УДК 004.056.5

ГІБРИДНІ ЗАГРОЗИ У СУЧАСНОМУ КІБЕРПРОСТОРІ

Янчишен Я. В.
yyanchishen@gmail.com
Черкаський державний фаховий бізнес-коледж
Захарова М.В.
м. Черкаси, Україна

Динамічний розвиток інформаційних технологій та глобалізація мережевого простору призвели до появи нових форм протистояння, де традиційні методи конфлікту замінюються гібридними впливами. Гібридні загрози у кіберпросторі представляють собою складний комплекс скоординованих дій, що поєднують технічні атаки на критичну інфраструктуру з інформаційно-психологічним тиском. Актуальність дослідження полягає у необхідності систематизації цих загроз для створення ефективних алгоритмів захисту та мінімізації ризиків у цифровому середовищі [1].

Мета роботи полягає у комплексному аналізі та систематизації сучасних гібридних загроз у кіберпросторі, дослідженні їхньої модульної архітектури та обґрунтуванні переходу до проактивної моделі захисту на основі інтелектуальних систем аналізу даних.

Одним із першочергових аспектів класифікації є розподіл загроз за механізмом їхнього впливу. Ключовим напрямком є техніко-деструктивні загрози, які спрямовані на порушення цілісності, доступності та конфіденційності даних. До цієї категорії належать цілеспрямовані атаки типу APT (Advanced Persistent Threat), використання вразливостей нульового дня (Zero-day) та експлуатація мережевих протоколів для несанкціонованого доступу до державних та корпоративних ресурсів [2]. Використання спеціалізованого шкідливого ПЗ (ransomware, wipers) стає інструментом не лише фінансового збагачення, а й стратегічного виснаження об’єкта атаки [3].

Важливим вектором гібридного впливу є інформаційно-когнітивні загрози. На відміну від технічних атак, вони спрямовані безпосередньо на користувача як «найслабшу ланку» системи безпеки. Ключовими елементами тут виступають

масові кампанії з дезінформації, використання бот-мереж у месенджерах (зокрема Telegram та Signal) для штучного формування громадської думки, а також соціальна інженерія. Сучасні алгоритми розповсюдження контенту дозволяють автоматизувати ці процеси, забезпечуючи високу швидкість та охоплення аудиторії при мінімальних витратах ресурсів [4].

Окрему увагу варто приділити інфраструктурно-ресурсним загрозам. Їхньою особливістю є комбінований вплив на автоматизовані системи керування технологічними процесами (SCADA). Атаки на енергетичні мережі, логістичні вузли та системи водопостачання створюють реальну загрозу фізичній безпеці населення. Важливим аспектом у цьому контексті є розробка механізмів виявлення аномалій у трафіку та впровадження принципів сегментації критичних мереж [5].

Логічно припустити, що архітектура сучасної гібридної атаки має модульний характер і може бути класифікована за функціональними компонентами (див.табл.1). Перспективним напрямком захисту є впровадження систем на основі машинного навчання (Machine Learning) для автоматичного аналізу логів та виявлення прихованих закономірностей у діях зловмисників. Це дозволить перейти від реактивної моделі безпеки («відповідь на інцидент») до проактивної, де потенційна загроза ідентифікується ще на етапі підготовки [7].

Оптимізація системи кібербезпеки в умовах гібридної війни вимагає не лише технічного переоснащення, а й розробки нових регуляторних стандартів. Важливим питанням залишається обмін даними про кіберинциденти між державним сектором та приватними компаніями. Це забезпечить створення централізованої бази знань про методи роботи хакерських угруповань та дозволить швидше реагувати на нові типи загроз [8].

Таблиця 1 – Функціональні модулі гібридної кібератаки

№	Назва модуля	Основна функція та інструментарій	Очікуваний результат
1	Проникнення та закріплення	Обхід Firewalls, IDS/IPS; використання Zero-day вразливостей.	Первинний доступ та стабільна присутність у системі.
2	Ексфільтрація даних	Приховане виведення конфіденційної інформації на зовнішні сервери.	Порушення конфіденційності; викрадення інтелектуальної власності.
3	Інформаційний супровід	Медійне висвітлення атаки, використання бот-мереж та дезінформації.	Штучне формування громадської думки, паніка.
4	Адаптивна протидія	Модифікація коду шкідливого ПЗ за допомогою штучного інтелекту.	Уникнення виявлення антивірусним ПЗ у реальному часі.

Проведене дослідження підтверджує, що сучасні гібридні загрози остаточно трансформувалися з суто технічних інцидентів у багатовекторні операції, де психологічний вплив на користувача є таким же критичним, як і атаки на SCADA-системи. Ключовим висновком є те, що ефективна оборона в умовах гібридної війни неможлива без впровадження Machine Learning для автоматичного аналізу аномалій, що дозволяє виявляти загрози ще на етапі їх підготовки.

У перспективі розвиток систем кіберзахисту має зосереджуватися на:

- Створенні інтелектуальних систем підтримки рішень, які допоможуть офіцерам безпеки діяти в умовах дефіциту часу.
- Поглибленні державно-приватного партнерства для оперативного обміну даними про нові методи роботи хакерських угруповань.
- Підготовці до нових викликів, таких як квантові обчислення та атаки на ланцюжки постачання ПЗ, що стануть визначальними у найближчі роки.

У майбутньому класифікація гібридних загроз може бути розширена шляхом додавання векторів, пов’язаних із квантовими обчисленнями та атаками на ланцюжки постачання програмного забезпечення. Подальші дослідження варто зосередити на створенні інтелектуальних систем підтримки прийняття

рішень для офіцерів кібербезпеки в умовах дефіциту часу та високої невизначеності.

Список використаних джерел:

1. Держспецзв’язку. Аналітичний звіт про кіберзагрози у світі та Україні. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ (дата звернення: 16.03.2026).
2. Горбулін В. П. Гібридна війна: всеохопний характер та інструменти реалізації. Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/ (дата звернення: 16.03.2026).
3. ENISA Threat Landscape 2025. Reports on the state of cybersecurity in the EU. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/ (дата звернення: 16.03.2026).
4. EU DisinfoLab. Deepfakes and AI-driven disinformation: new challenges for security. EU DisinfoLab Publications. URL: https://www.disinfo.eu/ (дата звернення: 16.03.2026).
5. NIST. Guide to Operational Technology (OT) Security. National Institute of Standards and Technology. URL: https://csrc.nist.gov/ (дата звернення: 16.03.2026).
6. McKinsey Digital. The role of Generative AI in modern cyberattacks and defense strategies. McKinsey & Company. URL: https://www.mckinsey.com/ (дата звернення: 16.03.2026).
7. Microsoft Security Blog. Defending against hybrid threats: Machine Learning in cybersecurity. Microsoft. URL: https://www.microsoft.com/security/blog/ (дата звернення: 16.03.2026).
8. Закон України. Про основні засади забезпечення кібербезпеки України від 05.10.2017 № 2163-VIII (зі змінами станом на 2025 рік). Верховна Рада України. URL: https://zakon.rada.gov.ua/ (дата звернення: 16.03.2026).