УДК 004.7

Л.А. Савицька[1], Т.І. Коробейнікова[2], О.І. Костюк[1],
І. С. Колесник[1], О. В. Дудник[1]

ЗАСОБИ ЗАХИСТУ INTERNET OF THINGS В КОРПОРАТИВНІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ

[1]Вінницький національний технічний університет, Вінниця

[2]Національний університет «Львівська політехніка»

Анотація. Дана робота стосується аналізу та удосконалення засобів захисту для Internet of Things (IoT) у корпоративних комп'ютерних мережах. Internet of Things охоплює широкий спектр даних, включаючи особисті відомості, що робить питання безпеки під час їх передачі вельми актуальним. Основна мета дослідження полягає в розробці вдосконаленого технологічного дизайну системи IoT для забезпечення високого рівня безпеки та конфіденційності інформації. Сучасний світ Інтернету речей вимагає аналізу та покращення захисту IoT в корпоративних комп'ютерних мережах. В процесі аналізу використоно загальнодоступні джерела інформації та наукові підходи, включно із сучасними науково-практичними публікаціями, аналітичними звітами та ресурсами від провідних компаній, таких як Cisco, що спеціалізуються на мережевому обладнанні та налаштуванні корпоративних мереж. Такий підхід дозволяє враховувати найсучасніші тенденції та технологічні рішення в галузі безпеки IoT. Однією з ключових проблем, на яку звертається увага, розробці розширеного та вдосконаленого технологічного дизайну системи IoT. Враховуючи постійний розвиток технологій, необхідно забезпечити високий рівень адаптивності та гнучкості захисних засобів, щоб вони ефективно працювали в різних умовах та обставинах. Додатковий акцент робиться на вивченні впливу розширеного та вдосконаленого технологічного дизайну системи IoT. Важливо забезпечити синергію між новими технологічними рішеннями та вже існуючими структурами мережі, щоб досягти максимального ефекту в удосконаленні безпеки та ефективності. Отже, наукова робота зосереджена на комплексному аналізі та впровадженні новітніх захисних засобів для IoT в корпоративних мережах з урахуванням сучасних тенденцій та вимог до безпеки даних.

Ключові слова: Internet Of Things, інформаційна безпека, рівні стеку, безпековий технологічний дизайн системи IoT, модель безпечного дизайну системи Internet Of Things.

Abstract. This work pertains to the analysis and enhancement of security measures for the Internet of Things (IoT) in corporate computer networks. The Internet of Things encompasses a wide range of data, including personal information, making the issue of security during their transmission highly relevant. The primary goal of the research is the development of an advanced technological design for the IoT system to ensure a high level of security and confidentiality of information. The modern world of the Internet of Things demands an analysis and improvement of IoT security in corporate computer networks. In the process of analysis, publicly available information sources and scientific approaches were utilized, including contemporary scientific publications, analytical reports, and resources from leading companies, such as Cisco, specializing in network equipment and configuration of corporate networks. This approach allows for the consideration of the latest trends and technological solutions in the field of IoT security. One of the key issues addressed is the development of an extended and improved technological design for the IoT system. Considering the constant evolution of technologies, it is essential to ensure a high level of adaptability and flexibility of security measures to effectively operate in various conditions and circumstances. An additional emphasis is placed on studying the impact of an extended and improved technological design of the IoT system. It is crucial to establish synergy between new technological solutions and existing network structures to achieve maximum effectiveness in enhancing security and efficiency. Therefore, the scientific work focuses on a comprehensive analysis and implementation of cutting-edge security measures for IoT in corporate networks, taking into account contemporary trends and data security requirements.

Key words: Internet Of Things, information security, stack levels, secure technological design of the IoT system, model of secure design of the Internet Of Things system.

DOI: https://doi.org/10.31649/1999-9941-2024-59-1-83-93.

Вступ та актуальність

Започаткування розвитку Internet of Things (IoT) та його використання відбулося у 2000-х роках. У цьому напрямку активно працюють численні відомі та інші компанії, такі як IBM, Intel, Google, Cisco, Microsoft, Amazon, і Siemens. [1-7]. Уже у період між 2018 і 2019 роками кількість пристроїв, які були підключені до мережі, вагомо перевищила населення Землі. Згідно з передбаченнями, до 2025 року кількість таких підключених пристроїв мала сягнути від 50 до 70 мільярдів одиниць. Це експоненційне зростання створює значні ризики для безпеки інформації, яка обробляється, передається та зберігається цими пристроями. Для запобігання цим ризикам необхідно дотримуватись вимог, включаючи ті, які встановлені Регламентом Європейського Парламенту і Ради ЄС 2016/679 від 27 квітня 2016 року щодо захисту особистих даних та вільного обігу таких даних, що відомий також як GDPR. [4, 8, 9]. Тому тема дослідження є актуальною.

Отже, потрібно провести аналіз та покращення захисту IoT в корпоративних комп'ютерних мережах. Основний акцент зроблено на розробці розширеного та вдосконаленого технологічного дизайну системи IoT.

Мета

Метою даного дослідження є підвищення безпеки та захисту пристроїв Internet Of Things всередині

корпоративної комп’ютерної мережі від несанкціонованого доступу. Це досягається за допомогою вдосконаленого технологічного дизайну системи IoT.

Задачі

1. Спроектувати вдосконалений технологічний дизайн системи Internet Of Things;
2. Запропонувати розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things;
3. Розробити модель безпечного дизайну системи Internet Of Things урахуванням 4-рівневого дизайну системи Internet Of Things;

Архітектура та ключові елементи системи IoT

Поняття Internet Of Things відображає глобальну систему взаємно підключених та зв'язаних пристроїв різного типу, що призначені для поліпшення процесу прийняття рішень різного характеру, заснованого на аналізі величезних обсягів даних, які накопичуються цими пристроями. Іншими словами, Internet Of Things – це мережа, в якій об'єкти і пристрої спілкуються між собою та надсилають дані для покращення різноманітних рішень.

Система Internet Of Things складається з багатьох компонентів і складових. До цього переліку входять пристрої виконання, сервіси і технології, які використовуються для оптимальної роботи цієї перспективної галузі. В цей перелік включаються різні типи сенсорів, пристроїв для збору даних, засоби передавання інформації, хмарні обчислення, аналітичні інструменти та багато інших компонентів. Усі вони спільно працюють, щоб забезпечити надійну і ефективну роботу Internet Of Things та підтримувати вирішення різних завдань та завдань у різних галузях та сферах життя [10, 11].

Перелічимо засоби, сервіси і технології:

- Сенсори (розумні датчики/виконавчі механізми): це вбудовані системи, які мають операційні системи реального часу та використовуються для збору даних. Вони також обладнані джерелами безперебійного живлення і використовують мікро-електромеханічні системи (МЕМС).
- Вбудовані системи зв'язку з датчиками: ці системи забезпечують зв'язок між датчиками. Зона охоплення бездротових персональних мереж може варіюватися від нульової відстані до 100 метрів. Для обміну даними між датчиками використовуються низькошвидкісні малопотужні інформаційні канали, які не завжди базуються на протоколі IP.
- Локальні обчислювальні мережі (LAN): зазвичай це системи обміну даними на базі протоколу IP, такі як 802.11 Wi-Fi, що використовуються для швидкої бездротової радіозв'язку. Ці мережі можуть бути як піринговими (Peer-to-peer), так і зірковими.
- Агрегатори, маршрутизатори, шлюзи (gateways), пограничні пристрої (Edge Device): ці пристрої служать постачальниками вбудованих систем і включають в себе різні компоненти, такі як процесори, динамічна оперативна пам'ять і системи зберігання даних. Вони також можуть бути виробниками модулів, пасивних компонентів, тонких клієнтів і радіосистем, а також надавати послуги з міжплатформного програмного забезпечення.
- Глобальна обчислювальна мережа: в цю категорію входять оператори стільникового зв'язку, оператори супутникового зв'язку, і оператори малопотужних глобальних мереж (Low-Power Wide-Area Network, LPWAN). Для IoT зазвичай використовуються транспортні протоколи Інтернету, такі як MQTT, CoAP, і навіть HTTP;
- Хмарна інфраструктура: хмарні ресурси виступають в ролі постачальників різноманітних послуг і платформ для системи Internet Of Things. Вони також надають інфраструктуру для обробки потокових і пакетних даних, баз даних і аналізу даних. Крім того, хмарні постачальники надають інструменти для аналізу та розробки програмного забезпечення, а також сервіси машинного навчання.
- Сервіси аналізу даних: величезні обсяги інформації передаються в хмару для проведення подальшого аналізу. Робота з великими даними і отримання конкретних результатів вимагають комплексної обробки даних та використання методів аналізу та машинного навчання.
- Забезпечення безпеки: під час інтеграції всіх компонентів архітектури в єдину систему постає питання забезпечення кібербезпеки. Безпека є критичним аспектом на всіх рівнях, від фізичних датчиків до центральних обчислювальних систем, включаючи системи зв'язку та протоколи передавання даних. На кожному рівні необхідно гарантувати конфіденційність, доступність та цілісність даних. У цьому ланцюжку не може бути слабких точок, оскільки екосистема Internet Of Things стає об'єктом атак з боку хакерів у всьому світі.

Ця архітектура Internet Of Things об'єднує різноманітні компоненти та послуги, щоб забезпечити збір, обробку, зберігання та аналіз даних. Вона включає в себе різні типи пристроїв, мереж і сервісів і

вимагає високого рівня безпеки для захисту інформації від потенційних загроз. На рисунку 1 наведено схематичне зображення архітектури Internet Of Things за версією компанії CISCO [4, 10].

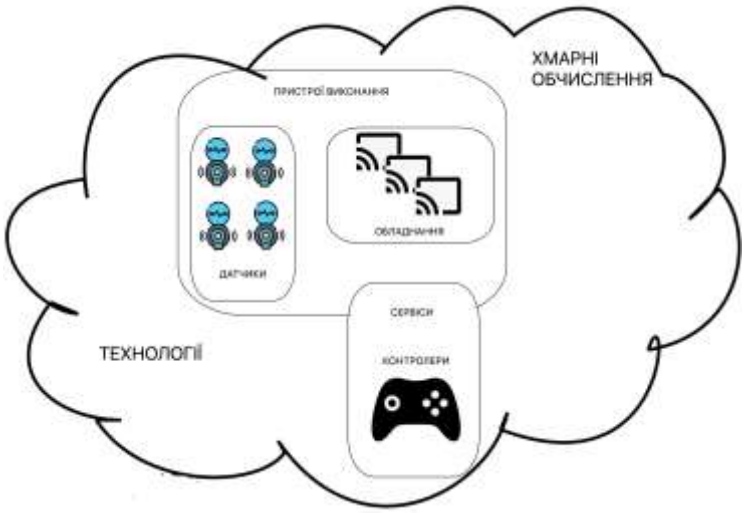

Рисунок 1 – Складові архітектури системи Internet Of Things

З різних поглядів компаній і спеціалізованих організацій архітектурна модель Internet Of Things може включати в себе різні рівні обслуговування та подання. Наприклад, Міжнародний союз електрозв'язку (MCE-T) вивів 4-х рівневу модель архітектури IoT, тоді як Всесвітній форум IoT (IoT World Forum, IWF) розробив еталонну модель, яка складається з 7 рівнів [12,13,14]. Відмінність між цими моделями полягає в їхній конкретній реалізації. У загальних рисах вони нагадують архітектуру традиційних систем автоматизації управління технологічними процесами.

Вдосконалений технологічний дизайн системи Internet Of Things

У таблиці 1, наведеній нижче, представлена одна з прикладних 3-рівневих моделей архітектури системи Internet Of Things, яка розглядає питання безпеки на кожному рівні та можливі варіанти їх вирішення. Наслідком цього є більш глибоке розуміння аспектів безпеки в контексті Internet Of Things [15, 16, 17].

Таблиця 1 – Складові трирівневої моделі системи Internet Of Things

РІВЕНЬ ВИКОНАВЧИХ ПРИСТРОЇВ	Безпека IoT	RFID-пристрої, бездротові сенсорні пристрої, GPS-пристрої
	Безпека мережі IoT	
ТРАНСПОРТНИЙ РІВЕНЬ	Доступ до мережі IoT	WIFI-мережі, Ad hoc-мережі
	WAN	Мобільний Інтернет, Інтернет
	LAN	Безпека локальної мережі
ПРИКЛАДНИЙ РІВЕНЬ	IoT Applications	Інформаційна логістика, інтелектуальна мережева безпека, моніторинг середовища
	IoT Application support	Безпека середовища розробки, платформи хмарних обчислень, поміжні технології безпеки

Як вже було відзначено в даній роботі, остаточний вигляд структури Internet Of Things залежить від багатьох факторів, включаючи потреби та особливості конкретного проекту і реальні можливості для їх впровадження. Розподіл функцій системи на її рівнях також є важливим аспектом, який потребує чіткості та розуміння.

Для поліпшення розподілу функцій автором пропонується розширений дизайн системи IoT (порівняно із див. Таблиця 1) з додатковим рівнем інтерфейсів, що надає новій архітектурі подібність до принципів побудови сервіс-орієнтованої архітектури (SOA). На рисунку 2 нижче наведено розширений дизайн системи IoT, що складається з 4 рівнів. Цей дизайн дозволяє краще розуміти та оптимізувати функціональний розподіл в контексті системи Internet Of Things.

3-LAYER MODEL	4-LAYER MODEL
Прикладний рівень	Службовий рівень
Транспортний рівень	Рівень корпоративної комп’ютерної мережі
Рівень виконавчих пристроїв	Рівень локальних інтерфейсів
	Рівень датчиків

Рисунок 2 – Запропонований розширений технологічний дизайн системи IoT

Кожен з вказаних компонентів на цьому ілюстрації виконує свою конкретну функцію. Рівень датчиків займається збором даних. Рівень локальних інтерфейсів відповідає за забезпечення взаємодії між різними учасниками системи, рівень корпоративної комп’ютерної мережі відповідає за передачу даних, і службовий рівень дозволяє створювати та управляти різними сервісами.

Ця ілюстрація демонструє, що кожен з компонентів в мережі має свою важливу функцію. Рівень датчиків відповідає за збір великої кількості різноманітних даних, рівень локальних інтерфейсів виконує роль посередника, який дозволяє різним частинам системи спілкуватися та обмінюватися інформацією. Рівень корпоративної комп’ютерної мережі відповідає за ефективну передачу цих даних між різними пристроями та підсистемами. Нарешті, службовий рівень включає в себе можливості створення, налагодження та керування різними сервісами та функціоналом мережі. Кожен із цих рівнів є важливою ланкою в цій складній системі, і їх спільна робота дозволяє Internet Of Things працювати ефективно та надійно.

Технологічний дизайн системи Internet Of Things

Відповідно до моделі сервіс-орієнтованої архітектури (Service-oriented architecture, SOA) технологічний дизайн системи Internet Of Things буде містити 4 чотири рівні, згідно досліджень (рис. 2). Відобразимо відкриту модель OSI, відомий протокольний стек TCP/IP, прототипну 3-рівневу модель та модель технологічного дизайну системи Інтернету речей за принципами SOA (рис. 3).

OSI	TCP/IP	3-LAYER Sec.IOT DESIGN	4-LAYER Sec.IOT DESIGN
7 Application 6 Presentation 5 Session	Application	Прикладний рівень	Службовий рівень
4 Transport	Transport	Транспортний рівень	Рівень корпоративної комп’ютерної мережі
3 Network	Network		
2 Data Link 1 Physical	Network Access	Рівень виконавчих пристроїв	Рівень локальних інтерфейсів Рівень датчиків

Рисунок 3 – Приведення технологічного дизайну системи Internet Of Things до відомих стандартів

Така архітектура забезпечує взаємодію між великою кількістю різних пристроїв. Кожен з цих рівнів має такі функції:

- Рівень датчиків взаємодіє з апаратними засобами та датчиками для визначення стану системи Інтернету речей та безпосередньо збирання даних (рівень 1);
- Рівень локальних інтерфейсів надає різні методи та засоби взаємодії системи Інтернету речей з безпечною мережею (LAN) (рівень 2);
- Рівень корпоративної комп’ютерної мережі надає повноцінну мережеву інфраструктуру, яка для стабільної підтримки з’єднань у корпоративній комп’ютерній мережі (рівень 3);
- Службовий рівень дає можливість керувати засобами та сервісами між користувачам та додатками (рівень 4).

За використання запропонованого технологічного дизайну, ця система розбивається на підсистеми, які взаємодіють між собою та можуть бути використані для підтримки функціонування новоствореної системи. Цей підхід гарантує безперебійну роботу, оскільки при відмові одного компонента інші продовжать функціонувати. У випадках, коли надійність та доступність є ключовими завданнями у проектуванні, ця модель виявляється найкращим вибором.

Цей підхід спрощує взаємодію з протоколами передавання даних та різними рівнями системи, оскільки сприяє покращенню взаємодії між об'єктами та спрощує процес керування. Модель технологічного дизайну системи Інтернету речей організована на основі принципів SOA, дає Інтернету речей можливість повністю реалізувати свій потенціал і показати всі свої переваги. Ця модель дозволяє створювати складні сервіси, де для виконання різних завдань можна виділити окремі об'єкти системи [19].

Розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things

У кожної системи є своя власна структура, або інакше кажучи, дизайн, що визначає, як взаємодіють всі її складові. Система Інтернету речей не є винятком. Після аналізу джерел було прийнято рішення зобразити взаємозв'язок компонентів системи IoT з аспектами безпеки. Цю залежність можна побачити на рисунку 4.

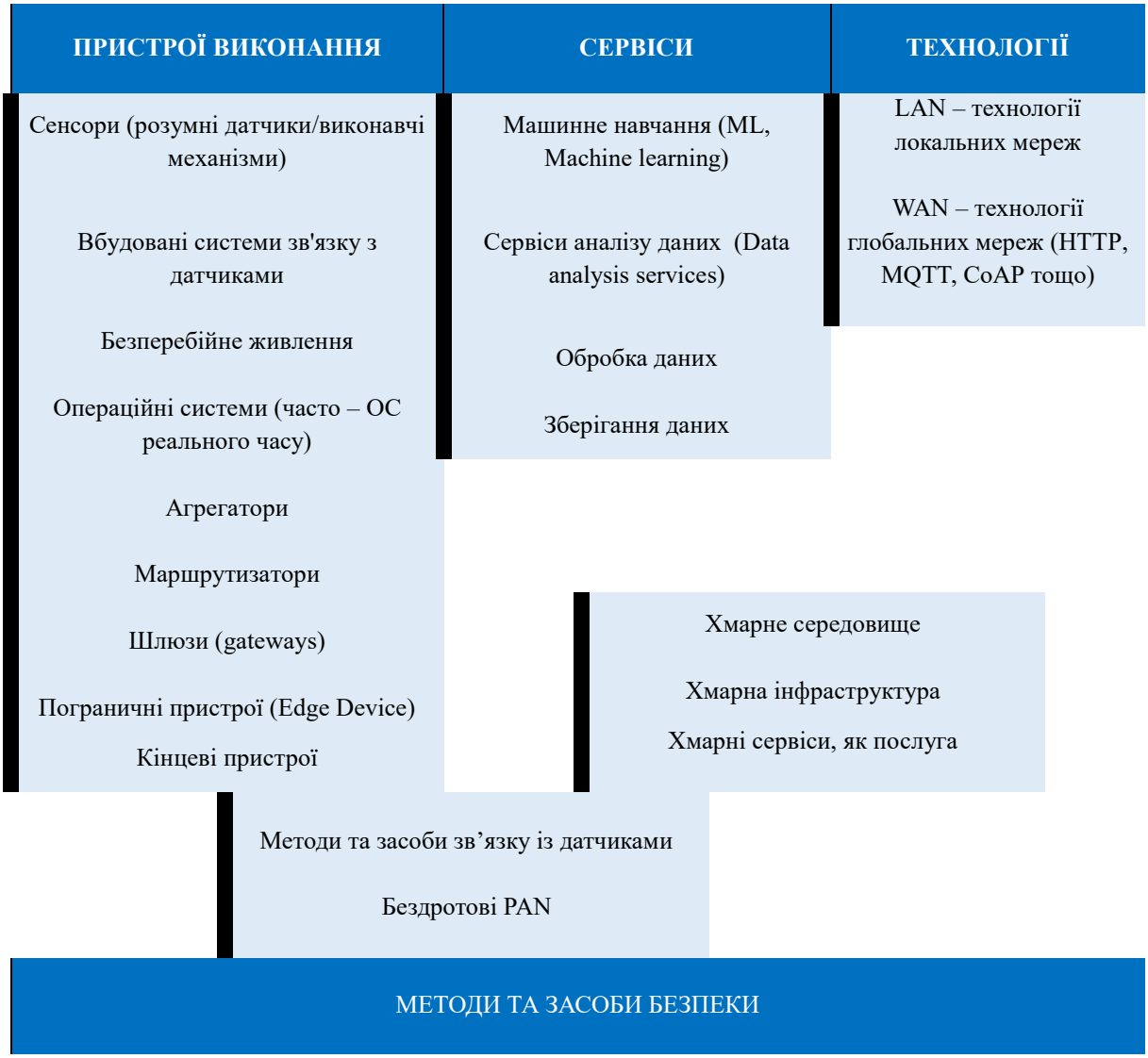

Рисунок 4 – Безпековий технологічний дизайн системи Internet Of Things

Нині цифрові технології проникають у всі сфери життя, запити до безперебійної роботи програмних чи апаратних продуктів стають все актуальнішими. Несанкціоноване втручання на різних рівнях таких

систем може завдати збитків. Тому під час розробки будь-якого програмного чи апаратного продукту, включно з цільовою системою Інтернету речей, забезпечення безпеки стає надзвичайно важливим [11].

На рисунку 5 зображено відповідність рівнів стеку системи IoT і проблем безпеки, притаманних цим рівням.

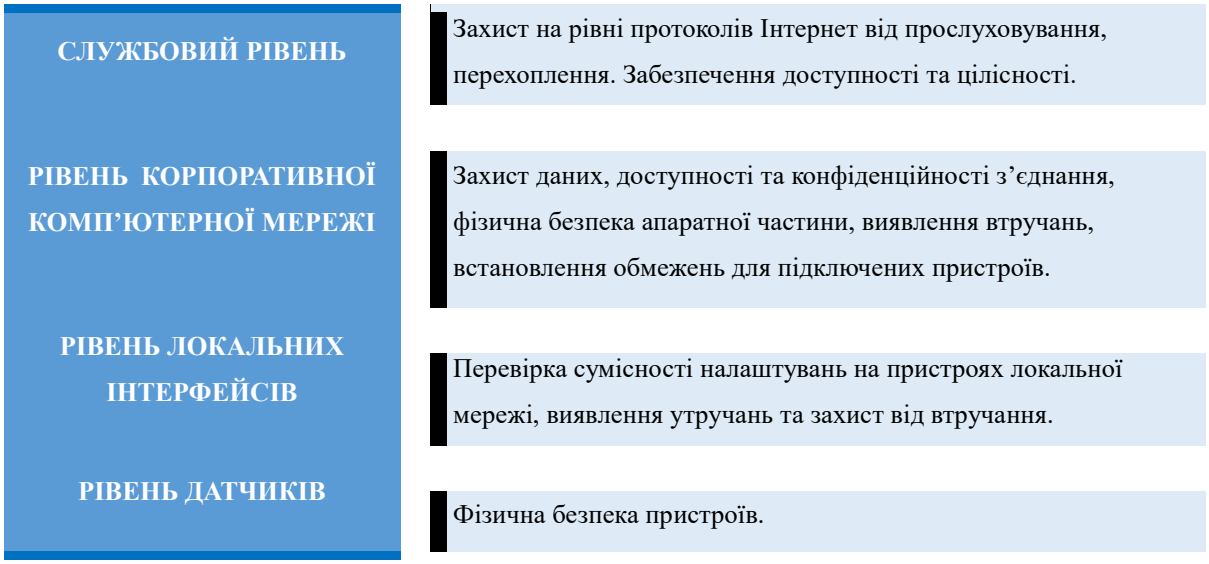

Рисунок 5 – Розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things

З урахуванням зростаючої мобільності, сучасна архітектура системи повинна бути високою у рівні адаптабельності для ефективної обробки різноманітних динамічних взаємодій на всіх рівнях її структури. Надання більш високого рівня абстракції, який може приховати деякі деталі реалізації, є безперечною перевагою стандартних архітектурних рішень і моделей.

Такий безпековий технологічний дизайн системи IoT є інтегрованою системою і гарантує надійну роботу своїх компонентів та забезпечує зв'язок між фізичними та віртуальними складовими.

Для створення цілісної системи обов'язково важливим є докладний підхід до проектування, з особливою увагою до процедур відновлення системи після виникнення неполадок. Враховуючи, що створення безпечного середовища має велике значення, важливо враховувати масштабність системи.

Модель безпечного дизайну системи Internet Of Things урахуванням 4-рівневого дизайну системи Internet Of Things

Якщо враховувати використання відкритих стандартів, тоді запропонуємо вирішення питань безпеки на різних рівнях технологічного дизайну системи Internet Of Things. З метою підвищення загальної захищеності системи IoT, кожен рівень стеку використовує різні протоколи, послуги та механізми безпеки. Отже, кожен рівень прагне досягти важливих цілей, включаючи забезпечення безпеки інформації, фізичної безпеки та стійкого функціонування системи управління безпекою, як окремо, так і в цілому. Розподілимо рівні технологічного дизайну системи Internet Of Things відповідно їх функціональним елементам та розпишемо кожен згідно архітектури IoT та з погляду безпеки та аналізу літературних джерел у вигляді таблиці 2.

У таблиці 2 наведені складові та задачі для окремого рівня моделі безпечного дизайну системи Internet Of Things із відображенням атак та вимоги безпеки, які необхідні для кожного з них. Подана таблиця 2.1 ілюструє перелік методів для вирішення проблем безпеки під час безпечного дизайну системи Internet Of Things [16-18].

Для того, щоб продемонструвати вимоги до безпеки в дизайні Internet Of Things на прикладі, використаємо запропонований розширений технологічний дизайн системи IoT, яка складається з рівнів: датчиків, локальних інтерфейсів, корпоративної комп’ютерної мережі та службового. Кожен з них має забезпечити сприяння чіткому процесу управління безпекою корпоративної комп’ютерної мережі, це забезпеченню контролю доступу, автентифікації та цілісності даних, також їх конфіденційності і наявності інструментів для захисту системи IOT від вірусів та атак.

Тож створювана модель безпечного дизайну системи Internet Of Things повинна мати можливість відстежувати кожен пристрій корпоративної комп’ютерної мережі, контролювати трафік та бути спроможною захистити або тимчасово обмежити використання пристрій/-оїв аби значно зменшити (в

ідеалі – унеможливити, пом’якшити) критичні наслідки для цілої екосистеми корпоративної комп’ютерної мережі, що містить IoT. Тепер коротко розглянемо запропонований розширений технологічний дизайн системи IoT.

Таблиця 2 – Модель безпечного дизайну системи Internet Of Things

SI	TCP/IP	ДИЗАЙН IOT	ОБ’ЄКТ ЗАХИСТУ (ПРОТОКОЛ, ТЕХНОЛОГІЯ, ТОЩО)	МЕТОД ЗАХИСТУ	ОПИС
7	Додатків	СЛУЖБОВИЙ РІВЕНЬ	DHCP, SSH, CoAP, AMQP, XMPP, masquerad	DHCP snooping, RSA, ACL, IPS, брандмауер, шифрування,	Хмарні послуги, сервіси аналізу даних, машинне навчання, зв’язок з пристроями (частково), безпека додатків
6					
5					
4	Транспортний	РІВЕНЬ КОРПОРАТИВНОЇ КОМП’ЮТЕРНОЇ МЕРЕЖІ	DDoS, DoS, IPv4, IPv6, MQTT та DDS, TLS / SSL, MITM, TCP, UDP	SYN protection, 6LowPAN,	Зв’язок з пристроями, провідні та безпровідні мережі, протоколи передавання даних (частково), корпоративні мережні пристрої (частково)
3	Інтернету				
2	Мережевого доступу	РІВЕНЬ ЛОКАЛЬНИХ ІНТЕРФЕЙСІВ	MAC, MIM, DNS, ARP, Адресні spoofing, STP, RFID, WSN, PKI, VLAN	PortSecurity, DAI, BPDU Guard IPSG, PortFast	Мережні пристрої (частково), протоколи передавання даних (частково), міжплатформне ПЗ
1		РІВЕНЬ ДАТЧИКІВ	selfish загроза, фізична безпека, порушення цілісності даних, зловмисне ПЗ	IPsec, IEEE 802.11 AH	Датчики, безперебійне живлення, ОС реального часу, безпека, GPS, Bluetooth

Безпека на рівні датчиків

Даний рівень розширений технологічний дизайн системи IoT можна охарактеризувати як сполучення трьох ланок, які забезпечують дані від: пристроїв збору інформації; місця розташування (функціонування) пристрою; безпосередньо від людей.

Для повноцінної реалізації функцій безпеки необхідно передбачене виробником виконання елементів безпеки в пристроях, тобто можливість аутентифікації, шифрування даних та обмеження в локальному збереженні зібраної інформації. Зі сторони корпоративної комп’ютерної мережі та персоналу, що їх конфігурує – врахування особливостей роботи підприємства.

Складними питаннями безпеки на рівні датчиків технологічного дизайну системи IoT є:

1. Фізична безпека та захист пристроїв збору даних. Найкраще – це коли передбачено ускладнений або неможливий доступ до пристрою.
2. Недостатня модернізація апаратної частини та програмної складової, що обслуговує пристрій (наприклад, версії ОС або прошивка). Часто в пристроях (іноді адміністратори роблять це навмисно) немає передбаченої можливості для їх оновлення чи переналаштування. Нові вразливості можуть виникати постійно, тож якщо пристрій не буде мати доступу для оновлення своїх налаштувань, це може послабити безпеку системи.

Безпека на рівні локальних інтерфейсів

Цей рівень є посередником між IoT системою в місцях розташування датчиків і мережевими службами, додатками. Він надає підтвердження того що взаємодія між додатками і системою є легітимною. Потенційними проблемами на цьому рівні є:

1. Необхідність однотипних (часто – подібних) налаштувань конфігурації на всіх пристроях для досягнення сумісності з точки зору конфігурації.
2. Забезпечення безпеки зібраних даних на цьому рівні технологічного дизайну системи IoT.

3. Створення ефективних програмно-апаратних рішень безпеки задля оптимізації процесу взаємодії з легальними користувачами і зловмисниками.

Рекомендаціями для вирішення проблем безпеки даного рівня є дотримання конфіденційності, цілісності та доступності, регулярне оновлення ПЗ, аутентифікація та авторизація користувачів та адміністратора.

Безпека на рівні корпоративної комп'ютерної мережі

Мережевий рівень є надважливою частиною розширеного технологічного дизайну системи IoT, оскільки є каналом передавання даних між іншими рівнями. Зважаючи на те, що екосистема IOT складається з великої кількості побічних гібридних систем, фактор проблеми масштабованості корпоративної комп'ютерної мережі, її складності та безпеки передавання даних є значним.

Серед проблем, які виникають тут можуть бути:

1. Забезпечення класичних вимог інформаційної безпеки –конфіденційності, цілісності та доступності.
2. Фізична безпека (якщо пристрої які забезпечують передавання даних можуть бути у вільному доступі).
3. Надмірна кількість підключень до корпоративної комп'ютерної мережі, що створює додаткові складнощі в обслуговуванні, надмірні витрати мережевих ресурсів (як програмного, так і апаратного гатунку) та збільшення вразливостей внаслідок ймовірного зловмисного впливу.
4. Можливість запобіганню зловмисного роду атак, на зразок «Man-In-The-Middle» для перехоплення інформації, що передається між об'єктами корпоративної комп'ютерної мережі.

Основними викликами до безпеки на рівні корпоративної комп'ютерної мережі в розумінні розширеного технологічного дизайну системи IoT є мінімізація можливості впливу зловмисників на екосистему та збільшення ефективності її роботи та, водночас, покращення якості обслуговування (Qos).

Безпека на службовому рівні

Службовий рівень розширеного технологічного дизайну системи IoT забезпечує ефективну взаємодію використання апаратних та програмних ресурсів і можливість повторного використання цих ресурсів. На службовому рівні відбувається аналіз отриманих даних від рівня датчиків, тож тут присутні служби обробки подій, служби інтеграції і аналітики тощо, які дозволяють обмін інформацією між сервісами та додатками, а також забезпечують виконання необхідних дій.

Виклики, які притаманні службовому рівню:

1. Забезпечення конфіденційності, цілісності та доступності.
2. Можливість недобросовісних маніпуляцій даними від служб та додатків службового рівня.
3. Створення захисту від різноманітних атак (на кшталт DoS та DDoS-атак).
4. Забезпечення аналізу трафіку для алміністраторів і обмеження для неавторизованих користувачів задля недопущення жодних маніпуляцій з даними.

Класичним підходом до вирішення і убезпечення від проблем на службовому рівні є відповідність стандартам та протоколам під час проектування та впровадженні дизайну системи IoT.

Висновки

У даній роботі досягнуто підвищення безпеки та захисту пристроїв Internet Of Things всередині корпоративної комп'ютерної мережі від несанкціонованого доступу за допомогою вдосконаленого технологічного дизайну системи IoT. В результаті аналітичного дослідження вдалося проаналізувати архітектуру і ключові компоненти екосистеми Internet Of Things та особливості роботи технології IoT з точки зору взаємодії, обробки даних та розподілу інформації в системах IoT і виконати грунтовний аналіз загроз інформаційній безпеці IoT. Внаслідок вдалося спроектувати 4-рівневий технологічний дизайн системи Internet Of Things із урахуванням запропонованого рівня інтерфейсів, що надає подібність до принципів побудови сервіс-орієнтованої архітектури.

Запропоновано розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things та вмонтовано цю ідею в модель безпечного дизайну системи Internet Of Things урахуванням 4-рівневого дизайну системи Internet Of Things. В результаті спроектовано модель корпоративної комп'ютерної мережі в програмному середовищі Packet Tracer з захистом у відповідності до запропонованого технологічного дизайну системи IoT.

Зокрема, результат полягає у такому:

1. Вдосконалена відома трирівнева модель системи Internet Of Things за рахунок приведення її до архітектури IoT від CISCO, що надає новій архітектурі подібність до принципів побудови сервіс-орієнтованої архітектури (SOA);
2. Запропоновано розширений технологічний дизайн системи IoT, що містить такі рівні:

датчиків, локальних інтерфейсів, корпоративної комп’ютерної мережі та службовий і це дає можливість поглибити безпекові аспекти в контексті IoT;

3. Розширено методологічну базу методів та засобів захисту IoT в межах корпоративної комп’ютерної мережі за рахунок приведення технологічного дизайну системи Internet Of Things до відомих стандартів;
4. Розширено методологічну базу методів та засобів захисту IoT в межах корпоративної комп’ютерної мережі за рахунок розподілу загроз безпеці по рівням технологічного дизайну системи IoT;
5. Запропоновано вдосконалену модель безпечного дизайну системи Internet Of Things.

Список літератури

[1] Сайт компанії IBM [Електронний ресурс] – Режим доступу: https://www.ibm.com/cloud/internet-of-things?mhsrc=ibmsearch_a&mhq=iot
[2] Сайт компанії Intel [Електронний ресурс] – Режим доступу: https://www.intel.com/content/www/us/en/internet-of-things/overview.html
[3] Сайт компанії Google [Електронний ресурс] – Режим доступу: https://cloud.google.com/iot-core
[4] Сайт компанії Cisco [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html
[5] Сайт компанії Microsoft [Електронний ресурс] – Режим доступу: https://azure.microsoft.com/en-us/services/iot-central/
[6] Сайт компанії Amazon [Електронний ресурс] – Режим доступу: https://aws.amazon.com/iot-core/
[7] Сайт компанії Siemens [Електронний ресурс] – Режим доступу: https://new.siemens.com/global/en/products/automation/topic-areas/industrial-iot.html
[8] Цифрова трансформація бізнесу / Інтернет речей [Електронний ресурс] – Режим доступу: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iotXXX
[9] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року, (GDPR) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text
[10] Introduction to IoT. [Електронний ресурс] – Режим доступу: https://lms.netacad.com/course/view.php?id=744659.
[11] Б. Ю. Жураковський, І.О. Зенів; *Технології інтернету речей. Навчальний посібник*, Київ: КПІ ім. Ігоря Сікорського, 2021.
[12] Т. І. Коробейнікова, С. М. Захарченко. *Комп'ютерні мережі: навчальний посібник*, Львів: Видавництво Львівської політехніки (НУЛП), 2022.
[13] Т. І. Коробейнікова, С. М. Захарченко, *Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник* , Львів: Видавництво Львівської політехніки (НУЛП), 2021.
[14] Інтернет речей: мережева архітектура та архітектура безпеки [Електронний ресурс] – Режим доступу: https://www.bizmaster.xyz/2020/12/internet-rechei-merezheva-arkhitektura-ta-arkhitektura-bezpeky.html.
[15] Д. С. Литвиненко, *Модель безпеки інформаційної системи на базі технологій IoT :* пояснювальна записка до кваліфікаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 123 Комп’ютерна інженерія , Харків. нац. ун-т радіоелектроніки. – Харків, 2021.
[16] Т. І. Коробейнікова, Т. В. Іськович, “Організація архітектури системи IoT в протокольному стекові”, *International scientific journal «Grail of Science»*, № 27, С. 341–346. 2023. https://doi.org/10.36074/grail-of-science.12.05.2023.053
[17] Т.І. Коробейнікова, Т. В. Іськович, “Безпековий технологічний стек IoT”, *International periodical scientific journal «SWorldJournal»*, № 19 (part 1), С. 24–32. 2023. DOI: 10.30888/2663-5712.2023-19-01-020.
[18] Jing, Qi & Vasilakos, Athanasios & Wan, Jiafu & Lu, Jingwei & Qiu, Dechao. (2014). *Security of the Internet of Things: Perspectives and challenges. Wireless Networks* DOI:. 20. 2481-2501. 10.1007/s11276-014-0761-7.
[19] С.М. Захарченко, Т. І. Трояновська, О.В. Бойко, *Побудова захищених мереж на базі обладнання компанії Cisco*, Вінниця : ВНТУ, 2017.
[20] Савицька Л.А., Коробейнікова Т.І. “Удосконалений метод розробки API підвищеної швидкодії”, *Інформаційні технології та комп`ютерна інженерія*,- №1 (50), С. 31–35. 2021.
[21] Л. А. Савицька, Н. В. Добровольська, В. О. Кондратюк, “Програмний модуль попереднього діагностування пацієнтів на основі нейронної мережі Кохонена”, *Інформаційні технології та комп`ютерна інженері,* № 1. – С. 66-74. 2023.

Стаття надійшла: 04.03.2024.

References

[1] IBM website [Online]. Available: https://www.ibm.com/cloud/internet-of-things?mhsrc=ibmsearch_a&mhq=iot

[2] Website Intel [Online]. Available: https://www.intel.com/content/www/us/en/internet-of-things/overview.html

[3] Website Google [Online]. Available: https://cloud.google.com/iot-core

[4] Website Cisco [Online]. Available: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html

[5] Website Microsoft [Online]. Available: https://azure.microsoft.com/en-us/services/iot-central/

[6] Website Amazon [Online]. Available: https://aws.amazon.com/iot-core/

[7] Website Siemens [Online]. Available: https://new.siemens.com/global/en/products/automation/topic-areas/industrial-iot.html

[8] Tsyfrova transformatsiya biznesu / Internet rechey [Online]. Available:: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iotKHKHKH

[9] Rehlament Yevropeys′koho Parlamentu i Rady (YES) 2016/679 vid 27 kvitnya 2016 roku, (GDPR) [Online]. Available: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

[10] Introduction to IoT. [Online]. Available: https://lms.netacad.com/course/view.php?id=744659.

[11] B. YU. Zhurakovs′kyy, I.O. Zeniv; *Tekhnolohiï internetu recheў. Navchal'nyy posibnyk*, Kyïv: KPI im. Ihorya Sikors′koho, 2021.

[12] T. I. Korobeinikova, S. M. Zakharchenko. *Komp'yuterni merezhi: navchal'nyy posibnyk*, L′viv: Vydavnytstvo L′vivs′koï politekhniky (NULP), 2022.

[13] T. I. Korobeinikova, S. M. Zakharchenko, *Tekhnolohiï zakhystu lokal'nykh merezh na osnovi obladnannya CISCO : navch. posibnyk* , L′viv: Vydavnytstvo L′vivs′koï politekhniky (NULP), 2021.

[14] Internet rechey: merezheva arkhitektura ta arkhitektura [Online]. Available: https://www.bizmaster.xyz/2020/12/internet-rechei-merezheva-arkhitektura-ta-arkhitektura-bezpeky.html.

[15] D. S. Lytvynenko Model′ bezpeky informatsiynoyi systemy na bazi tekhnolohiy IoT : poyasnyuval′na zapyska do kvalifikatsiynoyi roboty zdobuvacha vyshchoyi osvity na druhomu (mahisters′komu) rivni, spetsial′nist′ 123 Komp″yuterna inzheneriya , Kharkiv. nats. un-t radioelektroniky. – Kharkiv, 2021.

[16] T. I. Korobeynikova, T. V. Iskovych, “Orhanizatsiya arkhitektury systemy IoT v protokol′nomu stekovi”, *International scientific journal «Grail of Science»,* № 27, S. 341–346. 2023. https://doi.org/10.36074/grail-of-science.12.05.2023.053

[17] Korobeynikova T.I., Iskovych T. V., “Bezpekovyy tekhnolohichnyy stek IoT”, *International periodical scientific journal «SWorldJournal»*, № 19 (part 1), S. 24–32. 2023. DOI: 10.30888/2663-5712.2023-19-01-020.

[18] Jing, Qi & Vasilakos, Athanasios & Wan, Jiafu & Lu, Jingwei & Qiu, DechaoSecurity of the Internet of Things: Perspectives and challenges. *Wireless Networks* DOI:. 20. 2481-2501. 10.1007/s11276-014-0761-7. . 2014.

[19] Zakharchenko S.M., Troyanovs′ka T. I., Boyko O.V. *Pobudova zakhyshchenykh merezh na bazi obladnannya kompaniyi Cisco*, Vinnytsya : VNTU, 2017.

[20] L.A. Savytska, T.I. Korobeynikova “Udoskonalenyy metod rozrobky ARI pidvyshchenoyi shvydkodiyi”, *Informatsiyni tekhnolohiyi ta komp`yuterna inzheneriya*,- №1 (50), S. 31–35. 2021.

[21] L. A. Savytska, N. V. Dobrovolska, V. O. Kondratyuk, “Prohramnyy modul′ poperedn′oho diahnostuvannya patsiyentiv na osnovi neyronnoyi merezhi Kokhonena”, *Informatsiyni tekhnolohiyi ta komp`yuterna inzheneri*, № 1. – S. 66-74. 2023.

Відомості про авторів

Савицька Людмила Анатоліївна, к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Savytska Liudmyla, PhD, associate professor of computing engineering department, Vinnytsya national technical university

Коробейнікова Тетяна Іванівна, к.т.н., доцент кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Korobeinikova Tetiana, PhD, associate professor of information technology security department, National university “Lvivska Politechnika”

Костюк Олег Віталійович, магістр кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Kostiuk Oleh Vitaliyovych, magister of computing engineering department, Vinnytsya national technical university, department of the computer engineering

Колесник Ірина Сергіївна, к.т.н. доцент, доцент кафедри обчислювальної техніки

Kolesnyk Iryna Sergiivna, PhD candidate of engineering sciences, associate professor of department of the computing engineering, Vinnytsya national technical university

Дудник Олександр Вікторович, к.т.н., ст. викладач кафедри обчислювальної техніки

Dudnyk Oleksandr Viktorovich, PhD, senior lecturer of department of the computing engineering, Vinnytsya national technical university

L. Savytska[1], T. Korobeinikova[2], O. Kostiuk[1], I. Kolesnyk[1], O. Dudnyk [1]

INTERNET OF THINGS PROTECTION MEANS IN THE CORPORATE COMPUTER NETWORK

[1]Vinnytsya national technical university, Vinnytsya

[2]National university “Lvivska Politechnika”