Державний торговельно-економічний університет
Кафедра інженерії програмного забезпечення та кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Модель захисту пристроїв IoT від кібератак»

Студента 2 курсу, 8м групи, спеціальності 125 «Кібербепека та захист інформації», освітня програма «Безпека систем електронних комунікацій в економіці»

_____
підпис студента

Литвинюка Антона Віталійовича

Науковий керівник
кандидат технічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки

_____
підпис керівника

Звєрєв Володимир Павлович

Гарант освітньої програми
кандидат технічних наук, професор кафедри інженерії програмного забезпечення та кібербезпеки

_____
підпис гаранта

Хохлачова Юлія Євгеніївна

КИЇВ – 2024

Державний торговельно-економічний університет

Факультет інформаційних технологій
Кафедра інженерії програмного забезпечення та кібербезпеки
Освітній ступінь магістр
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Безпека системи електронних комунікацій в електроніці»

Затверджую
Зав. кафедри інженерії програмного забезпечення та кібербезпеки
Криворучко О. В.
«13» грудня 2023 р.

Завдання
на випускну кваліфікаційну роботу студентові
Литвинюку Антону Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи «Модель захисту пристроїв IoT від кібератак».

Затверджена наказом ректора від «27» листопада 2023 р. № 4194

2. Строк здачі студентом закінченої роботи 15 листопада 2024 р.

3. Цільова установка та вихідні дані до роботи

Мета роботи − полягає в розробці моделі захисту пристроїв Інтернету речей від кібератак, яка враховує різноманітність загроз, що стикаються з пристроями IoT, у змінному і динамічному кіберсередовищі, та забезпечує надійний захист від потенційних атак, включаючи методи захисту, такі як шифрування даних, аутентифікація, моніторинг безпеки.

Об'єкт дослідження – процес розробки та впровадження моделі захисту пристроїв Інтернету речей від кібератак, що включає аналіз загроз, визначення вимог до безпеки, розробку архітектури захисту, реалізацію заходів безпеки та тестування ефективності.

Предмет дослідження – підходи, методи та технології захисту пристроїв Інтернету речей від кібератак, оскільки їхнє використання має на меті

забезпечення надійності та безпеки цих пристроїв у зростаючому середовищі кіберзагроз та кібератак.

4. Консультанти роботи із зазначенням розділів, які консультують:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видав	Завдання прийняв

5. Зміст випускної кваліфікаційної роботи (перелік питань за кожним розділом)

ВСТУП

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

1.1. Проблеми безпеки Інтернету речей

1.2. Загрози безпеці систем Інтернету речей

1.3. Сучасні методи та технології захисту IoT пристроїв

1.4. Висновок до розділу 1

РОЗДІЛ 2. РОЗРОБКА МОДЕЛІ ЗАХИСТУ ПРИСТРОЇВ IOT

2.1. Визначення вимог до моделі захисту

2.2. Проектування архітектури моделі захисту

2.3. Розробка алгоритмів та методів захисту

2.4. Моделі безпеки Інтернету речей

2.5. Реалізація та інтеграція моделі захисту

2.6. Висновок до розділу 2

РОЗДІЛ 3. ТЕСТУВАННЯ МОДЕЛІ ТА ОЦІНКА ЕФЕКТИВНОСТІ МОДЕЛІ ЗАХИСТУ

3.1. Вимірювання показників ефективності (наприклад, швидкість реакції, чутливість до атак)

3.2. Аналіз отриманих даних та порівняння з попередніми дослідженнями

3.3. Оцінка надійності та стійкості моделі до різних типів кібератак

3.4. Висновок до розділу 3

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ДОДАТКИ

6. Календарний план виконання випускної кваліфікаційної роботи

№ пор.	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів випускної кваліфікаційної роботи	
		за планом	фактично
1	2	3	4
1.	*Вибір теми випускної кваліфікаційної роботи*	*06.11.2023*	*06.11.2023*
2.	*Розробка та затвердження завдання на роботу магістра*	*16.11.2023*	*16.11.2023*
3.	*Вступ та перелік літературних джерел*	*26.02.2024*	*26.02.2024*
4.	*Розробка технічного завдання*	*18.03.2024*	*18.03.2024*
5.	*Розділ 1. Теоретичні аспекти кібербезпеки пристроїв інтернету речей (іот)*	*15.04.2024*	*15.04.2024*
6.	*Розділ 2. Розробка моделі захисту пристроїв IoT*	*27.05.2024*	*27.05.2024*
7.	*Розділ 3. Тестування моделі та оцінка ефективності моделі захисту*	*24.06.2024*	*24.06.2024*
8.	*Розробка моделі захисту пристроїв IoT*	*17.10.2024*	*17.10.2024*
9.	*Написання наукової статті*	*20.05.2024*	*20.05.2024*
10.	*Висновки та пропозиції*	*23.10.2024*	*23.10.2024*
11.	*Здача випускної кваліфікаційної роботи на кафедру (перша перевірка)*	*01.11.2024*	*01.11.2024*
12.	*Підготовка автореферату та презентації доповіді*	*04.11.2024*	*04.11.2024*
13.	*Попередній захист випускної кваліфікаційної роботи*	*11.11.2024 – 15.11.2024*	*12.11.2024*
14.	*Здача зброшурованої випускної кваліфікаційної роботи*	*15.11.2024*	*15.11.2024*
15.	*Зовнішнє рецензування випускної кваліфікаційної роботи*	*15.11.2024*	*15.11.2024*
16.	*Підготовка до публічного захисту випускної кваліфікаційної роботи*	*за розкладом роботи ЕК*	*за розкладом роботи ЕК*

7. Дата видачі завдання «16» листопада 2023 р.

8. Науковий керівник випускної кваліфікаційної роботи Звєрєв В.П.
(прізвище, ініціали, підпис)

9. Гарант освітньої програми Хохлачова Ю.Є.
(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент Литвинюк А.В.
(прізвище, ініціали, підпис)

11. Відгук керівника випускної кваліфікаційної роботи

Науковий керівник випускної кваліфікаційної роботи
Звєрєв В.П.
(підпис, дата)

Відмітка про попередній захист Звєрєв В.П.
(ПІБ, підпис, дата)

12. Висновок про випускну кваліфікаційну роботу

Випускна кваліфікаційна робота студента Литвинюка А.В.
(прізвище, ініціали)
може бути допущена до захисту в екзаменаційній комісії.

Гарант освітньої програми Хохлачова Ю.Є.
(прізвище, ініціали, підпис)

Завідувач кафедри Криворучко О. В.
(підпис, прізвище, ініціали)

«_____»_____2024 р.

АНОТАЦІЯ

Відповідно до мети дослідження, робота присвячена розробці моделі захисту пристроїв Інтернету Речей (IoT) від кібератак. Недоліки в захисті пристроїв IoT можуть призвести до серйозних наслідків, включаючи порушення приватності, втрату конфіденційності даних та вразливість інфраструктури. Отже, метою цієї роботи є створення ефективної та надійної моделі захисту, яка забезпечить безпеку та захист від потенційних кібератак на пристрої IoT. Дослідження включає в себе аналіз загроз та вразливостей, розробку архітектури моделі захисту, розробку алгоритмів та методів захисту, а також тестування та оцінку ефективності розробленої моделі. Результатом цієї роботи буде вдосконалена модель захисту, яка забезпечить надійність та безпеку пристроїв IoT у сучасному цифровому середовищі.

Ключові слова: Інтернет речей, кібербезпека, захист, кібератаки, вразливості, модель захисту, пристрої IoT.

ABSTRACT

According to the research purpose, the work is dedicated to developing a model for protecting Internet of Things (IoT) devices from cyberattacks. Weaknesses in IoT device protection can lead to serious consequences, including privacy breaches, loss of data confidentiality, and infrastructure vulnerability. Therefore, the aim of this work is to create an effective and reliable protection model that ensures security and defense against potential cyberattacks on IoT devices. The research includes threat and vulnerability analysis, development of the protection model architecture, design of protection algorithms and methods, as well as testing and evaluation of the effectiveness of the developed model. The outcome of this work will be an enhanced protection model that ensures the reliability and security of IoT devices in the modern digital environment.

Keywords: Internet of Things, cybersecurity, protection, cyberattacks, vulnerabilities, protection model, IoT devices.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

IoT – інтернет речей (Internet of Things)

NN – нейронна мережа (Neural Network)

ML – машинне навчання (Machine Learning)

Edge Devices – крайові пристрої

Threats – загрози

IoT Devices – пристрої Інтернету речей

ML Models – моделі машинного навчання

Integrity – цілісність

Availability – доступність

Authentication – аутентифікація

Encryption – шифрування

Attack Detection – виявлення атак

Attack Prevention – запобігання атакам

Vulnerabilities – вразливості

DDoS – Distributed Denial of Service

AES – Advanced Encryption Standard

TLS – Transport Layer Security

CPU – Central Processing Unit

RAM – Random Access Memory

API – Application Programming Interface

ЗМІСТ

ВСТУП **11**

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ (IOT) **13**

1.1. Проблеми безпеки Інтернету речей **13**

1.2. Загрози безпеці систем Інтернету речей 15

1.3. Сучасні методи та технології захисту IoT пристроїв 18

1.4. Висновки до розділу 1 19

РОЗДІЛ 2 РОЗРОБКА МОДЕЛІ ЗАХИСТУ ПРИСТРОЇВ IOT **21**

2.1. Визначення вимог до моделі захисту 21

2.2. Проектування архітектури моделі захисту 22

2.3. Розробка алгоритмів та методів захисту 33

2.4. Моделі безпеки Інтернету речей 35

2.5. Реалізація та інтеграція моделі захисту 42

2.6. Висновки до розділу 2 45

РОЗДІЛ 3 ТЕСТУВАННЯ МОДЕЛІ ТА ОЦІНКА ЕФЕКТИВНОСТІ МОДЕЛІ ЗАХИСТУ **46**

3.1. Вимірювання показників ефективності (наприклад, швидкість реакції, чутливість до атак) 46

3.2. Аналіз отриманих даних та порівняння з попередніми дослідженнями 49

3.3. Оцінка надійності та стійкості моделі до різних типів кібератак 51

3.4. Висновок до розділу 3 52

ВИСНОВКИ ТА ПРОПОЗИЦІЇ **54**

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ **55**

ДОДАТКИ **56**

ВСТУП

Актуальність полягає в необхідності дослідження та розробці моделі захисту пристроїв Інтернету речей (IoT) від кібератак у зв'язку зі стрімким поширенням IoT-технологій, що викликає збільшення кількості потенційних точок атак, та наявністю загроз, які представляють кібератаки, загрози, що включають в себе різноманітні вектори нападу та методи, здатні серйозно підірвати безпеку та приватність користувачів, а також заподіяти значні матеріальні збитки внаслідок недостатнього захисту пристроїв IoT.

Мета дослідження: полягає в розробці моделі захисту пристроїв Інтернету речей від кібератак, яка враховує різноманітність загроз, що стикаються з пристроями IoT, у змінному і динамічному кіберсередовищі, та забезпечує надійний захист від потенційних атак, включаючи методи захисту, такі як шифрування даних, аутентифікація, моніторинг безпеки та та розробка ефективних алгоритмів та стратегій для виявлення та запобігання кіберзагрозам, щоб забезпечити стійкість та безпеку функціонування пристроїв Інтернету речей та їхніх мереж в довгостроковій перспективі.

Об'єкт дослідження: процес розробки та впровадження моделі захисту пристроїв Інтернету речей від кібератак, що включає аналіз загроз, визначення вимог до безпеки, розробку архітектури захисту, реалізацію заходів безпеки та тестування ефективності.

Предмет дослідження: підходи, методи та технології захисту пристроїв Інтернету речей від кібератак, оскільки їхнє використання має на меті забезпечення надійності та безпеки цих пристроїв у зростаючому середовищі кіберзагроз та кібератак.

У відповідності з метою дослідження поставлені наступні **завдання**:

- Провести аналіз сучасного стану в галузі кібербезпеки пристроїв IoT.
- Вивчити типові загрози та вразливості, що стосуються пристроїв IoT.
- Розробити модель захисту, що враховує особливості пристроїв IoT та їхнє використання.
- Реалізувати та протестувати запропоновану модель захисту на практиці.
- Оцінити ефективність та надійність розробленої моделі захисту.

Методи дослідження: аналіз та класифікація загроз, виявлення вразливостей та аналізу можливих загроз, розробка та моделювання безпекових механізмів, проведення тестування, а також статистичний аналіз результатів.

Наукова новизна дослідження полягає у створенні комплексної моделі захисту пристроїв Інтернету речей, яка поєднує в собі інноваційні підходи до виявлення, аналізу та запобігання кібератак, а також впровадження передових технологій кібербезпеки з урахуванням специфіки IoT-систем.

Практичне значення дослідження: проявляється у можливості практичного застосування розробленої моделі захисту пристроїв Інтернету речей в реальних умовах функціонування, що сприятиме підвищенню рівня кібербезпеки в системах IoT. Це сприятиме зменшенню ризику кібератак, що можуть тягнути за собою негативні наслідки, та гарантуватиме безпеку користувачів та конфіденційність їхніх особистих даних. Результати дослідження можуть бути використані для розробки та вдосконалення заходів кібербезпеки для пристроїв Інтернету речей. Це дозволить підвищити рівень захисту від кібератак, зменшити ризики вразливостей та забезпечити безпеку користувачів та їхніх персональних даних у сфері IoT. Реалізація розроблених методів і моделей може мати значний позитивний вплив на ефективність та стабільність інфраструктури Інтернету речей.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ КІБЕРБЕЗПЕКИ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

1.1. Проблеми безпеки Інтернету речей

Інтернет речей (IoT) визнається важливою складовою сучасних комп'ютеризованих систем у різних сферах діяльності. Ця концепція передбачає створення комп'ютерної мережі фізичних об'єктів, які обладнані вбудованими технологіями для взаємодії між собою або з зовнішнім середовищем, відображаючи організацію таких мереж як явище, здатне впливати на економічні та соціальні процеси, що вимагають меншої участі людини у виконанні дій та операцій. У цілому, технології IoT орієнтовані на збір, обмін та обробку даних з метою динамічної адаптації до конкретного контексту, що змінює бізнес-середовище та спосіб життя загалом [1-2].

Модель захисту пристроїв IoT від кібератак є важливою частиною кібератики, яка систематично досліджує кіберсуб’єкти в кіберпросторі, їхні властивості та функції, а також взаємозв'язки з об’єктами у фізичному, соціальному та ментальному середовищах. Кібератика не лише відтворює аспекти людського інтелекту, такі як інтелектуальне відчуття, прийняття рішень та управління, але й інтегрує природні властивості, включаючи динаміку, самоадаптацію та енергозбереження [3-4]. Зростання масштабу та складності систем IoT, поряд із зростаючими загрозами безпеці, обумовлює необхідність розробки моделей і інструментів управління безпекою, що враховують специфіку використання таких систем.

Зі зростанням використання Інтернету речей (IoT) збільшуються і ризики кібератак, спрямованих на різні рівні та компоненти IoT.

Зі зростанням використання Інтернету речей (IoT) збільшуються і ризики кібератак, спрямованих на різні рівні та компоненти IoT. Пристрої IoT є потенційною точкою входу для кіберзловмисників, які прагнуть здійснювати шкідливі дії, такі як прослуховування, викрадення інформації, порушення операційної діяльності та виведення з ладу обладнання. Сучасні рішення для забезпечення безпеки IoT ставлять виробників і операторів у складне становище, оскільки вони зазвичай зосереджені на периферійних аспектах і стримують кібератаки лише після їх ідентифікації (рис. 1.1).

Рис. 1.1. Проблеми безпеки систем IOT

Проблеми організації безпеки IoT розглядаються у численних публікаціях з різних точок зору. Загальні питання безпеки IoT розглядаються в [7, 8]. Безпека IoT з акцентом на вплив нових технологій

представлена у роботі [2]. Формування вимог безпеки до компонентів IoT розглядаються в [1, 4]. Огляд заходів безпеки для IoT представлено в [5]. Окреме місце в дослідженнях із забезпечення безпеки IoT займають роботи, орієнтовані на використання формалізованих знань та онтологій [3–5].

У зв'язку з цим актуальним є розробка моделі захисту пристроїв IoT від кібератак, яка враховує специфіку функціонування таких систем та спрямована на забезпечення їхньої безпеки і надійності.

1.2. Загрози безпеці систем Інтернету речей

Швидке зростання кількості підключених кінцевих точок Інтернету речей (IoT) у різних галузевих сегментах та типах пристроїв сприяло всеохопному підключенню, периферійним обчисленням і доступності надійної хмарної інфраструктури для виконання робочих навантажень додатків на основі даних. Кількість атак на системи IoT зростає пропорційно збільшенню їхнього масштабу та складності (рис. 1.2) [1, 3].

Рис. 1.2. Ризики безпеки систем IoT

Ризики безпеки систем IoT часто пов'язані з:

- Порушенням безпеки транспортних засобів – ризики зламу транспортних засобів можуть відбуватися без відома водія, що призводить до потенційно небезпечних ситуацій на дорозі.
- Втручанням у роботу пристроїв IoT – втручання в їх мікропрограму, що може призвести до втрати або пошкодження даних.

- Крадіжкою даних, спрямована на отримання доступу до фінансової чи особистої інформації.
- Незахищеністю підключення до Інтернету – відсутність стандартів безпеки робить пристрої IoT вразливими до атак, включаючи хакерські втручання.
- Вразливостями мікропрограмного забезпечення IoT з відкритим вихідним кодом, що може бути вразливим до атак.

У зв’язку з цим актуальним є розробка моделі захисту пристроїв IoT від кібератак, яка враховує специфіку функціонування таких систем та спрямована на забезпечення їхньої безпеки і надійності. Сучасні підходи до безпеки IoT включають впровадження стандартизованих методів автентифікації та шифрування, регулярне оновлення мікропрограмного забезпечення, а також постійний моніторинг та аналіз активності для виявлення потенційних загроз [4-5].

На рис. 1.3 представлено приклад класифікації загроз безпеці пристроїв Інтернету речей (IoT). Немає універсального рішення, яке б могло забезпечити повний захист усіх пристроїв IoT від різноманітних загроз, проте існує кілька стратегій, що можуть значно зменшити ризики, пов'язані з використанням цих пристроїв.

Перша стратегія полягає в належному налаштуванні та забезпеченні безпеки всіх IoT-пристроїв. Це передбачає створення та налаштування облікових записів користувачів і паролів, встановлення та налаштування брандмауерів та антивірусного програмного забезпечення, а також регулярне проведення оновлень безпеки.

Друга стратегія полягає у використанні захищених бездротових мереж для підключення IoT-пристроїв до корпоративних або глобальних мереж. Це допомагає захистити системи від атак та забезпечує, щоб конфіденційні дані не передавалися через незахищені мережі.

Рис. 1.3. Класифікація загроз системам IoT

Враховуючи сучасний розвиток технологій, важливо також впроваджувати додаткові заходи безпеки, такі як використання протоколів шифрування для захисту даних, проведення регулярних аудитів безпеки та впровадження механізмів автоматичного виявлення та реагування на загрози. Це допоможе забезпечити більш високий рівень захисту IoT-пристроїв та зменшити ймовірність успішних кібератак. Третя стратегія полягає в постійному моніторингу загроз безпеці IoT-пристроїв та впровадженні відповідних заходів захисту для запобігання можливим атакам [5-7]. Це забезпечує належне налаштування та захист пристроїв від кібератак, а також гарантує збереження конфіденційності особистої інформації користувачів.

Зважаючи на сучасні виклики у сфері кібербезпеки, дана стратегія також включає регулярне оновлення програмного забезпечення, проведення тестування на проникнення та використання передових інструментів для виявлення і аналізу загроз. Інтеграція штучного інтелекту та машинного навчання в системи безпеки дозволяє автоматизувати процеси виявлення аномалій та реагування на них, що значно підвищує ефективність захисту IoT-пристроїв.

1.3. Сучасні методи та технології захисту IoT пристроїв

У зв'язку з швидким розвитком і широким впровадженням Інтернету речей (IoT), питання кібербезпеки стають дедалі актуальнішими. Захист IoT-пристроїв вимагає застосування комплексних підходів і сучасних технологій. Нижче наведено огляд основних методів і технологій, що використовуються для захисту IoT-пристроїв. Одним з ключових методів є шифрування даних, яке забезпечує захист інформації, що передається між IoT-пристроями та центральними системами. Використання протоколів TLS (Transport Layer Security) та SSL (Secure Sockets Layer) дозволяє ефективно запобігти перехопленню та несанкціонованому доступу до даних [2-5].

Аутентифікація та авторизація також відіграють важливу роль у захисті IoT-пристроїв. Використання надійних методів аутентифікації, таких як двофакторна аутентифікація, та протоколів OAuth, Kerberos допомагає запобігти несанкціонованому доступу до пристроїв і забезпечує контроль прав доступу.

Захист на рівні мережі є ще одним важливим аспектом безпеки IoT. Використання брандмауерів, систем виявлення та запобігання вторгненням (IDS/IPS), а також віртуальних приватних мереж (VPN) дозволяє ефективно захистити IoT-пристрої від мережевих атак. Сегментація мережі, тобто розділення її на сегменти з окремими рівнями доступу, зменшує ризик поширення атаки у разі компрометації одного з пристроїв, що дозволяє краще контролювати трафік і забезпечувати вищий рівень безпеки.

Регулярне оновлення програмного забезпечення є критичним для підтримання безпеки IoT-пристроїв. Це включає своєчасне застосування патчів і оновлень для усунення вразливостей, які можуть бути використані зловмисниками. Інтеграція технологій штучного інтелекту (AI) та машинного навчання (ML) в системи кібербезпеки дозволяє автоматично виявляти аномалії та загрози. Штучний інтелект та машинне навчання

можуть аналізувати великі обсяги даних та виявляти підозрілу активність, яка може бути пропущена традиційними методами.

Контроль фізичного доступу до IoT-пристроїв також є важливою складовою загальної стратегії безпеки. Використання механічних замків, систем відеоспостереження та інших методів контролю доступу допомагає запобігти фізичним атакам на пристрої [2, 4, 7]. Апаратні засоби безпеки, такі як TPM (Trusted Platform Module) та HSM (Hardware Security Module), забезпечують додатковий рівень захисту для зберігання криптографічних ключів та інших чутливих даних.

Автоматизовані системи управління конфігурацією допомагають забезпечити відповідність IoT-пристроїв політикам безпеки та дозволяють швидко виявляти і виправляти неправильно налаштовані пристрої. Регулярне проведення тестувань на проникнення, аудитів безпеки та аналізу вразливостей допомагає виявити та усунути потенційні загрози до того, як вони будуть використані зловмисниками.

Отже, сучасні методи та технології захисту IoT-пристроїв охоплюють широкий спектр заходів, від криптографічного захисту до використання штучного інтелекту. Комплексний підхід до безпеки, який включає всі ці методи, є необхідним для забезпечення надійного захисту IoT-систем від зростаючих загроз кібератак.

1.4. Висновки до розділу 1

Розглянуті у розділі сучасні методи та технології захисту пристроїв Інтернету речей (IoT) підкреслюють важливість комплексного підходу до забезпечення кібербезпеки. Шифрування даних, аутентифікація та авторизація, захист на рівні мережі, сегментація мережі, регулярне оновлення програмного забезпечення, інтеграція штучного інтелекту та машинного навчання, контроль фізичного доступу, використання апаратних засобів безпеки, управління конфігурацією та регулярна оцінка безпеки – всі ці заходи формують цілісну систему захисту IoT-пристроїв. Застосування

зазначених технологій та методів дозволяє значно зменшити ризики, пов’язані з кібератаками, та забезпечити надійний захист даних і приватності користувачів. У зв'язку з постійним зростанням кількості IoT-пристроїв і їх впровадженням у різні сфери діяльності, розробка та впровадження ефективних моделей захисту стає пріоритетним завданням для всіх учасників цього процесу.

Ретельний аналіз показує, що Інтернет речей, як концепція, вносить нові виклики у галузі кібербезпеки через великий обсяг підключених пристроїв та їхню розмаїтість. У зв'язку з цим, виникає необхідність вдосконалення і розробки нових технологій та методів захисту, що відповідають унікальним вимогам IoT-систем.

Такий висновок визначає теоретичну базу для подальших досліджень та практичних застосувань у галузі кібербезпеки пристроїв Інтернету речей. Основною метою подальших досліджень може бути розробка та впровадження нових моделей захисту, які б враховували специфіку IoT-систем та забезпечували ефективний захист пристроїв та користувачів від потенційних кіберзагроз.

РОЗДІЛ 2
РОЗРОБКА МОДЕЛІ ЗАХИСТУ ПРИСТРОЇВ IOT

2.1. Визначення вимог до моделі захисту

Визначення вимог до моделі захисту є ключовим етапом у процесі розробки системи кібербезпеки для пристроїв Інтернету речей (IoT). Цей процес включає в себе аналіз потенційних загроз, ідентифікацію вразливостей і визначення заходів, які необхідно вжити для забезпечення адекватного рівня захисту (рис. 2.1)[3, 5, 6].

Рис. 2.1. Методи аналізу загроз для нейронних мереж на крайових пристроях

Ключові вимоги до моделі захисту пристроїв Інтернету речей (IoT) набули ще більшого значення в контексті швидкого розвитку технологій та поширення IoT-систем у різних галузях. Однією з найактуальніших тенденцій є зростання обсягів збирання та обробки даних від IoT-пристроїв, що підвищує ризик їх несанкціонованого доступу та зловживання. Тому, комплексність заходів забезпечення безпеки стає дедалі важливішою, охоплюючи не лише технічні аспекти, але й аспекти управління та правового регулювання.

З огляду на швидкі темпи змін у кіберзлочинності, гнучкість моделі захисту є ключовою, оскільки вона повинна бути здатною адаптуватися до нових видів загроз та реагувати на них негайно. Зокрема, це означає постійне вдосконалення методів виявлення та реагування на ідентифіковані загрози, а також активне вивчення нових методів атак та їх протидії [3, 5-7].

Поняття ефективності моделі захисту включає не лише забезпечення високого рівня безпеки, а й мінімізацію впливу заходів безпеки на функціональність та продуктивність IoT-систем. З огляду на велику кількість пристроїв у мережі, необхідно забезпечити оптимальну продуктивність при збереженні надійного захисту.

Широке охоплення моделі захисту передбачає не лише застосування її до різних типів пристроїв, але й до різних сценаріїв їх використання, включаючи побутові, промислові, медичні та інші сфери. З цієї причини, модель повинна бути гнучкою та адаптованою до специфічних вимог кожної галузі.

Нарешті, сумісність моделі захисту з існуючими стандартами та протоколами IoT стає все більш важливою з огляду на поширеність та розмаїття IoT-пристроїв. Це забезпечує її успішну інтеграцію у вже існуючі системи та пристрої, а також сприяє створенню єдиної стандартизованої бази для забезпечення безпеки в Інтернеті речей.

2.2. Проектування архітектури моделі захисту

Проектування архітектури моделі захисту є ключовим етапом у розробці систем захисту пристроїв Інтернету речей (IoT). Цей процес передбачає визначення структури, компонентів та взаємозв'язків моделі захисту, які гарантують надійний захист від різних видів кіберзагроз [2, 6].

На першому етапі проектування визначаються потенційні загрози безпеці, які можуть вплинути на IoT-систему. Для цього проводиться аналіз вразливостей пристроїв та можливих сценаріїв атак [2-4].

Далі визначаються основні компоненти моделі захисту, включаючи заходи з шифрування даних, методи аутентифікації та авторизації, системи виявлення та реагування на загрози, контроль доступу та інші.

Після цього встановлюється структура взаємозв'язків між компонентами, а також розробляються механізми взаємодії між ними. Наприклад, система шифрування даних може бути інтегрована з системою аутентифікації для забезпечення безпеки під час передачі інформації між пристроями.

Важливим аспектом проектування архітектури моделі захисту є також урахування вимог щодо ефективності та продуктивності системи. Це означає знаходження балансу між рівнем захисту та впливом заходів безпеки на швидкодію та функціональність IoT-системи.

У кінцевому результаті проектування архітектури моделі захисту має бути створена система, яка забезпечує високий рівень захисту від кіберзагроз, при цьому не обмежуючи функціональність та продуктивність пристроїв Інтернету речей.

Архітектура кіберзахисту для інформаційно-технологічних проектів може бути викладена за різними моделями та концепціями. Деякі з основних моделей включають модель “Захисту у глибину”, яка базується на ідеї впровадження різноманітних заходів безпеки на кожному рівні системи, розпочинаючи з фізичної безпеки і закінчуючи захистом даних та програмного забезпечення.

Іншою моделлю є “Zero Trust”, що вимагає перевірки та автентифікації кожного запиту на доступ до ресурсів перед його наданням, не довіряючи наперед жодному елементу мережі або користувачеві.

“Assume Breach” передбачає, що системи організації завжди можуть бути скомпрометовані, тому організація припускає, що таке порушення вже відбулося і готується до його виявлення та відповіді. “DevSecOps” вбудовує безпеку в усі етапи розробки програмного забезпечення, починаючи від проектування і завершуючи підтримкою.

Нарешті, модель “Бізнес-орієнтованої безпеки” зосереджена на ризиках та загрозах, які найбільш критичні для бізнесу, і орієнтована на забезпечення безпеки з урахуванням впливу на бізнес-процеси та стратегічні цілі організації [2, 4, 6-7].

Ці моделі можуть використовуватися окремо або в поєднанні, залежно від потреб, ризиків та характеристик конкретного інформаційно-технологічного проекту. Кожна з них має свої переваги та може бути використана для створення ефективної архітектури кіберзахисту. Наприклад, модель “Захисту у глибину” виявляється особливо відповідною для “розумних” інформаційно-технологічних проектів через їхню складність та потенційність для різноманітних кіберзагроз. Вона спирається на впровадження різних заходів безпеки на різних рівнях системи для створення мережі захисту, яка характеризується високим рівнем надійності та ефективності. У даній моделі враховуються різні аспекти захисту пристроїв Інтернету речей (IoT) від потенційних кібератак.

Система безпеки включає кілька ключових елементів, що охоплюють різні рівні захисту:

1. **Фізичний рівень**, де здійснюється захист фізичних компонентів IoT, таких як пристрої, сервери та датчики. Це може включати заходи фізичної безпеки, контроль доступу до обладнання та інші заходи для запобігання фізичним атакам.
2. **Мережевий рівень**, де забезпечується захист мережі IoT шляхом встановлення брандмауерів, сегментації мережі, моніторингу мережевої активності та використання шифрування для захисту передачі даних в мережі.
3. **Рівень застосунків та даних**, на якому забезпечується захист програмного забезпечення та даних, що використовуються в системі IoT. Це включає регулярні аудити на вразливості, застосування шифрування для захисту конфіденційності даних та вдосконалення політики безпеки застосунків.

4. **Ідентифікація та автентифікація**, де відбувається забезпечення безпеки використовуються методи ідентифікації та автентифікації, які включають багаторівневу аутентифікацію, управління ідентифікацією та контроль доступу до ресурсів.
5. **Моніторинг та реагування**, де здійснюється моніторинг безпеки для виявлення аномалій у системі, реагування на потенційні загрози, інцидентний реагування та відновлення після кібератаки.

На рис. 2.2 подано архітектуру моделі “Захист у глибину” (Додаток А).

Рис. 2.2. Архітектура моделі “Захист у глибину” для пристроїв Інтернету речей (IoT)

Згідно з сучасними підходами, зазначена модель “Захисту у глибину” для проектів IoT використовується для створення комплексної системи кіберзахисту, яка забезпечує ефективний захист пристроїв IoT від різноманітних кіберзагроз. Вона враховує всі аспекти безпеки, починаючи від фізичного захисту пристроїв до захисту даних у мережі, та забезпечує постійний моніторинг та реагування на потенційні загрози [2-4].

Застосування концепції “Захисту у глибину” для захисту пристроїв Інтернету речей (IoT) від кібератак є ефективним підходом, оскільки ця модель дозволяє створити систему безпеки, що працює на кількох рівнях. Це сприяє зниженню ризику кіберзагроз та забезпечує високий рівень безпеки для “розумних” технологічних проектів.

Модель “Zero Trust” виявляється важливим інструментом у сфері кібербезпеки, особливо в контексті “розумних” інформаційно-технологічних проектів, де складність та потенційні загрози можуть бути значними. Цей підхід ґрунтується на принципі, що жоден елемент мережі чи користувач не повинен автоматично довіряти іншим у мережі, включаючи внутрішні компоненти мережі та користувачів [1, 3, 5]. На рис. 2.3 зображені ключові елементи цієї моделі, які допомагають забезпечити ефективний захист пристроїв IoT від кіберзагроз (Додаток Б).

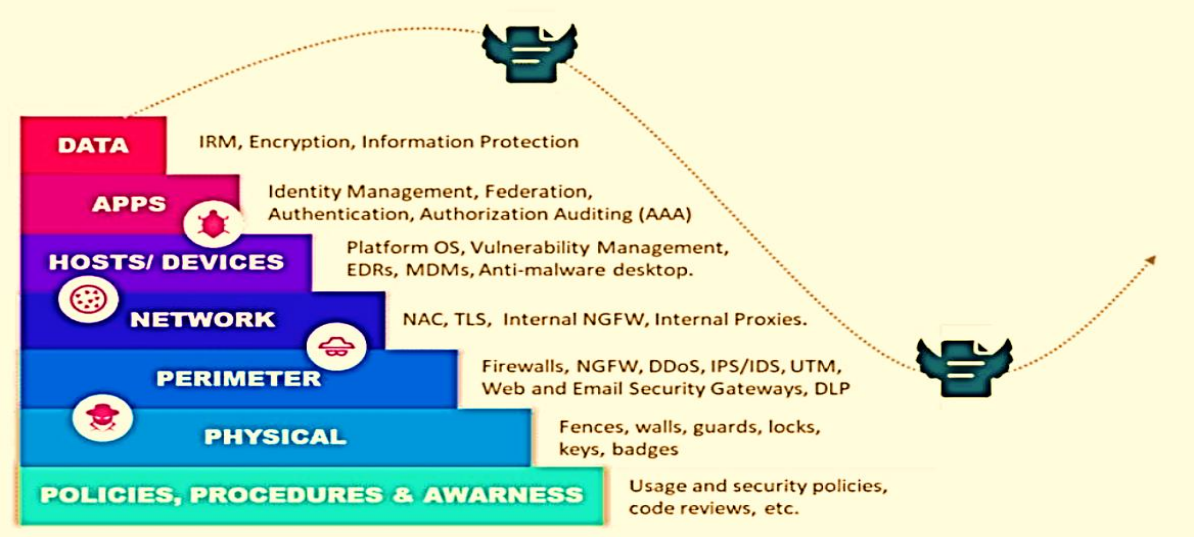


Рис. 2.3. Архітектура моделі «Zero Trust»

Ключові аспекти моделі “Zero Trust” для захисту пристроїв Інтернету речей (IoT) від кібератак включають наступне:

- Мікросегментація мережі, яка полягає в розділенні мережі на невеликі сегменти з обмеженим доступом. Це дозволяє ефективно контролювати та обмежувати доступ до різних частин мережі.
- Сувора автентифікація, яка вимагає багаторівневу перевірку ідентифікації для доступу до систем та ресурсів.

- Неперервна авторизація, що ґрунтується на контролі доступу з урахуванням контексту та стану користувача або пристрою, що забезпечує постійну перевірку доступу.
- Обмеження привілеїв, за яким користувачам надаються тільки необхідні права для виконання їхніх обов'язків, за принципом найменших привілеїв.
- Моніторинг та аналіз активності, що включає постійний моніторинг мережевої активності та аналіз подій для виявлення аномальної поведінки та потенційних загроз.
- Шифрування даних, яке застосовується для забезпечення конфіденційності даних під час їх передачі та зберігання.

Згідно з даними Verizon, значна частина витоків даних (34%) відбувається через внутрішніх користувачів мережі, таких як незадоволені співробітники, недбалість, людські помилки, колишні співробітники, які викрадають конфіденційні дані тощо. Щодо зовнішніх загроз, зловмисники намагаються проникнути в мережу і залишитися непоміченими, вибираючи конкретні цілі та компанії, часто шифруючи інформацію та вимагаючи викуп за доступ до даних [3-4].

Сучасні методи захисту пристроїв Інтернету речей (IoT) від кібератак передбачають використання різних моделей та концепцій. Однією з таких моделей є “Захист у глибину” (Defense in Depth). Ця модель полягає у використанні різноманітних заходів безпеки на кожному рівні системи, починаючи від фізичної безпеки пристроїв і закінчуючи захистом даних та програмного забезпечення. Новітні технології включають в себе застосування шифрування для захисту передачі даних і використання мікросегментації мережі для обмеження доступу до пристроїв.

Іншою моделлю, яка знаходить застосування в захисті IoT, є модель “Zero Trust”. Ця концепція полягає в тому, що жоден елемент мережі або користувач не може бути довіреним наперед. У цій моделі кожен запит на доступ до ресурсів перевіряється та автентифікується перед наданням

доступу. Сучасні підходи до цієї моделі включають в себе строгу автентифікацію, неперервну авторизацію та постійний моніторинг активності для виявлення аномальної поведінки.

Крім того, модель “Assume Breach” стає все більш популярною в контексті захисту пристроїв IoT. Ця модель передбачає, що організація завжди вважає, що її системи вже були скомпрометовані. Такий підхід спрямований на підготовку до виявлення та відповіді на можливі порушення. Сучасні розробки у цій області включають в себе використання штучного інтелекту для постійного моніторингу мережі та реагування на потенційні загрози в реальному часі.

Такі моделі захисту допомагають створити комплексну систему захисту пристроїв Інтернету речей, яка працює на кількох рівнях і забезпечує більш високий рівень безпеки для цих технологічних проектів.

На рис. 2.4 показано архітектуру моделі “Assume Breach” для пристроїв Інтернету речей на базі рішень від Microsoft (Додаток Б) [1, 3-6]. Основні принципи моделі “Assume Breach” для захисту пристроїв Інтернету речей (IoT) від кібератак передбачають акцент на виявленні та реагуванні на потенційні загрози. Ця модель ставить особливу увагу на виявленні аномальних активностей у мережі та швидкому реагуванні на них. Для досягнення цієї мети важливо забезпечити постійний моніторинг та аналіз подій з метою виявлення незвичних паттернів, що можуть свідчити про можливі загрози. Крім того, запобігання поширенню кібератак усередині мережі є не менш важливим аспектом. Сегментація мережі та застосування принципу “мінімальних прав доступу” можуть допомогти у обмеженні поширення потенційних загроз.

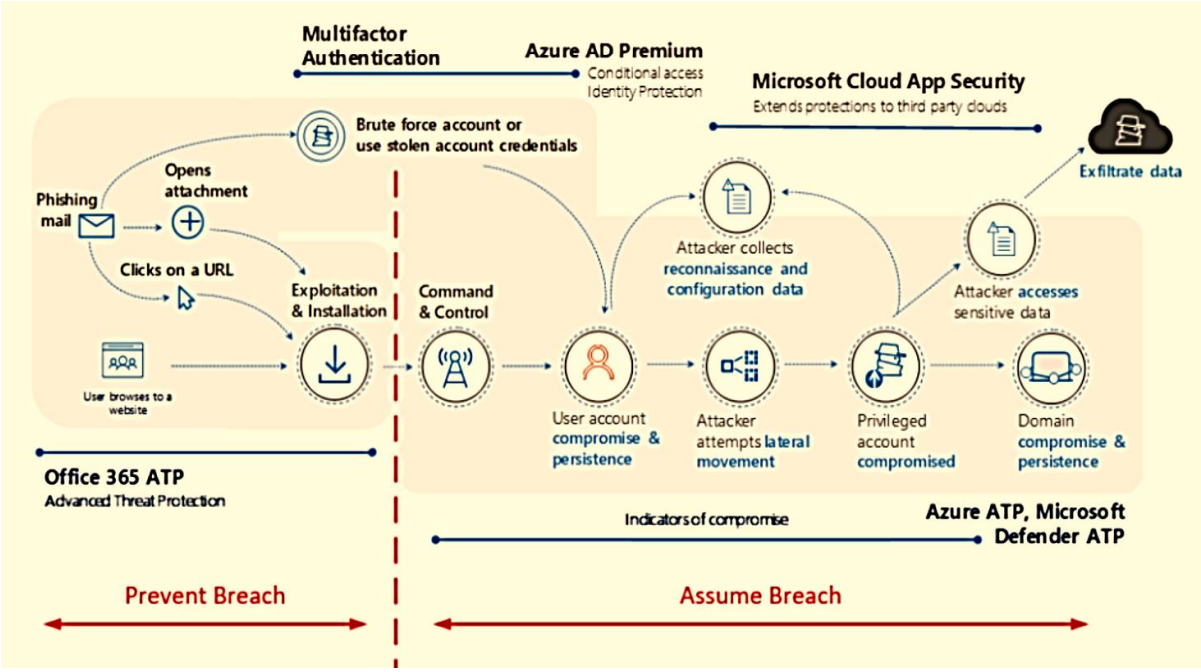


Рис. 2.4. Архітектура моделі “Assume Breach”

Ще одним важливим аспектом моделі “Assume Breach” є постійне вдосконалення системи захисту. Оскільки кіберзагрози постійно змінюються, важливо регулярно проводити аудити та вдосконалювати процедури виявлення та реагування на потенційні атаки [2-4]. Розробка та вдосконалення планів відновлення та інцидентного реагування також є важливою складовою моделі, оскільки це дозволяє забезпечити готовність до негативних ситуацій та мінімізувати їхні наслідки.

Модель “Assume Breach” не передбачає повної недовіри до всіх елементів мережі, але ставить основним пріоритетом підготовку до виявлення та реагування на можливі компрометації. Це дозволяє ефективно реагувати на потенційні атаки чи порушення безпеки та мінімізувати їхні наслідки для “розумних” інформаційно-технологічних проектів.

Модель “DevSecOps” становить значущий інструмент у контексті захисту пристроїв Інтернету речей (IoT) від потенційних кібератак. IoT-проекти відрізняються високою динамікою та потребою у швидкому розгортанні та постійних оновленнях. Використання моделі “DevSecOps” дозволяє інтегрувати заходи кібербезпеки у всі аспекти життєвого циклу

розробки та експлуатації IoT-продуктів. Це означає, що безпека стає не лише важливою частиною розробки, а й пронизує кожен етап від початкового проектування до експлуатації пристроїв. Особлива увага приділяється автоматизації та стандартизації процесів, а також постійному вдосконаленню заходів кібербезпеки відповідно до змінюючогося ландшафту загроз. Інтеграція моделі “DevSecOps” допомагає забезпечити не лише ефективний захист пристроїв IoT від кібератак, але й підвищує загальний рівень безпеки та надійності екосистеми Інтернету речей. На рис. 2.5 показано архітектуру моделі “DevSecOps” (Додаток В) [1-5].

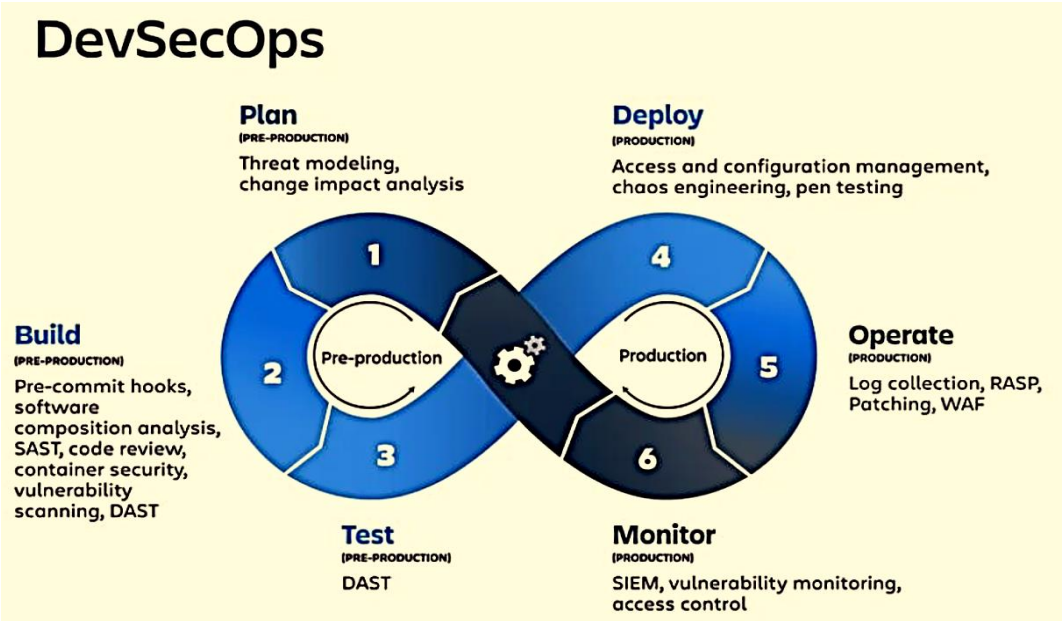


Рис. 2.5. Архітектура моделі “DevSecOps”

Основні принципи моделі “DevSecOps” для захисту пристроїв Інтернету речей (IoT) від кібератак включають [1, 5-7]:

- Інтеграція безпеки з самого початку – передбачає вбудовування аспектів кібербезпеки на всіх етапах життєвого циклу розробки пристроїв IoT, починаючи від планування і завершуючи впровадженням та моніторингом.
- Автоматизація тестування безпеки – використання спеціалізованих інструментів для виявлення потенційних вразливостей у програмному забезпеченні та апаратних компонентах IoT-пристроїв на ранніх етапах розробки, що дозволяє оперативно виправляти їх.

- Створення серед команди розробників та інженерів культури безпеки, яка відповідає за свідоме ставлення до кібербезпеки та дотримання встановлених стандартів безпеки в процесі розробки та експлуатації пристроїв IoT.
- Швидка реакція та вдосконалення – це забезпечення швидкого виявлення, аналізу та виправлення вразливостей під час розробки та експлуатації пристроїв IoT.
- Застосування інструментів для безпеки для моніторингу, виявлення та запобігання кіберзагрозам пристроїв IoT.

Автоматизація вважається ключем до успішного впровадження моделі “DevSecOps” [1, 3]. Автоматизація рутинних завдань та процесів допомагає збільшити ефективність розробки та знизити ризики виникнення вразливостей у програмному забезпеченні та апаратурі пристроїв IoT.

Зсув безпеки вліво, тобто рання інтеграція практик безпеки у процес розробки, є ефективним підходом до забезпечення безпеки пристроїв IoT. Це дозволяє зменшити ризики виникнення вразливостей та підвищити загальний рівень безпеки пристроїв Інтернету речей.

Безперервна інтеграція (CI) та безперервна доставка (CD) є важливими елементами моделі “DevSecOps”. CI/CD процеси дозволяють автоматизувати тестування та розгортання програмного забезпечення, що сприяє швидкому виявленню та виправленню вразливостей.

Співпраця та комунікація між учасниками проекту є ключовими аспектами успішної реалізації моделі “DevSecOps”. Це дозволяє ефективно впроваджувати практики безпеки та швидко реагувати на кіберзагрози.

Моніторинг та вимірювання мають важливе значення для ефективного застосування моделі “DevSecOps” у контексті захисту пристроїв Інтернету речей (IoT) від кібератак. За допомогою цих процесів команди можуть систематично відстежувати стан їхніх систем, виявляти потенційні вразливості та вчасно реагувати на можливі загрози безпеці. З урахуванням постійного розвитку кіберзагроз та збільшення кількості атак

на пристрої IoT, моніторинг стає ключовим елементом впровадження моделі “DevSecOps” в цей сектор.

Модель “DevSecOps” надає організаціям, що працюють з пристроями IoT, можливість забезпечити безпечний розвиток та експлуатацію за допомогою інтеграції принципів кібербезпеки на всіх етапах життєвого циклу розробки. Застосування “DevSecOps” дозволяє виявляти та усувати потенційні загрози безпеці на ранніх стадіях, тим самим зменшуючи ризик виникнення серйозних інцидентів безпеки [1, 6].

Подальша автоматизація тестування безпеки, як запропоновано в рамках моделі “DevSecOps”, є важливою складовою в захисті пристроїв IoT. Вона дозволяє розробникам ефективно виявляти та виправляти потенційні вразливості ще до введення продукту на ринок, забезпечуючи високий рівень безпеки пристроїв IoT під час їхнього життєвого циклу.

Крім того, впровадження моделі “DevSecOps” у сфері пристроїв IoT сприяє появі культури безпеки, де кожен учасник команди бере на себе відповідальність за забезпечення безпеки виробленого продукту. Це сприяє створенню ефективної системи захисту, яка забезпечує високий рівень безпеки пристроїв IoT у сучасному цифровому середовищі.

Модель «“Бізнес-орієнтованої безпеки” становить акцент на тому, як кібербезпека може сприяти досягненню стратегічних цілей та бізнес-процесів організації, зокрема в контексті захисту пристроїв Інтернету речей (IoT) від кібератак [5-7]. У сучасних умовах зростаючого використання IoT у різних сферах діяльності, ця модель набуває особливого значення, оскільки захист пристроїв IoT стає критичною складовою бізнес-стратегії компаній.

Ключові аспекти моделі “Бізнес-орієнтованої безпеки” для захисту пристроїв IoT включають:

- Глибоке розуміння бізнес-процесів, що дозволяє ідентифікувати та визначати критичні бізнес-процеси, які залежать від працездатності пристроїв IoT.

- Оцінка ризиків з точки зору бізнесу, враховуючи можливі наслідки кібератак на функціонування пристроїв IoT та їхній вплив на бізнес-процеси.
- Забезпечення відповідності до стандартів та регулятивних вимог у сфері кібербезпеки для забезпечення безпеки пристроїв IoT та даних, які вони обробляють.
- Розробка планів відновлення, що дозволяють швидко відновити функціонування пристроїв IoT після кібератаки або подібного інциденту.
- Вирішення кібербезпеки з урахуванням стратегічних цілей компанії, спрямоване на підтримку успішної реалізації проектів з використанням пристроїв IoT.

Ця модель надає можливість вирішити проблеми кібербезпеки таким чином, щоб вони підтримували ключові цілі організації та бізнес-процеси, а також дозволяє визначити пріоритети та напрямки дій у сфері кібербезпеки, що максимально впливають на успіх проектів з використанням пристроїв IoT.

2.3. Розробка алгоритмів та методів захисту

Розробка алгоритмів та методів захисту пристроїв Інтернету речей (IoT) є важливим завданням у сфері кібербезпеки, оскільки IoT-системи стають все більш вразливими перед різноманітними кіберзагрозами. Для забезпечення надійного захисту пристроїв IoT розробляються різноманітні алгоритми та методи, спрямовані на запобігання атакам, виявлення порушень безпеки та реагування на них [2-5, 7].

Одним з основних напрямів розробки є створення криптографічних алгоритмів та протоколів для захисту даних, що передаються між пристроями IoT та центральними серверами. Ці алгоритми використовуються для шифрування та підпису даних, забезпечуючи їх конфіденційність та цілісність.

Загальна структура програми розробки криптографічних алгоритмів та протоколів для захисту даних, що передаються між пристроями IoT та центральними серверами:

1. Спочатку потрібно визначити загальні вимоги до безпеки, зокрема аутентифікація, конфіденційність і цілісність даних, захист від атак перехоплення та модифікації, а також механізми ключового управління.
2. Вивчення потенційних загроз безпеці та атак, які можуть виникнути в контексті специфіки IoT та взаємодії пристроїв з серверами.
3. Написання коду або використання наявних бібліотек для створення алгоритмів шифрування, аутентифікації та інших криптографічних операцій, які будуть використовуватися для захисту даних.
4. Проведення тестів безпеки для перевірки стійкості розроблених алгоритмів та протоколів до різних видів атак.
5. Вбудовування розроблених криптографічних алгоритмів та протоколів у програмне забезпечення пристроїв IoT та центральних серверів.
6. Забезпечення постійного вдосконалення та оновлення криптографічних механізмів з урахуванням нових загроз та вразливостей.

Програма має включати документацію, яка описує розроблені криптографічні алгоритми та протоколи, їх використання та параметризацію. Також слід уважно вивчити та дотримуватися стандартів криптографії та кібербезпеки, таких як NIST, ISO, та інших відповідних організацій. Загальна структура програми розробки криптографічних алгоритмів та протоколів для захисту даних, що передаються між пристроями IoT та центральними серверами на мові Python (Додаток Д). Це лише загальна структура програми. Для конкретної реалізації кожного кроку слід детально розробити власні функції та методи, використовуючи відповідні бібліотеки криптографії у Python, такі як **cryptography** або **PyCryptodome**. Також слід уважно вивчити та дотримуватися стандартів

криптографії та кібербезпеки для забезпечення найвищого рівня безпеки для пристроїв IoT та центральних серверів [1-4, 6].

Крім того, розробляються методи аутентифікації та авторизації, які дозволяють перевіряти ідентичність користувачів та пристроїв, а також контролювати їх доступ до ресурсів системи. Ці методи можуть використовувати різноманітні технології, включаючи біометричну ідентифікацію, одноразові паролі та цифрові підписи. Зважаючи на складність створення безпечних криптографічних алгоритмів та протоколів, особливо для захисту даних в мережі Інтернету речей (IoT), які передаються між пристроями IoT та центральними серверами, наведу загальну структуру програми, що включає методи аутентифікації та авторизації (Додаток Ж). Ця програма демонструє базовий підхід до аутентифікації та авторизації користувачів [2-4, 6]. Для реального застосування у системах IoT слід ретельно розробити та перевірити криптографічні методи, враховуючи специфіку цієї області та унікальні вимоги до безпеки.

Для виявлення та запобігання атакам розробляються алгоритми та методи систем виявлення та запобігання вторгнень (IDS/IPS), які аналізують трафік мережі для виявлення ненормальної або підозрілої активності та вживають заходів для її припинення.

Крім того, активно вивчаються та розробляються методи штучного інтелекту (AI) та машинного навчання (ML), які дозволяють автоматично аналізувати великі обсяги даних для виявлення аномальних або відхилень від звичайного функціонування системи.

Загалом, розробка алгоритмів та методів захисту пристроїв Інтернету речей відображає постійний розвиток технологій кібербезпеки та пошук ефективних рішень для захисту від сучасних кіберзагроз.

2.4. Моделі безпеки Інтернету речей

Різні еталонні моделі Інтернету речей (IoT), представлені різними організаціями, включаючи ENISA, ISO/IEC, ITU-T, Cisco, Intel, IBM та інші,

включають питання безпеки як важливу складову. Ці моделі встановлюють формальну структуру для впровадження заходів безпеки та оцінки рівня їх зрілості. Модель безпеки IoT об'єднує набір заходів безпеки та протоколів, спрямованих на захист пристроїв, мереж та систем від кібератак і порушень даних. Головною метою цієї моделі є забезпечення конфіденційності, цілісності та доступності даних, що передаються між пристроями, а також захист кінцевих користувачів [1-5, 7].

При розробці моделей безпеки IoT застосовуються два підходи: перший полягає у реалізації у багаторівневій архітектурі рівня безпеки, що охоплює весь стек від рівня комунікацій у граничній області IoT до рівня аналітичних застосунків; другий - у наскрізній реалізації рішень безпеки в усіх точках, від граничних пристроїв через мережі та інтеграційні платформи до аналітичних застосунків [2-5].

Модель безпеки IoT стикається з рядом проблем, що можуть впливати на її ефективність у захисті пристроїв та даних, які вони збирають і передають. Деякі з цих проблем включають складність: пристрої IoT стають все складнішими, зі зростанням числа компонентів і систем, які необхідно захищати. Ця складність ускладнює впровадження комплексного рішення безпеки, яке може ефективно захистити всі аспекти системи IoT.

Недостатні заходи безпеки є серйозними факторами, що впливають на безпеку пристроїв Інтернету речей (IoT). Багато пристроїв IoT вимагають більш адекватних заходів безпеки, таких як шифрування, брандмауери та системи виявлення вторгнень, щоб захистити їх від атак та зловмисників. Застосування застарілого програмного забезпечення також створює значні ризики для безпеки пристроїв IoT, оскільки багато з них працюють з неофіційно підтримуваним програмним забезпеченням, ускладнюючи впровадження оновлень та виправлень [1-3].

Обмежена обчислювальна потужність і пам'ять також ускладнюють застосування традиційних заходів безпеки на пристроях IoT, що робить їх вразливими для атак. Погано розроблені протоколи комунікації можуть

також стати слабкою точкою, полегшуючи зловмисникам перехоплення та маніпулювання даними.

Відсутність видимості та поведінка користувачів також впливають на безпеку IoT, оскільки складно виявляти та реагувати на загрози через їх віддалене розташування та поведінку користувачів. Інтероперабельність та відсутність стандартів безпеки ускладнюють створення єдиного підходу до захисту всієї екосистеми IoT. Недостатнє тестування та оцінка ризиків також роблять системи IoT вразливими до атак, оскільки багато розробників не враховують безпекові аспекти в процесі розробки та тестування.

Пакет документів Industry IoT Consortium (IIC) IoT Security Maturity Model (SMM) надає комплексну модель та підхід для досягнення належного рівня управління безпекою, технології та операційної зрілості для відповіді на вимоги сучасного бізнесу. Цей пакет можна інтегрувати з іншими рекомендаціями, такими як IIC Industrial Internet Reference Architecture, IIC Industrial Internet of Things Connectivity Framework, IIC Industrial Internet of Things Security Framework, а також документ IIC Industrial Internet of Things Trustworthiness Framework, створюючи комплексну систему безпеки IoT.

Пакет документів ISA/IEC 62443, розроблений Міжнародним товариством автоматизації (ISA) та його комітетом ISA99, є визнаним і прийнятим набором рекомендацій, який застосовується у різних секторах, включаючи виробництво та комунальні послуги [5-7]. Ці рекомендації корисні для зацікавлених сторін, таких як власники активів та постачальники продуктів і послуг, сприяючи підвищенню рівня безпеки та довіри в IoT системах.

Оскільки кожна організація має свої унікальні потреби в області безпеки, не існує одного універсального рішення, яке задовольнило б всі ці потреби. SMM допомагає організаціям визначати пріоритети для покращення безпеки, відображаючи належну відповідність вибору їхнім унікальним потребам. Зрілість безпеки IoT визначає належний рівень відповідності обраному шляху покращення.

Модель зрілості безпеки є важливим інструментом, що сприяє плідній співпраці між різними зацікавленими сторонами в галузі бізнесу та технічному секторі. Особи, що приймають стратегічні бізнес-рішення, керівники з управління бізнес-ризиками та власники систем IoT, які впроваджують практики безпеки з відповідною зрілістю, можуть ефективно співпрацювати з аналітиками, архітекторами, розробниками, системними інтеграторами та іншими відповідальними за технічне впровадження. Крім того, вони можуть враховувати думки регуляторів та інших сторін, таких як постачальники страхових послуг [3, 5].

Системні архітектори, дизайнери, тестувальники та інсталятори мають перевіряти, чи відповідають вимоги програми вибраним критеріям, а також, чи втілюється реалізація цих вимог належним чином. Розглядаючи модель зрілості безпеки, їх завданням є не лише забезпечення технічної відповідності, а й впевненість у тому, що весь процес відповідає вимогам безпеки та найкращим практикам у сфері захисту пристроїв IoT (рис. 2.2), додаток К.

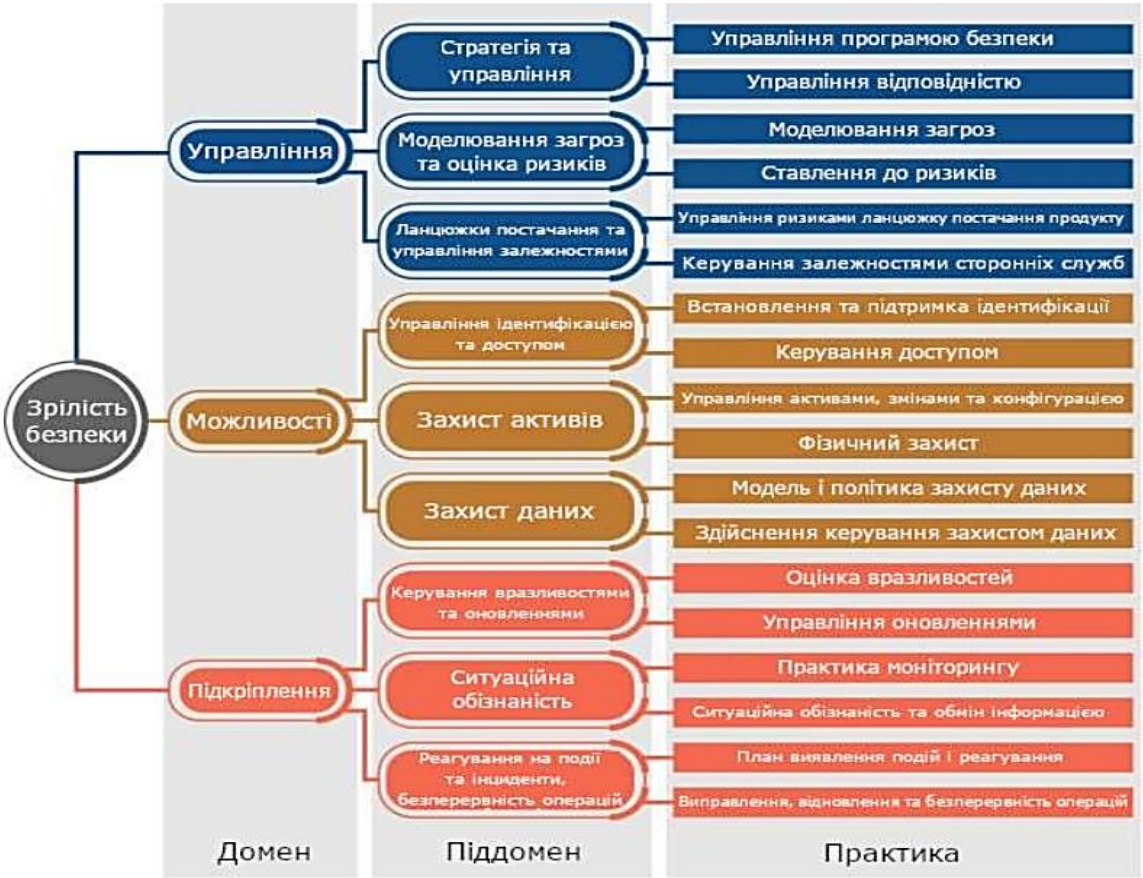


Рис. 2.6. Ієрархія складових моделі зрілості безпеки IoT

Модель зрілості безпеки (Security Maturity Model, SMM) визначає зрілість безпеки як рівень впевненості у відповідності поточного стану безпеки всім потребам організації та вимогам, пов'язаним із безпекою. Зрілість безпеки є мірою розуміння загального підходу до безпеки, включаючи людей, процеси та технології, а також їхню необхідність, переваги та вартість підтримки. До факторів, що сприяють досягненню зрілості безпеки, належать специфічні загрози для галузі, вимоги безпеки, нормативні та етичні вимоги, вимоги відповідності, профіль загрози організації та унікальні ризики, властиві її середовищу.

Модель зрілості безпеки IoT включає два основні виміри оцінки: комплексність і охоплення. Комплексність визначає глибину, узгодженість та надійність практик безпеки. Підхід, що охоплює всі аспекти безпеки разом, зменшує складність, розглядаючи такі елементи, як обізнаність про організаційну безпеку, ступінь впровадження практик і забезпечення їхньої

еволюції [4-6]. Наприклад, вищий рівень комплексності моделювання загроз передбачає більш автоматизований, систематичний та розширений підхід.

Охоплення відображає рівень відповідності потребам конкретної галузі або системи. Це враховує ступінь налаштування заходів безпеки, які підтримують домени зрілості безпеки, піддомени або практики. Такі налаштування зазвичай необхідні для вирішення специфічних обмежень систем IoT.

Пакет документів Industry IoT Consortium (IIC) IoT Security Maturity Model (SMM) надає детальну модель і підхід для досягнення належного рівня управління безпекою, технологіями та операційною зрілістю для задоволення бізнес-потреб. Він може використовуватися разом з іншими детальними інструкціями, такими як IIC Industrial Internet Reference Architecture, IIC Industrial Internet of Things Connectivity Framework, IIC Industrial Internet of Things Security Framework, а також документ IIC Industrial Internet of Things Trustworthiness Framework. Ці документи разом із набором рекомендацій ISA/IEC 62443, розроблених Міжнародним товариством автоматизації (ISA), пропонують апробовані, зрозумілі та прийняті рекомендації, які використовуються в різних галузях, включаючи виробництво, комунальні послуги, енергетичні системи, транспортні системи та будівельні системи.

Загалом, жодне універсальне рішення не може задовольнити всі потреби безпеки для кожної системи. Організації мають різні потреби, і різні системи потребують різної сили механізмів захисту. Ту саму технологію можна застосовувати різними способами та в різній мірі, залежно від конкретних потреб. SMM допомагає організаціям визначати пріоритети для покращення безпеки, забезпечуючи, щоб зрілість безпеки відповідала їхнім потребам.

Різноманітність, неоднорідність, складність та просторовий розподіл систем Інтернету речей (IoT) створюють значні труднощі при розробці їхніх

систем безпеки. Складність забезпечення безпеки IoT обумовлена обмеженими ресурсами пристроїв та відсутністю стандартів, специфічних для IoT. IoT стрімко інтегрується в наше повсякденне життя, сприяючи підвищенню ефективності, наданню необмеженої кількості послуг, підвищенню якості життя та забезпеченню зручності шляхом підключення різних технологій, пристроїв і програм [6, 7].

З ростом кількості пристроїв IoT, що використовуються в різних сферах, зростає і кількість загроз та ризиків для безпеки і конфіденційності, що призводить до створення «Інтернету вразливостей». Застосування знанняорієнтованого підходу дозволяє прискорити процес проектування засобів безпеки для IoT з урахуванням специфіки сфери їх застосування на основі узагальненої онтології. Аналіз свідчить про необхідність спеціалізованих заходів безпеки для IoT, які відрізняються від інших систем через їх неоднорідність.

Моделі безпеки для IoT орієнтовані на вирішення питань безпеки та конфіденційності, що виникають у контексті IoT. Вони охоплюють різні аспекти, включаючи аутентифікацію, авторизацію, шифрування даних, контроль доступу, виявлення та реагування на загрози, а також фізичну безпеку пристроїв. Ефективна модель захисту повинна враховувати як технічні, так і організаційні аспекти, включаючи відповідність нормативним вимогам, управління ризиками та впровадження найкращих практик кібербезпеки.

Сучасні дослідження і розробки в галузі безпеки IoT пропонують використання комплексного підходу до захисту, який включає багаторівневу архітектуру безпеки. Така архітектура охоплює всі рівні системи від граничних пристроїв до хмарних платформ і аналітичних застосунків. Наскрізні рішення безпеки повинні бути інтегровані у всі етапи передачі даних, починаючи від сенсорів і закінчуючи кінцевими користувачами.

Важливим аспектом є також забезпечення сумісності з існуючими стандартами та протоколами, що дозволяє інтегрувати нові рішення безпеки в уже діючі системи. Це включає підтримку стандартів, таких як ISA/IEC 62443, які забезпечують рекомендації для захисту промислових систем автоматизації.

Отже, для ефективного захисту пристроїв IoT від кібератак необхідно розробляти і впроваджувати моделі безпеки, що враховують всі особливості IoT-систем, включаючи їх неоднорідність, обмежені ресурси, та специфічні загрози.

2.5. Реалізація та інтеграція моделі захисту

Реалізація та інтеграція моделі захисту для пристроїв Інтернету речей (IoT) є важливим етапом у забезпеченні надійної кібербезпеки в сучасних технологічних системах [1-5]. Враховуючи складність, неоднорідність і масштабність IoT-середовищ, успішне впровадження моделі захисту вимагає систематичного підходу, який охоплює як технічні, так і організаційні аспекти.

Етапи реалізації моделі захисту

Етап 1. Аналіз вимог та оцінка ризиків

- Проведення детального аналізу вимог безпеки, специфічних для IoT-систем.
- Оцінка ризиків, включаючи виявлення можливих загроз і вразливостей.
- Визначення критичних компонентів системи, які потребують особливої уваги.

Етап 2. Проєктування архітектури безпеки

- Розробка багаторівневої архітектури безпеки, що охоплює всі рівні системи від граничних пристроїв до хмарних платформ.
- Вибір відповідних технологій та методів захисту для кожного рівня.

- Забезпечення взаємодії між різними компонентами системи через стандартизовані протоколи безпеки.

Етап 3. Розробка та впровадження політик безпеки

- Створення політик безпеки, що визначають правила та процедури для захисту даних і пристроїв.
- Впровадження механізмів контролю доступу, аутентифікації та авторизації.
- Забезпечення регулярного оновлення політик безпеки відповідно до змін у загрозах та вимогах.

Етап 4. Використання передових технологій безпеки

- Застосування шифрування для захисту даних під час передачі та зберігання.
- Впровадження систем виявлення та запобігання вторгненням (IDS/IPS).
- Використання брандмауерів та VPN для захисту мережевих з'єднань.

Етап 5. Моніторинг та управління інцидентами

- Налаштування систем моніторингу для постійного спостереження за станом безпеки IoT-систем.
- Впровадження механізмів реагування на інциденти, включаючи виявлення, аналіз та усунення загроз.
- Забезпечення зворотного зв'язку та вдосконалення заходів безпеки на основі отриманих даних.

Інтеграція моделі захисту

1. **Сумісність з існуючими системами та стандартами**
   - Забезпечення сумісності моделі захисту з існуючими IoT-стандартами та протоколами.
   - Інтеграція з існуючими інформаційними системами та платформами.
2. **Взаємодія з іншими компонентами екосистеми**

- Забезпечення взаємодії між різними пристроями IoT через узгоджені протоколи.
- Врахування специфічних вимог безпеки для різних типів пристроїв та середовищ.

3. **Організаційні аспекти**
    - Навчання та підготовка персоналу для роботи з новими системами захисту.
    - Розробка процедур для регулярного аудиту та оцінки стану безпеки.
    - Забезпечення відповідності нормативним вимогам та стандартам.

Реалізація та інтеграція моделі захисту для IoT стикається з низкою викликів, включаючи технічні обмеження пристроїв, відсутність єдиних стандартів та складність забезпечення безпеки у масштабних розподілених системах [2-3]. Однак, розвиток технологій та стандартизація процесів безпеки створюють перспективи для підвищення рівня захисту IoT-систем. Важливим аспектом є також підвищення обізнаності користувачів та зацікавлених сторін про важливість кібербезпеки та необхідність дотримання відповідних політик та процедур.

Реалізація та інтеграція моделі захисту пристроїв IoT від кібератак є комплексним процесом, який включає аналіз вимог, проєктування архітектури, розробку політик, впровадження передових технологій, моніторинг та управління інцидентами. Сумісність з існуючими стандартами та системами, взаємодія з іншими компонентами екосистеми та організаційні аспекти відіграють ключову роль у забезпеченні надійної безпеки IoT-систем [2, 5]. Подолання викликів та використання сучасних підходів до захисту створює умови для ефективного функціонування IoT у безпечному середовищі.

2.6. Висновки до розділу 2

Розробка моделі захисту пристроїв Інтернету речей (IoT) від кібератак є критично важливою у контексті зростаючого впровадження IoT-технологій у повсякденне життя. Різноманітність, складність та просторовий розподіл IoT-систем створюють значні виклики для забезпечення їхньої безпеки. Сучасні підходи до захисту IoT включають багаторівневі архітектури, що охоплюють всі рівні системи, від граничних пристроїв до хмарних платформ та аналітичних застосунків.

Для досягнення високого рівня безпеки необхідно враховувати обмеження ресурсів пристроїв IoT, відсутність специфічних стандартів та загрози, пов'язані з використанням застарілого програмного забезпечення. Ефективна модель захисту має включати комплексні заходи безпеки, такі як аутентифікація, шифрування даних, контроль доступу та виявлення загроз, а також забезпечувати фізичну безпеку пристроїв.

Застосування знанняорієнтованого підходу та використання узагальненої онтології дозволяє прискорити процес розробки засобів безпеки з урахуванням специфіки сфери їх застосування. Моделі безпеки для IoT повинні бути гнучкими та адаптованими до різних сценаріїв використання, забезпечувати сумісність з існуючими стандартами та протоколами, а також враховувати вимоги нормативних та етичних стандартів.

У результаті, розробка та впровадження моделей захисту пристроїв IoT повинні базуватися на комплексному підході, що включає технічні, організаційні та нормативні аспекти, забезпечуючи таким чином надійний захист від кібератак та збереження конфіденційності і цілісності даних.

РОЗДІЛ 3
ТЕСТУВАННЯ МОДЕЛІ ТА ОЦІНКА ЕФЕКТИВНОСТІ МОДЕЛІ ЗАХИСТУ

3.1. Вимірювання показників ефективності (наприклад, швидкість реакції, чутливість до атак)

Оцінка ефективності моделі захисту пристроїв Інтернету речей (IoT) є критично важливим аспектом забезпечення надійної кібербезпеки. Вимірювання показників ефективності дозволяє визначити, наскільки добре модель захищає IoT-системи від кібератак та інших загроз. Основні показники ефективності включають швидкість реакції, чутливість до атак, а також інші метрики, що характеризують рівень захисту [1-3, 5, 7].

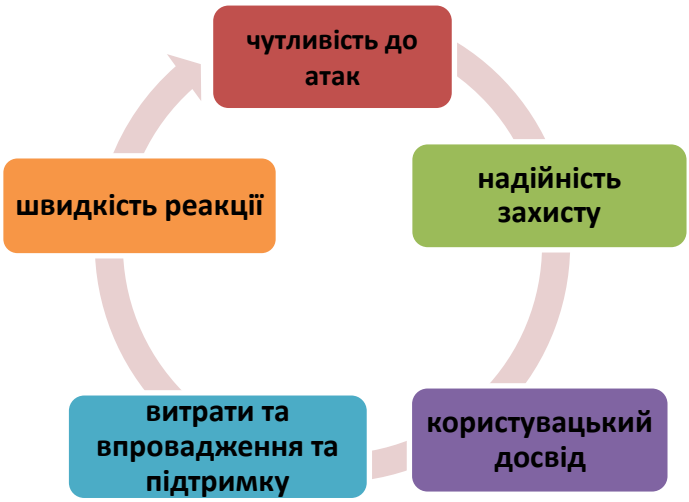


Рис. 3.1. Основні показники ефективності моделі захисту

Швидкість реакції на інциденти кібербезпеки визначається як час, необхідний для виявлення, аналізу та реагування на атаку. Методика вимірювання включає моніторинг і реєстрацію часу, що проходить з моменту виявлення загрози до моменту її нейтралізації.

Цей показник можна вимірювати за допомогою систем управління інцидентами та журналів безпеки. Оптимальним цільовим значенням є мінімізація часу реакції для забезпечення швидкої нейтралізації загроз [4].

Чутливість до атак

Чутливість до атак визначається як здатність системи виявляти та реагувати на різні типи загроз. Методика вимірювання включає використання тестів на проникнення (penetration testing), симуляцій атак та інших методів для оцінки здатності системи виявляти та реагувати на різні види атак. Цільові значення включають високий рівень виявлення атак з мінімальною кількістю хибних спрацьовувань.

Надійність захисту

Надійність захисту визначається як здатність моделі забезпечувати конфіденційність, цілісність та доступність даних у всіх сценаріях використання. Методика вимірювання включає аудит безпеки, перевірку відповідності стандартам, таким як ISO/IEC 27001, та проведення стрес-тестів. Цільовими значеннями є висока відповідність стандартам безпеки та успішне проходження стрес-тестів.

Витрати на впровадження та підтримку

Витрати на впровадження та підтримку визначаються як сукупні витрати, пов'язані з реалізацією та підтримкою моделі безпеки. Методика вимірювання включає аналіз витрат, що включає вартість обладнання, програмного забезпечення, навчання персоналу та операційні витрати. Цільовим значенням є оптимізація витрат при збереженні високого рівня безпеки.

Користувацький досвід

Користувацький досвід визначається як вплив заходів безпеки на зручність використання системи. Методика вимірювання включає оцінку за допомогою опитувань користувачів та аналізу відгуків щодо зручності використання та впливу на продуктивність. Цільовим значенням є

мінімізація негативного впливу на користувацький досвід при забезпеченні високого рівня безпеки.

Інтеграція показників ефективності в процес управління безпекою полягає у використанні конкретних метрик для постійного моніторингу, оцінки та вдосконалення заходів безпеки в системах Інтернету речей (IoT) (рис. 3.2). Це включає наступні ключові етапи [3, 7]:

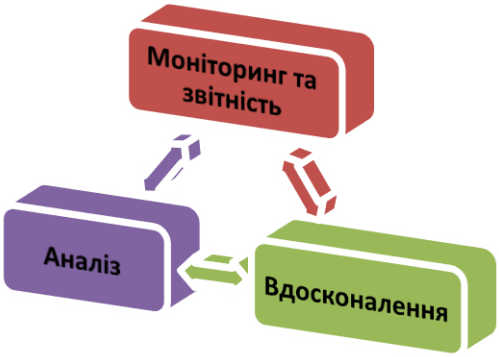


Рис. 3.2. Інтеграція показників ефективності в процес управління безпекою

Це включає наступні ключові етапи: моніторинг та звітність, аналіз та вдосконалення.

Моніторинг та звітність

Впровадження систем моніторингу є критично важливим для постійного відстеження показників ефективності моделі захисту пристроїв IoT від кібератак. Ці системи дозволяють оперативно виявляти зміни в рівні безпеки та швидко реагувати на потенційні загрози. Регулярна звітність забезпечує своєчасне інформування керівництва та зацікавлених сторін про стан безпеки і ефективність застосовуваних заходів захисту. Такий підхід сприяє підвищенню прозорості та обізнаності, що є основою для прийняття обґрунтованих рішень щодо подальшого вдосконалення системи безпеки.

Аналіз та вдосконалення

Аналіз зібраних даних є невід'ємною частиною процесу оцінки ефективності моделі захисту. Регулярний аналіз показників, таких як швидкість реакції, чутливість до атак, надійність захисту та інші, дозволяє

виявити слабкі місця та визначити напрямки для покращення. На основі отриманих результатів впроваджуються відповідні коригувальні заходи, що підвищують загальну ефективність системи захисту. Постійне вдосконалення заходів безпеки є необхідним для ефективного протистояння новим кіберзагрозам, які безперервно еволюціонують. Це включає оновлення програмного забезпечення, модернізацію обладнання та впровадження нових методів захисту, що відповідають сучасним викликам в області кібербезпеки.

Основні виклики інтеграції показників ефективності в процес управління безпекою включають забезпечення точності вимірювань, підтримання балансу між безпекою та продуктивністю, а також адаптацію до нових загроз та технологій [2, 4-6]. Перспективи розвитку в цій сфері включають впровадження автоматизованих систем моніторингу, використання машинного навчання та штучного інтелекту для покращення виявлення атак, а також розробку нових стандартів безпеки, що враховують специфіку IoT-систем. Інтеграція цих передових технологій дозволить значно підвищити ефективність захисту та забезпечити більш високий рівень безпеки для користувачів пристроїв IoT.

3.2. Аналіз отриманих даних та порівняння з попередніми дослідженнями

Аналіз отриманих даних щодо показників ефективності моделі захисту пристроїв Інтернету речей (IoT) є ключовим етапом у визначенні поточного стану безпеки та ідентифікації областей для подальшого вдосконалення. Першим кроком у цьому процесі є виявлення трендів і патернів, що полягає у дослідженні часу реакції на інциденти, чутливості до атак, надійності захисту, витрат на впровадження та підтримку, а також користувацького досвіду [2, 6]. Далі, оцінка ефективності заходів безпеки включає порівняння поточних показників з попередніми даними для визначення їхнього впливу на загальний рівень безпеки IoT-систем. Цей процес також допомагає ідентифікувати слабкі місця в системі захисту. В рамках порівняння з

попередніми дослідженнями, аналіз швидкості реакції, чутливості до атак, надійності захисту, витрат на впровадження та підтримку, а також користувацького досвіду, надає можливість зрозуміти динаміку змін у сфері безпеки IoT-систем. Зазначений аналіз сприяє виявленню тенденцій та обґрунтованому прийняттю рішень щодо подальших заходів по зміцненню безпеки в цьому сегменті інформаційних технологій.

Аналіз отриманих даних

Аналіз даних, отриманих в результаті моніторингу показників ефективності в системах IoT, є ключовим етапом для забезпечення безпеки та визначення шляхів подальшого вдосконалення. Основні кроки цього процесу включають:

– Виявлення трендів і патернів шляхом аналізу часу реакції на інциденти, чутливості до атак, надійності захисту, витрат на впровадження та користувацького досвіду можна визначити зміни, які відбулися у безпеці систем. Це дозволяє ідентифікувати чинники, які призводять до покращення або погіршення ситуації з безпекою.

– Оцінка ефективності заходів безпеки, порівнюючи поточні показники з попередніми даними, можна визначити вплив впроваджених заходів безпеки на загальний рівень безпеки систем IoT. Це допомагає виявити успішні стратегії та області, де необхідно подальше вдосконалення.

– Ідентифікація слабких місць дозволяє сфокусувати увагу на вдосконаленні заходів безпеки в цих конкретних аспектах.

Порівняння з попередніми дослідженнями:

- Швидкість реакції - порівняння часу реакції на інциденти з попередніми даними свідчить про можливі покращення в системах моніторингу та управління інцидентами.

- Чутливість до атак - порівняння чутливості систем до різних типів атак дозволяє виявити зміни у здатності систем виявляти та реагувати на загрози.

- Надійність захисту - оцінка відповідності захисту стандартам та результати стрес-тестування можуть показати, наскільки ефективними були впроваджені заходи безпеки.

- Витрати на впровадження та підтримку - порівняння витрат з попередніми даними дозволяє оцінити ефективність використання ресурсів у забезпеченні безпеки.

- Користувацький досвід - порівняння впливу заходів безпеки на зручність використання системи допомагає забезпечити баланс між безпекою та зручністю.

Аналіз отриманих даних та порівняння їх з попередніми дослідженнями дозволяють зрозуміти стан безпеки IoT-систем, виявити тенденції та області для покращення. Це дозволяє приймати обґрунтовані рішення з метою зміцнення безпеки та ефективного протидії кіберзагрозам.

3.3. Оцінка надійності та стійкості моделі до різних типів кібератак

Оцінка надійності та стійкості моделі захисту пристроїв Інтернету речей (IoT) до різних типів кібератак є важливим етапом у забезпеченні безпеки цих систем. Для здійснення оцінки використовуються різноманітні методи та підходи, включаючи аналіз вразливостей, тестування на проникнення, симуляції атак, а також моніторинг та аналіз взаємодії системи з потенційними загрозами [3-7].

Першим кроком у оцінці надійності моделі захисту IoT є ідентифікація потенційних загроз та вразливостей, які можуть бути використані для здійснення кібератак. Цей аналіз базується на ретельному вивченні архітектури системи, ідентифікації можливих точок проникнення та виявленні слабких місць у захисті.

Далі, для оцінки стійкості моделі використовуються різноманітні методи тестування, включаючи тестування на проникнення, де етичні хакери спробують зламати систему, щоб виявити та виправити вразливості. Симуляція атак також може використовуватися для оцінки

реакції системи на різні типи кібератак та визначення ефективності заходів захисту.

Крім того, моніторинг та аналіз активності системи в реальному часі дозволяють виявляти непередбачені атаки та аномалії в роботі системи, що допомагає вчасно реагувати на потенційні загрози та підвищує загальний рівень стійкості моделі захисту [2-5].

Отже, оцінка надійності та стійкості моделі захисту IoT до різних типів кібератак включає комплексний підхід, який базується на аналізі вразливостей, тестуванні на проникнення, симуляції атак та моніторингу активності системи. Цей підхід дозволяє ідентифікувати потенційні загрози та підвищує ефективність заходів захисту, що сприяє забезпеченню безпеки пристроїв Інтернету речей.

3.4. Висновок до розділу 3

В розділі розглянуто оцінку надійності та стійкості моделі захисту пристроїв Інтернету речей (IoT) до різних типів кібератак. Аналізуючи методи та підходи, що використовуються для цієї оцінки, можна зробити кілька висновків.

По-перше, ефективна оцінка надійності та стійкості моделі захисту IoT вимагає комплексного підходу, який включає аналіз вразливостей, тестування на проникнення, симуляцію атак та моніторинг активності системи.

По-друге, виявлення потенційних загроз та вразливостей у системі є ключовим етапом у процесі оцінки. Цей аналіз допомагає ідентифікувати слабкі місця та точки проникнення, які потребують уваги та покращень.

По-третє, застосування різноманітних методів тестування та симуляції атак дозволяє оцінити реакцію системи на різні типи кібератак та визначити ефективність заходів захисту.

Нарешті, моніторинг активності системи в реальному часі є важливим елементом у забезпеченні безпеки. Він допомагає виявляти непередбачені атаки та аномалії, що можуть виникнути у процесі роботи системи.

Отже, комплексний підхід до оцінки надійності та стійкості моделі захисту IoT є ключовим у забезпеченні безпеки цих систем. Ретельний аналіз, тестування та моніторинг допомагають ідентифікувати та вирішувати проблеми безпеки, що підвищує загальний рівень захищеності пристроїв Інтернету речей.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

На основі проведеного аналізу можна зробити декілька важливих висновків та сформулювати пропозиції щодо моделі захисту пристроїв Інтернету речей (IoT) від кібератак. Перш за все, важливо визнати, що складність та різноманітність IoT систем створюють виклики для їхньої безпеки. Для ефективного захисту від кібератак необхідно застосовувати комплексний підхід, який охоплює технічні, організаційні та правові аспекти. Важливо також враховувати постійну еволюцію загроз та реагувати на нові типи атак.

Пропозиції щодо покращення моделі захисту включають розвиток стандартів безпеки, підвищення рівня освіти з питань кібербезпеки, застосування штучного інтелекту для виявлення аномалій та створення механізмів взаємодії між зацікавленими сторонами. Остаточно, забезпечення безпеки Інтернету речей вимагає системного та координованого підходу залучених сторін та постійного вдосконалення заходів захисту.

- Важливо активно працювати над розвитком стандартів безпеки для IoT, що дозволить забезпечити єдність підходів та забезпечити високий рівень захищеності.
- Необхідно активізувати освітні програми з питань кібербезпеки серед користувачів IoT, розробників та інших зацікавлених сторін.
- Використання штучного інтелекту для виявлення та аналізу аномалій у поведінці IoT пристроїв може значно підвищити ефективність систем захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Williams P., Dutta I.K., Daoud H., Bayoumi M. A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things. 2022. Vol. 19. P. 100564. DOI: 10.1016/j.iot.2022.100564..
2. Kovalenko O., Kovalenko T. Knowledge Model and Ontology for Security Services. 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC). Kyiv, Ukraine, 2018. P. 1– 4. DOI: 10.1109/SAIC.2018.8516875.
3. Kovalenko O. Knowledge Driven Cyber-Convergent Systems Based on Situational Agents. IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT). 2022. P. 243–246. DOI: 10.1109/CSIT56902.2022.10000762.
4. Kovalenko O. Systems Convergence for Situational Control and Decision Making in Distributed Environments. IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). 2022. P. 344–347. DOI: 10.1109/TCSET55632.2022.9767006.
5. Ma J., Ning H., Huang R., Liu H., Yang L.T., Chen J., Min G. Cybermatics: A holistic field for systematic study of cyber-enabled new worlds. IEEE Access. 2015. Vol. 3. P. 2270–2280.
6. Madakam S., Ramaswamy R., Tripathi S. Internet of Things (IoT): A Literature Review. Journal of Computer and Communications. 2015. Vol. 3. P. 164–173. DOI: 10.4236/jcc.2015.35021.
7. Mullet V., Sondi P., Ramat E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. IEEE Access. 2021. Vol. 9. P. 23235–23263. DOI: 10.1109/ACCESS.2021.3056650

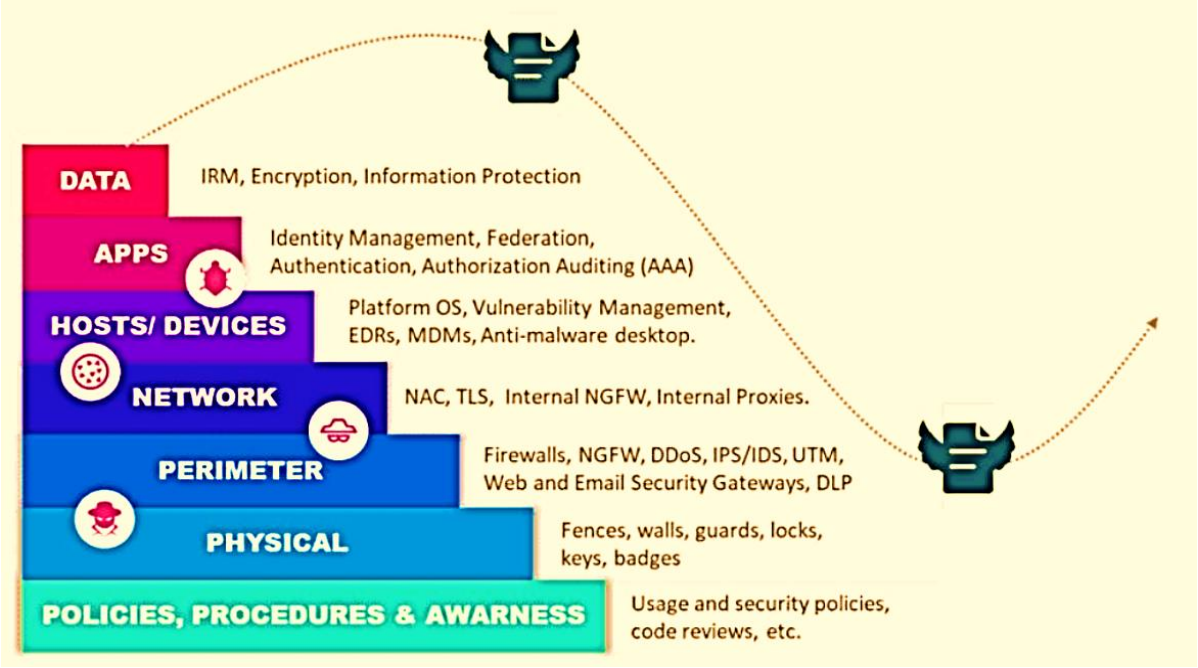
ДОДАТКИ

Додаток А

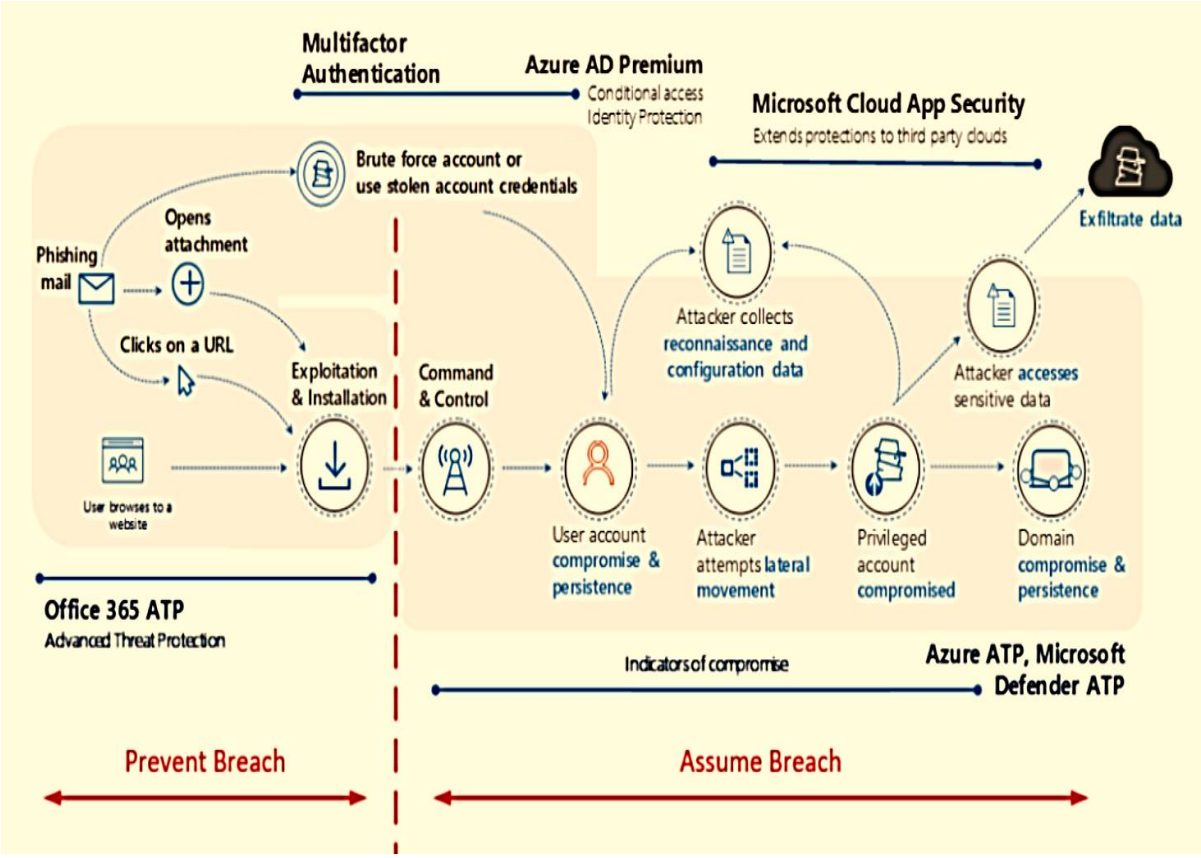
Архітектура моделі “Захист у глибину” для пристроїв Інтернету речей (IoT)

Додаток Б

Архітектура моделі «Zero Trust»

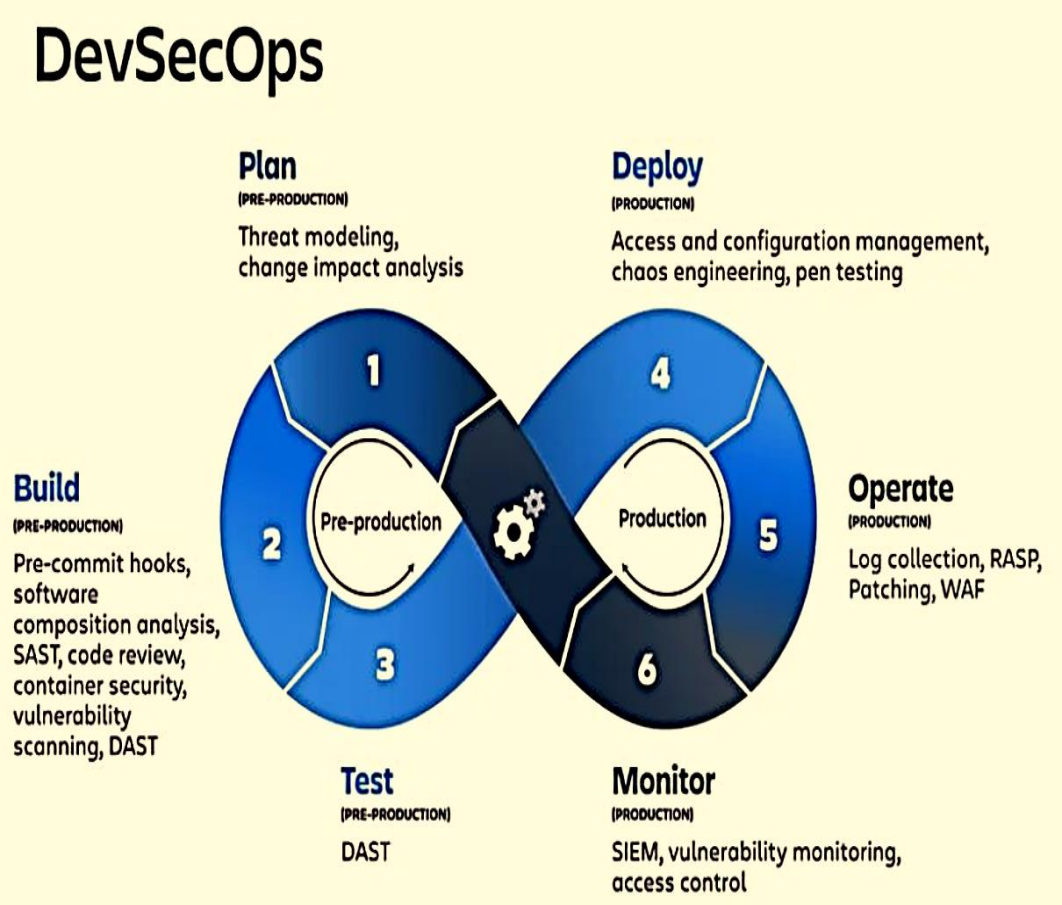


Архітектура моделі “Assume Breach”



Додаток В

Архітектура моделі “DevSecOps”



Додаток Д

Загальна структура програми розробки криптографічних алгоритмів та протоколів для захисту даних, що передаються між пристроями IoT та центральними серверами на мові Python:

1. Визначення вимог безпеки
Задати вимоги до аутентифікації, конфіденційності, цілісності даних та інші параметри безпеки.

2. Аналіз загроз та атак
Вивчити потенційні загрози безпеці та атаки, які можуть виникнути в контексті IoT та взаємодії з серверами.

3. Розробка криптографічних алгоритмів та протоколів
Написати код для створення алгоритмів шифрування, аутентифікації та інших криптографічних операцій.

4. Тестування та перевірка безпеки
Провести тести безпеки для перевірки стійкості розроблених алгоритмів та протоколів до різних видів атак.

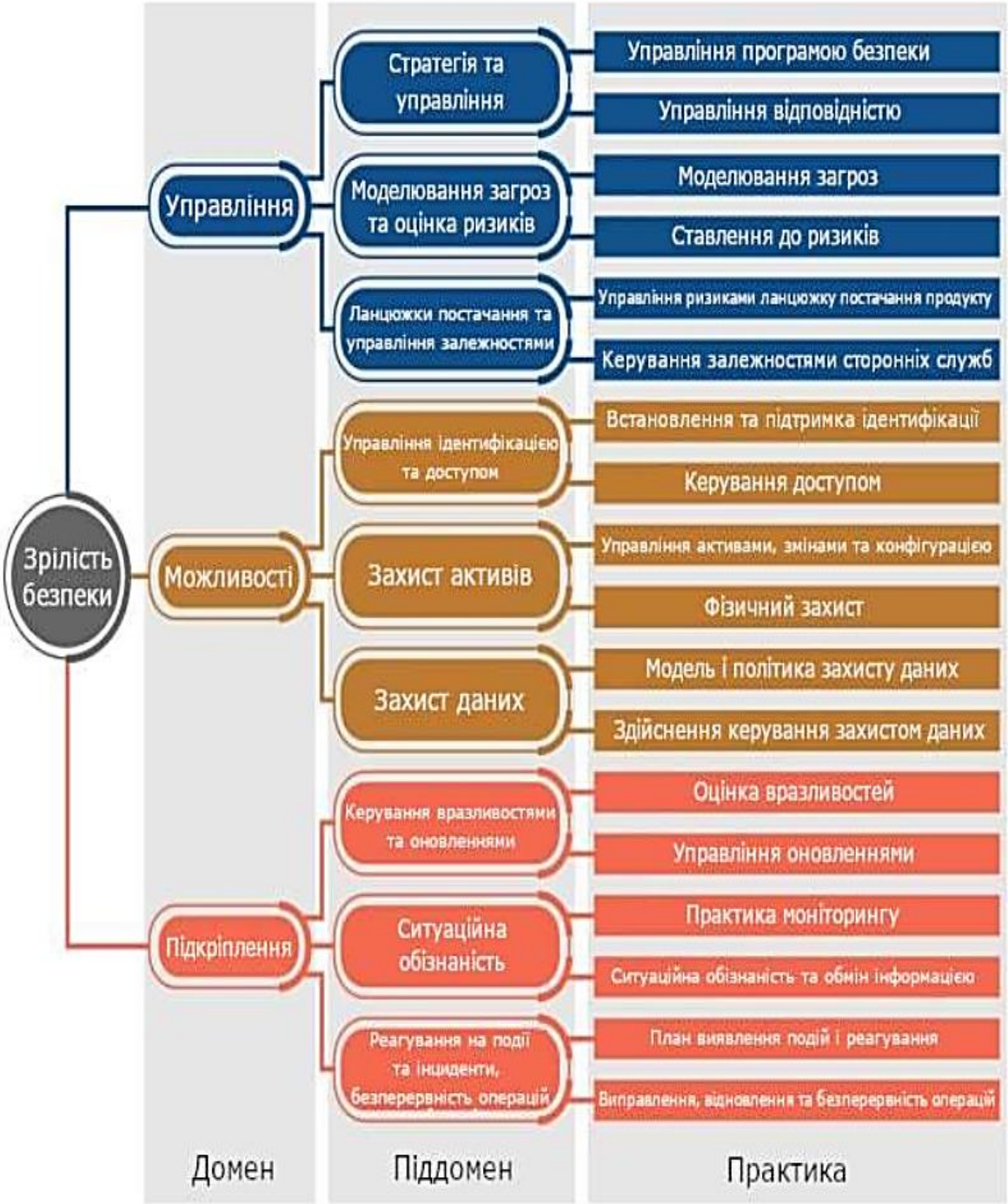
5. Імплементація в пристрої IoT та серверах
Вбудувати розроблені криптографічні алгоритми та протоколи у програмне забезпечення пристроїв IoT та центральних серверів.

6. Оновлення та підтримка
Забезпечити постійне оновлення та підтримку криптографічних механізмів з урахуванням нових загроз та вразливостей.

Додаток Ж

Структура програми, що включає методи аутентифікації та авторизації

```
import hashlib

class Authentication:
    def __init__(self, username, password):
        self.username = username
        self.password = password

    def hash_password(self):
        # Хешування пароля для зберігання у вигляді хешу
        hashed_password = hashlib.sha256(self.password.encode()).hexdigest()
        return hashed_password

    def verify_password(self, stored_password, input_password):
        # Перевірка введеного пароля зі збереженим хешем пароля
        input_password_hash = hashlib.sha256(input_password.encode()).hexdigest()
        return input_password_hash == stored_password

class Authorization:
    def __init__(self, user_roles):
        self.user_roles = user_roles

    def check_access(self, user_role, resource):
        # Перевірка доступу користувача до ресурсу на основі його ролі
        if user_role in self.user_roles:
            if resource in self.user_roles[user_role]['access']:
                return True
        return False

# Приклад використання
users = {'user1': {'password': 'password123', 'role': 'admin', 'access': ['read', 'write']},
         'user2': {'password': 'securepass', 'role': 'user', 'access': ['read']}}

# Створення об'єкту аутентифікації
auth_user1 = Authentication('user1', 'password123')
stored_password = auth_user1.hash_password()

# Перевірка пароля
print(auth_user1.verify_password(stored_password, 'password123'))  # Повинно повернути
True

# Створення об'єкту авторизації
authz = Authorization(users)

# Перевірка доступу користувача до ресурсу
print(authz.check_access('admin', 'write'))  # Повинно повернути True
print(authz.check_access('user', 'write'))   # Повинно повернути False
```

Додаток К

Ієрархія складових моделі зрілості безпеки IoT