КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.719
УДК 342.738:004.056.5:004.738.5

Ільєнко Анна Вадимівна
кандидат технічних наук, доцент, завідувач кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0001-8565-1117
anna.ilienko@npp.nau.edu.ua

Телющенко Валентина Анатоліївна
асистент кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0001-6026-5105
valentyna.teliushchenko@npp.nau.edu.ua

Дубчак Олена Вікторівна
старший викладач кафедри Кібербезпеки
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0001-9739-3960
3915922@npp.kai.edu.ua

СУЧАСНІ КІБЕРЗАГРОЗИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ТА СВІТУ

Анотація. Критична інфраструктура є основою стабільного функціонування держави та суспільства, однак її залежність від цифрових технологій робить її вразливою до кіберзагроз. У 2024 році було зафіксовано понад 3 мільйони подій інформаційної безпеки, серед яких 28 тисяч були класифіковані як критичні, що вимагає глибокого аналізу та розробки нових підходів до управління ризиками. У цій статті розглядаються сучасні кіберзагрози для критичної інфраструктури, включаючи кібершпигунство, викрадення коштів, інформаційно-психологічні операції та атаки на промислові системи. На основі аналізу було виділено основні типи атак: програми-вимагачі, DDoS-атаки, соціальна інженерія та експлойти нульового дня. Особливу увагу приділено секторам енергетики, транспорту, фінансів і цифрової інфраструктури, які є найуразливішими до атак. Стаття також містить аналіз міжнародного досвіду та стандартів, таких як ENISA Threat Landscape та директива NIS2, що демонструють ефективні практики забезпечення кібербезпеки. Аналіз міжнародного досвіду демонструє, що ефективний кіберзахист потребує багаторівневого підходу. Це включає моніторинг мереж у реальному часі, автоматизовані інструменти управління вразливостями, удосконалення систем оцінки ризиків, впровадження багатофакторної автентифікації та підвищення кіберобізнаності персоналу. Використання інноваційних підходів дозволить значно зменшити вплив кіберзагроз та забезпечити безперервну роботу критичної інфраструктури. Результати цього дослідження вказують на важливість інтеграції сучасних підходів та технологій у системи захисту критичної інфраструктури, що дозволить мінімізувати ризики та забезпечити стабільність функціонування ключових секторів держави.

Ключові слова: кібербезпека; захист даних; атаки; кіберзагрози; соціальна інженерія; критична інфраструктура; дезінформація; інформаційна безпека; вразливості.

ВСТУП

Постановка завдання дослідження

Критична інфраструктура є невід’ємною частиною сучасного суспільства та має вагоме значення для забезпеченні стабільності, добробуту та безпеки суспільства. Поняття «критична інфраструктура» викладено у Законі України «Про критичну інфраструктуру та її захист», де трактується як сукупність об’єктів, які є стратегічно

важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди важливим національним інтересам [1]. До цієї категорії належать об'єкти та системи, які забезпечують основні послуги: енергопостачання, водопостачання, телекомунікації, транспорт, фінансові послуги, охорона здоров'я, управління надзвичайними ситуаціями, тощо. Порушення в роботі цих систем можуть викликати серйозні наслідки для соціальної та економічної сфери держави, створити загрозу для життя людей, негативно вплинути на рівень обороноздатності та національної безпеки країни. Тому, основним завданням критичної інфраструктури є забезпечення безперервного надання життєво необхідних послуг.

Враховуючи залежність критичної інфраструктури від інформаційних технологій, вона стає вразливою до кіберзагроз, тому функціонування, управління та безпека її залежить від кіберзахищеності цифрових систем. Сьогодні кіберзлочинці все частіше використовують складні методи атак, які спрямовані на дестабілізацію об'єктів критичної інфраструктури, що в свою чергу спричиняє масштабні збої в роботі і приводить до негативно наслідків у економічній сфері, завдаючи величезних збитків, провокує соціальні кризи, екологічні катастрофи, порушує національну безпеку країни.

Тільки у 2023 році урядова команда CERT-UA, яка функціонує при Держспецзв'язку України, опрацювала 2543 кіберінциденти, що на 15,9% більше порівняно з попереднім роком. Зростання кількості атак обумовлене, зокрема, повномасштабною російською агресією. Основними цілями зловмисників залишаються урядові організації, місцеві органи влади, сектор безпеки та оборони, комерційні компанії, енергетична галузь, телекомунікації та критична інфраструктура. Найпоширеніші методи атак включають розповсюдження шкідливого програмного забезпечення, фішинг, шкідливі підключення, компрометацію облікових записів і систем [2]. За даними Державної служби спеціального зв'язку та захисту інформації України, урядова команда CERT-UA у 2024 році опрацювала 4315 кіберінцидентів, що на 69,8% більше порівняно з 2023 роком, коли було зафіксовано 2541 інцидент [15]. Зокрема, 19 грудня 2024 року сталася одна з наймасштабніших кібератак на державні реєстри України, організована російськими хакерами. Через цю атаку було тимчасово припинено роботу єдиних та державних реєстрів, підпорядкованих Міністерству юстиції, що спричинило значні перебої у функціонуванні критично важливої інфраструктури. За даними компанії Check Point Research, у 2024 році кількість кібератак на енергетичні компанії США зросла на 70% порівняно з аналогічним періодом 2023 року, що свідчить про глобальну тенденцію до зростання кіберактивності проти критичної інфраструктури. Необхідно дослідити основні типи загроз для об'єктів критичної інфраструктури з метою впровадження комплексного підходу для їхнього попередження, виявлення та нейтралізації.

Аналіз останніх досліджень та публікацій. Останні дослідження та публікації у сфері захисту критичної інфраструктури висвітлюють актуальні виклики та пропонують шляхи їх подолання. Науковим дослідженням окремих питань безпеки об'єктів критичної інфраструктури присвячено роботи таких науковців, С. Гнатюк, А. Андрух, Ю. Юрченко, О. Юдін, Л. Арсенович, С. Братель, О. Батюк, І. Гора, Б. Леонов, Я. Маніулов, О. Скіцько, Р. Ширшов, Д. Мельник.

У науковій статті кандидата юридичних наук, професора, першого проректора Одеського державного університету внутрішніх справ С. Братель проаналізовано міжнародний досвід у сфері захисту критичної інфраструктури, зокрема розвиток державної політики та впровадження ефективних механізмів безпеки в різних країнах [3].

Сучасні виклики, пов'язані з кібербезпекою об'єктів критичної інфраструктури розглядалися у статті головного наукового співробітника О. Скіцько та наукового співробітника Р. Ширшова Національної академії Служби безпеки України. У статті звертається увага на значну вразливість цифрової інфраструктури України перед атаками з боку державних і кримінальних кіберзловмисників, особливо в таких ключових секторах, як енергетика та фінанси. Наголошується, що ці атаки часто спрямовані на дестабілізацію державних інститутів і критично важливих галузей економіки, що створює потенційну загрозу для національної безпеки [4].

Орієнтовний перелік об'єктів вітчизняної критичної інформаційної інфраструктури, що потребують посиленого захисту, представлений в науковому дослідженні кандидата юридичних наук, доцента, провідного наукового співробітника Міжвідомчого науково-дослідного центру при Раді національної безпеки і оборони України Д. Мельника. [5].

Незважаючи на значні дослідження в даній сфері на сьогодні необхідно більш детальніше проаналізувати типові загрози об'єктів критичної інфраструктури для вдосконалення комплексного підходу захисту інформаційних систем даних об'єктів.

Постановка проблеми

Метою даної статті є узагальнення сучасних загроз критичній інфраструктурі, оцінка їхнього впливу на стійкість інформаційних систем та ідентифікація перспективних напрямів захисту на основі вітчизняного та міжнародного досвідів. У роботі аналізуються сучасні кіберзагрози, спрямовані на об'єкти критичної інфраструктури, такі як енергетика, транспорт, фінанси та державне управління.

Основні завдання:

1. Провести аналіз типових кіберзагроз, які впливають на функціонування критичних систем.
2. Оцінити сучасний ландшафт кіберзагроз у 2024 році, враховуючи найактивніші загрози, такі як кібершпигунство, викрадення коштів та інформаційно-психологічні операції.
3. Визначити особливості впливу атак на об'єкти критичної інфраструктури в Україні.
4. Узагальнити міжнародний досвід у галузі виявлення та управління кіберзагрозами для формування перспектив подальших досліджень.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Відповідно до Закону України «Про критичну інфраструктуру», об'єкти відносять до критичної інфраструктури на основі сукупності критеріїв, які визначають їхню важливість: соціальну, політичну, економічну, екологічну і підтримують обороноздатність країни, безпеку громадян, суспільства, держави тощо. До цих критеріїв відносять: забезпечення такими об'єктами життєво важливих національних інтересів, наявність загроз, уразливість таких об'єктів, що призведе до негативних наслідків в економіці, втрати природних ресурсів, заподіяння шкоди здоров'ю населення, неможливість забезпечувати критичні потреби суспільства, гарантувати державний суверенітет. Також враховуються масштабність негативного впливу, тривалість ліквідації наслідків, їхній подальший вплив на державу та функціонування інших секторів критичної інфраструктури [1].

Для встановлення рівня вимог щодо захисту об’єктів критичної інфраструктури (ОКІ) відповідно до їх важливості та впливу на життєво важливі функції, проводиться категоризація об’єктів за рівнем критичності.

Законом України встановлено чотири категорії критичності об’єктів критичної інфраструктури, що враховують масштаби можливих наслідків від порушення функціонування таких об’єктів та рівень їх впливу на інші елементи критичної інфраструктури. Об’єкти розподіляються за рівнями критичності: національного значення, регіонального, локального значення. Категоризація об’єктів критичної інфраструктури є основою для забезпечення їх належного захисту. Вона допомагає визначити рівень загроз і пріоритетність заходів безпеки залежно від впливу об’єкта на життєво важливі функції країни, регіонів чи місцевих громад. Завдяки цьому забезпечується узгодженість у прийнятті рішень щодо захисту стратегічно важливих об’єктів, що сприяє підвищенню національної безпеки та стійкості країни до кризових ситуацій.

З огляду на важливу роль об’єктів критичної інфраструктури у забезпеченні стабільного функціонування держави, добробуту суспільства та наданні життєво необхідних послуг, без яких неможлива нормальна діяльність різних сфер життя, необхідно постійно розробляти й впроваджувати ефективні стратегії та методи ідентифікації потенційних загроз. Це дозволить визначити їхні основні типи та забезпечити оперативне реагування з метою запобігання, нейтралізації та мінімізації можливих негативних наслідків.

Сучасні загрози все більше спрямовані на цифрові та інформаційні технології і стають дедалі складнішими, витонченими та руйнівними, тому особливу увагу необхідно приділяти підвищенню рівня кібербезпеки ОКІ.

За даними Служби безпеки України (СБУ), кількість кібератак на об’єкти систем зв’язку, управління Сил оборони, об’єкти критичної інфраструктури України та банківського сектора суттєво зросла з 800 у 2020 році до 4500 у 2022 та 2023 роках.

У 2024 році ландшафт кіберзагроз для критичної інфраструктури України залишався динамічним і багатогранним. Було зафіксовано 3 мільйони подій інформаційної безпеки, з яких 28 000 класифікувалися як критичні та вимагали втручання експертів. У результаті детального аналізу ідентифіковано 1 042 кіберінцидентів (рис. 1).

Рис. 1. Загальний ландшафт кіберзагроз критичної інфраструктури України у 2024 році

На міжнародному рівні ключовим центром експертизи у сфері кібербезпеки та одним із основних координаторів є Агентство Європейського Союзу з кібербезпеки (ENISA), яке надає аналітичну підтримку, проводить дослідження та розробляє стратегії підвищення кібербезпеки в країнах Євросоюзу. Агентство аналізує поточні кіберзагрози, розробляє рекомендації для зміцнення безпеки, організовує навчання і симуляції кіберінцидентів, а також підтримує міжнародні ініціативи з кібербезпеки. Політики в Європейській комісії та Європейському парламенті часто покладаються на досвід ENISA для формулювання пропозицій, пов'язаних з кібербезпекою, наприклад, розробка нових директив чи оновлення існуючих правових інструментів.

ENISA також регулярно публікує звіти про ландшафт кіберзагроз, що дозволяє державам-членам і підприємствам оперативно адаптувати свої стратегії кібербезпеки відповідно до актуальних викликів.

Згідно з останнім звітом «ENISA Threat Landscape 2024», опублікованим у вересні 2024 року, було визначено сім основних типів кіберзагроз [6]:

1. Програми-вимагачі (Ransomware) — тип кібератаки, коли зловмисники отримують контроль над активами організації (включаючи шифрування даних) і вимагають викуп за відновлення доступу до них або вимагають додаткову плату за те, щоб не розголошувати отриману конфіденційну інформацію державним органам, конкурентам або громадськості. Залишаються однією з найсерйозніших загроз.
2. Шкідливе програмне забезпечення (Malware) — включає віруси, трояни, шпигунське ПЗ та інші загрози.
3. Соціальна інженерія (Social Engineering) — включає фішинг, вішинг (голосовий фішинг), смішинг (SMS-фішинг) та інші методи маніпуляції.
4. Загрози щодо даних (Threats against Data) — порушення чи витік безпеки даних. Основними цілями є особисті та корпоративні дані, що можуть бути продані або використані для шантажу.
5. Загрози доступності: Відмова в обслуговуванні (Denial-of-Service, DoS & DDoS) — атаки на інфраструктуру з метою перевантаження сервісів. DDoS-атаки стають більш потужними та часто використовуються у кіберконфліктах.
6. Маніпулювання інформацією та втручання (Disinformation & Manipulation) — використання фейкових новин, маніпуляцій у соціальних мережах. Часто застосовується у геополітичних конфліктах.
7. Атаки на ланцюг постачання (Supply Chain Attacks) — атаки через компрометацію постачальників IT-послуг або виробників обладнання.

Для порівняння загроз за роками проаналізуємо звіти ENISA за період 2022–2024 роки. В цих звітах слід звернути увагу на основні категорії загроз і зміни в їх тенденціях. Загальний підсумок тенденції розподілу кіберзагроз за роками представлено на рис. 2.

Проаналізувавши дані, можна відмітити, як змінювалися тенденції загроз. Як видно із діаграми на рис. 2 програми-вимагачі та DDoS-атаки (атаки на відмову в обслуговуванні) були найпоширенішими типами загроз протягом останніх років і залишаються провідними загрозами на даний час. У 2023 році зросла кількість інцидентів, пов'язаних із програмами-вимагачами у порівнянні з 2022 роком, але вже у 2024 році DDoS-атаки зайняли лідерську позицію у порівнянні з іншими типами загроз. Атаки стають масштабнішими, більш складнішими порівняно з попередніми роками. Зросла кількість атак понад 100 Гбіт/с і тривалістю більше трьох годин, спостерігалися кілька атак зі швидкістю понад 1 Тбіт/с [7]. Це збільшення можна пояснити геополітичною напруженість у всьому світі включаючи російсько-український конфлікт

та зростаючим впливом хактивізму (з політичними мотивами) серед груп, які виступають проти різних режимів. Хактивісти використовують хакерство, щоб вплинути на певну форму політичних чи соціальних змін.

У 2023 роком соціальна інженерія показала зростання. Це можна пояснити тим, що в соціальній інженерії основним вектором атаки є фішинг, який спрямований на викрадення важливої інформації, такої як номери кредитних карток, паролі за допомогою електронних листів із застосуванням соціальної інженерії та обману. Війна в Україні стала одним із чинників збільшення використання фішинкових сайтів, електронних листів з темами, пов'язаними з військовим конфліктом, включаючи гуманітарну допомогу, збір коштів, тощо. Зростання витоку даних через соціальну інженерію та вразливості відкритих проєктів, використання інструментів штучного інтелекту кіберзлочинцями для маніпуляції інформацією.

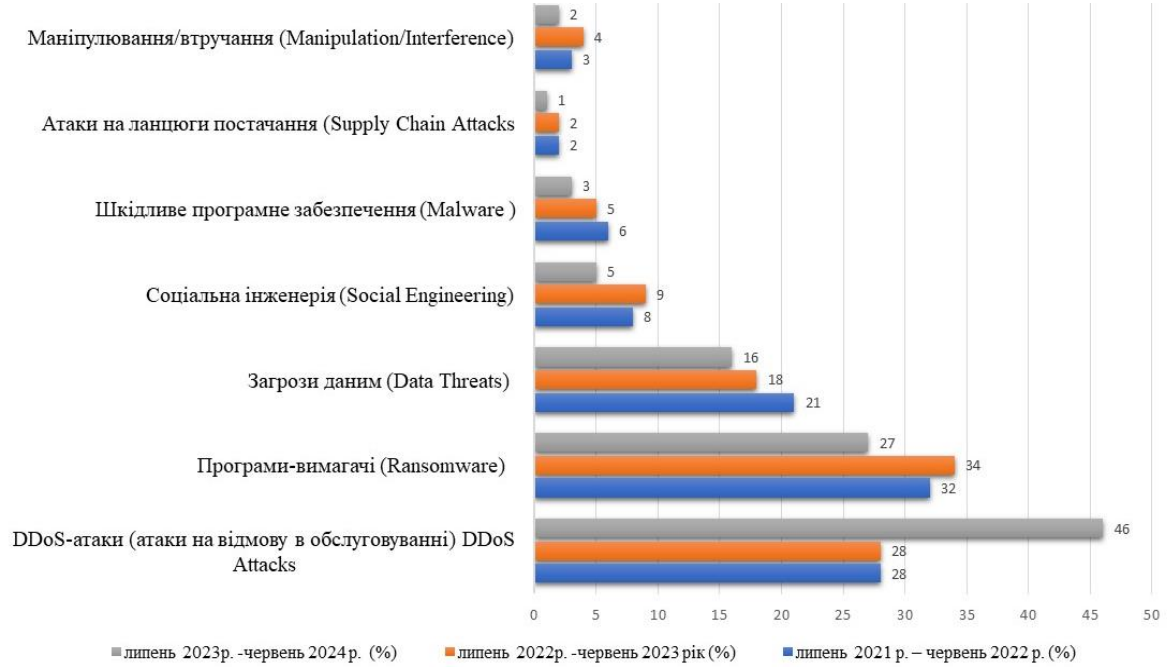

Рис. 2. Розподіл кількості загроз у ЄС за групами загроз 2022–2024 роки

Кількість інцидентів маніпулювання інформацією чи дезінформація за період липень 2022 р. – червень 2023 рік зросла. Переважна більшість проаналізованих подій стосується діяльності, яка, ймовірно, пов'язана з загарбницькою війною росії проти України. З точки зору маніпуляції інформації виділяють три найкращі тактики: розробка контенту, що включає створення тексту, зображення чи іншого контенту; максимізація впливу — зробити доступ цільової аудиторії до контенту про інцидент чи кампанію максимальним за допомогою заливання, посилення та перепощення інформації; розвиток наративу для досягнення довгострокового стратегічного наративного домінуваня. Тобто кампанії з дезінформації зосереджена на використанні заходів онлайн чи офлайн з щоденного просування та посиленні цих меседжів [8].

Атаки на ланцюги постачання — це новий тренд у кіберзлочинності, який дозволяє зловмисникам уражати велику кількість організацій через одного постачальника. За останні роки являється достатньо серйозною загрозою, тому що ці атаки часто пов'язані з викраденням облікових даних програмами-вимагачами, зламом системи, впроваджуванням шкідливого програмного забезпечення.

Використання різноманітних методів поширення зловмисного програмного забезпечення (ПЗ) залишається одним із способів викрадення конфіденційної інформації. Протягом 2023 та 2024 років було зафіксовано найпоширеніші штампи зловмисного ПЗ: RedLine: зловмисне програмне забезпечення, яке викрадає збережені облікові дані, дані автозаповнення та банківську інформацію; Vidar: шкідливе троянське програмне забезпечення, яке викрадає конфіденційну інформацію через комп'ютер і після успішного викрадання даних самознищується [6]. Крім того, існує безфайлове зловмисне ПЗ, яке обходить традиційні антивірусні рішення і використовує вбудовані системні інструменти для виконання своїх шкідливих функцій. Соціальна інженерія змушує користувачів завантажувати шкідливі програми через фішингові кампанії. Не останню роль у поширенні шкідливого ПЗ відіграє реклама, яка містить вбудоване зловмисне ПЗ в онлайн-оголошенні, розширюючи поверхню атаки та націлюючись на широкий спектр користувачів.

Аналіз кіберзагроз для критичної інфраструктури є надзвичайно важливим у сучасному цифровому середовищі. Проведемо галузевий аналіз інцидентів, пов'язаних з основними типами актуальних кіберзагроз, скориставшись звітом ENISA Threat Landscape 2024, який містить дані про найпоширеніші кіберзагрози за період 2023–2024 років. В даному звіті сектори відповідають класифікації категорій секторів у Директиві про мережеву та інформаційну безпеку NIS2 (Network and Information Security Directive 2), яка була прийнята 14 грудня 2022 року і є оновленою та розширеною версією першої Директиви NIS (2016/1148), яка була ухвалена Європейським Союзом у 2016 році. Ця директива значно розширює сферу застосування, включає більше секторів, вводить нові вимоги щодо звітності та посилює санкції за недотримання норм кібербезпеки у порівнянні з попередньою директивою NIS1. Згідно цій директиві галузі поділяються на «основні» (Essential Entities) та «важливі» (Important Entities), залежно від їхнього рівня значущості для національної безпеки та стійкості держави [9].

До основних галузей, які є стратегічно важливими для стабільного функціонування держави та її економіки відносять: енергетика — виробництво, постачання та розподіл електроенергії, нафти та газу; транспорт – авіація, залізничні перевезення, морські порти та вантажні перевезення; банківський сектор — комерційні банки, інститути, що управляють фінансовими ринками; фінансові ринки — інфраструктури фондових бірж, платіжні системи; охорона здоров'я — лікарні, лабораторії, постачальники медичних послуг; водопостачання — управління питною водою, водоочисні споруди; цифрова інфраструктура — інтернет-провайдери, дата-центри, оператори хмарних сервісів; державне управління — міністерства, органи державної влади, ключові державні установи.

Згідно звіту ENISA Threat Landscape 2024 цільовими секторами (галузями) за кількістю інцидентів у звітний період були сектори державного управлінні (19%), транспорт (11%), фінансовий сектор (9%), цифрова інфраструктура (8%) і бізнес-послуги. Також значну кількість інцидентів були спрямовані на громадянське суспільство, сюди відносять інциденти, пов'язані із соціальною інженерією та маніпуляцією інформацією [6]. Розглянемо більш детально розподіл кіберзагроз відповідно до цих секторів. Дані представлено в табл. 1.

Для галузевого аналізу сектори були згруповані відповідно до положень Директиви NIS2 і у кожному із цих секторів виділені найбільш поширені типи загрози, що зумовлено їхньою специфікою, а також рівнем цифронізації.

Найбільш уразливим сектором виявився державний сектор і найпоширенішими атаками в ньому були DDoS-атаки (33%), які призводять до відмови в обслуговуванні урядових порталів та цифрових сервісів. Програми-вимагачі (20%) також стали одними

із найпоширеніших атак в державному секторі і як їх наслідок блокування державних баз даних та вимоги викупу за їх розшифрування. Методи соціальної інженерії (10%) широко застосовуються для компрометації співробітників державних установ та отримання доступу до конфіденційної інформації.

Таблиця 1

Галузевий розподіл кіберзагроз за період 2023-2024 роки

Галузь	**Основні загрози**		**Основні інциденти**
	Тип загроз	**%**	
Державне управління	**DDoS**	**33%**	Масові атаки на урядові системи
	Ransomware	20%	
	Social Engineering	10%	
	Загрози даним (Data Threats)	12	
	Malware	11%	Атаки на логістичні та перевізні компанії
Транспорт	**DDoS**	**21%**	
	Malware	18%	
	Ransomware	14%	
Фінанси	**Phishing**	**25%**	Зломи банківських систем, крадіжка даних
	Social Engineering	18%	
	DDoS	12%	
	Загрози даним (Data Threats)	9%	
Цифрова інфрастуктура	**Malware**	**25%**	Компрометація цифрових платформ, витоки даних
	Social engineer	15%	
	Загрози даним (Data Threats)	10%	
	DDoS	6%	
Бізнес-послуги	**Ransomware**	**19%**	Компрометація постачальників послуг, витоки даних
	Supply Chain Attacks	15%	
	Загрози даним (Data Threats)	9%	

Найбільш поширеними атаками в транспортному секторі були DDoS-атаки (21%), що спрямовані на зупинку роботи аеропортів, портів та залізничних систем, шкідливе програмне забезпечення (18%), яке впроваджується у мережі підприємств з метою отримання доступу до операційних даних та Програми-вимагачі (14%).

У фінансовому секторі доля DDoS-атаки (12%) становить меншу частку від всіх інших загроз, а от соціальна інженерія (18%) та фішинг (25%) — є найбільш поширеними видами кіберзагроз. Фінансовий сектор є привабливий для зловмисників для отримання несанкціонованого доступу до банківських рахунків, різних фінансових активів та викрадення персональних даних.

В цифровій інфраструктурі найсерйознішими загрозами є шкідливе програмне забезпечення (25%), яке використовується для викрадення або модифікації даних, а також витоки даних (10%). Провайдери цифрових послуг та дата-центри часто стають об’єктами атак і це тягне за собою фінансові та репутаційні втрати.

Отже, аналіз загроз по секторам показав, що DDoS-атаки залишаються однією з найбільш поширених загроз, особливо для державного сектору (33%) та транспортної інфраструктури (21%). Програми-вимагачі (Ransomware) є основною загрозою для бізнесу (19%) та державних установ (20%). Фішинг (25%) залишається найбільш популярним методом атак у фінансовому секторі, тоді як витоки даних (10%) та шкідливе ПЗ (25%) мають критичне значення для цифрової інфраструктури. Атаки на ланцюги постачання (15%) все більше набирають популярності у сфері бізнес-послуг.

Аналізуючи частоту, серйозність та типи ідентифікованих загроз, організації можуть визначати пріоритети у виправленні вразливостей, раціонально розподіляти ресурси та

мінімізувати потенційні ризики. Такий підхід сприяє створенню більш безпечного та стійкого цифрового середовища, зменшуючи ймовірність порушень безпеки та кібератак.

Для проведення більш точного і комплексного аналізу кіберзагроз потрібно дослідити потенційні вразливості в апаратному, програмному забезпеченні, що дасть можливість випередити загрози, усунути критичні недоліки безпеки та сформувати ефективну стратегію кібербезпеки.

У сфері кібербезпеки існують стандарти та системи, що допомагають ідентифікувати, оцінювати та класифікувати вразливості в програмному та апаратному забезпеченні.

Для уніфікації термінології щодо вразливостей, що дозволяє спеціалістам з кібербезпеки швидко отримувати інформацію про нові загрози створено спеціалізований каталог CVE (Common Vulnerabilities and Exposures). CVE є відкритим стандартом, що підтримується MITRE Corporation під егідою Агентства з кібербезпеки та безпеки інфраструктури США (CISA).

CVE (Common Vulnerabilities and Exposures) — це стандартизована система каталогізації вразливостей та ризиків у програмному та апаратному забезпеченні, яка використовується для полегшення ідентифікації, відстеження та усунення загроз, що можуть бути використані зловмисниками [10].

CNA (CVE Numbering Authority) — це організація, відповідальна за ідентифікацію та присвоєння унікальних ідентифікаторів CVE (Common Vulnerabilities and Exposures) нововиявленим вразливостям для забезпечення точності та узгодженості інформації про вразливості, що робить їх більш доступними для аналізу в системах управління кібербезпекою та інформаційних базах даних.

CVSS (Common Vulnerability Scoring System) — представляє собою безкоштовний і відкритий галузевий стандарт для оцінки серйозності вразливостей безпеки комп’ютерних систем від 0 до 10, де вищі значення вказують на більшу серйозність вразливості. Потім числову оцінку можна перевести в якісне представлення (наприклад, низький, середній, високий і критичний), щоб допомогти організаціям належним чином оцінити та визначити пріоритети своїх процесів управління вразливістю на основі їх потенційного впливу [11].

CWE (Common Weakness Enumeration) — це каталог поширених недоліків у програмному та апаратному забезпеченні, включаючи проблеми безпеки, помилки кодування та використовується як довідник відомих уразливостей безпеки програмного забезпечення для кращого розуміння цих слабких місць під час процесу розробки програмного забезпечення [12].

CWE опублікувало Топ 25 небезпечних вразливостей за 2024 рік, що містить найбільш небезпечні програмні недоліки, слабкі місця, які можуть призвести до серйозних вразливостей у системах безпеки [12]. Дані представлені в табл. 2

Аналізуючи дані табл. 2 можна виділити вразливості пам’яті та управління ресурсами, (CWE-787, CWE-416, CWE-119), вразливості авторизації та автентифікації (CWE-862, CWE-287, CWE-863), вразливості файлів та конфігурації (CWE-22, CWE-434, CWE-798), логічні помилки у програмному забезпеченні (CWE-190, CWE-502, CWE-400). Всі ці вразливості є небезпечними і можуть привести до зламу систем, компрометації конфіденційних даних, виконання шкідливого коду або відмови в обслуговуванні. Розуміння цих властивостей надає змогу забезпечити стійкість інформаційних систем від кіберзагроз.

Таблиця 2

Топ 25 найбільш небезпечних вразливостей за 2024 рік

CWE ID	Назва вразливості	Опис вразливості	Наслідки
CWE-79	Неправильна нейтралізація введення під час генерації веб-сторінки. (Cross-site Scripting (XSS))	Програма не належним чином обробляє введені користувачем дані.	Виконання шкідливого JavaScript-коду в браузері жертви
CWE-787	Запис за межами буфера	Помилка управління пам'яттю, що дозволяє записувати дані за межами буфера.	Може призвести до пошкодження пам'яті та виконання довільного коду
CWE-89	Неправильна нейтралізація спеціальних елементів в SQL-запиті (SQL Injection)	Зловмисник може вводити шкідливі SQL-запити для отримання доступу до баз даних.	Несанкціонований доступ до баз даних
CWE-352	Міжсайтовий запит підробки (Cross-Site Request Forgery (CSRF))	Атакуючий змушує користувача виконати небажані дії на веб-додатку.	Несанкціоноване виконання дій від імені користувача
CWE-22	Неправильне обмеження шляху до обмеженого каталогу (Path Traversal)	Можливість доступу до файлів за межами дозволеного каталогу.	Доступ до файлів за межами дозволеної області
CWE-125	Читання за межами буфера	Читання пам'яті за межами виділеного буфера може призвести до витоку інформації.	Витік конфіденційних даних або нестабільність системи
CWE-78	Неправильна нейтралізація спеціальних елементів в команді ОС (OS Command Injection)	Виконання довіль Використання після звільнення них команд операційної системи на вразливому сервері.	Виконання команд ОС зловмисником
CWE-416	Використання після звільнення (Use-After-Free)	Вразливість управління пам'яттю, яка виникає, коли програма звертається до динамічно виділеної пам'яті після її звільнення.	Витік конфіденційних даних, виконання довільного коду
CWE-862	Відсутність авторизації	Система дозволяє доступ до ресурсів без належної перевірки користувача.	Зловмисник отримує доступ до заборонених ресурсів
CWE-434	Необмежене завантаження файлів небезпечного типу	Завантаження файлів без перевірки може дозволити зловмиснику виконувати шкідливі програми.	Виконання довільного коду на сервері, компрометації системи, розповсюдження шкідливих програм або обходу механізмів безпеки
CWE-94	Неправильний контроль генерації коду (Code Injection)	Найнебезпечніша Дозволяє виконувати довільний код, зламувати системи, змінювати їхній функціонал та отримувати доступ до конфіденційних даних.	Виконання шкідливих команд, компрометації системи або отримання несанкціонованого доступу
CWE-20	Невірна валідація введення	Програма не перевіряє введені користувачем дані, що може призвести до експлуатації вразливостей. Є основою багатьох критичних уразливостей, таких як SQL Injection, XSS, Command Injection, Path Traversal.	Зловмисник може несанкціонований доступ, викликати відмову в обслуговуванні (DoS)

CWE-77	Неправильна нейтралізація спеціальних елементів у команді (Command Injection)	Програма виконує команду операційної системи використовуючи користувацьке введення без належної фільтрації або нейтралізації спеціальних символів.	Приводить до витоку даних або виконання шкідливого коду
CWE-287	Невірна автентифікація	Відсутність належної автентифікації дозволяє доступ до критичних функцій.	Несанкціонований доступ до системи
CWE-269	Невірне управління привілеями	Неправильне управління правами доступу дозволяє користувачам отримувати додаткові привілеї.	Підвищення привілеїв, компрометації даних або захоплення системи
CWE-502	Десеріалізація небезпечних даних	Небезпечна десеріалізація (відновлення об’єктів із збережених даних) без перевірки їхнього вмісту.	Виконання довільного шкідливого коду при обробці даних
CWE-200	Розкриття конфіденційної інформації	Система ненавмисно надає доступ до конфіденційних даних.	Витік конфіденційних даних або приватної інформації
CWE-863	Невірна авторизація	Помилка у перевірці прав доступу	Несанкціоновані дії неавторизованими користувачами
CWE-918	Підробка запитів на стороні сервера (Server-Side Request Forgery (SSRF))	Зловмисник змушує сервер виконувати небажані запити до внутрішніх або зовнішніх ресурсів.	Доступ до внутрішніх серверів або витік даних
CWE-119	Неконтрольовані операції з пам’яттю	Програма неналежним чином контролює межі буфера пам’яті під час виконання операцій.	Впровадження та виконання шкідливого коду, отримання доступу до ключів шифрування або паролей
CWE-476	Розіменування вказівника NULL	Програма намагається отримати доступ до пам’яті через вказівник, що містить значення NULL	Може спричинити аварійне завершення програми
CWE-798	Використання жорстко закодованих облікових даних (Hardcoded Credentials)	Жорстко закодовані паролі або API-ключі можуть бути знайдені у вихідному коді.	Зловмисник отримує доступ до жорстко закодованих паролів
CWE-190	Integer Overflow	Переповнення числового типу може дозволити обходити перевірки або спричиняти некоректні обчислення.	Обхід перевірок та порушення логіки
CWE-400	Неконтрольоване споживання ресурсів	Відсутність обмежень на споживання ресурсів (CPU, пам’яті, дискового простору, мережевого трафіку тощо)	Перевантаження сервера, витік пам’яті, DoS-атака
CWE-306	Відсутня автентифікація для критичної функції	Виконання критичних функцій без автентифікації дозволяє зловмиснику контролювати систему.	Приводить до несанкціонованого доступу, модифікації даних або порушення безпеки

Розглянемо ландшафт загроз у звіті ENISA Threat Landscape 2024. В ньому представлено динаміку вразливостей загального рівня (CVE) та їхній розподіл за критеріями тяжкості та вектором атаки. Всього за аналізований період було ідентифіковано 19 754 вразливості. Ці вразливості були класифіковані за рівнем серйозності відповідно до системи CVSS (Common Vulnerability Scoring System) і розподілилися наступним чином [6]:

- Критичні (Critical) — 9,3% від загальної кількості.
- Високі (High) — 21,8%.
- Середні (Medium) — 26,8%
- Низькі (Low) — 0,9 найменша категорія.

Також у звіті відображений відсоток вразливостей, для яких не зазначено критерій серйозність і він становить 41,2%. Ця категорія вразливостей показує існування вразливостей, оцінка серйозності яких або очікує на розгляд, або ще не визначена з якоїсь причини. Тобто існують невизначеності або прогалини в класифікації цих вразливостей на основі їх серйозності. Близько 30% усіх вразливостей (Критичні + Високі) становлять серйозну загрозу і потребують термінового виправлення.

Якщо розглядати вектор атаки то 76% атак здійснюються на мережевому рівні, 19% на локальному рівні, решта стосується фізичного рівня чи інших способів взаємодії.

Найбільш популярними і небезпечними вразливостями представленими у звіті є:

- Неправильна нейтралізація введення під час генерації веб-сторінки (Cross-Site Scripting (XSS)) — 22,68% — найбільш поширена уразливість.
- Неправильна нейтралізація спеціальних елементів в SQL-запиті (SQL Injection) — 9,32% — також входить до групи найбільш критичних.
- Запис за межами буфера (Out-of-bounds Write) — 6,37%.
- Міжсайтове підроблення запиту (Cross-Site Request Forgery (CSRF)) — 6,28%.
- Відсутність авторизації (Missing Authorization) — 4,82% — проблема управління доступом.

Таким чином можна сказати, що SQL Injection, XSS і CSRF є основними вразливостями на даний час. Звідси випливає, що організації, об’єкти критичної інфраструктури повинні акцентувати свою увагу на усунення критичних мережевих вразливостей, впровадженні ефективних методів автентифікації, валідації введених даних для захисту своїх ресурсів від потенційних загроз.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Отримані дані свідчать про необхідність посилення кіберзахисту у секторах критичної інфраструктури, що регулюються Директивою NIS2. Основними напрямами захисту є впровадження систем багатофакторної автентифікації, розширення заходів з моніторингу мереж, підвищення обізнаності персоналу щодо соціальної інженерії та використання сучасних технологій протидії DDoS-атакам. Подальші дослідження мають зосередитися на адаптації заходів безпеки відповідно до нових методів атак, що розвиваються у кіберпросторі.

Важливим є впровадження інноваційних рішень, зокрема використання аналітики даних, машинне навчання, штучний інтелект, щоб відстежувати поведінку мережі та автоматично реагувати на загрози. штучного інтелекту та технологій машинного навчання, які дозволяють автоматизовано аналізувати великі обсяги даних, оперативно виявляти аномальну активність у критичних системах, прогнозувати можливі загрози та

запобігати потенційним атакам. Використання передових кіберзахисних технологій сприятиме підвищенню стійкості інформаційних систем, зміцненню їхньої безпеки та забезпеченню ефективного реагування на інциденти в режимі реального часу.

Крім того, важливим аспектом є розвиток міжнародної співпраці та обмін інформацією між державними органами, приватним сектором і спеціалізованими організаціями, що дозволить своєчасно реагувати на нові виклики. Міжнародна співпраця та обмін досвідом між країнами стають важливими інструментами у боротьбі з глобальними загрозами, а впровадження світових стандартів, таких як директива NIS2, дозволяє створювати універсальні механізми кіберзахисту. Водночас особливу увагу слід приділити навчанню персоналу та розробці чітких політик доступу до інформаційних систем, оскільки людський фактор продовжує залишатися одним із найбільш уразливих елементів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. On Critical Infrastructure, Law of Ukraine No. 1882-IX (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. The government's CERT-UA team handled 2543 cyber incidents in 2023. (2024). State Service for Special Communications and Information Protection of Ukraine. https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti
3. Bratel, S. (2023). Experience of foreign countries in ensuring the security of critical infrastructure facilities. *Theoretical and practical aspects of national security*, *3*, 261–265.
4. Skitsko, O., & Shyrshov, R. (2024). Topical issues of ensuring cybersecurity of critical infrastructure facilities. *Legal scientific electronic journal*, *20*, 312–315.
5. Melnyk, D. S. (2022). Protection of the national critical information infrastructure: current problems and solutions. *Administrative law and process: a scientific and practical journal*, *3(38)*, 5–16.
6. *Enisa Threat Landscape 2024. July 2023 to June 2024. September 2024.* (n. d.). https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf/
7. *The Evolution of DDoS: Return of the Hacktivists.* (2023). https://www.akamai.com/site/en/documents/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.pdf
8. *Framework*. (n. d.). DISARM Foundation. https://www.disarm.foundation/framework
9. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022. (2022). *Official Journal of the European Union.*
10. *Common Vulnerabilities and Exposures.* (n. d.). https://www.cve.org/
11. *Common Vulnerability Scoring System.* (n. d.). https://www.first.org/cvss/
12. *CWE - Common Weakness Enumeration.* (2024). CWE - Common Weakness Enumeration. https://cwe.mitre.org/index.html
13. *Cyber Digest Cybersecurity Overview.* (2024). https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest/Cyber%20digest_Jan_2024_UA.pdf?utm_source=chatgpt.com
14. *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service.* (2021). Atlantic Council. Countering Cyber Proliferation. https://www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf
15. *CERT-UA handled 4315 cyber incidents last year.* (2025). State Service of Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
16. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Anna Ilyenko
Candidate of Technical Sciences, Associate Professor
Head of the Cybersecurity Department
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0000-0001-8565-1117
anna.ilienko@npp.nau.edu.ua

Valentyna Teliushchenko
Assistant of the Cybersecurity Department
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0000-0001-6026-5105
valentyna.teliushchenko@npp.nau.edu.ua

Olena Dubchak
Senior Lecturer of the Cybersecurity Department
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0000-0001-9739-3960
3915922@npp.kai.edu.ua

MODERN CYBER THREATS TO CRITICAL INFRASTRUCTURE IN UKRAINE AND THE WORLD

Abstract. Critical infrastructure is the basis for the stable functioning of the state and society, but its dependence on digital technologies makes it vulnerable to cyber threats. In 2024, more than 3 million information security events were recorded, of which 28,000 were classified as critical, requiring in-depth analysis and development of new approaches to risk management. This article examines the current cyber threats to critical infrastructure, including cyber espionage, embezzlement, information and psychological operations, and attacks on industrial systems. Based on the analysis, the main types of attacks are identified: ransomware, DDoS attacks, social engineering and zero-day exploits. Particular attention is paid to the energy, transport, finance and digital infrastructure sectors, which are the most vulnerable to attacks. The article also contains an analysis of international experience and standards, such as the ENISA Threat Landscape and the NIS2 directive, which demonstrate effective cybersecurity practices. Analysis of international experience shows that effective cyber defence requires a multi-level approach. This includes real-time network monitoring, automated vulnerability management tools, improved risk assessment systems, implementation of multi-factor authentication, and increased cyber awareness of staff. The use of innovative approaches will significantly reduce the impact of cyber threats and ensure the uninterrupted operation of critical infrastructure. The results of this study indicate the importance of integrating modern approaches and technologies into critical infrastructure protection systems, which will minimise risks and ensure the stability of key sectors of the state.

Keywords: cybersecurity; data protection; attacks; cyber threats; social engineering; critical infrastructure; disinformation; information security; vulnerabilities.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. On Critical Infrastructure, Law of Ukraine No. 1882-IX (2024) (Ukraine). https://zakon.rada.gov.ua/laws/show/1882-20#Text
2. The government's CERT-UA team handled 2543 cyber incidents in 2023. (2024). State Service for Special Communications and Information Protection of Ukraine. https://cip.gov.ua/en/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti
3. Bratel, S. (2023). Experience of foreign countries in ensuring the security of critical infrastructure facilities. *Theoretical and practical aspects of national security, 3,* 261–265.
4. Skitsko, O., & Shyrshov, R. (2024). Topical issues of ensuring cybersecurity of critical infrastructure facilities. *Legal scientific electronic journal, 20,* 312–315.

5. Melnyk, D. S. (2022). Protection of the national critical information infrastructure: current problems and solutions. *Administrative law and process: a scientific and practical journal, 3(38),* 5–16.
6. *Enisa Threat Landscape 2024. July 2023 to June 2024. September 2024.* (n. d.). https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf/
7. *The Evolution of DDoS: Return of the Hacktivists.* (2023). https://www.akamai.com/site/en/documents/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.pdf
8. *Framework*. (n. d.). DISARM Foundation. https://www.disarm.foundation/framework
9. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022. (2022). *Official Journal of the European Union.*
10. *Common Vulnerabilities and Exposures.* (n. d.). https://www.cve.org/
11. *Common Vulnerability Scoring System.* (n. d.). https://www.first.org/cvss/
12. *CWE - Common Weakness Enumeration.* (2024). CWE - Common Weakness Enumeration. https://cwe.mitre.org/index.html
13. *Cyber Digest Cybersecurity Overview.* (2024). https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/Cyber%20digest/Cyber%20digest_Jan_2024_UA.pdf?utm_source=chatgpt.com
14. *Countering Cyber Proliferation: Zeroing in on Access-as-a-Service.* (2021). Atlantic Council. Countering Cyber Proliferation. https://www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf
15. *CERT-UA handled 4315 cyber incidents last year.* (2025). State Service of Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
16. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise. Textbook.* Lviv: Publisher Marchenko T. V.