ІНФОРМАЦІЙНА БЕЗПЕКА В КІБЕРПРОСТОРІ: КЛАСИФІКАЦІЯ ЗАГРОЗ ТА ТЕХНІЧНІ ЗАСОБИ ЇХ НЕЙТРАЛІЗАЦІЇ

Лотюк Юрій
кандидат педагогічних наук, доцент кафедри
інформаційних систем та обчислювальних методів
Приватного вищого навчального закладу
«Міжнародний економіко-гуманітарний університет
імені академіка Степана Дем’янчука»

Соловей Людмила
старший викладач кафедри
інформаційних систем та обчислювальних методів
Приватного вищого навчального закладу
«Міжнародний економіко-гуманітарний університет
імені академіка Степана Дем’янчука»

Грисюк Андрій
викладач кафедри
інформаційних систем та обчислювальних методів
Приватного вищого навчального закладу
«Міжнародний економіко-гуманітарний університет
імені академіка Степана Дем’янчука»
м. Рівне, Україна

У сучасному цифровому суспільстві кіберпростір став не лише середовищем передачі та зберігання інформації, але й ключовим чинником функціонування державних інституцій, економічних структур, соціальних взаємодій та безпеки особистості. З поширенням хмарних сервісів, мобільних пристроїв, систем Інтернету речей (IoT), штучного інтелекту та дистанційного доступу обсяг оброблюваної й передаваної інформації зростає експоненційно, що водночас посилює ризики її несанкціонованого доступу, втрати, підміни або блокування [1].

Загрози в кіберпросторі еволюціонують разом із технологіями: зловмисники дедалі частіше застосовують складні багатовекторні атаки, інструменти соціальної інженерії та автоматизовані механізми штучного інтелекту для здійснення хакерських атак. Особливу небезпеку становлять атаки на критичну інформаційну інфраструктуру — енергетичні системи, медичні заклади, транспортну логістику, урядові ресурси — які можуть

призвести не лише до економічних збитків, а й до загрози життю та здоров'ю громадян [2].

Гарантування інформаційної безпеки в кіберпросторі є надзвичайно актуальним завданням, яке потребує системного, міждисциплінарного та технологічно інноваційного підходу. Її ефективне вирішення є запорукою стабільності суспільства, державного суверенітету та безпечного функціонування інформаційної екосистеми в умовах цифрової трансформації.

У сфері інформаційної безпеки виділяють такі основні *типи кіберзагроз* [3]:

− Мережеві атаки — спрямовані на перехоплення, модифікацію або блокування інформаційного потоку.

− Програмні загрози — шкідливе програмне забезпечення, включаючи віруси, трояни, бекдори, руткіти.

− Атаки соціальної інженерії — маніпуляція користувачем для отримання доступу до конфіденційних даних.

− Фізичні загрози — знищення або пошкодження IT-інфраструктури.

− Інсайдерські загрози — дії співробітників або партнерів, які мають законний доступ до систем.

− Загрози конфіденційності та приватності — несанкціонований доступ до персональних даних.

Для ефективної *протидії загрозам в кіберпросторі застосовуються такі технічні засоби* [4]:

− Мережеві екрани (фаєрволи) — фільтрація мережевого трафіку за заданими правилами;

− Системи виявлення та запобігання вторгненням (IDS/IPS) — моніторинг активності з метою виявлення атак;

− Антивірусне та антишпигунське ПЗ — виявлення й усунення шкідливого коду;

− Системи контролю доступу — автентифікація, авторизація, аудит дій користувачів;

− Шифрування даних — забезпечення конфіденційності при зберіганні та передачі даних;

− SIEM-системи (Security Information and Event Management) — централізований аналіз безпекових подій;

− Технічні засоби резервного копіювання — забезпечення відновлення даних у разі втрати або пошкодження;

− Безпечне конфігурування та оновлення систем — запобігання використанню відомих вразливостей.

Для *підвищення інформаційної безпеки* у кіберпросторі потрібні:

− Розвиток нормативно-правової бази: Актуалізація національних стандартів інформаційної безпеки, гармонізація з міжнародними нормами (ISO/IEC 27001, NIST тощо).

− Підвищення цифрової грамотності користувачів: проведення тренінгів та навчальних програм з кібергігієни.

− Впровадження інноваційних технологій: інтеграція рішень на базі ШІ для проактивного виявлення загроз.

− Розвиток національних CERT-структур: забезпечення оперативного реагування на кіберінциденти.

− Координація зусиль на міжнародному рівні: участь у глобальних ініціативах кіберзахисту, обмін досвідом.

Інформаційна безпека у кіберпросторі є однією з фундаментальних умов стабільного функціонування цифрового суспільства. Класифікація загроз дозволяє більш чітко ідентифікувати вектори атак, тоді як технічні засоби захисту — реалізувати дієвий механізм протидії [5].

Комплексний підхід до гарантування кібербезпеки має включати не лише технологічні, а й організаційні, правові та освітні компоненти. Зважаючи на стрімкий розвиток цифрових технологій та ускладнення методів атак, постійне вдосконалення систем захисту та формування культури кібербезпеки набувають критичного значення.

До *перспективних* напрямів подальших досліджень варто віднести:

− Розроблення моделей проактивного кіберзахисту, що ґрунтуються на використанні штучного інтелекту, зокрема агентних мереж і систем самонавчання;

− Аналіз ефективності адаптивних криптографічних алгоритмів у контексті атак квантового типу;

− Інтеграція систем моніторингу загроз у режимі реального часу (SIEM/SOAR) з елементами самостійного реагування на інциденти;

− Моделювання ризиків кібербезпеки у складних гетерогенних інфраструктурах, зокрема в державному управлінні, освіті, охороні здоров’я;

− Вивчення психолого-поведінкових факторів користувачів, що впливають на ефективність засобів технічного захисту (людський фактор).

ЛІТЕРАТУРА

1. Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors, 21*(11), 3654.

2. Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials, 22*(1), 616–644.

3. Li, X., Xu, M., Vijayakumar, P., Kumar, N., & Liu, X. (2020). Detection of low-frequency and multi-stage attacks in industrial internet of things. *IEEE Transactions on Vehicular Technology*, *69*(8), 8820–8831.
4. Inayat, U., Shahzad, B., & Anwar, Z. (2024). Insider threat mitigation: A systematic literature review. *Journal of Information Security and Applications*, *78*, 103614.
5. ENISA. (2023). *Threat Landscape 2023: Cybersecurity threats and trends in the EU*. European Union Agency for Cybersecurity.