БОРИСЕНК*О Микита Дмитрович*
Київський інститут Національної гвардії України

СИСТЕМА КІБЕРЗАХИСТУ ЯК НЕОБХІДНА УМОВА ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Кіберзахист є невід'ємною складовою сучасного інформаційного суспільства, особливо в умовах воєнного стану, коли рівень кіберзагроз суттєво зростає. Інформаційні технології стали ключовим елементом функціонування державних інститутів, критичної інфраструктури, військових структур та приватного сектору. Відповідно, забезпечення надійної системи кіберзахисту набуває стратегічного значення, оскільки кібератаки можуть завдавати непоправної шкоди безпеці держави, її економіці та громадянам. Однією з основних передумов ефективного кіберзахисту є розуміння його сутності. Кіберзахист – це комплекс правових, технічних, організаційних та процедурних заходів, спрямованих на запобігання, виявлення та нейтралізацію кіберзагроз. Умовно його можна розділити на такі складові: захист інформаційно-комунікаційних систем, забезпечення конфіденційності даних, попередження несанкціонованого доступу та швидке реагування на інциденти. [1].

У забезпеченні кіберзахисту беруть участь різні суб'єкти, включаючи державні органи, приватні компанії, громадські організації та міжнародних партнерів, зокрема:

– Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) – відповідає за формування політики кібербезпеки;

– Національний координаційний центр кібербезпеки (НКЦК) – здійснює аналіз загроз та розробляє рекомендації;

– Служба безпеки України (СБУ) – виконує контррозвідувальні заходи у кіберпросторі;

– Приватні ІТ-компанії – розробляють програмне забезпечення, надають послуги кіберзахисту та займаються аудитом безпеки;

– Організації НАТО, ЄС, ООН та інші – підтримують Україну у зміцненні кібербезпеки, надаючи технологічну та фінансову допомогу;

– Освітні та наукові установи здійснюють підготовку фахівців з кібербезпеки, розробляють нові технології та методи захисту [2].

Об’єктами кіберзахисту є інформаційні ресурси та системи, які мають стратегічне значення, а саме: об’єкти критичної інфраструктури (енергетика, транспорт, телекомунікації, системи водопостачання та охорони здоров’я), вихід з ладу яких, у тому числі внаслідок кібератак, може призвести до катастрофічних наслідків. Також, державні інформаційні ресурси (реєстри, бази даних, системи електронного врядування), які забезпечують функціонування держави. Крім того, інформаційна безпека громадян (персональні дані, фінансові рахунки, соціальні мережі), які часто стають об’єктами атак з метою викрадення інформації або шахрайства [3].

Для ефективного захисту від кібератак використовуються основні методи: шифрування даних (забезпечує конфіденційність інформації), системи моніторингу та виявлення загроз (SIEM) (дозволяють в реальному часі аналізувати події та ідентифікувати потенційні атаки), мультифакторна автентифікація (MFA) (зменшує ризик несанкціонованого доступу до систем), сегментація мережі (обмежує можливість поширення атаки всередині інформаційної системи), тренування персоналу (оскільки людський фактор залишається однією з головних вразливостей, навчання співробітників є важливим елементом кіберзахисту), резервне копіювання даних (дозволяє швидко відновити роботу системи після кібератаки або технічного збою), аудит безпеки (регулярні перевірки дозволяють виявити слабкі місця в системі та вчасно усунути їх) [4].

В умовах воєнного стану кіберзагрози стають частиною гібридної війни. Зловмисники можуть здійснювати атаки на критичну інфраструктуру з метою дестабілізації держави, поширювати дезінформацію для підриву морального

духу населення, викрадати секретну інформацію, яка може бути використана проти держави, паралізувати роботу державних установ через атаки типу DDoS.

Прикладами таких загроз є – кібератака вірусу Petya у 2017 році, яка паралізувала роботу багатьох українських компаній та державних структур.

28 березня 2022 року український провайдер Укртелеком зазнав потужної атаки, під час якої хакери намагались проаналізувати, як влаштована IT-інфраструктура, вивести з ладу обладнання та сервіси, а також отримати контроль над мережею та обладнанням компанії [5].

На мою думку, на сьогодні, основними викликами для України у сфері кіберзахисту є недостатнє фінансування та застаріле обладнання, брак кваліфікованих кадрів, високий рівень залежності від іноземних технологій, постійна еволюція кіберзагроз, які стають дедалі складнішими.

Водночас, Україна має значний потенціал для посилення кіберзахисту. Розробка національних програм, інтеграція з міжнародними системами кібербезпеки, створення центрів реагування на інциденти та підтримка IT-сектору — це перспективні напрямки для зміцнення кібербезпеки.

Підсумовуючи вище сказане необхідно зазначити, що система кіберзахисту є ключовою умовою забезпечення кібербезпеки в умовах воєнного стану. Її ефективність залежить від взаємодії державних і приватних структур, використання сучасних технологій, підготовки кадрів та міжнародної співпраці. У сучасному світі кібербезпека є не лише технічним питанням, а й невід'ємною складовою національної безпеки, що потребує постійного вдосконалення та адаптації до нових викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». URL: https://ippi.org.ua/baranov-oa-pro-tlumachennya-ta-viznachennya-ponyattya-%E2%80%9Ckiberbezpeka%E2%80%9D (дата звернення 10.04.2025).

2. Правова база кібербезпеки в Україні: загальний огляд і аналіз; Квітень 2021; Лілія Олексюк. Міжнародна фундація виборчих систем. URL: https://ifesukraine.org/wp-content/uploads/2021/04/IFES-Ukraine-Cybersecurity-

Legal-Framework-Overview-2020-v2-2021-04-01-Ukr.pdf (дата звернення 10.04.2025).

3. Про національну гвардію України: Закон України від 13 березня 2014 року № 876-VII. Відомості верховної ради України. 2014. № 17. Ст.594. URL: https://zakon.rada.gov.ua/laws/show/876-18#Text (дата звернення 15.04.2025).

4. SNT. Моніторинг інформаційної безпеки (SIEM). URL: https://www.snt.ua/portfolio/it-resheniya/informacionnaya-bezopasnost/monitoring-informacionnoj-bezopasnosti-siem (дата звернення 10.04.2025).

5. Український телекомунікаційний портал PORTALTELE. URL: https://portaltele.com.ua/news/companies/kiberataka-na-ukrtelekom-28-bereznya-detali.html#google_vignette (дата звернення 10.04.2025).