УДК:

Гладкий Є. В.

Кирилащук Т. Г.

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ КРИТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Вінницький національний технічний університет

Анотація

У статті досліджено актуальні проблеми забезпечення кібербезпеки критичних інформаційних систем. Проаналізовано основні типи кіберзагроз, характерні для сучасного цифрового середовища, а також наведено ефективні методи захисту інформаційних ресурсів. Особливу увагу приділено забезпеченню конфіденційності, цілісності та доступності інформації в умовах зростання кількості кібератак.

Ключові слова: кібербезпека, критичні інформаційні системи, кібератаки, захист інформації, інформаційна безпека.

Abstract

The article examines current issues of cybersecurity of critical information systems. The main types of cyber threats typical for the modern digital environment are analyzed, as well as effective methods for protecting information resources. Special attention is paid to ensuring confidentiality, integrity and availability of information.

Keywords: cybersecurity, critical information systems, cyberattacks, information protection, information security.

ВСТУП

Критичні інформаційні системи є основою функціонування державних органів, енергетичних об’єктів, транспортної інфраструктури та фінансового сектору. Порушення їх роботи внаслідок кібератак може призвести до значних економічних втрат та створити загрозу національній безпеці. У зв’язку з цим питання забезпечення кібербезпеки критичних систем набуває особливої актуальності. З розвитком інформаційних технологій та цифрової трансформації суспільства значення критичних інформаційних систем постійно зростає. До таких систем належать інформаційні системи енергетичних підприємств, транспортних мереж, банківських установ, систем управління водопостачанням, телекомунікаційних мереж та державних реєстрів. Надійність функціонування цих систем безпосередньо впливає на стабільність економіки, безпеку громадян та ефективність державного управління. Саме тому питання їх захисту від кіберзагроз є одним із ключових завдань сучасної кібербезпеки.

ОСНОВНА ЧАСТИНА

Сучасні критичні інформаційні системи характеризуються високим рівнем складності та інтеграцією з глобальними мережами зв'язку. До основних загроз їх безпеці належать шкідливе програмне забезпечення, цільові атаки, атаки типу «відмова в обслуговуванні», а також внутрішні загрози, пов'язані з людським фактором.

Однією з характерних особливостей критичних інформаційних систем є їх висока взаємозалежність. Порушення роботи одного елемента системи може спричинити каскадні збої в інших підсистемах. Наприклад, кібератака на енергетичну інфраструктуру може призвести до зупинки промислових підприємств, порушення роботи транспортних систем та зв'язку. Саме тому забезпечення безпеки таких систем потребує комплексного підходу, який охоплює технічні, організаційні та правові заходи.

Серед найбільш поширених кіберзагроз для критичних інформаційних систем можна виділити шкідливе програмне забезпечення, фішингові атаки, атаки типу «відмова в обслуговуванні» (DDoS), а також складні цільові атаки, відомі як APT-атаки (Advanced Persistent Threats). Такі атаки часто здійснюються організованими групами та можуть бути спрямовані на тривале приховане проникнення в систему з метою отримання конфіденційної інформації або порушення її функціонування.

Важливою проблемою залишається також людський фактор. Недостатня обізнаність працівників щодо правил інформаційної безпеки, використання слабких паролів або недотримання політик доступу можуть стати причиною успішної реалізації кібератак. Тому одним із ключових елементів захисту є підвищення рівня кіберграмотності персоналу та регулярне проведення навчань з інформаційної безпеки.

Для протидії сучасним кіберзагрозам використовуються різноманітні технологічні рішення. До них належать системи виявлення та запобігання вторгненням (IDS/IPS), міжмережеві екрани, антивірусні системи, засоби моніторингу мережевого трафіку та системи управління подіями інформаційної безпеки (SIEM). Застосування криптографічних методів захисту дозволяє забезпечити конфіденційність і цілісність переданої інформації.

Крім технічних засобів захисту важливу роль відіграє розробка та впровадження ефективних політик інформаційної безпеки. До таких політик належать правила управління доступом до інформаційних ресурсів, процедури резервного копіювання даних, регулярне оновлення програмного забезпечення та проведення аудиту безпеки. Дотримання міжнародних стандартів у сфері інформаційної безпеки, зокрема стандартів серії ISO/IEC 27000, дозволяє підвищити рівень захищеності організаційних систем.

У сучасних умовах особливо актуальним є використання проактивних методів кіберзахисту. До них належать аналіз кіберзагроз, моделювання атак, тестування на проникнення (penetration testing) та постійний моніторинг мережевої активності. Такі заходи дозволяють своєчасно виявляти потенційні вразливості та усувати їх до моменту використання зловмисниками.

Для ефективного захисту критичних систем застосовуються комплексні заходи, що включають використання криптографічних алгоритмів, систем виявлення та запобігання вторгненням, багатофакторної автентифікації та регулярного оновлення програмного забезпечення. Важливу роль відіграє впровадження політик інформаційної безпеки та навчання персоналу.

Перехід до проактивних методів кіберзахисту дозволяє своєчасно виявляти потенційні загрози та мінімізувати негативні наслідки кібератак. Таким чином, забезпечення кібербезпеки критичних інформаційних систем є безперервним процесом, що потребує системного підходу.

ВИСНОВКИ

Забезпечення кібербезпеки критичних інформаційних систем є важливою складовою національної безпеки держави. Комплексне застосування технічних, організаційних та кадрових заходів дозволяє значно підвищити рівень захищеності інформаційних ресурсів та забезпечити стабільне функціонування критичної інфраструктури.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Столлінгс В. Криптографія і захист мереж / В. Столлінгс. – Київ : Вільямс, 2017. – 768 с.

https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security/P200000003329

2. Гавриленко В. С. Основи кібербезпеки : навч. посіб. / В. С. Гавриленко. – Харків : ХНУРЕ, 2019. – 312 с.

https://nure.ua/wp-content/uploads/Main_Docs_NURE/osnovy-kiberbezpeky.pdf

3. ISO/IEC 27001:2013 Information security management systems – Requirements. – Geneva : International Organization for Standardization, 2013.

https://www.iso.org/standard/54534.html

4. Снігур О. М. Захист інформації в комп'ютерних системах : навч. посіб. – Львів, 2018. – 256 с.

https://lpnu.ua/sites/default/files/2020/pages/zakon/zahyst-informatsiyi-v-kompyuternyh-systemah.pdf

5. Stallings W. Network Security Essentials: Applications and Standards / W. Stallings. – 6th ed. – Boston : Pearson, 2018. – 640 p. –

https://www.pearson.com/en-us/subject-catalog/p/network-security-essentials/P200000003319

Науковий Керівник: Кирилащук Тетяна Геннадіївна – асистент кафедри захисту інформації, Вінницький Національнй Технічний Університет, Вінниця. kgt0998@gmail.com

Scientific Supervisor: Tetiana H. Kyrylashchuk – assistant of the Department of Information

Protection, Vinnytsia National Technical University, Vinnytsia. kgt0998@gmail.com