

ІНФОРМАЦІЙНА БЕЗПЕКА АВТОМАТИЗОВАНИХ СИСТЕМ

Вінницький національний технічний університет

Анотація

Розглянуто основні аспекти інформаційної безпеки автоматизованих систем, їх загрози та сучасні методи захисту. Проведено аналіз основних категорій загроз, описано ключові методи забезпечення безпеки, особливу увагу приділено перспективам розвитку інформаційної безпеки, зокрема впровадженню штучного інтелекту, технології блокчейн та концепції Zero Trust Architecture.

Ключові слова: інформаційна безпека, автоматизовані системи, кіберзагрози, криптографія, Zero Trust, блокчейн, штучний інтелект, моніторинг, контроль доступу, кіберфізичні системи.

Abstract

The main aspects of information security of automated systems, their threats and modern protection methods are considered. The main categories of threats are analyzed, key security methods are described, and special attention is paid to the prospects for the development of information security, in particular, the implementation of artificial intelligence, blockchain technology and the Zero Trust Architecture concept.

Keywords: information security, automated systems, cyber threats, cryptography, Zero Trust, blockchain, artificial intelligence, monitoring, access control, cyber-physical systems.

Вступ

В умовах цифровізації та широкого впровадження автоматизованих систем (АС) питання інформаційної безпеки набуває критичного значення. Автоматизовані системи, що керують виробничими, логістичними, фінансовими та іншими процесами, стають об'єктами кіберзагроз, які можуть призвести до значних фінансових та репутаційних втрат [1].

Метою даної статті є аналіз ключових аспектів інформаційної безпеки АС, загроз, механізмів захисту та перспектив розвитку в цій сфері. Основна увага приділяється виявленню потенційних загроз, оцінці методів їхнього усунення та перспективам розвитку інформаційної безпеки в умовах швидких технологічних змін.

Результати дослідження

Загрози інформаційній безпеці АС можна поділити на кілька категорій:

- Кібератаки та зловмисні дії: включають атаки типу «відмова в обслуговуванні» (DoS/DDoS), шкідливе програмне забезпечення, хакерські атаки на мережеві інфраструктури [2].
- Вразливості апаратного та програмного забезпечення: помилки в коді, слабкі алгоритми шифрування, незахищені протоколи обміну даними [3].
- Внутрішні загрози: недобросовісні працівники, які мають доступ до конфіденційної інформації, або помилки персоналу через недостатню підготовку.
- Фізичні загрози: збої в обладнанні, природні катастрофи, крадіжка пристроїв з важливою інформацією.

Таблиця 1. Основні загрози інформаційній безпеці АС

Категорія загроз	Приклад загроз
Кібератаки	DDoS, віруси, фішинг
Вразливості ПЗ	Некоректний код, незахищені API
Внутрішні загрози	Шкідливі дії співробітників
Фізичні загрози	Втрата носіїв, крадіжка

Для захисту АС використовують наступні методи та технології:

- Мережева безпека: застосування міжмережевих екранів (Firewall), системи виявлення та запобігання вторгненням (IDS/IPS), сегментування мережі [4].
- Криптографічний захист: використання алгоритмів шифрування AES, RSA, ECC для захисту переданих та збережених даних.
- Контроль доступу: багаторівнева аутентифікація (MFA), біометрична ідентифікація, розмежування доступу відповідно до ролей користувачів.
- Моніторинг та аудит: системи управління інформаційною безпекою (SIEM), журналювання подій та аналіз інцидентів безпеки [5].
- Захист фізичних компонентів: резервне копіювання даних, використання безпечних серверних приміщень, контроль фізичного доступу.

З розвитком технологій змінюються і підходи до забезпечення інформаційної безпеки АС. Основні перспективи:

- Впровадження штучного інтелекту (ШІ) та машинного навчання для прогнозування та виявлення аномальної активності в мережах АС [6].
- Технологія блокчейн для підвищення надійності та прозорості транзакцій, що використовуються в критично важливих автоматизованих системах.
- Zero Trust Architecture (ZTA) – модель, що передбачає перевірку кожного користувача та пристрою перед наданням доступу до ресурсів АС.
- Інтеграція кіберфізичних систем (CPS), що дозволяє забезпечити комплексний захист як цифрової, так і фізичної інфраструктури.

Висновки

Інформаційна безпека автоматизованих систем є ключовим аспектом захисту сучасного цифрового середовища. В умовах зростаючої кількості загроз необхідно застосовувати комплексні підходи, що поєднують технологічні, організаційні та фізичні методи захисту. Подальший розвиток цієї сфери буде визначатися впровадженням інноваційних технологій, таких як штучний інтелект, блокчейн та Zero Trust моделі. Тільки інтегрований підхід дозволить ефективно протидіяти загрозам та забезпечити стабільну роботу автоматизованих систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ISO/IEC 27001:2013. Information Security Management Systems – Requirements. – Geneva: International Organization for Standardization, 2013.
2. Stalling W. Network Security Essentials: Applications and Standards. – Pearson, 2018.
3. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – Wiley, 2015.
4. Shostack A. Threat Modeling: Designing for Security. – Wiley, 2014.
5. NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems and Organizations. – National Institute of Standards and Technology, 2013.
6. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. – Pearson, 2020.

Василенко Валентин Васильович – студент групи ІСТ-246, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: 01-24-007.stud@vntu.vn.ua

Гармаш Володимир Володимирович – канд. техн. наук, доцент кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця.

Vasylenko Valentyn Vasylovich - Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, email : 01-24-007.stud@vntu.vn.ua

Garmash Volodymyr Volodymyrovych - Ph.D. (Eng), Assistant Professor of Department of Automation and Intelligent Information Technology, Vinnytsia National Technical University, Vinnytsia.