Павленко К.Ю., магістрант,
Срібна І.М., д.т.н., професор,
Державний університет інформаційно-комунікаційних технологій

МОДЕЛЮВАННЯ ЗАГРОЗ БЕЗПЕЦІ В IOT-СИСТЕМАХ ОХОРОНИ: ПІДХОДИ ДО МІНІМІЗАЦІЇ РИЗИКІВ

Інтернет речей (IoT) трансформує сучасні охоронні системи, впроваджуючи нові можливості для автоматизації та підвищення ефективності. Водночас збільшення кількості пристроїв, які взаємодіють через мережу, створює значні загрози безпеці. Несанкціонований доступ, витік даних і кібератаки є основними викликами, що потребують уваги. Для забезпечення надійної роботи IoT-систем охорони важливо розробити підходи, які дозволять мінімізувати ризики, пов'язані із загрозами інформаційної безпеки.

Актуальність цього дослідження зумовлена необхідністю забезпечення захищеності IoT-систем, які використовуються в охоронних цілях. Основними завданнями стали виявлення основних загроз безпеці IoT-систем, аналіз існуючих методів мінімізації ризиків, розробка моделей загроз для оцінки ризиків у реальних сценаріях використання IoT, а також запропонування інноваційних рішень для зниження ризиків. Метою роботи є моделювання загроз для IoT-систем охорони та розробка практичних рекомендацій для зменшення потенційних ризиків.

У процесі дослідження проаналізовано основні загрози для IoT-систем охорони, серед яких: несанкціонований доступ, перехоплення даних, атаки типу DoS, а також уразливості в прошивках пристроїв. На основі цього запропоновано модель загроз, що враховує специфіку охоронних IoT-систем, зокрема багатофакторну класифікацію ризиків (технічні, організаційні, людські). Для мінімізації ризиків розроблено підхід, що передбачає використання протоколів шифрування даних, регулярне оновлення програмного забезпечення пристроїв та впровадження систем багаторівневої аутентифікації.

Ефективність запропонованих рішень було підтверджено шляхом симуляції роботи охоронної IoT-системи. Результати показали зниження кількості успішних атак на 60%. Запропоновані заходи дозволяють істотно підвищити рівень захищеності IoT-систем і зменшити ймовірність виникнення загроз.

Висновки дослідження підтверджують, що моделювання загроз безпеці є важливим етапом забезпечення надійності IoT-систем охорони. Запропоновані підходи демонструють свою ефективність і можуть бути використані для створення надійних охоронних систем. Подальші дослідження будуть спрямовані на інтеграцію штучного інтелекту для автоматичного виявлення та реагування на загрози, а також на розробку методів оцінки ризиків у розподілених IoT-системах.

Список використаних джерел

1. Hamed Taherdoost. "Security and Internet of Things: Benefits, Challenges, and Future Perspectives." *Electronics*. 2023. URL: https://www.mdpi.com/2079-9292/12/8/1901 (дата звернення: 21.11.2024).
2. "Internet of Things (IoT) Security Trends." *Datamation*, 2024. URL: https://www.datamation.com/ (дата звернення: 21.11.2024).
3. Wenjuan Wang, Zhiqiang Wei. "Internet of Things: Architecture, Applications, and Security Issues." *International Journal of Computer Applications*, 2024. URL: https://www.ijcaonline.org/ (дата звернення: 21.11.2024).
4. R. Roman, et al. "Securing the Internet of Things." *IEEE Computer*, 2018. URL: https://ieeexplore.ieee.org/document/8474764 (дата звернення: 21.11.2024).
5. ISO/IEC 27001:2013. "Information Security Management Systems—Requirements." URL: https://www.iso.org/standard/54534.html (дата звернення: 21.11.2024).