цю загрозу є критично важливою для збереження стабільності та безпеки країни. Тому боротьба з певними складовими інформаційної війни вимагає комплексних заходів, включно з кіберзахистом, підвищенням обізнаності громадськості та міжнародною співпрацею.

1. Shumka A. V., Chernyk P. H. Теоретичні аспекти інформаційних війн та національна безпека. *Науково-теоретичний альманах Грані*. 2015. 18(9). С. 10–16. URL: https://doi.org/10.15421/1715168

2. Рибак М. І., Атрохов А. В. До питання про інформаційні війни. *Наука і оборона*. 2018. № 2. С. 65–68.

Скрипник Богдан Геннадійович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

ІНФОРМАЦІЙНИЙ СУВЕРЕНІТЕТ ДЕРЖАВИ

Так само як і в інших державах в Україні спостерігається зростання ролі інформаційної сфери, переосмислення її значення як найважливішого фактора життя, що безпосередньо впливає на всі види національної безпеки, у зв’язку

з чим у країні динамічно розвиваються процеси інформатизації (побудова цифрової держави, цифрового уряду, становлення цифрового правосуддя тощо). Все частіше виникає потреба правової оцінки та регламентації інформаційних відносин. Склалося розуміння, що якими б складними не були наслідки інформаційної війни, що почалася проти України, свобода інформації – це неодмінний атрибут громадянського суспільства.

Захист інформаційного простору в умовах сьогодення є одним із базових завдань і суспільства, і держави. Відповідно, інформаційна безпека набуває все більшої значущості в загальній системі забезпечення національної безпеки країни в цілому. Зважаючи на значний розвиток інформаційно-комунікаційних технологій та загальну цифровізацію, виникли принципово нові категорії – інформаційне суспільство, кіберпростір. Становлення інформаційного суспільства призвело до появи безлічі загроз у ключових сферах життя країни, тому інформаційна безпека розглядається як окремий елемент національної безпеки [1, с. 284]. Кожна держава або група держав розробляє власні стратегії дій, внутрішню і зовнішню політику інформаційної безпеки, що відповідають поточному стану розвитку комунікацій. Для Європи характерний пошук балансу між державними інтересами та захистом прав людини від незаконного втручання [2, с. 20–21].

Національна розвідувальна політика має бути збалансована і розвиватися як об'єктивна складова національної безпеки і як частина загальної політики, що ґрунтується на життєво важливих національних інтересах. Інформаційна політика повинна здійснюватися на засадах правових і демократичних принципів, відповідно до національного та міжнародного права, через розроблення та реалізацію відповідних державних доктрин, стратегій і програм [3, с. 68].

За словами П. Біленчука, безпека в інформаційній сфері містить забезпечення інформаційного суверенітету; забезпечення захисту національного інформаційного простору та недопущення державної монополії в інформаційній сфері [4, с. 54–55]. Про інформаційний суверенітет пише й О. Вайцеховська, де зазначає, що нормативне визначення «державного інформаційного суверенітету» міститься в Законі України «Про Національну програму інформатизації» 1998 р., згідно з яким це здатність держави контролювати та регулювати надходження інформації з-за меж держави з метою додержання законів України, прав і свобод громадян та забезпечення національної безпеки держави [5, с. 243]. Проте зазначений закон втратив чинність через Закон України «Про Національну програму інформатизації» від 1 грудня 2022 року, в якому ця категорія більше не згадується.

Підсумовуючи, вважаємо за необхідне розмежувати власне розуміння поняття інформаційного суверенітету – це верховенство держави в інформаційній сфері на власній території, а також невід'ємна можливість вільно та незалежно надавати об'єктивну інформацію про специфіку вітчизняної зовнішньої та внутрішньої політики.

Захист інформаційного суверенітету є частиною розвитку сучасної України. Результатом інформаційних воєн є деформація цінностей суспільства, що негативно впливає на інші сфери державного життя, насамперед політичну, правову тощо. З одного боку, розвиток інформаційно-комунікаційних технологій розширює можливості людей і суспільства, але з іншого боку, також несе низку загроз. Отже, реалізація умов інформаційної діяльності має забезпечувати дотримання принципів свободи вираження поглядів і переконань, свободи поширення, обміну та отримання інформації, права на інформацію, відкритості та доступності інформації, гарантії достовірності та повноти інформації, захист особи від втручання в особисте та сімейне життя, безпеку процесів обміну інформацією, що має велике значення як для окремої країни, так і для міжнародної спільноти в цілому. Тому інформаційну безпеку треба розглядати не лише з конкретно-прикладного аспекту, а як стабільний та безпечний стан усієї соціальної системи.

1. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна*. Серія : Право. 2020. № 29. С. 281–288.

2. Парахонський Б. О. Зовнішня політика України в умовах кризи міжнародного безпекового середовища : аналіт. доп. Київ : НІСД, 2015. 100 с.

3. Бондар І. Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. № 1. С. 68–75.

4. Біленчук П. Д. Правові засади інформаційної безпеки України. Харків. 2018. 289 с.

5. Вайцеховська О. Р. Міжнародний фінансовий правопорядок: теоретичні засади та актуальні проблеми в умовах глобалізації : дис. д-ра юрид. наук. Харків, 2020. 472 с.

Солдатенков Роман Олексійович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОПТИМІЗАЦІЇ ФУНКЦІНУВАННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Один із ключових факторів для підвищення ефективності боротьби із злочинністю полягає в широкому використанні сучасних досягнень науково-

технічного прогресу, які останніми роками суттєво поліпшилися у галузі інформаційних технологій. На сьогодні майже неможливо уявити функціонування будь-якого підрозділу Національної поліції України без активного використання інформаційної підтримки та системи збору, обробки та упорядкування інформації в базах даних. Це підтверджує важливість тези, яка стала загальновідомою: «Той, хто володіє інформацією, володіє контролем над ситуацією» [1].

Під час розробки загальних технічних вимог до системи інтелектуального відеоспостереження був проведений аналіз досвіду розробників та впроваджувачів системи Єдиного аналітично-сервісного центру (UASC) в Донецькій області, а також було використано інформацію з відкритих джерел інтелектуального аналізу (OSINT) у мережі «Інтернет». За результатами цього аналізу зроблено висновок, що система інтелектуального відеоспостереження являє собою комплекс апаратних та програмних засобів, що здатний якісно обробляти відеодані і звільнити оператора від рутинного спостереження за великою кількістю камер з метою виявлення порушень. Розвиток систем відеоспостереження базується на двох головних технологіях: трекінгу (відеодетекторі) й ідентифікації, які лежать в основі функцій сучасних інтелектуальних систем відеоспостереження.Трекінг – це спеціальний алгоритм обробки відеоматеріалів, який визначає та класифікує об’єкти, що рухаються, описує їх характеристики (розмір, колір, швидкість) та контролює їх рух в кадрі. Трекінг може бути реалізований в різних варіаціях, і найпоширенішими з них є ситуаційні та сервісні детектори. Ситуаційні детектори визначають ситуації, коли об’єкт спостереження перетинає визначені зони в кадрі, і відповідна система видає тривогу [2].

Останнім часом Україна стикалася зі значущими загрозами для інформаційної безпеки публічних органів. Ці загрози містять у собі розповсюдження шкідливого програмного забезпечення, такого як Petya і WannaCry, атаки на енергетичний сектор у 2015–2016 роках, атаки на президентські вибори у 2014 році, інциденти, пов’язані з інформаційними системами та мережами державних органів і державних компаній у 2016 році, а також інциденти, пов’язані з подіями Євромайдану у 2013–2014 роках, та інші кіберзлочини. До того ж наявний інший напрям негативного зовнішнього інформаційного впливу, де використовуються сучасні інформаційні технології для впливу на свідомість громадян. Цей вплив спрямований на підтримку міжнаціональної та релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу та порушення суверенітету, територіальної цілісності України, громадського порядку та безпеки. Загрози можуть бути різного характеру і походити від різних суб’єктів з різними мотивами. Вони можуть впливати на різні об’єкти та мати різні наслідки [3].

Тож ми можемо зазначити про те, що НПУ з початку реформи з 2014 року, набувши досвіду закордонних країн, почала прогресувати у сфері інформаційних технологій і розробки власних програм і ресурсів (наприклад,

система «Цунамі»).

1. Використання інформаційних технологій в діяльності Національної поліції України.URL: https://univd.edu.ua/science-issue/issue/379

2. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото і кінозйомки, відеозапису. Аналіз закордонного досвіду. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/5a48c83f-6d5b-4435-b9d4-0cbd34d42dc8/content ст. 35

3. Інформаційне забезпечення діяльності патрульної поліції. URL: http://surl.li/mzqmm

Ткаченко Павло Олександрович
аспірант кафедри
кримінально-правових дисциплін
Дніпропетровського державного
університету внутрішніх справ,
член Асоціації правників України
Науковий керівник:
Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНАМИ ДЕРЖАВНОЇ БЕЗПЕКИ

У сучасному світі інформаційні технології відіграють ключову роль у всіх сферах суспільного життя. Цифрова трансформація спричинила значне збільшення обсягу інформації, яку обробляють. Від цього залежить успішність функціонування сучасних організацій та держав в цілому. Однак разом з розвитком інформаційних технологій зросли загрози для безпеки інформації. Тому останнє десятиріччя особливо актуальною стала проблема забезпечення інформаційної безпеки, зокрема органами державної безпеки.

Більшість теоретиків вважає, що забезпечення інформаційної безпеки органами державної безпеки – це система заходів та стратегій, спрямованих на запобігання несанкціонованому доступу, використанню, розголошенню чи пошкодженню інформації, яка є важливою для національних інтересів та безпеки країни.

Водночас, на нашу думку, забезпечення інформаційної безпеки органами державної безпеки полягає не лише в захисті інформації, як такої. У

складі ключового органу забезпечення державної безпеки країни – Служби безпеки України ефективно функціонує підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, який щоденно, щохвилинно здійснює захист інформаційних систем, електронних платформ державних органів від злочинних посягань, інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури від кібератак, здійснює контррозвідувальне та оперативне забезпечення всіх гілок держави, що в підсумку виражається в захищеності цих об'єктів від протиправних посягань.

Сьогодні рівень професіоналізму представників підрозділів КІБ СБУ знаходиться на найвищому рівні, адже фахівці саме цього, особливо важливого органу забезпечують інформаційну та кібернетичну безпеку Збройних Сил України, Національної гвардії України, Державної прикордонної служби України, Державної спеціальної служби транспорту України та інших військових формувань, які утворені відповідно до чинного законодавства України.

Забезпечують Збройні Сили України від перешкоджання законній діяльності останніх, виявляючи осіб та документуючи їх протиправну діяльність, притягують до кримінальної відповідальності.

Щодо загальної площини забезпечення інформаційної безпеки органами державної безпеки, то варто зауважити, що ця діяльність є надзвичайно важливим завданням в умовах сучасного цифрового суспільства, коли інформація стала ключовим активом для багатьох сфер діяльності, включно з обороною, економікою, наукою, політикою та громадським життям. Органи державної безпеки забезпечують захист інформації з обмеженим доступом від втрати, несанкціонованого доступу, розголошення чи пошкодження. Важливими аспектами забезпечення інформаційної безпеки органами державної безпеки є кібербезпека, сутність якої полягає в тому, що органи державної безпеки розробляють стратегії та заходи для захисту державних інформаційних систем від кіберзагроз. Це містить заходи щодо виявлення, запобігання та реагування на кібератаки, віруси, хакерські атаки та інші електронно-інформаційні загрози.

Правове регулювання полягає в розробці та впровадженні відповідного законодавства, яке регулює обіг та захист інформації. Організаційна безпека – розроблення політик, процедур та правил внутрішньої організації для забезпечення інформаційної безпеки в установі чи організації. Це містить навчання персоналу та формування безпекової культури в організації. Боротьба з дезінформацією та фейками повинна містити у собі розроблення стратегій та методів виявлення та запобігання поширенню дезінформації та фейків, особливо в соціальних мережах та медіа, що на сьогодні ефективно забезпечується саме підрозділами КІБ СБУ, під контролем яких перебувають всі соціальні мережі та інформаційні платформи.

Технічні заходи безпеки полягають в застосуванні технологічних засобів для забезпечення безпеки інформації, зокрема шифрування, використання

безпечного програмного забезпечення, мережеві заходи безпеки та інші технічні методи. Моніторинг та реагування ґрунтується на постійному моніторингу захищеності систем та інфраструктури для виявлення можливих атак та негайного реагування на них.

Отже, забезпечення інформаційної безпеки є актуальним завданням для органів державної безпеки в умовах сучасного цифрового світу. Швидкий та непередбачуваний розвиток інформаційних технологій відкриває безліч можливостей для збереження, обробки та передачі інформації, але водночас створює загрози для її конфіденційності та цілісності. Органи державної безпеки повинні вживати комплексних заходів для гарантування інформаційної безпеки.

Кібербезпека є основним компонентом забезпечення інформаційної безпеки. Захист інформаційних систем від кібератак, застосування сучасних технологій шифрування та виявлення загроз є невід'ємною частиною цього процесу. Важливо вдосконалювати та адаптувати кіберзахист відповідно до нових загроз та атак. Технічні засоби безпеки та організаційна безпека є важливими аспектами для захисту важливої інформації та уникнення загроз. Впровадження сучасних технологій та розробка ефективних процедур дозволяють убезпечити системи від несанкціонованого доступу та атак.

Інформаційна освіта та навчання мають ключове значення для підвищення рівня обізнаності населення та співробітників у сфері інформаційної безпеки. Вони дозволяють ефективно реагувати на загрози та уникати можливих негативних наслідків.

Усі ці компоненти повинні бути інтегровані в систему забезпечення інформаційної безпеки, яка повинна бути постійно оновлюваною та адаптованою до змін у технологічному та соціальному середовищі. Лише комплексний підхід та спільні зусилля можуть гарантувати ефективність заходів забезпечення інформаційної безпеки в умовах сучасного світу.

Ткачова Юлія Володимирівна
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Косиченко
Олександр Олександрович
доцент кафедри інформаційних
технологій Дніпропетровського
державного університету внутрішніх
справ, кандидат технічних наук, доцент

ПОНЯТТЯ КІБЕРЗЛОЧИННІСТЬ ТА ШЛЯХИ ЇЇ ПОДОЛАННЯ В УМОВАХ ВОЄННОГО СТАНУ

Інформаційні технології стають все більш важливими у житті суспільства. Вони використовуються в усіх сферах, від особистого спілкування до управління державою. Однак зростання використання ІТ також призвело до зростання кіберзлочинності. Практично кожен чув про кіберзлочинність і, можливо, навіть особисто з нею зіштовхувався. Кіберзлочинність містить у собі різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі «Інтернет». Об'єктом цих злочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектора. Саме тому кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні [1].

Кіберзлочинність – це злочинна діяльність, яка передбачає використання комп'ютерів, комп'ютерних мереж або мережевих пристроїв. Тому умови воєнного стану створюють лише додаткові можливості для кіберзлочинців. Вони можуть використовувати кіберпростір для дезінформації, пропаганди, а також для завдавання шкоди критичній інфраструктурі.

Кіберзлочинність – це широкий термін, який охоплює широкий спектр злочинів, пов'язаних з використанням ІТ. До кіберзлочинів можна віднести:

• Шахрайство: використання ІТ для обману людей з метою отримання їхніх особистих даних або грошей.

• Зловживання: використання ІТ для шкоди або порушення прав інших осіб.

• Незаконне поширення інформації: поширення інформації, яка є незаконною або шкідливою.

• Атаки на критичну інфраструктуру: атаки на системи, які є життєво важливими для суспільства, такі як енергетичні системи, системи зв'язку та

фінансові системи.

Умови воєнного стану в Україні створюють серйозні загрози у сфері кібербезпеки. Кіберзлочинці можуть активно використовувати хакерські атаки та інші кіберзагрози, спрямовані на отримання важливої інформації, завдання шкоди критичній інфраструктурі і вплив на звичайний спосіб життя населення. Уряд України вживає рішучих заходів для забезпечення кібербезпеки, зокрема співпрацю з міжнародними партнерами. Також важливу роль у цьому належить інформаційній грамотності громадян і підприємств, які повинні дбати про захист своїх даних і мереж в умовах підвищеної загрози кібератак.

Для подолання кіберзлочинності в умовах воєнного стану необхідно вжити комплекс заходів, зокрема:

1. Посилити правоохоронну діяльність: правоохоронні органи повинні посилити боротьбу з кіберзлочинністю, зокрема шляхом створення спеціалізованих підрозділів та використання сучасних технологій.

2. Створити спеціалізовані підрозділи: Національна поліція повинна створити спеціалізовані підрозділи, які будуть займатися боротьбою з кіберзлочинністю. Ці підрозділи повинні мати достатню кількість кадрів та ресурсів для ефективної боротьби з кіберзлочинністю.

3. Використовувати сучасні технології: правоохоронні органи повинні використовувати сучасні технології для боротьби з кіберзлочинністю. Ці технології можуть містити у собі системи виявлення кібератак, системи відстеження IP-адрес та системи аналізу даних.

4. Забезпечити проведення навчальних семінарів та вебінарів: необхідно проводити навчальні семінари та вебінари для населення про кіберзлочинність та способи захисту від неї. Ці семінари та вебінари повинні бути доступними для широкого кола людей. Це допоможе людям усвідомити загрозу кіберзлочинності та вжити заходів для захисту себе.

5. Посилити захист критичної інфраструктури: критична інфраструктура, така як енергетичні системи, системи зв’язку та фінансові системи, є особливо вразливою до кібератак. Тому критична інфраструктура повинна бути оснащена сучасними засобами захисту, такими як системи виявлення та запобігання вторгненням, системи резервного копіювання та системи відновлення після інциденту.

6. Розробити міжнародне співробітництво: міжнародне співробітництво є важливим для успішної боротьби з кіберзлочинністю. Це містить у собі обмін інформацією та досвідом між правоохоронними органами різних країн, а також розробку міжнародних правових норм у сфері кібербезпеки, оскільки в інших країнах для боротьби з цим видом злочину створені спеціалізовані підрозділи, які займаються виявленням, розслідуванням комп’ютерних злочинів та збором іншої інформації з цього питання на національному рівні [2].

Кіберзлочинність є серйозною проблемою, яка може завдати значних збитків суспільству. В умовах воєнного стану вона має низку особливостей,

які ускладнюють боротьбу з нею. Тому для подолання кіберзлочинності в умовах воєнного стану необхідно вжити комплекс заходів, які містять посилення правоохоронної діяльності, посилення захисту критичної інфраструктури та просвітницьку роботу.

1. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. *Ресурсний центр ГУРТ*. URL: gurt.org.ua

2. Круль С. М. Злочини у сфері інформаційних технологій: національний та міжнародний аспекти. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/apvchzu_2008_20_32.pdf

Чорний Артур Артемович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Рибальченко
Людмила Володимирівна
доцент кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат економічних наук, доцент

ХАКЕРСЬКІ АТАКИ ПІД ЧАС ВОЄННОГО СТАНУ В УКРАЇНІ

На сьогодні інформаційна та комунікаційна безпека є дуже важливим питанням, тому що інформація під час війни є потужним інструментом, вона дозволяє вигравати війни та політичні кризи без жодного пострілу, формуючи та розпалюючи внутрішні суперечності. Така тактика характерна для війн нового формату – гібридних, де безпосередній військовий фактор є лише однією зі складових цілого. Зараз в умовах, коли більша частина інформації в Інтернеті та в житті спрямована на маніпулювання думкою та свідомістю людини і зазвичай подається за допомогою фізіологічних і психологічних методів або засобів її сприйняття, постає питання низького рівня інформаційної культури, що спричиняє зниження можливості людини до сприйняття істини, для аналізу та оцінки отриманої інформації.

У такому разі висловити власну думку дуже складно, а враховуючи всі ці аспекти – неможливо. Кожен повинен дотримуватись власної думки, але до цього потрібно ще дійти. Поставити себе так, що ти керуєш своїм життям, вирішуєш ти, що треба робити і чого не треба. Не вірити у те, що ллється з

невідомих джерел та поширюється рекламою завдяки піару, розраховану на неусвідомлену аудиторію людей, яка потім її поширює та наводить паніку й хаос.

Інформаційна безпека держави характеризується ступенем захищеності і стійкістю основних сфер життєдіяльності: економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості тощо стосовно небезпечних інформаційних впливів.

Також до початку війни українські інформаційні системи зазнали потужних атак російських хакерів. Від початку повномасштабної відкритої агресії рф інтенсивність кібератак не знижується. Російські військові хакери намагаються отримати доступ до персональних даних українців, а також завдати шкоди українським інформаційним системам. Ці атаки координуються з атаками на критичну інфраструктуру і є частиною воєнної агресії рф.

Інформаційною безпекою є:

1) контроль над медіа, коли Уряд повинен вживати заходів для забезпечення об'єктивності та достовірності інформації, яка поширюється через ЗМІ та Інтернет. Це допомагає запобігти паніці та поширенню дезінформації;

2) посилення кіберзахисту інформаційних інфраструктур та критичних систем включає в себе заходи для запобігання кібератакам та відновлення роботи мереж і систем після атак;

3) завданнями контррозвідки є розвідка та контррозвідка, які є важливими для виявлення шпигунів та забезпечення безпеки конфіденційної інформації.

Економічною безпекою є:

1) фінансова стабільність, яка підтримує фінансову стабільність країни в умовах військового стану. Це може містити у собі регулювання фінансового ринку та забезпечення функціонування банків;

2) забезпечення ресурсів, коли країна повинна забезпечити стабільний доступ до енергетичних ресурсів, продовольства, води та інших життєво важливих ресурсів;

3) захист виробництва важливий для забезпечення безпеки виробництва та постачання товарів і послуг. Це може містити у собі заходи для захисту виробничих об'єктів та транспорту;

4) мобілізація економіки в умовах військового стану може потребувати нових вимог для виробництва військової техніки та обладнання. Планування і реалізація таких заходів важлива для ефективного функціонування в умовах військового конфлікту.

Отже, можна зазначити єдність усіх цих складових для захисту від кібератак та надійності інформаційного простору України. Саме забезпечення інформаційної безпеки під час війни – складне завдання, що вимагає ретельного планування та готовності до непередбачуваних обставин. Кожна

ситуація у нашому житті різна та може вимагати індивідуального підходу, але завжди треба добре обмірковувати свої дії та намагатись розвивати себе для кращого результату як у своїй безпеці, так і в житті. Загальний підхід полягає в тому, щоб вживати комплексних заходів для забезпечення інформаційної та економічної безпеки в умовах військового стану. Це передбачає співпрацю між військовими та цивільними владами, а також готовність до швидкого реагування на ситуацію, що змінюється, та використання сучасних технологій для забезпечення цих видів безпеки.

Також під час військового стану заборонено поширювати недостовірну інформацію, яка може привернути увагу або ввести в оману інших громадян, та чим далі це зайде, тим гірше буде всім, а тим, хто буде це все розплутувати, буде тяжко, особливо якщо це стосується економічної та інформаційної безпеки.

Отже, інформаційна безпека стає невід'ємною частиною загальної безпеки держави в умовах військового стану, а її забезпечення вимагає завдань як на рівні влади, так і на рівні індивідуальної готовності та свідомості громадян. Кожен повинен ставитись до цього серйозно та дуже відповідально.

1. Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/284104

2. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку. URL: https://www.kmu.gov.ua/news/vymohy-do-zakhystu-informatsii-v-informatsiinykh-systemakh-u-voiennyi-chas-roziasnennia-derzhspetszviazku

Чупілко Олександр Сергійович
аспірант кафедри економіки
та соціально-трудових відносин
Університету митної справи та фінансів
Науковий керівник:
Бобровська Олена Юріївна
професор кафедри економіки
та соціально-трудових відносин
Університету митної справи та фінансів,
доктор наук з державного управління

ТЕХНОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ДЛЯ УПРАВЛІННЯ В ЕКОНОМІЦІ ТА ЙОГО БЕЗПЕКА

Сучасний рівень науки і техніки формує технологічне та інформаційне середовище, визначає нові можливості системи управління в економіці. Науковий підхід до управління соціально-економічних систем ґрунтується на новітніх інформаційних та комп'ютерних технологіях, різноманітних

математичних методах та підходах, що дозволяє всебічно вивчати соціально-економічні процеси і чинники, що впливають на них, і на основі наукового підходу прогнозувати їх розвиток, автоматизувати процеси і забезпечувати конфіденціальність інформації, робити управління ефективним, результативним і гнучким.

Технологічне забезпечення систем управління в економіці містить такі аспекти, як системний підхід, безпеку інформаційного середовища, автоматизацію процесів управління, аналіз даних і моделювання, співпрацю і комунікацію, стратегічне управління, інновації та розвиток. Безпека економічного інформаційного середовища полягає в розробці та використанні інформаційних систем, які забезпечують збір, обробку, зберігання і передачу інформації для ухвалення управлінських рішень. Захищеність інформації від несанкціонованого доступу, використання, внесення змін, знищення тощо характеризує інформаційну безпеку держави і стійкість різних сфер життєдіяльності, зокрема економіки до інформаційних впливів та інших дестабілізаційних факторів.

Питанння інформаційної безпеки стосується всіх аспектів захисту даних, в якій би формі вони не перебували, але це є особливо актуальним для технічних інформаційних систем управління, зокрема таких, що використовують розподілену інформацію. Захист інформації забезпечується комплексною системою заходів, до якої відносять міжнародні стандарти, резервне копіювання, політику прав доступу, двофакторну аутентифікацію тощо. Для реалізації цих можливостей відбувається розробка методів аналізу загроз, рівня інформаційної безпеки суб'єкта економіки, систем її забезпечення. Безпека даних і захист економічної інформації забезпечується за допомогою технічних засобів і програмних застосунків, які дозволяють здійснювати контроль інформаційної безпеки системи управління.

Міжнародна професійна Асоціація аудиту і контролю інформаційних систем, яка об'єднує більше 115 000 членів із 180 країн, орієнтована на інформаційно-технологічне управління. У межах цієї організації в Україні працює 50 ІТ-професіоналів, які представляють організації різних форм власності. У процесі розробки і формалізації єдиних правил управління ІТ-процесами та ІТ-системами, ефективних підходів до питань безпеки інформації задіяні фахівці ІТ-аудиту, ІТ-консалтингу, управління ІТ-ризиками та інформаційною безпекою.

Якість управління інформаційною безпекою базується на комплексному підході, який охоплює всі компоненти інформаційної системи, враховує фактори ризику, є узгодженим із бізнес-завданнями і стратегією суб'єкта економіки, використовує і генерує адекватну інформацію, зв'язує процеси управління в єдиний цикл планування, впровадження, перевірки, аудиту і корегування.

1. Управління інформаційною безпекою / уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. КПІ ім. Ігоря Сікорського; Електронні текстові дані (1 файл: 1114 Кбайт). Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.

Ярошенко Олександр Павлович
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції
Науковий керівник:
Гребенюк Андрій Миколайович
завідувач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ,
кандидат технічних наук, доцент

КІБЕРЗЛОЧИННІСТЬ ПІД ЧАС ВОЄННОГО СТАНУ В УКРАЇНІ

24 лютого 2022 року у зв'язку з військовою агресією російської федерації проти України Указом Президента України № 64/2022 було введено воєнний стан. Відповідно до Закону України «Про правовий режим воєнного 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 [1].

Як відомо, війна «нового зразка», або «нового покоління» відрізняється від класичного розуміння війни і містить у собі різноманітні аспекти, які виходять за межі традиційних бойових дій на полі бою. Одним з ключових елементів такої війни є кіберзлочинність.

Відповідно до статті 1 ЗУ «Про основи 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 [2].

Кіберзлочинність може мати різні форми, зокрема крадіжку даних, шпигунство, саботаж систем і мереж, а також кібератаки на критичну інфраструктуру. Вона може бути використана як засіб проведення гібридної воєнної кампанії, спрямованої на дестабілізацію супротивника.

У випадку з Україною боротьба з кіберзлочинністю стала особливо актуальною під час воєнного стану. Після повномасштабного вторгнення росії на територію України кількість кримінальних правопорушень у сфері інформаційних технологій різко збільшилась. Країна-агресор використовує інтернет-технології для дезінформації щодо вторгнення в Україну, пропаганди ворожих ідей тощо.

У процесі реагування на швидке зростання рівня кіберзлочинності

Верховна Рада України здійснила оптимізацію кримінального та кримінально-процесуального законодавства, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності кіберзлочинців. Зокрема, було внесено зміни до відповідних законів: «Про внесення змін до Кримінального процесуального кодексу України, «Про електронні комунікації» з питання підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15 березня 2022 року № 2137-IX та «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24 березня 2022 року№ 2149-IX. Законом України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» від 24.03.2022 р. № 2149-IX було запропоновано нову редакцію ст. 361 КК України та внесено зміни й доповнення до ст. 361-1 КК України [3; 4].

Тож до ст. 361-1 КК України було внесено такі зміни:

– змінено формулювання предмета відповідного кримінального правопорушення (словосполучення «електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку» було замінено на «інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі»);

– при характеристиці мети відповідного правопорушення було додано вказівку на протиправність зазначених дій, що фактично звужує застосування цієї норми та легалізує непротиправне (передбачене законом) застосування шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж;

– дещо посилена альтернативна санкція ч. 1 ст. 361-1 КК (максимальний строк позбавлення волі було збільшено з двох до трьох років);

– шляхом внесення змін до примітки ст. 361 КК України було збільшено розмір значної шкоди, передбаченої як кваліфікуюча ознака у ч. 2 ст. 361-1 КК України [5].

Справді, враховуючи показники діяльності правоохоронних органів після внесення відповідних змін до законодавства, прослідковується підвищення ефективності боротьби зі злочинністю у сфері інформаційних технологій. Розширення меж діяльності правоохоронних органів щодо розслідування кіберзлочинів, посилення санкцій, додаткова криміналізація окремих діянь – стримують потенційних шахраїв [6].

Проте необхідно зазначити, що хоча ці заходи можуть бути ефективними для стримування потенційних шахраїв, вони не є панацеєю від кіберзлочинності. Кіберзлочинці постійно адаптуються та вдосконалюють свої методики, щоб уникнути виявлення та покарання.

Тому, крім законодавчих заходів, необхідно також зосередитися на профілактиці та освіті. Це може містити навчання користувачів безпеці в Інтернеті, поширення інформації про загрози та способи їх уникнення, а також створення надійних систем захисту інформації.

Крім того, важливою є міжнародна співпраця у боротьбі з кіберзлочинами, оскільки ця проблема має глобальний характер. Багато країн вже працюють над створенням механізмів для спільного розслідування та притягнення до відповідальності кіберзлочинців.

Отже, для побудови ефективної системи запобігання злочинності у сфері інформаційних технологій доцільно не лише посилювати відповідальність за вчинені кримінальні правопорушення, а й розробляти та впроваджувати комплексні заходи, спрямовані на профілактику таких злочинів.

---

1. Про правовий режим воєнного стану : Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text

2. Про основи забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.02.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text

4. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text

5. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. *Юридичний науковий електронний журнал*. Запоріжжя, 2022. № 12. С. 409–414.

6. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. *Науковий вісник Ужгородського університету*. Серія : Право. Ужгород : Видавничий дім «Гельветика», 2023. Т. 2. Вип. 75. С. 83–87.

Наукове видання

СУЧАСНІ ПРІОРИТЕТИ РОЗВИТКУ УКРАЇНИ: ЕКОНОМІЧНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Матеріали
Всеукраїнської науково-практичної конференції
(м. Дніпро, 10 жовтня 2023 р.)

Редактор, оригінал-макет – *А. В. Самотуга*
Редактор *О. М. Врублевська*

Підп. до друку 01.05.2024. Формат 60х84/16. Друк – цифровий. Папір офісний.
Гарнітура – Times. Ум.-друк. арк. 7,67. Обл.-вид. арк. 8,25. Зам. № 09/24-зб

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, sed@dduvs.edu.ua

Свідоцтво про внесення до Державного реєстру ДК № 6054 від 28.02.2018