можливість працівникам підрозділів кримінального аналізу, застосовуючи високий рівень теоретичної підготовки, практичного досвіду та спеціалізованого програмного забезпечення, на високому рівні виконувати покладені на підрозділи кримінального аналізу функції із розкриття злочинів та притягнення до відповідальності винних осіб.

Список використаних джерел

1. Закон України «Про Національну поліцію». 2015. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.

2. Наказ МВС України від 03.08.2017 № 686 «Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України». 2017. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text.

3. Наказ Національної поліції України 31.01.2020 року № 77 «Про затвердження Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України». 2020. URL: https://media-www.npu.gov.ua/npu-pre-prod/sites/1/Docs/Struktura/Polohena11.pdf.

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

ЗАХИСТ КРИТИЧНО ВАЖЛИВОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Захист критично важливої інформаційної інфраструктури (далі ЗКІІ) є основою для зусиль країн у сфері кібербезпеки. Для політиків, перед якими стоїть завдання розвивати національну систему кібербезпеки, питання визначення і 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.

Список використаних джерел

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#.

Денисенко Богдан Анатолійович,
експерт з питань спеціалізованих
правоохоронних органів
Консультативної місії Європейського
Союзу в Україні

МЕТОДОЛОГІЧНІ ЗАСАДИ OSINT

Процес цифровізації (діджиталізації), та, таким чином, генерування все більше і більше даних та інформації онлайн (та офлайн), не спинити. Таким чином, збільшується можливість більше, глибше та детальніше знаходити та верифікувати дані, інформацію щодо осіб, компаній, транспортних засобі, інших об'єктів та елементів дослідження, таким чином створюючи аналітичну розвідку (intelligence) з відкритих джерел (OSINT).

То *що ж таке OSINT (Opens Source Intelligence)*? Компанія «Reuser's Information Service» (RIS) у своєму тренінгу «OSINT Pathfinder» фокусує увагу на численних маніпуляціях з цим поняттям та визначенням. OSINT необхідно розглядати як процес, інструмент, механізм збору та продажу програмних продуктів. OSINT є спільною, інтегрованою методологією та процесом створення, де вимоги клієнта щодо аналітичної розвідки співпадають з наданою дієвою аналітичною розвідкою (*actionable intelligence*), створеною через процес синтезу та аналізу репрезентативної вибірки інформації з відкритих джерел, яка була валідованою, є надійною, вчасною та точною.