DOI: 10.32347/2412-9933.2024.60.146-155
УДК 004.738

Шабала Євгенія Євгенівна
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії,
https://orcid.org/0000-0002-0428-9273
Київський національний університет будівництва і архітектури, Київ
Корнійчук Борис Валерійович
Кандидат технічних наук, доцент, доцент кафедри професійної освіти,
https://orcid.org/0000-0003-3881-1581
Київський національний університет будівництва і архітектури, Київ

МЕТОДОЛОГІЯ ОЦІНЮВАННЯ БЕЗПЕКИ IoT НА ПРОМИСЛОВИХ ОБ'ЄКТАХ

Анотація. *У статті розглянуто питання забезпечення безпеки Інтернету речей (IoT) на промислових об'єктах, де IoT-пристрої активно впроваджуються для контролю, моніторингу та автоматизації виробничих процесів. Це супроводжується збільшенням ризиків безпеки, здатних негативно позначитися на функціонуванні підприємств. Промислові IoT-системи, які інтегровані з корпоративними мережами та Інтернетом, відкриті для зовнішніх загроз, що може допомогти зловмисникам отримати доступ до критичних даних або навіть керувати пристроями. Серед основних проблем безпеки можна виокремити недостатню частоту оновлення програмного забезпечення для пристроїв на віддалених об'єктах, низький рівень фізичної захищеності та відсутність єдиних стандартів безпеки. Дослідження зосереджено на аналізі можливих загроз для IoT-систем, у т.ч. вразливостей пристроїв, протоколів зв'язку та мережевої інфраструктури. Як результат, надано рекомендації для посилення безпеки промислових IoT-мереж із використанням комплексного підходу до тестування, моделювання можливих атак та оцінки фізичного захисту. Також наголошено на важливості застосування інструментів Wireshark і tcpdump для ретельного аналізу мережевого трафіку та виявлення аномальних ситуацій. У статті виокремлено основні критерії для вибору протоколів зв'язку в IoT-системах: надійність передачі, мінімізація затримки, високий рівень безпеки, можливість масштабування, енергоефективність, стійкість до помилок і сумісність із різними технологіями. Промислові IoT-додатки вимагають використання протоколів, здатних забезпечувати стабільне передавання даних та відповідний рівень захисту. Особливо важливою є також можливість моделювання поведінки пристроїв у мережі, що дає змогу здійснювати оцінювання ризиків, перевіряти надійність і знаходити оптимальні сценарії роботи системи. Для цього пропонується застосування марковських моделей, які уможливлюють передбачити стани пристроїв чи вузлів мережі та оцінити ймовірність їх уразливості до атак.*

Ключові слова: інтернет речей (IoT); кіберзагроза; трафік мережі; марковська модель; вразливість

Вступ

З розвитком промислового Інтернету-речей (Industrial IoT) усе більше підприємств впроваджують IoT-пристрої для моніторингу, управління й оптимізації виробничих процесів. Однак цей розвиток супроводжується зростанням загроз безпеці, які можуть негативно вплинути на роботу об'єктів. Індустріальні IoT-системи часто підключені до корпоративних мереж та Інтернету, що робить їх вразливими до зовнішніх атак. Хакери можуть використовувати вразливості в протоколах передачі даних для проникнення в систему і отримання доступу до критично важливих даних або управління пристроями. Багато IoT-пристроїв працюють на віддалених локаціях або мають обмежену функціональність, що ускладнює регулярне оновлення прошивок та усунення вразливостей. Це призводить до накопичення проблем з безпекою.

Промислові системи можуть складатися з тисяч IoT-пристроїв, що ускладнює моніторинг та управління безпекою всієї мережі. Якщо хоча б один пристрій виявиться вразливим, це може загрожувати всій інфраструктурі. Для зниження ризиків, пов'язаних із використанням IoT-пристроїв, критично важливо регулярно проводити тестування безпеки.

Фахівці з кібербезпеки проводять імітацію реальних атак на IoT-системи, щоб перевірити їхню стійкість до зовнішніх і внутрішніх загроз. Це допомагає виявити практичні сценарії атак і розробити заходи для їх запобігання.

Аналіз останніх досліджень і публікацій

Інтернет-речей (IoT) став важливою технологією, яка радикально змінює промисловий сектор. Завдяки можливості підключення різноманітних пристроїв і датчиків до єдиної мережі, промислові об'єкти можуть значно підвищити ефективність своєї роботи, оптимізувати витрати та підвищити безпеку. Така технологія дає змогу реалізувати взаємозв'язок людей, машин і речей в будь-який час і в будь-якому місці [2]. Проте, як і будь-яка інноваційна технологія, IoT на промислових об'єктах несе із собою певні виклики, особливо в галузі кібербезпеки й управління великими масивами даних. Інтернет-речей на промислових об'єктах (Industrial Internet of Things, IIoT) – це інтеграція датчиків, машин і інформаційних систем на підприємствах для моніторингу й автоматизації процесів. IIoT включає в себе велику кількість пристроїв, підключених до мережі, які збирають та передають дані в реальному часі. Такі системи дають змогу підприємствам отримувати актуальну інформацію про стан обладнання, процесів виробництва та навколишнє середовище, що допомагає приймати обґрунтовані рішення. Актуальність пропонованої теми підкріплюється попитом бізнесу на інтелектуальні системи, зростаючою кількістю досліджень та інновацій у цій сфері [3].

Підключення всіх цих речей до інтернету також означає, що їх можуть атакувати зловмисники. Зі зростанням кількості підключених гаджетів підвищується ризик виникнення проблем.

Мета статті

Основною метою дослідження є розроблення методології тестування безпеки IoT, а також аналіз загроз, розроблення методики тестування та визначення інструментів для забезпечення безпеки IoT. Одна з таких проблем полягає в тому, що виробники компонентів системи Інтернет-речей не приділяють належної уваги питанням інформаційної безпеки, які виникають під час повсякденного використання як окремих компонентів системи, так і цілого апаратно-програмного комплексу. З виходом на ринок великої кількості виробників кінцевого, комунікаційного та керуючого обладнання постало питання про інтероперабельність компонентів складної структури, а також про можливість їхньої роботи без загрози виникнення несанкціонованого доступу, витоку або розкриття інформації, що циркулює в системі [1]. Отже, метою дослідження є визначення ключових загроз для безпеки IoT на промислових об'єктах, аналіз проблем, пов'язаних із захистом IoT-систем та розроблення дієвих методів тестування їхньої безпеки. Дослідження фокусується на виявленні вразливих місць та створенні рекомендацій для покращення захищеності IoT-інфраструктури в промисловості шляхом впровадження методів тестування на проникнення, аналізу вразливостей та оцінки фізичного захисту пристроїв.

Виклад основного матеріалу

Різні компанії створюють різноманітні типи гаджетів і не завжди можуть домовитися про найефективніший спосіб їх захисту. Крім того, деякі пристрої досі використовують застарілі методи захисту, які вже не забезпечують належного рівня безпеки.

Інтернет-речей автоматизує процеси, підвищуючи ефективність виробництва й оптимізуючи управління об'єктами. Однак разом із перевагами цієї технології зростають і ризики, пов'язані із загрозами безпеці. Використання IoT на промислових об'єктах відкриває нові перспективи для зловмисників, здатних спричинити значні економічні збитки та порушення в роботі систем.

Рисунок 1 – Основні загрози безпеці IoT для промислових об'єктів

Кібератаки через незахищені пристрої. Чимало промислових IoT-пристроїв мають недостатній рівень захисту, що робить їх вразливими для кіберзлочинців. Незахищені датчики, контролери та інші підключені пристрої можуть бути використані для доступу до інфраструктури підприємства, що уможливлює здійснювати атаки на виробничі процеси, збирати конфіденційну інформацію або навіть спричиняти фізичні пошкодження обладнання.

Незахищені протоколи зв'язку. У промислових умовах часто застосовуються протоколи зв'язку, які не завжди відповідають сучасним стандартам безпеки. У випадку передачі даних через незахищені канали зловмисники можуть перехоплювати інформацію, змінювати її або підробляти команди

управління, що може спричинити збої в роботі систем або несанкціоновані зміни у виробничих процесах.

Атаки типу DDoS (розподілене заперечення обслуговування). IoT-пристрої можуть бути залучені до ботнетів – мереж заражених девайсів, що використовуються для здійснення DDoS-атак. Промислові об'єкти, особливо ті, що залежать від безперервної роботи підключених пристроїв, є вразливими до подібних атак, оскільки відмова в обслуговуванні може призвести до серйозних збоїв у роботі підприємства.

Фізичний доступ до пристроїв. На промислових об'єктах IoT-пристрої можуть бути розташовані в різних зонах, де контроль за фізичним доступом є недостатнім. Це створює можливість для зловмисників втручатися в роботу пристроїв, змінювати їхні налаштування або впроваджувати шкідливе програмне забезпечення, що ставить під загрозу безпеку всього об'єкта.

Атаки на ланцюг постачання. Оскільки на виробничих об'єктах часто застосовуються IoT-пристрої від різних постачальників, існує ймовірність, що вразливості можуть виникнути вже на стадії виробництва або доставки. Атаки на ланцюг постачання надають зловмисникам можливість отримати доступ до даних і управління ще до інтеграції пристроїв у виробничу інфраструктуру.

Недостатня сегментація мережі. На багатьох промислових об'єктах IoT-пристрої підключені до тієї ж мережі, що й основні виробничі та IT-системи. Відсутність сегментації мережі підвищує ризик того, що атака з одного скомпрометованого пристрою поширяться на всю інфраструктуру, що може мати серйозні наслідки для безперервності виробничих процесів та безпеки даних.

IoT є точкою входу в організацію, на яку націлені кіберзловмисники з метою вчинення шкідливих дій: прослуховування, викрадення інформації, порушення операційної діяльності, виведення з ладу обладнання тощо [4].

Сучасні рішення безпеки, доступні для захисту систем із використанням IoT, ставлять виробників і операторів у складне становище. Як правило, такі рішення орієнтовані на периферійні області IoT і стримують кібератаки та загрози лише після їх ідентифікації. Визначають різні проблеми безпеки систем IoT, які представлені на рис. 2.

Впровадження систематичного тестування на всіх рівнях уможливлює виявити слабкі місця та забезпечити надійний захист промислових IoT від потенційних загроз, які можуть серйозно вплинути на роботу підприємства.

Тестування безпеки IoT на промислових об’єктах включає декілька рівнів, кожен із яких потребує специфічного підходу.

На рівні пристроїв виконується аналіз вразливостей прошивки на наявність вразливостей, таких як вбудовані бекдори або незашифровані конфіденційні дані. Тестування охоплює відновлення прошивки для аналізу її коду і виявлення можливих проблем. Також відбувається перевірка фізичної доступності пристроїв, особливо якщо вони розташовані в зонах з обмеженим контролем. Це включає захист від втручання, а також огляд корпусів і точок доступу, щоб унеможливити маніпуляції чи встановлення шкідливого програмного забезпечення. Наприкінці здійснюється оцінювання комунікаційних протоколів із дослідженням протоколів зв’язку, які використовуються пристроєм, наприклад, MQTT, CoAP або HTTP.

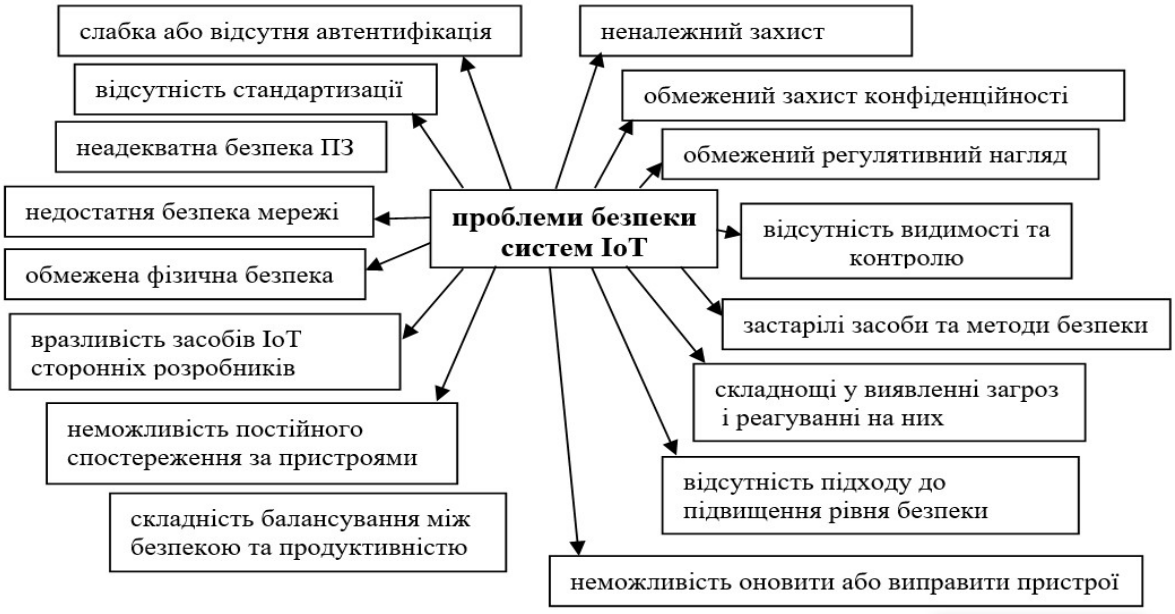

Рисунок 2 – Проблеми безпеки систем IoT

На мережевому рівні відбувається перевірка правильного розподілу IoT-пристроїв в окремих сегментах мережі, щоб запобігти поширенню атаки в разі компрометації одного пристрою, та оцінка захищеності протоколів і методів передавання даних, таких як захищені канали передачі даних, наявність VPN, шифрування TLS/SSL для захисту від перехоплення та модифікації даних.

На рівні платформи здійснюється перевірка на відсутність уразливих компонентів, таких як застарілі модулі, бібліотеки або небезпечні налаштування в IoT платформах. Також відбувається аналіз доступу та прав користувачів, де оцінюється коректність налаштувань ролей і дозволів для обмеження доступу до критичних функцій лише необхідним користувачам. Це включає захист від атак типу «привілейоване підвищення».

Важливим етапом є тестування механізмів аутентифікації і авторизації для користувачів і пристроїв з метою підтвердження автентичності всіх підключень і дій у системі.

На рівні додатків та інтерфейсів відбувається аналіз безпеки API для забезпечення захисту даних, які передаються між пристроями і платформою. Це охоплює перевірку правильності авторизації, автентифікації та наявності шифрування даних у запитах.

Також перевіряється безпека вебдодатків та мобільних додатків з тестуванням на проникнення для вебінтерфейсів і мобільних додатків, які надають доступ до IoT платформи. Особливу увагу приділяють вразливостям типу SQL-ін'єкцій, XSS, CSRF тощо.

Необхідним етапом є оцінювання управління сесіями з тестуванням механізмів управління сесіями, включаючи шифрування сесійних токенів, захист від викрадення сесій і налаштування тайм-аутів для автоматичного завершення неактивних сесій. Під час тестування безпеки IoT застосовуються системи моніторингу загроз для безперервного відстеження підозрілих дій і швидкого реагування на спроби зловмисних вторгнень.

Пасивна розвідка

Пасивний збір інформації, також відомий як OSINT (розвідка з відкритих джерел), включає отримання цільових даних без прямого контакту із системами. Це базовий етап будь-якої оцінки, який допомагає сформувати загальне уявлення про стан безпеки. Наприклад, можна завантажити технічні специфікації пристроїв або чіпсетів, дослідити форуми та соціальні мережі, а також отримати інформацію від користувачів або технічного персоналу за допомогою непрямих запитань. Також можливо зібрати внутрішні імена хостів із сертифікатів TLS, що надаються через сертифікатну прозорість, – стандарт, який зобов'язує центри сертифікації реєструвати видані сертифікати у відкритих журналах, що дає змогу виявляти помилкові чи зловмисно видані сертифікати.

Посібники та документи

Системні посібники можуть надати величезну кількість інформації про внутрішню роботу пристроїв. Їх зазвичай можна знайти на офіційному сайті виробника пристрою. Вони можуть виявити імена користувачів і паролі за замовчуванням, які часто залишаються у виробничому середовищі, детальні специфікації системи та компоненти, мережеві схеми та архітектури, а також теми усунення несправностей, які допомагають виявити слабкі місця.

Ще одним корисним ресурсом для пристроїв, що використовують радіозв’язок, є онлайнова база даних FCC ID. Ідентифікатор FCC – це унікальний ідентифікатор, присвоєний пристрою, зареєстрованому у Федеральній комісії зв’язку США. Усі пристрої безпровідникового випромінювання, що продаються в США, повинні мати ідентифікатор FCC.

Здійснюючи пошук FCC ID конкретного пристрою, можна знайти детальну інформацію про робочу частоту бездротової мережі та потужність обладнання, внутрішні фотографії пристрою, інструкції користувача тощо. Ідентифікатор FCC зазвичай гравірується на корпусі електронного компонента або пристрою [5]. Знання цієї інформації допомагає більш детально розібратися у принципах роботи пристроїв та розробити план атаки.

Патенти

Патенти можуть містити важливу інформацію про внутрішню структуру пристроїв. Зазвичай вони включають блок-схеми, що дають змогу оцінити канали зв’язку між пристроєм та іншими системами. Віддалений доступ до системи створює потенційні ризики, такі як злам через незахищений мобільний додаток або саму віддалену інфраструктуру (часто реалізовану в хмарі).

Тестування фізичного рівня пристроїв IoT є важливою частиною для захисту від несанкціонованого доступу та інших загроз, що можуть виникнути через фізичне втручання в обладнання. Це сприяє виявленню можливих вразливостей ще на етапі розгортання системи IoT і допомагає забезпечити стабільну та безпечну роботу у виробничому середовищі.

Основні етапи тестування фізичного рівня IoT:

- Аналіз місця розміщення IoT-пристроїв;
- Перевірка фізичного доступу та обмежень;
- Аналіз стійкості до фізичного втручання;
- Перевірка цілісності кабельних з'єднань;

– Аналіз енергопостачання та резервного живлення;

– Оцінка можливостей зняття даних при фізичному доступі.

Атаки на мережевий протокол і сервіси

Атаки на мережеві протоколи і сервіси складаються з таких етапів: сканування вразливостей, аналіз мережевого трафіку, реверс-інжиніринг і робота протоколу або служби. Ви також можете виконувати сканування вразливостей незалежно від інших кроків, в іншому випадку вам потрібно виконувати кроки послідовно [5].

Тестування потрібно почати з перевірки баз даних, таких як National Vulnerability Database (NVD) або VulnDB, для пошуку відомих вразливостей у відкритих мережевих службах. У деяких випадках система може бути настільки застарілою, що звіт від автоматичного сканера вразливостей стає досить об'ємним.

Деякі вразливості можна навіть використовувати дистанційно без необхідності автентифікації. Якщо буде виявлено серйозну вразливість, наприклад, віддалене виконання коду, це може забезпечити доступ до командного інтерфейсу пристрою. Для аналізу та моніторингу мереж пропонується використання Wireshark – це графічний інструмент аналізу мережі, який уможливлює візуалізувати та фільтрувати пакети даних. Він забезпечує зручний інтерфейс для перегляду мережевого трафіку у реальному часі та в режимі аналізу пакетів. Його можливості допомагають виявити проблеми, такі як перевантаження мережі, аномалії у комунікаціїі між пристроями, атаки та інші аномалії.

Також, Wireshark є потужним інструментом для відлагодження мережевих додатків та служб. Інженери мереж можуть використовувати його для визначення причин низької продуктивності мережі та забезпечення її оптимізації. Tcpdump, з іншого боку, є консольним інструментом для перехоплення та аналізу пакетів даних. Він забезпечує можливість моніторити мережевий трафік у реальному часі, а також записувати його для подальшого аналізу. Tcpdump особливо корисний для адміністраторів мереж, які працюють у середовищах командного рядка і вимагають точного контролю над процесом аналізу мережі.

На рис. 3 представлено результат захоплення трафіку мережі.

Розглянемо докладніше це вікно за пунктами, вказаними на ньому:

1. Панель фільтрів допомагає знайти необхідну інформацію (можна вводити текст фільтра вручну, використовуючи спеціальні команди та оператори Wireshark для точного визначення потрібного трафіку).

2. Панель найменувань, що поділяє інформацію з пункту 3 на номер, час від початку захоплення трафіку, джерело та адресат, а також протокол, розмір пакета і невелику інформацію про мережевий пакет.

3. Панель пакетів оновлюється в реальному часі. Тут інформація про пакети розділена на стовпці, визначені на панелі найменувань.

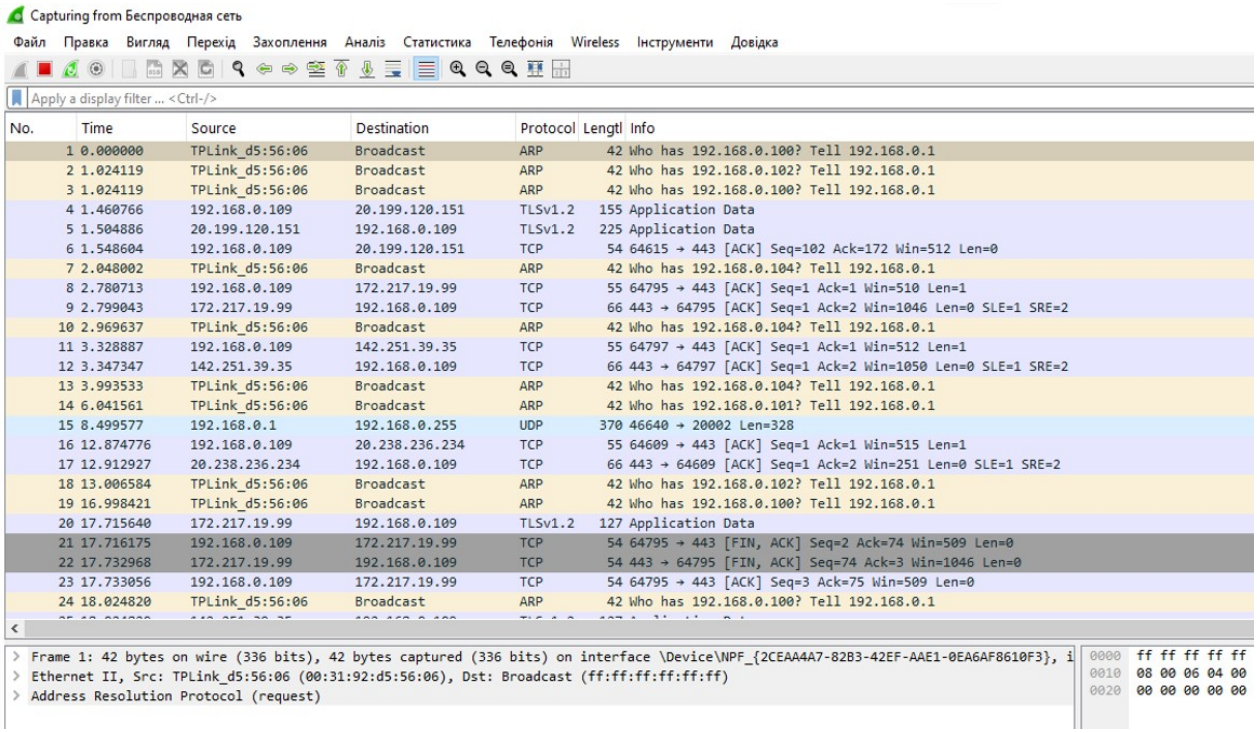

Рисунок 3 – Захоплення трафіку мережі

4. Панель рівнів, що описує рівні моделі OSI вибраного мережного пакета.

5. Панель метаданих, що представляє дані у шістнадцятковому коді та символах.

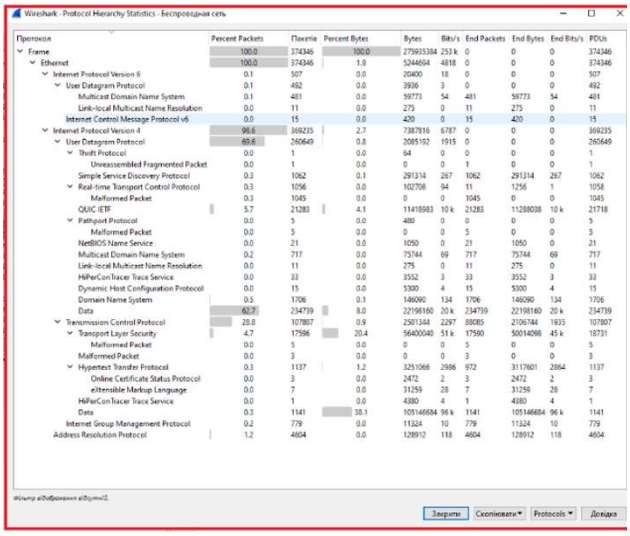

Рисунок 4 – Ієрархія протоколів

На рис. 4 можна побачити ієрархію всіх захоплених протоколів, що допоможе визначити, які саме протоколи домінують у мережі.

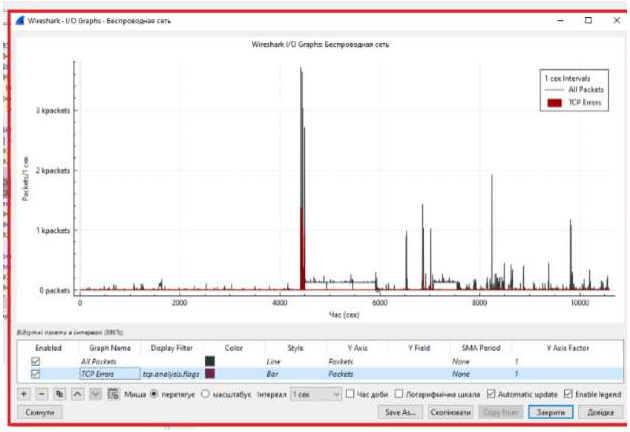

Рисунок 5 – Графіки вводу/виводу

На рис. 5 можна спостерігати динаміку трафіка в мережі, зокрема сплески або падіння активності.

Для аналізу безпеки IoT-пристроїв доцільно буде використання IoT Inspector, який дає змогу перевіряти мережевий трафік, виявляти підключені пристрої та оцінювати можливі вразливості. Для промислових об'єктів IoT Inspector надає корисні можливості, оскільки може ідентифікувати небезпечні з'єднання, некоректні налаштування безпеки та інші фактори ризику, що можуть вплинути на надійність і безпеку виробничих процесів.

Після запуску IoT Inspector відбувається пошук пристроїв, які підключені (рис. 6).

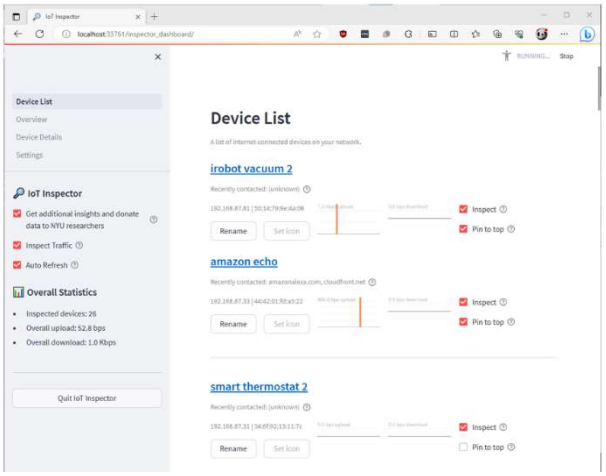

Рисунок 6 – Знайдені IoT Inspector підключені пристрої

Також можна проаналізувати, з якими доменами зв'язуються пристрої IoT (рис. 7).

Також можна зробити налаштування пристроїв та визначити їх локацію [6].

Центральним елементом функціональності й ефективності цих екосистем Інтернету-речей є протоколи зв'язку, що лежать в їх основі і керують обміном даними між пристроями. Ці протоколи гарантують, що пристрої з різними можливостями і обмеженими ресурсами можуть взаємодіяти надійно і безпечно [7].

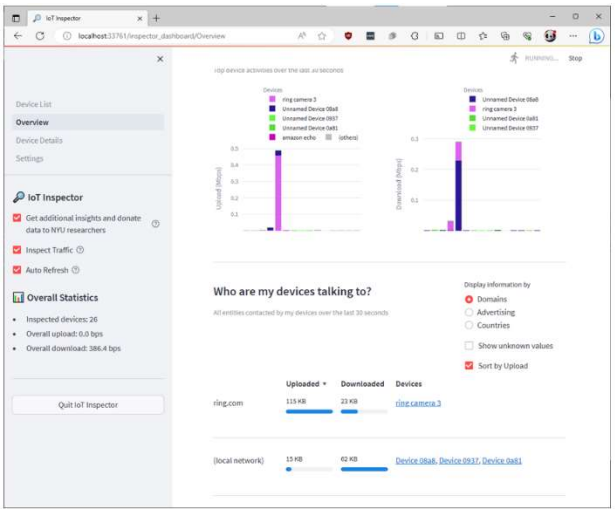

Рисунок 7 – Зв'язок пристроїв IoT і доменів

Основні критерії вибору стеку протоколів для IoT-додатка на промислових об'єктах:

1. Надійність передачі даних. У промислових IoT-додатках надійність передачі даних є надзвичайно важливою, адже втрата або спотворення інформації можуть призвести до збоїв у роботі обладнання або навіть небезпечних ситуацій. Протоколи, які мають вбудовані механізми контролю (наприклад, TCP або CoAP з розширеними гарантіями надійності), можуть стати вибором для забезпечення надійної доставки даних.

2. Пропускна здатність і затримка в мережі. Промислові додатки зазвичай вимагають високої швидкості передавання даних і мінімальної затримки, що є критичним для систем реального часу. Протоколи, такі як MQTT або DDS, можуть забезпечити ефективні комунікації при низьких затримках.

3. Безпека та конфіденційність. Промислові IoT-системи часто працюють з конфіденційними даними і можуть бути об'єктами кіберзагроз, тому безпека є важливою умовою. Протоколи з підтримкою шифрування й автентифікації, такі як TLS/DTLS або IPsec, забезпечують захист від несанкціонованого доступу та витоків даних.

4. Масштабованість. У разі необхідності підтримки сотень або тисяч пристроїв, протокол повинен мати можливість масштабуватися відповідно до таких вимог. Наприклад, CoAP або AMQP, розроблені для масштабованих мереж, здатні витримувати велике навантаження і підтримувати значну кількість підключених пристроїв без втрати продуктивності.

5. Енергоспоживання. У промислових умовах широко застосовуються пристрої з обмеженими ресурсами, наприклад, автономні сенсори з обмеженою ємністю батареї. Протоколи з низьким рівнем енергоспоживання, такі як LoRaWAN або 6LoWPAN, оптимальні для довготривалої роботи пристроїв без частого обслуговування.

6. Стійкість до помилок та можливість відновлення. Промислові IoT-додатки потребують протоколів, що мають вбудовану стійкість до помилок та підтримку автоматичного відновлення підключення у разі розриву зв’язку. Протоколи з функціями відновлення, такі як TCP або DDS, забезпечують стабільну роботу навіть за умов мережевих збоїв.

7. Сумісність і взаємодія між системами. У промисловому середовищі, де використовується багато різних пристроїв і платформ, протокол повинен підтримувати взаємодію з широким спектром технологій. Наприклад, HTTP і MQTT забезпечують сумісність з різними стандартами, що робить їх ефективними у промислових умовах.

Для IoT-додатків на промислових об'єктах потрібно підбирати протоколи, які забезпечують надійну передачу даних, стійкість до мережевих збоїв, безпеку та низьке енергоспоживання. Також важливим є моделювання поведінки пристроїв і загальної системи, що уможливлює прогнозувати ефективність мережі, оцінювати ризики, тестувати відмовостійкість і виявляти оптимальні сценарії роботи.

Для моделювання поведінки пристроїв і системи під час різних атак пропонується використати Марковську модель. Відомі приклади застосування марковських ланцюгів для визначення ймовірностей станів організаційно-технічних або соціальних систем засновані на структурній і параметричній подобі оригіналів цих систем їхнім відображенням — марковським моделям [8]. Марковська модель для системи IoT може допомогти змоделювати стани пристроїв або вузлів у мережі та оцінити їхню надійність або уразливість до атак. Розглянемо базову модель, яка включає кілька типових станів для IoT-пристрою в промисловій мережі.

1. Визначення станів:

Нехай у нас є IoT-пристрій у промисловій мережі, який може перебувати в таких станах:

S_0: Нормальна робота — пристрій працює без збоїв або атак.

S_1 : Уразливий стан — пристрій потенційно уразливий (наприклад, виявлено відкритий порт або незахищений канал).

S_2: Компрометований стан — пристрій зазнав атаки або його захоплено.

S_3 : Відновлений стан — після компрометації пристрій пройшов відновлення.

2. Перехідні ймовірності:

Розглянемо ймовірності переходу між станами за одиницю часу t . Наприклад:

P_{01}: Ймовірність переходу з нормального стану S_0 до уразливого стану S_1 через виявлення потенційної вразливості.

P_{12} : Ймовірність переходу з уразливого стану S_1 до компрометованого S_2 , якщо на пристрій здійснюється успішна атака.

P_{23} : Ймовірність того, що компрометований пристрій S_2 відновлюється до стану S_3 .

P_{30} : Ймовірність повернення відновленого пристрою S_3 до нормального стану S_0 .

P_{10} : Ймовірність усунення вразливості, коли пристрій повертається до нормального стану S_0 .

P_{33} : Ймовірність того, що відновлений пристрій залишається у відновленому стані без повернення до нормальної роботи.

3. Марковська матриця переходів:

Матриця переходів для цього процесу матиме вигляд:

$$P = \begin{pmatrix} P_{00} & P_{01} & 0 & 0 \\ P_{10} & P_{11} & P_{12} & 0 \\ 0 & 0 & P_{22} & P_{23} \\ P_{30} & 0 & 0 & P_{33} \end{pmatrix}, \qquad (1)$$

де кожен елемент P_{ij} матриці відповідає ймовірності переходу зі стану S_i у стан S_i :

P_{00} **:** Ймовірність того, що пристрій залишиться у нормальному стані S_0, без переходу в інші стани.

P_{01} **:** Ймовірність переходу із нормального стану S_0 до уразливого стану S_1, коли пристрій виявляється вразливим.

P_{10} **:** Ймовірність повернення з уразливого стану S_1 до нормального стану S_0, наприклад, після виправлення вразливості.

P_{11} **:** Ймовірність того, що пристрій залишиться в уразливому стані S_1, не переходячи до компрометованого стану або повернення до нормального.

P_{12} **:** Ймовірність переходу з уразливого стану S_1 до компрометованого стану S_2, наприклад, у випадку успішної атаки.

P_{22} : Ймовірність того, що пристрій залишиться у компрометованому стані S_2, без переходу до відновлення.

P_{23} : Ймовірність того, що пристрій перейде з компрометованого стану S_2 до відновленого стану S_3, наприклад, після усунення наслідків атаки.

P_{30} : Ймовірність того, що пристрій перейде з відновленого стану S_3 назад до нормального стану S_0, завершивши цикл відновлення.

P_{33} : Ймовірність того, що пристрій залишиться у відновленому стані S_3, тобто поки що не повернеться до нормальної роботи.

На рис. 8 представлено розмічений граф станів моделі.

Марковські мережі застосовуються переважно для моделювання атак і прогнозування стану інформаційних систем [9]. У випадку з промисловими IoT-системами, де функціонування залежить від великої кількості взаємопов'язаних пристроїв, Марковські моделі допомагають оцінити, як надійність та стійкість до збоїв залежать від різних умов.

4. Сталість станів та аналіз ризику

Для довготривалого аналізу ризику компрометації пристрою можна визначити сталий розподіл станів $\pi = (\pi_0, \pi_1, \pi_2, \pi_3)$, де кожен елемент відповідає ймовірності пристрою бути в тому чи іншому стані в стабільному режимі:

$$\pi P = \pi \,, \tag{2}$$

$$\sum_{i=0}^{3} \pi_i = 1 \,. \tag{3}$$

Ймовірність компрометації визначається значенням сталого розподілу для скомпрометованого стану дає оцінку ризику компрометації пристрою в довготривалій перспективі.

Ймовірність відновлення означає те, що інші стани можуть відповідати нормальному функціонуванню, очікуванню оновлення, необхідності ремонту тощо. Сталі ймовірності цих станів можуть свідчити про час, який пристрій перебуває в безпечному режимі або в режимі відновлення.

Розрахунок сталого розподілу уможливить оцінити ризики – ймовірність компрометації та час відновлення пристроїв у системі.

Для оцінки безпеки IoT-системи можна використовувати цю модель для прогнозування впливу вразливостей, ефективності відновлення, часу простою пристроїв і визначення найуразливіших ділянок системи, що допоможе ухвалити обґрунтовані рішення для підвищення безпеки.

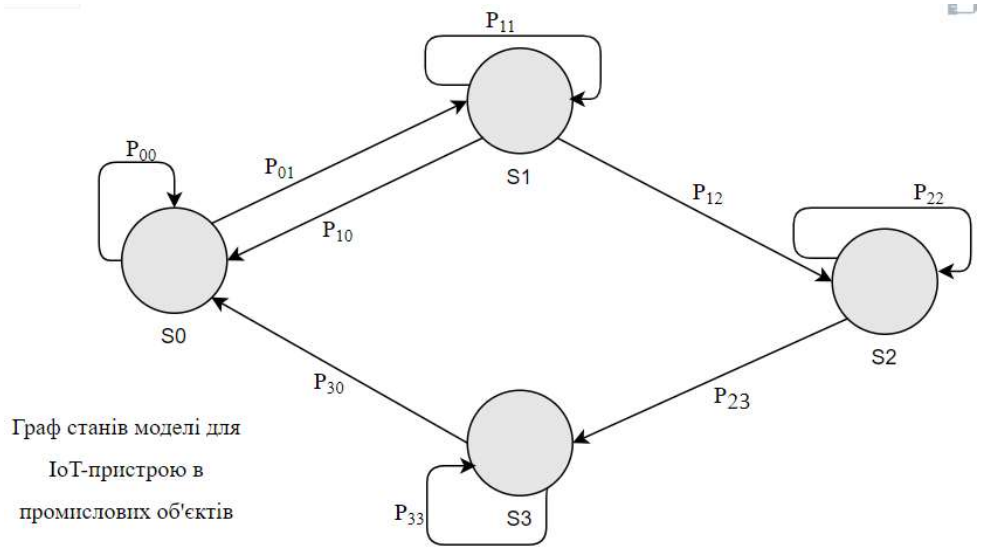

Рисунок 8 – Граф станів моделі IoT для промислових об'єктів

Припущення та обмеження:

Переходи, позначені як 0 у матриці, вказують на неможливі або відсутні прямі переходи між відповідними станами.

Всі ймовірності в кожному рядку мають у сумі дорівнювати 1, оскільки вони описують повний набір можливих станів для кожного етапу пристрою.

Висновки

Інтернет-речей дедалі більше перетворюється на основний чинник проривних змін у сфері інформаційних технологій [10]. Підключення промислових IoT-систем до корпоративних мереж та Інтернету робить їх потенційною ціллю для зовнішніх атак, що потребує посиленого захисту інформації та контролю доступу.

Запропонована у статті методологія оцінювання безпеки включає інструменти для тестування, зокрема Wireshark і tcpdump, які уможливлюють проводити глибокий аналіз мережевого трафіку та виявляти аномалії. Окремо виділено критерії для вибору протоколів зв'язку в IoT-системах, які мають забезпечувати надійну передачу, низьку затримку, високу безпеку, масштабованість та енергоефективність. Додаткову увагу приділено моделюванню поведінки пристроїв у мережі з метою оцінювання ризиків та визначення оптимальних сценаріїв роботи системи.

Запропоновані підходи дають змогу врахувати ключові аспекти захисту промислових IoT-рішень та гарантують стабільну роботу системи навіть в умовах постійних кіберзагроз. Зокрема, моделювання на основі марковських процесів допомагає передбачати стани пристроїв та оцінювати їхню вразливість до атак, що є важливим кроком до підвищення захищеності промислової IoT-інфраструктури.

Список літератури

1. Завгородній В. В., Дроздова Є. А., Козел В. М. Аналіз проблем безпеки IoT пристроїв. *Вісник Херсонського національного технічного університету*. 2020. №4 (75). URL: https://cyberleninka.ru/article/n/analiz-problem-bezpeki-iot-pristroyiv (дата звернення: 20.10.2024).

2. Гончаренко Т. А. Сучасні інформаційні технології для моделювання міського середовища та розробки цифрових двійників міських об'єктів. *Управління розвитком складних систем*. Київ, 2022. № 51. С. 87 – 93.

3. Рябчун Ю. В., Середа Д. Е., Кохан В. Р., Доля О. В. Можливості та переваги українського ринку технологій «розумний будинок». *Управління розвитком складних систем*. Київ, 2023. № 56. С. 181 – 187.

4. Морозов А. О., Ященко В. О. Технології прийняття рішень у військових системах. виклики та перспективи. *Математичні машини і системи.* 2023. № 4. С. 3–10.

5. Lady Liberty. Загрози у світі речей інтернету (Методологія тестування безпеки). 2023. URL: https://hackyourmom.com/osvita/chastyna-3-zagrozy-u-sviti-rechej-internetu-metodologiya-testuvannya-bezpeky/ (дата звернення 20.10.2024).

6. Danny Y. Huang. Iot-inspector-client. Screenshots (Windows). 2023. URL: https://github.com/nyu-mlab/iot-inspector-client/wiki/Screenshots-(Windows) (дата звернення 21.10.2024).

7. Парфенюк Т. М. Застосування сучасних протоколів у мережах IOT / Т. М. Парфенюк ; наук. керівник Ю. Г. Лотюк. *Збірник наукових праць здобувачів вищої освіти та молодих учених Приватного вищого навчального закладу «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука»* / МОН України, ПВНЗ «МЕГУ ім. акад. Степана Дем'янчука». Вип. 1. Рівне: О. Зень, 2024. С. 120–124.

8. Руденко С. В., Романенко М. В., Катуніна О. Г., Колеснікова К. В. Розробка марковської моделі зміни станів пацієнтів у проектах надання медичних послуг. *Управління розвитком складних систем*. Київ, 2012. №12. С. 86–90.

9. Никифоров О. В., Путятін В. Г., Куценко С. А. Математичні моделі та методи для вирішення деяких питань інформаційної безпеки. *Реєстрація, зберігання і обробка даних*, 2023, Т. 25, № 2 С. 27–65.

10. Журило О., Ляшенко О. Архітектура та системи безпеки IoT на основі туманних обчислень. *Сучасний стан наукових досліджень та технологій в промисловості.* 2024. № 1(27), С. 54–66.

Стаття надійшла до редколегії 04.11.2024

Yevheniia Shabala
Ph.D., associate professor, associate professor of Department of cyber security and Computer Engineering,
https://orcid.org/0000-0002-0428-9273
Kyiv National University of Construction and Architecture, Kyiv
Borys Korniichuk
Ph.D., associate professor, associate professor of Department of Vocation education,
https://orcid.org/0000-0003-3881-1581
Kyiv National University of Construction and Architecture, Kyiv

METHODOLOGY FOR ASSESSING IOT SECURITY AT INDUSTRIAL FACILITIES

Abstract. *The article examines the issue of ensuring the security of the Internet of Things (IoT) at industrial facilities, where IoT devices are actively implemented to control, monitor and automate production processes. This is accompanied by an increase in security risks that can negatively affect the functioning of enterprises. Industrial IoT systems that are integrated with corporate networks and the Internet are open to external threats, which could allow attackers to gain access to critical data or even control devices. Among the main security problems, we can highlight the insufficient frequency of software updates for devices at remote sites, a low level of physical security, and the lack of uniform security standards. The main goal of the article is to develop a methodology for comprehensive security testing of industrial IoT systems, which includes the assessment of cyber threats, the development of testing approaches, and the selection of tools to ensure reliable protection. The research focuses on analyzing possible threats to IoT systems, including vulnerabilities in devices, communication protocols, and network infrastructure. As a result, recommendations are provided for strengthening the security of industrial IoT networks using a comprehensive approach to testing, modeling possible attacks, and evaluating physical defenses. The importance of using Wireshark and tcpdump tools to thoroughly analyze network traffic and detect anomalies is also emphasized. The article highlights the main criteria for choosing communication protocols in IoT systems: reliability of transmission, minimization of delay, high level of security, scalability, energy efficiency, error tolerance and compatibility with various technologies. Industrial IoT applications require the use of protocols capable of providing stable data transmission and an appropriate level of protection. Particularly important is also the possibility of modeling the behavior of devices in the network, which allows you to assess risks, check reliability and find optimal scenarios of system operation. For this purpose, the use of Markov models is proposed, which allow predicting the states of devices or network nodes and estimating the probability of their vulnerability to attacks.*

Keywords: Internet of Things (IoT); cyber threat; network traffic; Markov model; vulnerability

References

1. Zavgorodniy, V., Drozdova, E. & Kozel, V. (2020). Analysis of security problems of IoT devices. *Bulletin of the Kherson National Technical University*, 4 (75). URL: https://cyberleninka.ru/article/n/analiz-problem-bezpeki-iot-pristroyiv.

2. Honcharenko, T. (2022). Modern information technologies for simulation of the urban environment and creation of digital duplicate of city objects. *Management of Development of Complex Systems*, 51, 87–93.

3. Riabchun, Yu., Sereda, D., Kokhan, V. & Dolya, E., (2023). Opportunities and Advantages of the Ukrainian Technology Market «Smart Home». *Management of Development of Complex Systems*, 56, 181–187.

4. Morozov, A. & Yashchenko, V. (2023). Decision-making technologies in military systems. *Challenges and prospects. Математичні машини і системи*, 4, 3–10.

5. Lady, Liberty (2023). Threats in the Internet of Things (Security Testing Methodology). URL: https://hackyourmom.com/osvita/chastyna-3-zagrozy-u-sviti-rechej-internetu-metodologiya-testuvannya-bezpeky/

6. Danny, Y. Huang. (2023). Iot-inspector-client. Screenshots (Windows). URL: https://github.com/nyu-mlab/iot-inspector-client/wiki/Screenshots-(Windows).

7. Parfenyuk, T. (2024). Application of modern protocols in IOT networks. *Collection of scientific works of higher education graduates and young scientists of the Private Higher Educational Institution "International University of Economics and Humanities named after Academician Stepan Demyanchuk"*, 1, 120–124.

8. Rudenko, S., Romanenko, M., Katunina, O. & Kolesnikova, K. (2012). Development of a Markov model of changes in patients' conditions in projects for the provision of medical services. *Management of the development of complex systems*, 12, 86–90.

9. Nikiforov, O., Putyatin, V. & Kutsenko, S. (2023) Mathematical models and methods for solving some issues of information security. *Registration, storage and processing of data*, 25 (2), 27–65.

10. Zhurilo, O. & Lyashenko, O. (2024). IoT architecture and security systems based on fog computing. *The current state of scientific research and technology in industry*, 27 (1), 54–66.

Посилання на публікацію

APA Shabala, Ye. & Korniichuk, B. (2024). Methodology for assessing IoT security at industrial facilities. *Management of Development of Complex Systems*, 60, 146–155, dx.doi.org\10.32347/2412-9933.2024.60.146-155.

ДСТУ Шабала Є. Є., Корнійчук Б. В. Методологія оцінювання безпеки IoT на промислових об’єктах. *Управління розвитком складних систем.* Київ, 2024. № 60. С. 146 – 155, dx.doi.org\10.32347/2412-9933.2024.60.146-155.