УДК 351/354

Ю В. Гончарук
Національний лісотехнічний університет України, Львів, Україна,
ORCID 0009-0000-0314-1579

КІБЕРБЕЗПЕКА ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВНИХ УСТАНОВ В УМОВАХ ВІЙНИ

Анотація: У сучасних умовах війни кібератаки на державні установи стають однією з головних загроз національній безпеці. Кібербезпека виступає ключовим елементом системи захисту інформації, оскільки забезпечує безперебійну роботу критичних інформаційних систем та захист конфіденційних даних. У тезах розглядається важливість впровадження систем управління інформаційною безпекою на основі міжнародних для державних установ. Застосування цих фреймворків дозволяє ефективно управляти ризиками, підвищувати стійкість до кібератак та забезпечувати належний рівень захисту інформаційної інфраструктури в умовах підвищених загроз.

Ключові слова: кібезбезпека, національна безпека, кіберзагрози.

В умовах повномасштабного вторгнення з боку Росії, війна відбувається не тільки на полі бою, а й у кіберпросторі. Державні установи є об'єктами постійних кібератак. Ці атаки можуть мати катастрофічні наслідки для національної безпеки. В зв’язку з цим кібербезпека стає ключовим елементом інформаційної безпеки, дозволяючи захищати критичні державні системи та дані.

Україна є яскравим прикладом країни, яка в умовах війни з Росією зіштовхується з постійними кібератаками. Численні атаки, які скеровуються на енергетичну інфраструктуру, урядові портали та банки показали важливість кібербезпеки як невід'ємного елементу національної безпеки. Успішна протидія цим атакам була можлива завдяки тісній міжнародній співпраці, покращенню систем моніторингу та реагування, а також розвитку власних кіберсил.

Кібербезпека державних установ є критично важливою для забезпечення захисту інформаційних ресурсів, персональних та інших чутливих даних, а також національної безпеки. Основні правила кібербезпеки для державних установ охоплюють різні аспекти, спрямовані на захист від кіберзагроз.

Основними загрозами кіберпростору під час війни є диверсії, кібершпигунство, атаки на критичну інфраструктуру, інформаційні атаки та дезінформація (табл. 1)

Таблиця 1

Основні загрози кіберпростору під час війни

№ з/п	Види загроз	Характеристика загрози
1	Атаки на критичну інфраструктуру	Порушення функціонування критично важливих систем життєзабезпечння, таких як транспорт, водопостачання, енергетика тощо.
2	Диверсії	Спроби вивести з ладу державні системи управління, енергетичні або комунікаційні мережі.
3	Дезінформація та інформаційні атаки	Маніпулювання суспільною думкою, посилення паніки або політичної нестабільності.
4	Кібершпигунство	Збір конфіденційної інформації про державні установи та військові стратегії.

Для подолання загроз кіберпростору під час війни необхідно виробити стратегію кібербезпеки.

Основними напрямами стратегії кібербезпеки для державних установ є зміцнення захисту мереж та систем шляхом впровадження сучасних систем захисту, які включають такі елементи:

- обмеження доступу та використання мультифакторної авторизації (MFA);
- міжмережеві екрани (Firewall);
- системи виявлення та запобігання несанкціонованим вторгненням (IDS/IPS);
- шифрування критичних даних та інформації;
- регулярне оновлення програмного забезпечення для усунення вразливостей;
- постійний моніторинг мереж та систем для виявлення підозрілої активності;
- створення регулярних резервних копій критично важливих даних;
- впровадити політику щодо використання персональних пристроїв на робочих місцях (BYOD);
- проведення регулярного навчання персоналу з питань кібербезпеки, включаючи розпізнавання фішингових атак, а також запровадження політики "безпечної поведінки в інтернеті" для всіх працівників.
- створення та регулярне тестування планів відновлення після кібератак і впровадження стратегії безперервності роботи критичних систем.
- створення кібероперацийних центрів, що реагують на інциденти та проводять їх розслідування та співпраця з міжнародними кібербезпековими агентствами для отримання оперативної інформації про нові загрози.

Окрім цього є нагальна потреба здійснювати постійний моніторинг діяльності співробітників для виявлення можливих зловживань або порушень.

Стратегію кібербезпеки можна побудувати на основі розробки системи керування інформаційної безпеки базуючись на вимогах та рекомендаціях таких фреймворків:

- ISO 27001:2022 - міжнародний стандарт, який забезпечує основу для систем управління інформаційною безпекою (СУІБ) для забезпечення постійної конфіденційності, цілісності та доступності інформації, а також відповідності законодавству [1].
- NIST Cybersecurity Framework - це рамковий стандарт Національного інституту стандартизації США (NIST). Цей стандарт формує підхід до розуміння, оцінки, планування та впровадження функцій кібербезпеки для підприємств, які є об'єктами критичної інфраструктури [2].

Впровадження бодай одного з цих фреймворків дозволить зменшити ризик кіберзагроз і забезпечити належний рівень захисту державних установ від потенційних атак.

Важливим елементом ефективного функціонування системи інформаційної безпеки є проведення регулярних незалежних аудитів, в тому числі тестування на проникнення (Penetration Testing). Залучення зовнішніх компаній для проведення таких аудитів є більш ефективним, оскільки, зазвичай, вони кращу технічну експертизу та можуть принести свіжий погляд для усунення виявлених проблем та ризиків.

Окрім цього державні установи повинні тісно співпрацювати з приватним сектором шляхом об'єднання зусиль для розробки нових технологій кіберзахисту та обміну інформацією про нові види загроз та вразливостей.

На сьогодні кібербезпека є критично важливим аспектом функціонування державних установ, оскільки загрози кібератак та несанкціонованого доступу до конфіденційних даних зростають. Впровадження систем управління інформаційною безпекою основі стандартів ISO 27001:2022 та NIST CSF забезпечує систематичний підхід до захисту даних, що є важливим для підтримки стабільності та захисту національних інтересів та є важливим кроком для забезпечення безпеки критичної інформаційної інфраструктури та ефективної роботи державних установ під час воєнного стану.

1. ISO/IEC 27001:2022 Information Security, Cybersecurity, and Privacy Protection — Information Security Management Systems — Requirements. International Organization for Standardization, 2022. Retrieved from https://www.iso.org/standard/27001

2. *National Institute of Standards and Technology. (2023). Cybersecurity Framework 2.0: Improving Critical Infrastructure Cybersecurity. Gaithersburg, MD: NIST. Retrieved from https://www.nist.gov/cyberframework*