DOI: https://doi.org/10.30837/EK.2024.033
**Шейко І.А.,**
*к.е.н., доцент, доцент кафедри економічної кібернетики та управління економічною безпекою,*
*Харківський національний університет радіоелектроніки,*
*ORCID: https://orcid.org/0000-0002-5770-3677*
**Мартиненко М.С.,**
*здобувач вищої освіти,*
*Харківський національний університет радіоелектроніки*
*ORCID: https://orcid.org/0009-0002-8926-2703*
**Нєронов П.Є.,**
*здобувач вищої освіти,*
*Харківський національний університет радіоелектроніки*
*ORCID: https://orcid.org/0009-0003-7597-1346*
**Кузовкіна К.Р.,**
*здобувач вищої освіти,*
*Харківський національний університет радіоелектроніки*
*ORCID: https://orcid.org/0009-0001-8097-3907*

# РИЗИКИ КІБЕРБЕЗПЕКИ ДЛЯ СУЧАСНОГО БІЗНЕСУ

З розвитком цифрового ландшафту організації стикаються з дедалі складнішими проблемами щодо захисту своїх активів від складних кіберзагроз. Інтеграція цифрових технологій у стратегії кібербезпеки стала ключовою для пом’якшення цих ризиків. Наслідки кібератак можуть бути катастрофічними: від фінансових втрат до втрати репутації,. Тому, ефективна протидія кіберзагрозам є одним з ключових завдань для забезпечення безперебійної роботи бізнесу.

Згідно зі звітами Європейського Агентства з кібербезпеки (ENISA) [1], найбільш поширеними інцидентами кібербезпеки у країнах Європейського Союзу з червня 2023 по липень 2024 стали (рис. 1):

– відмова у доступі (DoS/DDoS – атаки);

– програми вимагачі;

– витік даних та інциденти втрати конфіденційності;

– загрози соціальної інженерії (провокування персоналу компаній на дії, що сприяють порушенню кібербезпеки);

– шкідливе програмне забезпечення.

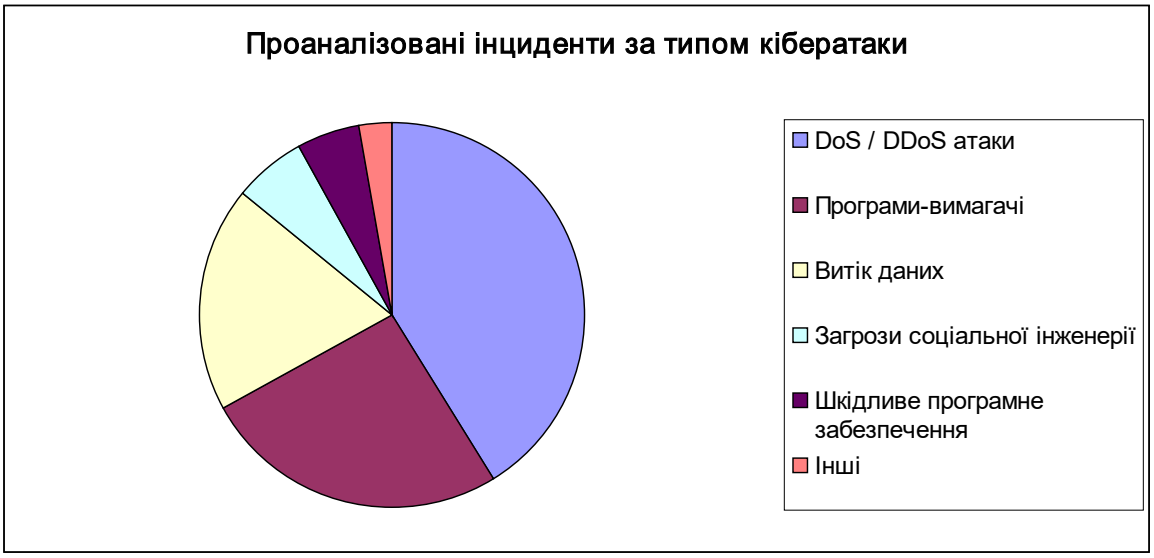


Рисунок 1 – Найбільш розповсюджені типи кібератак у країнах ЄС з червня 2023 р. по липень 2024 [1]

За аналізований період щомісячна кількість зафіксованих інцидентів кібербезпеки у країнах ЄС змінювалася від 250 до 700 інцидентів (рис. 2) [1].

У звіті ENISA також визначено чотири різних типів мотивації, які можна пов’язати з суб’єктами загрози [1]:

– фінансова вигода: будь-яка фінансово пов’язана дія (здійснюється здебільшого групами кіберзлочинців);

– шпигунство: отримання інформації про ІВ (інтелектуальну власність), конфіденційні дані, секретні дані (здебільшого здійснюється групами, спонсорованими державою);

– знищення: будь-яка руйнівна дія, яка може мати незворотні наслідки;

– ідеологічні: будь-яка дія, підкріплена ідеологією, що стоїть за нею (наприклад, хактивізм).

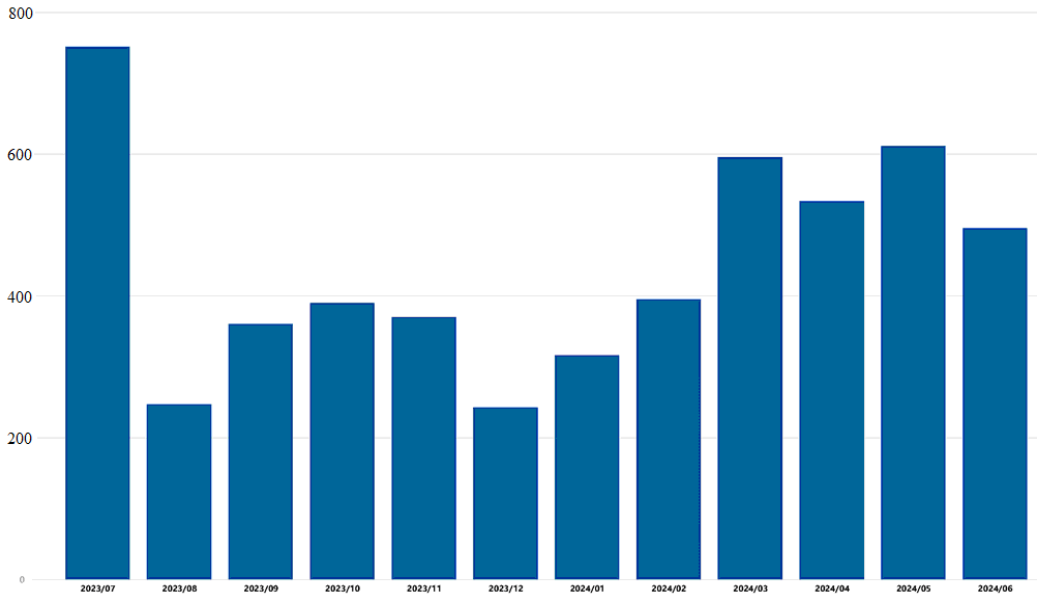


Рисунок 2 – Кількість інцидентів кібербезпеки у країнах ЄС за липень 2023-червень 2024 [1]

У більшості випадків основні загрози можна віднести до однієї або кількох мотивацій, причому певні мотиви виявляються більш домінуючими, ніж інші. Як і у випадку з попередньою ітерацією у сфері атак програм-вимагачів, хоча основною мотивацією зазвичай є фінансова вигода, є невеликий відсоток випадків, коли руйнівний мотив також відіграє певну роль. Крім того, більшість загроз, пов’язаних із даними, були пов’язані з кількома мотиваціями, головною причиною

яких була фінансова вигода. Ідеологія та шпигунство також відігравали значну роль, оскільки зловмисники прагнули просувати конкретні плани або викрадати стратегічну інформацію. Це підкреслює різноманітні мотиви, що стоять за кіберзагрозами, починаючи від фінансових стимулів і закінчуючи ідеологічними цілями та цілями збору розвідувальної інформації [1].

Для ефективної протидії кіберзагрозам компанії повинні впроваджувати комплексний підхід, який включає:

– *технічні засоби захисту*: антивірусні програми, системи виявлення вторгнень, шифрування даних тощо;

– *організаційні заходи*: розробка політик безпеки, проведення регулярних тренінгів для співробітників, створення резервних копій даних;

– *інженерія безпеки*: вбудовування безпеки в усі аспекти розробки програмного забезпечення.

Сучасні цифрові пристрої вразливі до кібератак. Особливо це стосується пристроїв Інтернету речей. Інтернет речей (IoT) – це революційна концепція, яка об'єднує фізичні пристрої, програмне забезпечення, датчики, актуатори та мережі, дозволяючи їм збирати та обмінюватися даними. Хоча IoT відкриває безліч нових можливостей, він також створює значні ризики для кібербезпеки.

До причин вразливості IoT до кібератак можна віднести [2]:

– *величезну кількість пристроїв:* зростання кількості підключених пристроїв створює величезну атакуючу поверхню, що ускладнює захист всієї мережі;

– *слабка безпека:* багато IoT-пристроїв мають слабкі або відсутні механізми безпеки, такі як застаріле програмне забезпечення, стандартні паролі та відсутність шифрування. Багато IoT-пристроїв або не використовують шифрування взагалі, або використовують слабкі алгоритми шифрування, що робить дані, які передаються між пристроями, вразливими для перехоплення та

дешифрування. Крім того, заводські налаштування з використанням стандартних і легко здогаданих паролів є поширеною проблемою в IoT-пристроях. Це дозволяє хакерам легко отримати доступ до пристрою;

– *децентралізацію управління:* різноманітність IoT-пристроїв ускладнює їх централізоване управління та оновлення Багато виробників IoT-пристроїв не забезпечують регулярних оновлень програмного забезпечення для усунення виявлених вразливостей, що робить пристрої вразливими до відомих атак;

– *вразливі протоколи:* Для забезпечення низького енергоспоживання та мінімальних обчислювальних ресурсів, IoT-пристрої часто використовують спрощені протоколи, які можуть мати менший рівень безпеки порівняно зі складнішими протоколами, що використовуються в традиційних комп'ютерних мережах.

Зловмисники можуть отримати несанкціонований доступ до пристроїв IoT і використовувати їх для різних цілей, таких як збір даних, відмова в обслуговуванні або навіть фізичний контроль над пристроєм. Типові загрози для мереж Інтернету речей можна поділити на такі типи [2-4]:

– *дистанційне управління:* зловмисники можуть отримати дистанційний доступ до пристроїв і використовувати їх для своїх цілей;

– *витік даних:* конфіденційні дані, зібрані IoT-пристроями, можуть бути викрадені. Вразливі IoT-пристрої можуть бути використані для збору приватної інформації про користувачів і її подальшого використання в злочинних цілях;

– *відмова в обслуговуванні (DOS/DDOS-атаки):* зловмисники можуть перевантажити мережу або пристрої, що призведе до відмови в обслуговуванні;

– *ботанети:* зламані IoT-пристрої можуть бути об'єднані в ботанети для проведення масштабних кібератак. Вразливі IoT-пристрої можуть бути використані як плацдарм для розповсюдження шкідливого програмного забезпечення в інші частини мережі;

– *фізичний доступ:* у деяких випадках зловмисники можуть отримати фізичний доступ до пристроїв і модифікувати їх програмне забезпечення.

Я наслідки кібератак на IoT компанії можуть понести матеріальні збитки (через фізичних пошкоджень обладнання та інфраструктури), фінансові втрати (дія програм-вимагачів, витік конфіденційних даних), втрату репутації компанії та соціальні наслідки у разі порушення критичної інфраструктури.

Для захисту мереж Інтернету речей стануть у нагоді такі дії [2-4]:

– *оновлення програмного забезпечення:* регулярне оновлення програмного забезпечення всіх IoT-пристроїв усуває вже виявлені вразливості;

– *сильні паролі:* використання складних, унікальних паролей для кожного пристрою знизить вірогідність інцидентів кібербезпеки.

– *шифрування:* обов'язкове шифрування даних, що передаються між пристроями.

– *сегментація мережі:* можна створити окрему мережу для IoT-пристроїв, щоб обмежити потенційну шкоду в разі зараження або розділити IoT-мережу на сегменти для обмеження поширення зловмисного програмного забезпечення.

– *моніторинг мережі:* регулярний моніторинг мережі на предмет підозрілої активності дозволить виявити зовнішнє втручання.

– *навчання персоналу:* навчання персоналу основам захисту даних, створенню безпечних паролей, роботи з конфіденційною інформацією знизить вірогідність людської помилки;

– *співпраця між компаніями та урядами:* компанії та урядові організації почали тісніше співпрацювати для обміну інформацією про загрози та розробки спільних стратегій захисту.

Як приклад однієї із успішних кібератак на пристрої Інтернету речей можна виділити Mirai. Mirai – це масштабна атака, здійснена за допомогою ботнету Mirai, який вперше з'явився у 2016 році. Mirai орієнтований на пристрої Інтернету речей

(IoT), такі як камери спостереження, роутери, тощо. Він використовує слабкі місця в захисті цих пристроїв, зокрема стандартні паролі та некоректно налаштовані системи. Mirai сканує мережі на наявність пристроїв IoT, використовуючи відомі облікові дані для входу. Після зламу пристрій стає частиною ботнету та використовується для запуску DDoS-атак (розподілених атак на відмову в обслуговуванні). У жовтні 2016 року Mirai був використаний для DDoS-атаки на DNS-провайдера Dyn. В результаті низка великих вебсайтів, включаючи Twitter, Netflix, і Spotify, стали недоступними [3].

Mirai став небезпечним прецедентом, продемонструвавши, наскільки вразливі пристрої IoT. Розробників Mirai затримали в 2017 році, але код ботнету був викладений у відкритий доступ, що призвело до появи численних його модифікацій. Постраждали не тільки компанії, а й кінцеві користувачі через порушення сервісів та зловживання ресурсами пристроїв.

У 2013 році хакери успішно зламали мережу Target і викрали інформацію про кредитні картки з мільйонів транзакцій. Вони вкрали облікові дані для входу у постачальника HVAC, який використовував датчики IoT, щоб допомогти Target контролювати споживання енергії та підвищувати ефективність своїх систем [4].

У 2017 році управління США з харчових продуктів та ліків (FDA) оголосило, що понад 465 000 імплантованих кардіостимуляторів були вразливі до зламу. Контролюючи один із цих пристроїв, хакер міг би буквально вбити когось, розрядивши батарею, змінивши частоту серцевих скорочень або застосувавши електрошок. Порушення безпеки IoT фактично перетворило рятівний пристрій на потенційно смертоносну зброю [4].

У 2015 році пара експертів з кібербезпеки вирішила зламати новенький Jeep Grand Cherokee за допомогою його мультимедійної системи. Вони були успішними. І вони продемонстрували, що вони можуть використовувати мультимедійну систему для підключення до іншого програмного забезпечення в

автомобілі, перепрограмувати його, а потім керувати двигуном, кермом, гальмами, трансмісією тощо. В епоху безпілотних автомобілів ця демонстрація є наполегливим нагадуванням про те, що ізоляція підключених пристроїв є ключовим компонентом безпеки Інтернету речей [4].

На захисті цифрових пристрої від кібератак можуть стати самі цифрові технології. У нашому дослідженні досліджується використання передових цифрових технологій (таких як штучний інтелект (AI), системи моніторингу в реальному часі та платформи мережевої безпеки) задля підсилення кібербезпеки.

Технології штучного інтелекту та машинного навчання (ML) радикально змінили виявлення та запобігання кіберзагрозам. Ці технології дозволяють організаціям аналізувати великі обсяги даних, виявляти закономірності та аномалії, що вказують на потенційні порушення. Наприклад, фінтех-компанії використовують інструменти на основі ШІ для покращення виявлення шахрайства та оцінки ризиків. Наприклад, Humanize, американський стартап із кібербезпеки, використовує штучний інтелект для кількісної оцінки кіберризиків, оцінки вразливостей і надання дієвих стратегій виправлення. Такі інструменти не тільки спрощують ідентифікацію загроз, але й оптимізують розподіл ресурсів для пом’якшення критичних ризиків [5].

Моніторинг у реальному часі став ключовим інструментом захисту критичної інфраструктури. В енергетичному секторі прикладом цього підходу є ініціатива Міністерства енергетики США «Охоронець сусідства». Завдяки застосуванню технології, яка забезпечує майже миттєву видимість електричних мереж, програма покращила моніторинг системи з 5% до 70%. Розвідувальні дані про загрози, які анонімно передаються зацікавленим сторонам, покращують механізми колективного захисту, забезпечуючи швидке реагування на кібератаки [5].

Платформи мережевої безпеки відіграють важливу роль у захисті систем зв’язку та операційних технологій. Канадський стартап CCX Technologies

розробив «SystemX», платформу кібербезпеки для військових і аерокосмічних програм. Він включає системи виявлення та запобігання вторгненням, які захищають військові мережі зв'язку на повітряних, наземних і морських транспортних засобах [5].

Механізми шифрування та захисту даних широко використовуються для захисту конфіденційної інформації від несанкціонованого доступу. Галузі роздрібної торгівлі та охорони здоров'я значною мірою покладаються на ці технології для захисту даних клієнтів і пацієнтів відповідно. Heal Security, платформа кібербезпеки для охорони здоров'я, усуває ризики, пов'язані з витоком даних і зломом медичних пристроїв, шляхом постійного моніторингу та аналізу загроз у реальному часі. Ці заходи підвищують довіру та забезпечують дотримання суворих правил захисту даних. [5]

Ці приклади підкреслюють інтеграцію передових технологій, таких як штучний інтелект, моніторинг у реальному часі та безпека мережі в різних галузях для ефективної боротьби з кіберзагрозами.

Але у звіті Deloitte також зазначено декілька проблем щодо використання цифрових технологій, які можуть збільшити онлайн-ризики [6]:

– через велику кількість цифрових пристроїв важко захистити всі від кібератак;

– конвергенція цифрового та фізичного світу робить наслідки кібератак важче передбачуваними з більшою потенційною шкодою від атак.

Критичний характер цифрової інфраструктури робить її мішенню для кіберзлочинців, які бачать, що її власники готові заплатити викуп, щоб уникнути дешифрування [6].

Незважаючи на свою ефективність, цифрові технології стикаються з обмеженнями у вирішенні динамічної природи кіберзагроз. Зловмисники постійно адаптують свою тактику, що вимагає постійних інновацій у інструментах

кібербезпеки. Інтеграція цифрових технологій у стратегії кібербезпеки є значним прогресом у боротьбі з кібератаками. Штучний інтелект, моніторинг у реальному часі, безпека мережі та технології шифрування відіграють важливу роль у зниженні ризиків у різних секторах. Оскільки кіберзагрози продовжують розвиватися, постійні інновації та співпраця мають вирішальне значення для забезпечення надійних та адаптивних структур кібербезпеки.

**Перелік джерел посилань**

1. European Union Agency for Cybersecurity (ENISA). Threat Landscape 2024. September, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

2. Lee I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet*. 2020. № 12. p. 157.

3. Radanliev P., De Roure D. C., Maple, C., Nurse J. R., Nicolescu R., Ani U. Cyber Risk in IoT Systems. *Preprints.* 2019. 2019030104. https://doi.org/10.20944/preprints201903.0104.v1

4. Henke C. What is IoT security? Risks, examples and solutions. *Emnify*. 24 February, 2023. URL: http://surl.li/vvqoyv.

5. Startus. 10 Prominent Cybersecurity Examples in 2024. URL: https://www.startus-insights.com/innovators-guide/cybersecurity-examples/

6. Deloitte Insights. Incentives are key to breaking the cycle of cyberattacks on critical infrastructure. 08 March 2022. URL: https://www2.deloitte.com/us/en/insights/industry/public-sector/cyberattack-critical-infrastructure-cybersecurity.html.