

Наведена класифікація корупційних кримінальних правопорушень, за елементами криміналістичної характеристики, дає можливість правильно, обрати методику розслідування і залежно від слідчої ситуації - тактику проведення окремих слідчих (розшукових) дій.

ЛІТЕРАТУРА:

1. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. URL : <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення 05.04.2025).
2. Закон України Про запобігання корупції (Відомості Верховної Ради (ВВР), 2014, № 49, ст.2056). URL: <https://zakon.rada.gov.ua/laws/show/1700-18#Text> (дата звернення 05.04.2025).
3. Призначення судових експертиз у кримінальних провадженнях про корупційні правопорушення [Текст] : метод. рек. / О. М. Шрамко, В. В. Юсупов, Ю. О. Пілюков, А. А. Саковський. Київ : Нац. акад. внутр. справ, 2021. – 92 с.

УДК 004.056

Уразовська О. С.

*кандидат юридичних наук, адвокат НААУ,
заступник начальника управління –
начальник відділу УКРНОІВІ
ORCID ID: 0009-0004-4136-7711*

Кібербезпека: новітні технології і виклики

У сучасних умовах кібербезпека набуває критичного значення. Цифрові (комунікаційні та/або технологічні) системи зберігають чутливу інформацію щодо безпеки і оборони нашої країни в цілому. Атаки на військових, спрямовані на отримання доступу, контролю та викрадення розвідувальної інформації зі спеціалізованих систем ситуаційної обізнаності залишаються стратегічною військовою ціллю противника.

Закон України «Про основні засади забезпечення кібербезпеки України» містить визначення важливих термінів з даної тематики, зокрема, кібербезпека, кібератака, кіберзагроза, кіберзахист, кіберзлочинність, критична інформаційна інфраструктура тощо. *Кібербезпека* – 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. *Кіберзагроза* – 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 [1].

Законодавство у сфері кібербезпеки, зокрема:

Закон України «Про основні засади забезпечення кібербезпеки України» – регулює основи кібербезпеки, визначає правові, організаційні та технічні вимоги для захисту інформаційних систем і мереж; Закон України «Про державну таємницю» – регулює порядок охорони інформації, що має статус державної таємниці; Закон України «Про інформацію» – забезпечує основи інформаційного захисту і визначає права та обов'язки стосовно обробки інформації; Закон України «Про захист персональних даних» – регулює обробку і захист персональних даних; Закон України «Про захист інформації в інформаційно-комунікаційних системах» – визначає вимоги до захисту інформації в інформаційних системах; Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» – визначає правові основи захисту інформації України; Стратегія забезпечення національної безпеки; Стратегія кібербезпеки України; Стратегія інформаційної безпеки; Стратегія воєнної безпеки України; Стратегія розвитку оборонно-промислового комплексу України тощо.

Верховна Рада України 27 березня 2025 року прийняла у повторному другому читанні та в цілому проект Закону про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури (реєстр. №11290) [2].

Суб'єкти забезпечення кібербезпеки.

Президент України здійснює координацію діяльності у сфері кібербезпеки як складової національної безпеки України.

Державна служба спеціального зв'язку та захисту інформації України є центральним органом виконавчої влади, що забезпечує здійснення повноважень регулятора комунікаційних послуг при наданні хмарних послуг.

Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, координацію суб'єктів національної системи реагування.

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю тощо [1].

Об'єктами кібербезпеки є: конституційні права і свободи людини і 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.

У період із жовтня 2023 по вересень 2024 року світовий кіберландшафт зазнав значних змін, пов'язаних з ескалацією кіберзагроз, еволюцією технологій та посиленням глобального протистояння у кіберпросторі. *Викликами є:* атаки на критичну інфраструктуру, масштабні шпигунські кампанії та зростаюча загроза від програм-вимагачів. Окрема увага приділяється впливу новітніх технологій, таких як штучний інтелект та квантові обчислення, на кіберпростір та способи посилення кіберстійкості [3].

У квітні 2024 року Європарламент ухвалив Акт про кіберсолідарність: створення кіберрезерву на рівні Європейський Союз (ЄС). В жовтні 2024 року ЄС прийняв Акт про кіберстійкість (Cyber Resilience Act). Намагаючись створити більш гнучкі механізми реагування на інциденти, у травні 2024 року Європейська Рада схвалила Керівні настанови, що сприятимуть створенню гібридних груп швидкого реагування. Вони будуть орієнтовані на протидію дезінформації, кібератакам, атакам на критичну інфраструктуру тощо [3].

Україна продовжує нарощувати власні спроможності щодо реагування на кіберінциденти. Зокрема, розширює практику проведення кібернавчань, запускає нові інструменти кібергігієни (наприклад Мінцифра запустила тест на знання правил безпеки в мережі «Кіберграм»). Україна, за підтримки міжнародних партнерів, активно розвиває систему підготовки кадрів у сфері кібербезпеки, акцентуючи на практичних заходах.

Також Україна активно розбудовує міжнародну співпрацю, у листопаді 2023 року Україна підписали Робочу угоду про співпрацю з ENISA (Європейською агенцією кібербезпеки). Для ENISA це стало першою такою угодою з партнером з-поза меж ЄС. Підписання таких документів – важливий елемент на шляху формування глобальної кіберкоаліції для протидії загрозам [3].

Новітні технології кібербезпеки:

штучний інтелект (AI) і машинне навчання (використовуються для моніторингу мережевої активності та виявлення аномалій у режимі реального часу, це допомагає виявляти кібератаки ще до того, як вони завдадуть шкоди);

шифрування даних військового рівня (використання сучасних протоколів шифрування (наприклад, AES-256) для захисту персональних та операційних даних);

блокчейн-технології (забезпечують прозорий і незмінний облік даних. Доступ можливий лише для авторизованих осіб, що унеможливорює підробку або несанкціонований перегляд);

інтегровані системи реагування на інциденти Security Information and Event Management (автоматизовані платформи для збору, аналізу та реагування на інциденти в мережі, допомагають швидко і точно ідентифікувати загрози);

кіберполігони та тренажери (спеціальні симуляційні середовища для навчання персоналу реагувати на кібератаки, без шкоди для реальних систем);

хмарні захищені платформи (використання спеціалізованих військових або сертифікованих хмарних середовищ для зберігання і обробки даних) тощо [4].

У поєднанні ці технології формують надійний кіберзахист, здатний протистояти навіть найскладнішим викликам.

Окремо слід виділити законодавство про кібертероризм. У цій галузі діє Рамкове рішення Ради ЄС від 2008 року, що вимагає криміналізувати публічне підбурювання до вчинення терористичного злочину, вербування та тренування терористів із використанням інтернету.

Найбільш відомі справи про кіберзлочинність у Європі:

Справа шведсько-німецької хакерської групи BOTNET. Її учасники створювали ботнети для кібератак на сайти та сервери різних компаній. Заподіяна шкода сягнула позначки у 85 млн євро.

Справа хакерської групи Rex Mundi, яка зламала системи низки провідних компаній Франції та вимагала викуп за неопублікацію викрадених даних.

Гучна справа хакерів Guccifer 2.0, які зламали сервери Демократичної партії США під час виборчої кампанії 2016 року. Належним чином ця справа не розслідувалась аж до сьогодні.

Кілька резонансних справ проти учасників Anonymous – міжнародного руху «хактивістів», які зламували урядові, військові, корпоративні сайти на знак протесту.

Низка гучних арештів членів Lizard Squad – хакерської групи, відомої атаками на Sony, Facebook, Пентагон, а також ігровий сервіс Xbox Live.

Крім кримінального покарання, до кіберзлочинців можуть застосовуватися процедури цивільно-правового характеру. Наприклад, стягнення збитків, позбавлення права займатися певним видом діяльності, конфіскація знаряддя і доходів від злочину, депортація з країни тощо [5].

Отже, аналізуючи досліджені матеріали, можна зробити висновок, що інвестиції в нові технології, захист робочої сили та випередження регуляторних змін матимуть вирішальне значення для забезпечення стійкості перед викликами кіберзагроз.

ЛІТЕРАТУРА:

1. Закон України «Про основні засади забезпечення кібербезпеки України». URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
2. Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури»: URL: <https://itd.rada.gov.ua/74d5da97-fe19-488d-b1b5-71bcb1cd8ecd>.
3. Річний аналітичний огляд: ключові події, тенденції та виклики у сфері кібербезпеки у 2024 році. URL: <https://www.rnbo.gov.ua/ua/Diialnist/7095.html>.
4. Інформаційні технології та кібербезпека в умовах воєнного часу [Електронний ресурс] : матеріали студ. наук.-практ. конф. (Київ, 18 квіт. 2024 р.) / відп. ред. К. В. Хорольська. – Київ : Держ. торг.-екон. ун-т, 2024. – 482 с.
5. Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю. URL: <https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu>.