УДК 004.056

ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ В СИСТЕМАХ IIOT

Савченко Т. В.[1], Власенко Л. О.[1], Луцька Н. М.[2]
[1] Державний торговельно-економічний університет, sv_t@ukr.net
[2] Національний університет харчових технологій

Оцінка ризиків [1] кібербезпеки в системах промислового Інтернету речей (IIoT) є важливою частиною забезпечення безпеки і надійності промислових процесів. IIoT включає в себе велику кількість підключених пристроїв, систем збору та обробки даних, і створює багато можливостей для атак та порушень безпеки.

Аналіз ризиків в системах промислового IoT може бути проведений за допомогою якісних методів оцінки, які орієнтовані на описову або категоріальну оцінку ризиків. Ризики в IIoT можуть бути різними та розподілятися на кілька категорій. Аналіз допомагає ідентифікувати різні ризики, які впливають на системи IIoT, та класифікувати їх відповідно до їхньої категорії. Кожен ризик може потребувати специфічних заходів для мінімізації або управління ним. Ризики можна ранжувати за ступенем важливості та ймовірності, що допоможе розвивати стратегію керування ризиками та підвищити загальний рівень безпеки IIoT [2, 3].

Для включення кількісної ваги оцінки ризику та ранжування можна використовувати числовий показник для кожного ризику та його ранжування за зростанням чи спаданням. У таблиці наведено рекомендації для керування ризиками, числову вагу ризику (де більший числовий показник вказує на вищий ризик) та ранг (де найнижчий ранг вказує на найвищий ризик). Оцінка ризиків ранжується від високого до низького ризику залежно від числової ваги та рангу ризику.

Рекомендації для керування ризиками

Ризик	Оцінка ризику	Числ. вага ризику	Ранг	Наслідки ризику	Рекомендації для керування ризиками
Кібератаки					
DDoS-атаки	Середній ризик	3	5	Перерва роботи мережі, втрати продуктивності	Встановлення системи виявлення та відновлення інцидентів. Застосування заходів для запобігання DDoS-атак
Зловмисні програми та віруси	Високий ризик	4	4	Пошкодження даних, порушення конфіденційності	Застосування антивірусного програмного забезпечення. Постійне оновлення систем безпеки та антивірусів
Втрати даних					
Витік конфіденційних даних	Високий ризик	4	3	Втрата конфіденційної інформації, можливі правові наслідки	Шифрування конфіденційних даних. Встановлення систем контролю доступу та аудиту
Втрати даних через несправність обладнання	Середній ризик	3	6	Втрата даних, вплив на продуктивність	Регулярне резервне копіювання та відновлення даних. Забезпечення надійності обладнання та систем зберігання даних

Ризик	Оцінка ризику	Числ. вага ризику	Ранг	Наслідки ризику	Рекомендації для керування ризиками
Втрати фінансові					
Простій виробництва	Високий ризик	4	2	Втрати прибутку, вплив на репутацію	Розроблення процедур відновлення виробництва. Запаси та бекапи для відновлення виробництва
Вартість відновлення системи	Середній ризик	3	7	Фінансові витрати на відновлення системи	Налагодження системи моніторингу та виявлення інцидентів. Регулярні аудити систем безпеки
Фізичні ризики					
Зловживання фізичним доступом	Середній ризик	3	8	Несанкціонований доступ до обладнання	Забезпечення фізичної безпеки об'єктів IIoT. Контроль доступу та моніторинг фізичного доступу
Загроза довкілля	Середній ризик	3	9	Пошкодження обладнання внаслідок стихійних лих	Резервне живлення та захист від стихійних лих. Плани надійності та відновлення під час надзвичайних ситуацій
Забезпечення критичності					
Недостатній захист важливих активів	Високий ризик	4	1	Втрата важливих активів, вплив на виробництво	Захист важливих активів за допомогою автентифікації та авторизації
Недостатня якість забезпечення	Середній ризик	3	10	Пошкодження або втрата забезпечення, вплив на ефективність	Оновлення та патчі для програмного забезпечення та обладнання. Постійний аудит та контроль якості забезпечення

Розроблена таблиця є загальною і може застосовуватися до різних типів пристроїв та систем IIoT, що включає в себе різноманітні сенсори, контролери, обладнання та системи, які взаємодіють між собою та з центральними системами. Оцінка ризиків та рекомендації для керування ризиками можуть бути специфічними для конкретних типів пристроїв та систем, а конкретні заходи та рекомендації для керування ризиками повинні враховувати типи та характеристики пристроїв IIoT, їх використання та специфіку виробничих процесів, які вони обслуговують.

1. Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. Технічні науки та технології. 2021. № 1(23). – С. 62–68.

2. Jhanjhi, N., Humayun, M., & Almuayqil, S. N. Cyber Security and Privacy Issues in Industrial Internet of Things. Computer Systems Science & Engineering, 2021, vol. 37, no. 3, pp. 361-380. DOI:10.32604/csse.2021.015206.

3. The Business Viewpoint of Securing the Industrial Internet Executive Overview. Industrial Internet Consortium. Available at: https://hub.iiconsortium.org/securing-industrial-internet-exec-overview.