Кирило ЧЕРЕВКО,
кандидат юридичних наук, доцент, професор кафедри кримінального права та кримінології Навчально-наукового інституту №1 Харківського національного університету внутрішніх справ, Харків, Україна
ORCID: https// orcid.org/0000-0002-3384-8388
e-mail:cherevko.kyrylo@gmail.com

DOI: https://doi.org/10.32620/pls.2025.67.32

ЩОДО ПИТАННЯ КІБЕРАТАК НА ІНФОРМАЦІНУ ІНФРАСТРУКТУРУ ТА КРИТИЧНУ ІНФРАСТРУКТУРУ В УКРАЇНИ

Анотація: *В ході військової агресії проти України ворог широко використовує комп'ютерні технології для вчинення воєнних злочинів шляхом здійснення кібератак на об'єкти критичної інфраструктури. Отже актуальним є вивчення питань кваліфікації таких кримінальних діянь, починаючи із основних понять з технічної сфери, розуміння яких є критичним для вирішення питання щодо достатності підстав для притягнення до кримінальної відповідальності. Тези доповіді присвячені визначенню та вивченню понять, що є визначними для складу даного виду кримінальних правопорушень: поняття «критичної інфраструктури» та віднесення певного об'єкту до критичної інфраструктури, а також поняття «кібератака», «кіберзахист» та «кіберзлочин». Використовує комп'ютерні технології для вчинення воєнних злочинів шляхом здійснення кібератак на об'єкти критичної інфраструктури.*

Ключові слова: *інформаційна* інфраструктура, критична інфраструктура, кібератака, кіберзлочин, кіберзахист.

Розвиток інформаційної інфраструктури в Україні є важливою умовою забезпечення її безпеки, основою для розвитку національної економіки та драйвером підвищення якості життя населення. При цьому спеціальним організаційним та правовим фундаментом побудови відкритого для всіх інформаційного суспільства виступає саме національна інформаційна інфраструктура як особлива система інформаційних ресурсів, інформаційних систем, засобів обміну інформації та систем забезпечення функціонування інформаційної інфраструктури.

Для повного та всебічного розуміння нам потрібно з'ясувати основні поняття пов'язані з кібератаками на інформаційну інфраструктуру та об'єкти критичної інфраструктури.

Так, «інформаційна інфраструктура»/«інформаційна система» – це сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування;

Крім технічних, цінність «інформаційної інфраструктури» /«інформаційна система» визначається такими її компонентами, як:

- інформація, яка може приймати вигляд наукових або ділових баз даних, записів звуків, бібліотечних архівів і т.п.;
- програмне забезпечення, яке дозволяє користувачам маніпулювати даними, отримувати доступ і переглядати великі масиви інформації;
- стандартні мережі і коди передач, які полегшують встановлення взаємозв'язків між мережами, забезпечують захист інформації і надійність мереж.

Виходячи з цього інформаційну інфраструктуру/«інформаційну систему» можна умовно розділити на наступні складові:

- адміністративно-господарська складова – це набір правил і інструкцій для користувачів інформаційної системи, а також адміністративні заходи обмеження доступу службовців до тієї або іншої інформації; це сукупність інформаційних служб і обчислювальних підрозділів. До цієї складової можна також відноситись підрозділи, що здійснюють управління підприємством та її координацію проектів, що виконуються відділами організації, в т.ч. інформаційними.
- системотехнічна складова – це сукупність засобів обчислювальної техніки, комунікаційного обладнання, технічних пристроїв, призначених для збору, реєстрації, зберігання, обробки, передачі і

відображення інформації, а також сукупність програмного забезпечення необхідного для роботи ІС: сукупність територіально розподілених та локальних мереж, баз даних і баз знань і т.і.

Отже, роблячи висновок можна сказати, що до «інформаційної інфраструктури» можна віднести механізми створення, передачі, обробки, збереження та використання будь якої інформації різної природи (в тому числі критичної інфраструктури), що формується та передається за допомогою програмного забезпечення, технічних засобів, правил та законів.

Наступним поняттям є об'єкти критичної інфраструктури. Так, до об'єктів інфраструктури відносимо 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

Категорія критичності об’єкта критичної інфраструктури визначається на основі аналізу рівня негативного впливу, якого особа, суспільство, навколишнє природне середовище, економіка, національна безпека та обороноздатність країни можуть зазнати внаслідок порушення або припинення функціонування об’єкта інфраструктури відповідно до критеріїв

Відповідно до Постави Кабінету міністрів України у нас існує 25 секторів, які віднесені до критичної інфраструктури. Основні з них це: Паливно-енергетичний сектор; Цифрові технології; Захист інформації; Системи життєзабезпечення; Харчова промисловість та агропромисловий комплекс; Державний матеріальний резерв; Охорона здоров’я; Ринки капіталу та організовані товарні ринки; Фінансовий сектор; Транспорт і пошта; Промисловість; Сектор громадської безпеки; Цивільний захист населення і територій; Міграція (імміграція та еміграція); Охорона навколишнього природного середовища; Сектор оборони; Національна безпека; Правосуддя; Тримання під вартою; Наукові дослідження та розробки; Фінансовий сектор; Вибори та референдуми; Соціальний захист; Інформаційні послуги; Державна влада та місцеве самоврядування.

Це вичерпний перелік всіх об’єктів які відповідно до нашого законодавства відносяться до критичної інфраструктури і будь яка атака на них може привести до незворотних негативних наслідків, особливо в час повномасштабного вторгнення російсько федерації на нашу країну.

Наступним важливим терміном для розуміння є «кібератака» (хакерська атака) - кібернетична атака це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, інформаційної інфраструктури/системи що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан.

Хакерська атака (кібератака) – спроба реалізації загрози. Тобто, це дії кібер-зловмисників (хакерів) або шкідливих програм, які спрямовані на захоплення інформаційних даних віддаленого комп'ютера, отримання повного контролю над ресурсами комп'ютера або на виведення системи з ладу.

Під атакою (англ. attack, англ. intrusion) на інформаційну інфраструктуру, систему розуміють дії (процеси) або послідовність зв'язаних між собою дій порушника, які приводять до реалізації загроз інформаційним ресурсам шляхом використання вразливостей цієї інформаційної системи.

Типи атак на інформаційні інфраструктури/системи:

- Віддалене проникнення (remote penetration),
- Локальне проникнення (local penetration),
- Атака на відмову в обслуговуванні (denial of service),
- Мережні сканери (network scanners),
- Сканери уразливостей (vulnerability scanners),
- Зламувачі паролів (password crackers),
- Аналізатори протоколів (sniffers),
- Спам e-mail (Mailbombing),
- Перехоплення каналу зв'язку (Man-in-the-Middle),
- Фішинг,
- SQL-ін’єкції,
- Міжсайтові сценарії (XSS).

Переважна більшість складів кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку є матеріальними, тому можуть бути виявлені за

наслідками. Отже, під час кваліфікації та їх відмежуванні від суміжних складів кримінальних правопорушень, необхідно оцінювати розмір та значення заподіяної шкоди з точки зору характеристики її предмету.

K. Cherevko

On the issue of cyberattacks on information and critical infrastructure in Ukraine.

Abstract: In the course of military aggression against Ukraine, the enemy widely uses computer technologies to commit war crimes by means of cyber attacks on critical infrastructure facilities. Therefore, it is relevant to study the issues of qualification of such criminal acts, starting with the basic concepts from the technical field, the understanding of which is critical to resolve the issue of the sufficiency of the grounds for criminal prosecution. The theses of the report are devoted to the definition and study of the concepts that are crucial for the composition of this type of criminal offenses: the concept of "critical infrastructure" and the classification of a certain object as critical infrastructure, as well as the concepts of "cyberattack", "cyber defense" and "cybercrime". It uses computer technology to commit war crimes by conducting cyberattacks on critical infrastructure facilities.

Keywords: information infrastructure, critical infrastructure, cyberattack, cybercrime, cyber defense.

Зразок для цитування:

Черевко К. Щодо питання кібератак на інформаціну інфраструктуру та критичну інфраструктуру в України. Пропілеї права та безпеки, 2025. №6-7. С. 114-116. DOI: https://doi.org/10.32620/pls.2025.67.32.