УДК 343.3/344 *DOI: https://doi.org/10.32631/vca.2024.1.15*

Дмитро Валентинович ПАШНЄВ,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ, м. Харків)

Кирило Олександрович ЧЕРЕВКО,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ, м. Харків)

КІБЕРАТАКИ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ ВЕДЕННЯ ВІЙНИ: КЛЮЧОВІ ПОНЯТТЯ

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. Стаття присвячена 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».

Ключові слова: *критична інфраструктура, інформаційна інфраструктура, кібератака, інформаційна система, ведення війни, війна, кримінальне правопорушення, злочинність, протидія злочинності*.

Постановка проблеми. Сучасний світ розвивається в умовах процесів діджиталізації всіх сфер нашого суспільства. Інноваційні технології стають невід'ємною частиною життя і вже відіграють ключову роль в організації нашої роботи та відпочинку. Проте більшість усіх технологій базується виключно на використанні даних, інформації різного типу, яка опрацьовується відповідними програмними продуктами, новітніми технологіями. Інформація на сьогодні вже є не лише одним із базових ресурсів, від якого залежить існування, функціонування тих, або інших об'єктів, явищ, систем, але це й ресурс їх оновлення, трансформації та розвитку. Відповідно, така важлива роль інформації в нашому житті, в організації ефективного функціювання окремих економічних об'єктів зумовлює постійний пошук учених у створенні найбільш досконалих методів та механізмів роботи з даними, які дозволяли б максимально спростити ті процеси, які доцільно автоматизувати, уніфікувати. Інформація – це ресурс також змін та управління, оскільки саме її обіг усередині окремих систем дозволяє їм розвиватися, удосконалюватися, адаптуватися під зміни зовнішнього світу й постійно забезпечувати власний розвиток, виконувати необхідні функції.

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.

На різному рівні проблеми кібератак на критичну інфраструктуру, зокрема, інформаційну, розглядались в працях таких вітчизняних науковців, як О. Ю. Козлова, В. Г. Кононович, І. В. Кононович, М. Г. Романюков, Л. М. Тимошенко та ін. Втім, лишаються вільни зони наукового пошуку, пов'язані з дослідженням означеної проблематики в умовах війни.

Виклад основного матеріалу. За даними Держспецзв'язку[1], кількість кібератак у першому півріччі 2023 року зросла на 123% — із 342 за аналогічний період минулого року. Так, 28 серпня 2023 року, згідно повідомлення Держспецзв'язку, в Україні зафіксували нову хакерську атаку на органи юстиції та нотаріату. Хакери розповсюджують електронні листи зі шкідливою програмою «AsyncRAT». За даними відомства хакери надсилають електронні листи із вкладеннями у вигляді BZIP, GZIP чи RAR-архіву. Відкриття файлу призводить до ураження комп'ютера шкідливою програмою «AsyncRAT», яка надає віддалений доступ до пристрою. Небезпечні листи мають специфічні теми та назви файлів. Наприклад: Лист відділу з питань нотаріату у Дніпропетровській області – «.rar». Лист до

[1] Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua.

відома та виконання – «.cmd». Лист МЮУ для доведення до відома та врахування в роботі – «.exe; .bzip».

Для повного та всебічного розуміння та з'ясування основних понять, пов'язаних з кібератаками на об'єкти критичної інфраструктури, очевидно слід почати із поняття **«**інформаційна інфраструктура**»**, складові частини якої найчастіше є безпосередніми об'єктами вказаних атак.

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[1].

Крім технічних, ***цінність «інформаційної інфраструктури» / «інформаційної системи» визначається такими її компонентами, як:***

5 інформація, яка може приймати вигляд наукових або ділових баз даних, записів звуків, бібліотечних архівів і т. п.;

6 програмне забезпечення, яке дозволяє користувачам маніпулювати даними, отримувати доступ і переглядати великі масиви інформації;

7 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:

8 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.

9 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. ін.

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.

[1] Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL: https://www.kmu.gov.ua/npas/246420577.

В ході кібератаки об'єкт інформаційної інфраструктури може бути безпосереднім об’єктом завдання шкоди або виступати системою керування іншим ***об'єктом критичної інфраструктури,*** що є наступним поняттям, яке слід з’ясувати. До об'єктів критичної інфраструктури відносимо системи, їх частини та їх сукупність, які є ***важливими для економіки, національної безпеки та оборони,*** порушення функціювання яких може завдати шкоди життєво важливим національним інтересам[1].

Категорія ***критичності*** об’єкта 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 функціювання об’єкта інфраструктури відповідно до критеріїв.

Відповідно до Постави Кабінету міністрів України існує 25 секторів, які віднесені до критичної інфраструктури: 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[2].

В свою чергу виділяються наступні типи основних послуг в цих сферах: виробництво електричної енергії, забезпечення функціонування ринку електричної енергії, організація купівлі-продажу електричної енергії на ринку, управління системами передачі та енергопостачання, розподіл електричної енергії, видобуток вугілля для генерації електроенергії на теплоелектростанціях та теплоелектро-централях, зберігання та постачання вугілля, розробка родовищ торфу, видобування корисних копалин, видобуток нафти, передача (транзит) нафти та нафтопродуктів, очищення, переробка та обробка нафти, експлуатація нафтопроводів, зберігання та постачання нафти та нафтопродуктів, видобуток газу, переробка та очищення газу, передача (транзит) газу, розподіл газу, забезпечення роботи систем зрідження природного газу, експлуатація газотранспортної системи, зберігання природного газу, забезпечення роботи систем зрідження природного газу, виробництво ядерного палива, експлуатація ядерних підкритичних установок, ядерних реакторів, які включають критичні та підкритичні збірки дослідницьких реакторів, експлуатація атомних електростанцій, підприємств і установок по

[1] Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

[2] Деякі питання об’єктів критичної інфраструктури : постанова Кабінету міністрів України від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.

збагаченню та переробці палива, а також сховищ відпрацьованого палива, надання електронних довірчих послуг, електронної ідентифікації та автентифікації, забезпечення функцій центрального засвідчувального органу, адміністрування адресного простору українського сегмента Інтернету, забезпечення функціонування системи електронної взаємодії органів виконавчої влади, забезпечення функціонування системи міжвідомчої взаємодії між органами державної влади, органами місцевого самоврядування та суб'єктами господарювання, надання електронних публічних послуг, автоматизація процесів надання адміністративних послуг, забезпечення функціонування правового режиму Дія Сіті, надання послуг (сервісів) кіберзахисту, постачання теплової енергії, постачання гарячої води, централізоване питне водопостачання, централізоване водовідведення, поводження з побутовими відходами, виробництво та переробка сільськогосподарської та/або харчової продукції, виробництво ветеринарних препаратів, експлуатація елеваторів, експлуатація зрошувальних систем, каналів, забезпечення зберігання запасів державного матеріального резерву, забезпечення надання екстреної медичної допомоги, забезпечення надання первинної медичної допомоги, забезпечення надання вторинної (спеціалізованої) медичної допомоги, забезпечення надання третинної (високоспеціалізованої) медичної допомоги, забезпечення надання паліативної медичної допомоги, забезпечення надання реабілітації у сфері охорони здоров'я, заготівля і тестування донорської крові та компонентів крові, контроль за інфекційними захворюваннями та/або епідеміями, оплата згідно з тарифом за надані пацієнтам медичні послуги (включаючи медичні вироби) та лікарські засоби за договорами про медичне обслуговування населення за програмою медичних гарантій, функціонування електронної системи охорони здоров'я, виробництво та постачання лікарських засобів і медичних виробів, наукові дослідження в медичній галузі, забезпечення функціонування ринків капіталів та організованих товарних ринків, планування, виконання та моніторинг виконання бюджетів, розрахунково-касове обслуговування розпорядників та одержувачів бюджетних коштів, здійснення контролю за надходженням до бюджетів та державних цільових фондів податків, зборів, платежів, управління повітряним рухом, авіаперевезення (робота авіаційного транспорту), забезпечення роботи аеропортів та допоміжного обладнання, що розташоване в аеропортах, автобусні перевезення (міжміські, міжнародні), міські перевезення (автобуси, трамваї, тролейбуси, метрополітен), технічне обслуговування транспортної інфраструктури (доріг, мостів, тунелів, шляхопроводів), служби контролю трафіку, функціонування інтелектуальних транспортних систем (управління рухом, мобільністю, взаємодія з іншими видами транспорту), пасажирські залізничні перевезення, вантажні залізничні перевезення, експлуатація та технічне обслуговування залізниці, забезпечення роботи вокзалів та вузлових станцій, контроль і управління судноплавством, операції на внутрішньому, морському або прибережному

пасажирському та вантажному транспорті, функціонування керуючих органів портів або суб'єктів експлуатації портового обладнання, експлуатація та обслуговування інфраструктури (каналів, дамб, фарватерів тощо), регулювання руху суден, лоцманське проведення суден, надання послуг поштового зв'язку, виробництво промислового газу, виробництво добрив або азотистих сполук, виробництво пестицидів або інших агрохімічних продуктів, виробництво вибухових речовин, виробництво основних органічних хімічних речовин, виробництво основних неорганічних речовин, гірничо-металургійний комплекс (металургійне виробництво та добування залізних руд), виробництво коксу та коксопродуктів, розробка, виробництво, модернізація та утилізація продукції військового призначення (оборонно-промисловий комплекс), виробництво та постачання космічної техніки, космічна діяльність, космічні технології та послуги, виробництво та постачання продукції авіаційної промисловості, суднобудування та постачання продукції суднобудування, охорона публічного (громадського) порядку, фізичний захист критичної інфраструктури, надання екстреної допомоги населенню за єдиним телефонним номером 112, реагування на надзвичайні ситуації, проведення аварійно-рятувальних та інших невідкладних робіт з ліквідації наслідків надзвичайних ситуацій, надання допомоги постраждалим, оформлення документів, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус, забезпечення задоволення потреб населення і галузей економіки у водних ресурсах, проектування, будівництво і реконструкція систем захисту від шкідливої дії вод, групових і локальних водопроводів, систем водопостачання та каналізації у сільській місцевості, гідротехнічних споруд, водогосподарських об'єктів багатоцільового використання, захист від підтоплення захисних масивів, протипаводковий і протиповеневий захист, довгострокове зберігання і захоронення радіоактивних відходів, охорона, раціональне використання земель та надр, охорона, раціональне використання і відтворення об'єктів природно-заповідного фонду, ведення лісового і мисливського господарства, поводження з відходами, небезпечними хімічними речовинами, пестицидами та агрохімікатами, створення, дослідження та практичне використання генетично модифікованих організмів у відкритій системі, оборона, забезпечення зберігання боєприпасів, вибухових речовин, виробництво ракет, боєприпасів, вибухових речовин, захист національної державності, охорона державної таємниці, боротьба з тероризмом, здійснення правосуддя, тримання засуджених та осіб, взятих під варту, в установах виконання покарань та слідчих ізоляторах Державної кримінально-виконавчої служби, наукова діяльність, надання послуг з використання наукового обладнання (у тому числі інструментів, приладів, інвентарю), дослідницька діяльність, надання банківських послуг, зберігання банками запасів готівки Національного банку та проведення операцій із ними, надання електронних довірчих послуг у банківській системі, надання небанківських фінансових послуг, надання платіжних послуг, організація підготовки та проведення

виборів та референдумів, забезпечення пенсійних виплат, надання матеріального забезпечення і страхових виплат, забезпечення соціальних виплат та надання соціальних послуг, надання адміністративних послуг соціального характеру в електронній формі, надання послуг у сфері телебачення та радіомовлення, надання послуг в інформаційній та видавничій сферах, виконання функцій держави, виконання функцій місцевого самоврядування[1].

Це вичерпний перелік всіх сфер, об'єкти у яких відповідно до нашого законодавства відносяться до критичної інфраструктури і будь-який зовнішній вплив на них може привести до незворотних негативних наслідків, особливо під час повномасштабного вторгнення російської федерації у нашу країну.

Наступним важливим терміном для розуміння є ***«кібератака»*** (кібернетична атака, хакерська атака) – це цілеспрямовані (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, 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[2].

Пов'язаним поняттям зі сфери кібербезпеки є ***«кіберзагроза» –*** наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на її стан[3]. Хакерська атака (кібератака) – це фактично спроба реалізації кіберзагрози. 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.

Отже, під ***«кібератакою»*** слід розуміти атаку на інформаційну інфраструктуру, як сукупність (систему) зв'язаних між собою дій порушника (ініційованих ним процесів), які приводять до реалізації загроз інформаційним ресурсам шляхом використання вразливостей певної інформаційної системи як частини інформаційної інфраструктури.

Умовно можна виділити два типи кібератак в залежності від

[1] Деякі питання об'єктів критичної інфраструктури : постанова Кабінету міністрів України від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

[2] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[3] Там само.

місцезнаходження зловмисника в момент атаки, що суттєво для визначення кола винних осіб та ступеня їх вини:

10 локальне проникнення (local penetration) – зловмисник знаходиться всередині об'єкта і використовує прямий доступ до інформаційної системи;

11 віддалене проникнення (remote penetration) – зловмисник знаходиться зовні об'єкта і використовує віддалений доступ до інформаційної системи[1].

Найбільш розповсюдженими видами віддалених (зовнішніх) кібератак є наступні.

Атака на відмову в обслуговуванні (denial of service або DoS) – це атака, що має своєю метою змусити сервер не відповідати на запити. Такий вид атаки не передбачає отримання деякої секретної інформації, але іноді буває підмогою в ініціалізації інших атак. Наприклад, деякі програми через помилки в своєму коді можуть викликати виняткові ситуації, і при відключенні сервісів здатні виконувати код, наданий зловмисником або атаки лавинного типу, коли сервер не може обробити величезну кількість вхідних пакетів. DDoS (від англ. Distributed Denial of Service - Розподілена DoS) – підтип DoS-атаки, що має ту ж мету що і DoS, але що проводяться не з одного комп'ютера, а з декількох комп'ютерів в мережі. У даних типах атак використовується або виникнення помилок, що призводять до відмови сервісу, або спрацьовування захисту, що приводить до блокування роботи сервісу, а в результаті також до відмови в обслуговуванні. DDoS використовується там, де звичайний DoS неефективний. Для цього кілька комп'ютерів об'єднуються, і кожен виробляє DoS-атаку на систему жертви. Разом це називається DDoS-атака. Будь-яка атака являє собою не що інше, як спробу використовувати недосконаліть системи безпеки жертви або для отримання інформації, або для нанесення шкоди системі, тому причиною будь-якої вдалої атаки є професіоналізм крекерів і цінність інформації, а також недостатня компетенція адміністратора системи безпеки зокрема, недосконаліть програмного забезпечення та недостатня увага до питань безпеки в компанії в цілому[2].

Спам e-mail (Mailbombing) – вважається найстарішим методом атак, хоча суть його проста і примітивна: велика кількість поштових повідомлень роблять неможливими роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Для цієї мети було розроблено безліч програм, і навіть недосвідчений користувач може зробити атаку, вказавши всього лише e-mail жертви, текст повідомлення, і кількість необхідних повідомлень. Такі програми дозволяють ховати реальний IP-адрес відправника, використовуючи для розсилки анонімний поштовий сервер. Цій атаці складно запобігти, так як навіть поштові фільтри провайдерів не

[1] Інформаційна безпека в комп'ютерних мережах : навч. посіб. / О. А. Смірнов, О. К. Конопліцька-Слободенюк, С. А. Смірнов та ін. Кропивницький : Видавець Лисенко В. Ф., 2020. С. 87.

[2] Хакерська атака / Новини в світі IT-технологій. URL: http://kompnews.at.ua/index/ataka_na_vidmovu_v_obslugovuvanni/0-28

можуть визначити реального відправника спаму. Провайдер може обмежити кількість листів від одного відправника, але адреса відправника і тема часто генеруються випадковим чином[1].

Перехоплення каналу зв'язку (Man-in-the-Middle) – вид атаки, коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. При отриманні доступу на такому рівні зловмисник може модифікувати інформацію потрібним йому чином, щоб досягти своєї цілі. Мета такої атаки – незаконне отримання, крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі. Такі атаки вкрай складно відстежити, оскільки зазвичай зловмисник знаходиться всередині організації[2].

Фішинг – це надсилання шахрайських електронних листів від імені авторитетних компаній або інших надійних джерел. Зловмисники використовують фішинг, щоб отримувати доступ до даних у персональній або корпоративній мережі[3].

SQL-ін'єкції – це спосіб поширення шкідливого ПЗ через програми, як-от LinkedIn і Target, який дає змогу кіберзлочинцям викрадати або видаляти дані, а також керувати ними[4].

Міжсайтові сценарії (XSS) – міжсайтові сценарії полягають у тому, що кіберзлочинець надсилає заспамлені або вражені сценаріями посилання на вашу електронну пошту. Щойно ви їх відкриваєте, зловмисник отримує ваші персональні дані[5].

Для пошуку способів проникнення у інформаційну систему широко використовуються спеціальні програмно-технічно засоби: мережні сканери (network scanners), сканери уразливостей (vulnerability scanners), зламувачі паролів (password crackers), аналізатори протоколів (sniffers) тощо[6].

Зокрема, аналізатори протоколів (sniffers) **–** досить поширений спосіб отримання інформації, заснований на роботі мережевої карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. В такому режимі всі пакети, отримані мережевою картою, пересилаються на обробку спеціальному додатку, званому сніффером. В результаті зловмисник може отримати велику кількість службової інформації: хто, звідки і куди передавав пакети, через які адреси ці пакети проходили. Найбільшою небезпекою такої атаки є отримання самої інформації, наприклад логінів і паролів співробітників, які можна використовувати для незаконного

[1] Управління інформаційною та/або кібербезпекою / Основи кібербезпеки. URL: https://e-tk.lntu.edu.ua/pluginfile.php/25378/mod_resource/content/1/%D0%A2%D0%95%D0%9C%D0%90%2019.pdf.

[2] Управління інформаційною та/або кібербезпекою / Основи кібербезпеки. URL: https://e-tk.lntu.edu.ua/pluginfile.php/25378/mod_resource/content/1/%D0%A2%D0%95%D0%9C%D0%90%2019.pdf.

[3] Що таке кібератака? / Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack.

[4] Там само.

[5] Там само.

[6] Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. Суми : Сумський державний університет, 2021. С. 24.

проникнення в систему під виглядом звичайного співробітника компанії[1].

Висновки. До «інформаційної інфраструктури» слід відносити 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. В ході кібератаки об'єкт інформаційної інфраструктури може бути безпосереднім об’єктом критичної інфраструктури, якому завдається шкода, або виступати системою керування іншим об'єктом критичної інфраструктури, вичерпний перелік яких надається в законодавстві.

Щодо поняття «кібератака» (хакерська атака) можна сказати, що це – атака спрямованої (навмисної) дії в кіберпросторі, яка здійснюється за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямована на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, 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 захищені об’єкти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. Суми : Сумський державний університет, 2021. 99 с.
2. Деякі питання об’єктів критичної інфраструктури : постанова Кабінету міністрів України від 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text.
3. Інформаційна безпека в комп’ютерних мережах : навч. посіб. / О. А. Смірнов, О. К. Конопліцька-Слободенюк, С. А. Смірнов та ін. Кропивницький : Видавець Лисенко В. Ф., 2020. 295 с.
4. Офіційний сайт Державної служби спеціального зв’язку та захисту інформації України. URL: https://cip.gov.ua/ua.
5. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

[1] Безпека інформації : конспект лекцій / укладач О. С. Кушнерьов. Суми : Сумський державний університет, 2021. С. 25.

7. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL: https://www.kmu.gov.ua/npas/246420577.

8. Управління інформаційною та/або кібербезпекою / Основи кібербезпеки. URL: https://e-tk.lntu.edu.ua/pluginfile.php/25378/mod_resource/content/1/%D0%A2%D0%95%D0%9C%D0%90%2019.pdf.

9. Хакерська атака / Новини в світі IT-технологій. URL: http://kompnews.at.ua/index/ataka_na_vidmovu_v_obslugovuvanni/0-28.

10. Що таке кібератака? / Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack.

Стаття надійшла до редакції 10.03.2024

Dmytro V. PASHNIEV,
PhD in Law, Associate Professor
(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)

Kyrylo O. CHEREVKO,
PhD in Law, Associate Professor
(Kharkiv National University of Internal Affairs, Kharkiv, Ukraine)

CYBER ATTACKS ON CRITICAL INFRASTRUCTURE FACILITIES IN WARFARE: KEY CONCEPTS

In the course of military aggression against Ukraine, the enemy widely uses computer technologies to commit war crimes by carrying out cyber attacks on critical infrastructure objects. 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 for solving the question of the sufficiency of the grounds for bringing criminal responsibility. The article is devoted to the definition and study of concepts that are significant for the composition of this type of criminal offense: the concept of «critical infrastructure» and the problems of assigning a certain object to critical infrastructure, as well as the concept of «cyber attack».

Keywords: *critical infrastructure, information infrastructure, cyberattack, information system, warfare, war, criminal offence.*