УДК 004.056.5:004.738.5

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИСТРОЇВ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ АВТОМАТИЗАЦІЇ ВИРОБНИЧИХ ПРОЦЕСІВ

Уляна Пановик[1,2], Тетяна Король[1], Сергій Кутас[2]
[1]Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна
[2]Українська академія друкарства, м. Львів, Україна

Анотація. Розглядається актуальне питання кібербезпеки для пристроїв у мережі Інтернету речей. Проведено аналіз загроз та викликів, що виникають у зв'язку з розширенням IoT, та досліджено засоби та стратегії для забезпечення захисту інформації для підвищення рівня безпеки та стійкості IoT-пристроїв у сучасному інтернет-середовищі. Дослідження спрямоване на вдосконалення заходів інформаційної безпеки та захисту конфіденційності в мережі Інтернету речей.
Ключові слова: пристрої Інтернету речей (IoT), загрози кібербезпеці, засоби захисту інформації.

Abstract. The topical issue of cybersecurity for devices on the Internet of Things network is considered. An analysis of the threats and challenges arising from the expansion of the IoT is carried out, and the means and strategies to ensure the protection of information to increase the level of security and resilience of IoT devices in today's Internet environment are explored. The study is aimed at improving information security and privacy protection measures on the Internet of Things network.
Keywords: Internet of Things (IoT) devices, cyber security threats, information protection tools.

Основними процесами в роботі систем Інтернету речей (IoT) є збір, передача й аналіз даних. Датчики, що встановлені на пристроях, реєструють інформацію про стан об'єкта або довкілля. Після цього отримані дані передаються на сервери або хмарні сервіси, де проводиться обробка й аналіз цих даних. Після аналізу генеруються відповідні команди, які надсилаються виконавчим пристроям або системам для виконання необхідних дій. Для передачі даних у системах IoT використовуються як дротові, так і бездротові мережі. Дротові мережі включають Ethernet, оптоволоконні кабелі та інші типи кабельних з'єднань, у той час, як бездротові мережі використовують технології, такі як Wi-Fi, Bluetooth, Zigbee, LoRaWAN, мобільні мережі (3G, 4G, 5G) й інші бездротові засоби передачі даних [1].

IoT значно впливає на виробничі процеси і промисловість загалом, зокрема на автоматизацію виробництва. За допомогою IoT-пристроїв, таких як роботи, сенсори та контролери, можна автоматизувати багато виробничих операцій, забезпечуючи високу точність, швидкість та ефективність. Окрім автоматизації, IoT допомагає впроваджувати системи обслуговування обладнання, завдяки збору та аналізу даних із датчиків. Це дає змогу передбачити потребу в обслуговуванні або ремонті обладнання, запобігаючи збоям і зупинкам виробництва. IoT сприяє підвищенню продуктивності в промисловості, даючи можливість моніторити та оптимізувати роботу обладнання і персоналу. Це призводить до зменшення витрат на енергію, сировину та робочу силу. Застосування IoT відкриває також нові можливості для віддаленого моніторингу і управління виробничими процесами, що дає змогу операторам реагувати на зміни умов виробництва і уникати втрат часу та ресурсів.

Попри популярність та зручність IoT-пристроїв, вони мають свої недоліки. Особливо важливою є кібербезпека, оскільки кожен пристрій IoT може бути потенційною вразливою точкою входу в мережу та виробничих процесів. З розвитком технологій безпека IoT-пристроїв стає дедалі важливішою. Забезпечення безпеки пристроїв Інтернету речей (IoT) є важливою складовою сучасної мережі в організаціях[2]. ІТ-команди мають включити ці ризики у свої протоколи кібербезпеки і працювати над їх мінімізацією. Без належних практик щодо безпеки IoT, компанії можуть зіткнутися з новими кіберзагрозами, які надходять із кіберпростору. Наприклад, зловмисники, які спрямовані на розумні пристрої, можуть отримати доступ до критичних ресурсів компанії, подолавши вразливі розумні пристрої, які підключені до них. Це дає їм можливість збирати конфіденційні дані або влаштовувати систему виснажливих кібератак [3, 4].

Ризики, пов’язані з IoT, інколи легко прогледіти, якщо не використовувати відповідні інструменти. Іноді фахівці з інформаційної безпеки можуть недооцінювати важливість інвентаризації кінцевих точок, що може призвести до недооцінки потенційно вразливих пристроїв, які не отримують належної уваги. Найпоширенішими атаками на IoT є: DDoS-атаки, експлойти програмного забезпечення, атаки типу «людина посередник» (MITM-атаки), фізичне втручання, брутфорс-атаки та викрадення прошивки. Із цього випливає, що основні компоненти систем IoT вразливі до кібератак, і безпека має бути важливою на кожному етапі їхньої розробки та інтеграції. Для запобігання кібератакам на пристрої IoT і загальному зменшенню ризиків безпеки, компанії можуть застосовувати такі практики:

Управління поверхнею атаки. Планування заходів забезпечення безпеки IoT має включати створення карт, що охоплюють усі підключені пристрої для їхньої інвентаризації. Інформація про кількість пристроїв, виробників, серійні номери, версії обладнання та прошивки є важливою для команди безпеки, щоб керувати ризиками IoT.

Моніторинг, аналіз та звітність у режимі реального часу. Важливо, щоб компанії мали можливість постійно відстежувати стан безпеки IoT-пристроїв і реагувати на потенційні загрози в реальному часі. Використання програмних продуктів для інвентаризації та моніторингу підключених IoT-пристроїв допомагає відстежувати їхню активність і виявляти можливі аномалії та загрози.

Сегментація мережі є важливим кроком для запобігання доступу до всієї мережі організації, обмеження поверхні атаки та мінімізації можливих збитків. Сегментація мережі полягає в розділенні внутрішньої мережі на окремі підмережі. Ці сегменти можуть спілкуватися між собою, але вони зазвичай є незалежними та ізольованими. Цей підхід дає можливість зосереджувати увагу на критичних частинах мережі для посилення їх безпеки.

Створення надійних паролів для пристроїв IoT є також важливим заходом безпеки. Багато IoT-пристроїв постачаються зі слабкими попередньо встановленими паролями, які можуть бути легко підібрані. Під час реєстрації нового IoT-пристрою в мережі, рекомендується негайно змінити його попередньо встановлений пароль на складніший. Цей новий пароль має бути стійким до підбору, унікальним для кожного пристрою та відповідати політиці керування паролями вашої команди з безпеки IT.

Фізичний захист пристроїв на фізичному рівні має велике значення, оскільки доступність пристроїв ззовні може призвести до фізичних втручань зловмисників із метою несанкціонованого доступу або завантаження шкідливого програмного забезпечення. Тому варто забезпечити надійне місце дислокації пристроїв, щоб до них не було відкритого доступу.

Своєчасне оновлення прошивок є важливим кроком у забезпеченні безпеки IoT. Нові версії прошивок можуть містити виправлення вже відомих програмних вразливостей пристрою. Проте оновлення прошивок також повинно перевірятися на автентичність, оскільки зловмисники можуть намагатися під виглядом оновлень завантажити на пристрій шкідливе програмне забезпечення. Необхідно контролювати версійну актуальність та завжди використовувати останні безпечні версії прошивок.

Виконання цих заходів безпеки допоможе користуватися пристроями IoT безпечно в організації, максимізуючи їх користь та мінімізуючи можливі ризики. Проте важливо пам’ятати, що кіберзагрози постійно розвиваються, тому потрібно залишатися в курсі нових подій у кіберпросторі та регулярно оновлювати заходи безпеки, використовуючи передові рішення для моніторингу та аналізу атак.

Інформаційні джерела

1. Internet of things (IoT). URL: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT#
2. Пановик У., Кутас С., Брич Т. Керування безпекою інтернету речей на основі індексу довіри. *Інформаційна безпека та інформаційні технології*: тези доп. IV Міжнар. науково-практ. конф. ІБІТ 2022, м. Львів, 30 листоп. 2022 р. Львів. С. 39–41. URL: https://sci.ldubgd.edu.ua/jspui/handle/123456789/11434.
3. Internet of Things: information security challenges and solutions. URL: https://www.researchgate.net/publication/326559393_Internet_of_Things_information_security_challenges_and_solutions.
4. Spiegelmock M. IoT Security Through Open Certification. URL: https://spiegelmock.com/2017/08/14/iot-security-through-open-certification/