ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ
АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження методів захисту інформації в мережах IoT»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ярослав АНДРЕЄВ
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСД-41
Ярослав АНДРЕЄВ
Ім'я, ПРІЗВИЩЕ

Керівник: Ольга ЖИДКА
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

Ступінь вищої освіти бакалавр

Спеціальність 126 Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІПЗАС
_____Каміла СТОРЧАК
«____» _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Андреєву Ярославу Олексійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Дослідження методів захисту інформації в мережах IoT

керівник кваліфікаційної роботи Ольга ЖИДКА,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» 02.2024 р. № 36

2. Строк подання кваліфікаційної роботи «31» травня 2024р.

3. Вихідні дані до кваліфікаційної роботи:
1. Науково-технічна література з теми бакалаврської роботи.
2. Архітектура мережей IoT.
3. Методи захисту мережей в IoT.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Проведення аналізу сучасних проблем безпеки мереж IoT
2. Аналіз ефективності захисних заходів у мережах IoT
3. Рекомендації та висновки щодо поліпшення безпеки мереж IoT

5. Ілюстративний матеріал: *презентація*

6. Дата видачі завдання «27» лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Планування та визначення теми	28.01.2024 - 12.02.2024	
2	Літературний огляд та збір інформації	13.02.2024 - 10.03.2024	
3	Формулювання мети та завдань	11.03.2024 - 22.03.2024	
4	Проведення аналізу сучасних проблем безпеки мереж IoT	23.03.2024 - 20.04.2024	
5	Аналіз ефективності захисних заходів у мережах IoT	21.04.2024 - 01.05.2024	
6	Рекомендації та висновки щодо поліпшення безпеки мереж IoT	02.05.2024 - 10.05.2024	
7	Редагування та корегування роботи	11.05.2024 - 15.05.2024	
8	Оформлення роботи	16.05.2024 - 20.05.2024	

Здобувач вищої освіти _____ Ярослав АНДРЕЄВ

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ольга ЖИДКА

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра :51 стор., 4 рис., 23 джерел.

Мета роботи – дослідження методів забезпечення безпеки мереж Інтернету речей (IoT) із використанням штучного інтелекту (ШІ) та оцінка їх ефективності.

Об'єкт дослідження – Захист інформації в мережах IoT.

Предмет дослідження – Методи штучного інтелекту для підвіщення рівня захисту інформації в мережах IoT.

Короткий зміст роботи: У першому розділі роботи подано основні поняття, пов'язані з Інтернетом речей, їх визначення, а також розглянуто основні проблеми безпеки. Описано взаємозв'язок між IoT та Big Data, а також методи навчання штучного інтелекту та його застосування у сфері IoT, зокрема в кібербезпеці. У другому розділі представлено аналіз світових тенденцій у сфері IoT, виявлення та аналіз вразливостей систем IoT, а також оцінка ефективності захисних заходів та реакції на кіберзагрози. Вивчено процес розробки, навчання та тестування моделей ШІ для виявлення загроз у мережах IoT, а також процес їх імплементації та постпродакшену. Третій розділ присвячено аналізу основних проблем безпеки в мережах IoT, найбільш ефективним методам захисту інформації, використаним методам машинного навчання для виявлення загроз, прикладам успішної інтеграції ШІ в системи безпеки IoT, а також рекомендаціям щодо поліпшення стандартів безпеки в IoT. У роботі висвітлено комплексний підхід до забезпечення безпеки в мережах IoT, включаючи встановлення строгих стандартів, інтеграцію ШІ для виявлення та реагування на загрози, постійний моніторинг та оновлення програмного забезпечення, а також навчання користувачів та адміністраторів.

КЛЮЧОВІ СЛОВА: ІНТЕРНЕТ РЕЧЕЙ, БЕЗПЕКА, ШТУЧНИЙ ІНТЕЛЕКТ, МАШИННЕ НАВЧАННЯ, КІБЕРБЕЗПЕКА, ВРАЗЛИВОСТІ, ЗАХИСНІ ЗАХОДИ, АНАЛІЗ ДАНИХ.

ABSTRACT

Text part of the master's level qualification work: 51 pages, 4 pictures, 9 tables, 23 sources.

The purpose of the work – to study security methods for Internet of Things (IoT) networks using artificial intelligence and evaluate their effectiveness.

Object of research – Internet of Things networks.

Subject of research – security methods for IoT networks using artificial intelligence.

Summary of the work: The first section provides basic concepts related to the Internet of Things (IoT), their definitions, and addresses key security issues. The interconnection between IoT and Big Data is described, as well as AI training methods and its application in IoT security. The second section presents an analysis of global trends in IoT, identification and analysis of IoT system vulnerabilities, and evaluation of the effectiveness of security measures and response to cyber threats. The process of developing, training, and testing AI models for threat detection in IoT networks, as well as their implementation and post-production processes, is studied. The third section is dedicated to analyzing key security issues in IoT networks, the most effective information protection methods, machine learning methods used for threat detection, examples of successful AI integration into IoT security systems, and recommendations for improving IoT security standards. The work highlights a comprehensive approach to ensuring security in IoT networks, including establishing strict standards, integrating AI for threat detection and response, continuous monitoring and software updates, and user and administrator training.

KEYWORDS: INTERNET OF THINGS, SECURITY, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, CYBERSECURITY, VULNERABILITIES, SECURITY MEASURES, DATA ANALYSIS.

ЗМІСТ

ВСТУП

Актуальність. В сучасному інформаційному суспільстві зростає значення безпеки в контексті розвитку Інтернету речей (IoT). Швидкі темпи інтеграції цифрових технологій у наш повсякденний життя призводять до необхідності пошуку ефективних заходів захисту від потенційних кіберзагроз. Актуальність теми дослідження полягає у тому, що розвиток IoT відкриває нові можливості, але одночасно створює серйозні виклики у сфері кібербезпеки.

Наукова та практична значимість цього дослідження полягає у можливості розробки ефективних систем захисту IoT в контексті підвищення рівня безпеки та захищеності інфраструктури підприємств. Це особливо актуально для України, яка шукає способи захисту власної кіберінфраструктури в умовах геополітичних напруг.

Метою даної кваліфікаційної роботи є аналіз сучасних методів та розробка ефективної системи захисту IoT на базі інтегрованих кіберзаходів. Завданнями дослідження є:

− Проведення аналізу сучасного стану захисту IoT та ідентифікація потенційних загроз.

− Розробка концепції та архітектури системи захисту IoT з використанням інтегрованих кіберзаходів.

− Впровадження та тестування розробленої системи захисту на практиці.

Оцінка ефективності та можливостей масштабування розробленої системи захисту IoT.

Об'єктом дослідження є процес захисту інформації в мережах IoT, який включає в себе аналіз, розробку та впровадження систем захисту. Предметом дослідження є методи та технології захисту IoT, а також практична реалізація розробленої системи захисту на базі інтегрованих кіберзаходів.

У даній роботі виконано:

− Аналіз науково-технічної літератури та публікацій з питань захисту IoT.

− Аналіз сучасних технологій та методів кіберзахисту.

− Аналіз новин в формі публікацій що висвітлюють проблеми бізнесу що пов’язані з темою дослідження

Отримані результати мають як наукову, так і практичну цінність. Новизна полягає у пропозиції рішень, що можуть вирішити проблему захисту IoT з використанням інтегрованих кіберзаходів, що може бути використана для підвищення рівня кібербезпеки підприємств та звичайних користувачів. Практична значимість полягає у можливості використання отриманих результатів для розробки та впровадження сучасних систем захисту IoT

1 ТЕОРЕТИЧНІ ОСНОВИ ТА СУЧАСНИЙ СТАН ДОСЛІДЖЕННЯ БЕЗПЕКИ В ІНТЕРНЕТІ РЕЧЕЙ

З швидким розвитком технологій у нашому сучасному світі мережі Інтернету речей стали не просто реальністю, а невід'ємною частиною нашого повсякденного життя. Однак, разом зі зростанням кількості підключених пристроїв і обсягу обміну даними з'являються серйозні питання щодо безпеки та конфіденційності інформації.

Це коротке введення призначене для вступу в тему захисту інформації в мережах IoT та підготовки до подальшого розгляду основних аспектів в першому розділі дипломної роботи. Ми звернемося до сучасних наукових досліджень та аналізу технічних аспектів захисту в IoT-системах, а також буде розглянуто виклики та перспективи в цій області.

1.1 Основні поняття

1.1.1 Інтернет речей: визначення, основні проблеми безпеки

Інтернет речей представляє собою мережу фізичних об’єктів, таких як пристрої, транспортні засоби, будівлі та інші «розумні» об'єкти, які обладнані датчиками, програмним забезпеченням і технологіями для обміну даними з іншими пристроями і системами через інтернет. Основною ідеєю IoT є підключення всіх об'єктів до мережі з метою автоматизації і підвищення ефективності різних процесів.

Проблеми безпеки IoT:

− Відсутність стандартизації, різноманітність пристроїв і протоколів призводить до проблем сумісності та безпеки.

− Недостатня захищеність пристроїв, багато IoT пристроїв мають обмежені ресурси для забезпечення комплексного захисту.

− Атаки на мережеву інфраструктуру, IoT пристрої можуть бути вразливими до різних типів атак, таких як DDoS атаки, підробка даних та перехоплення інформації.

− Приватність даних, збір та обробка великої кількості даних створює ризики для конфіденційності особистої інформації.

1.1.2 Взаємозв'язок Big Data та IoT

Великі Дані (Big Data) означають обробку і аналіз великих обсягів даних, що надходять з різних джерел. У контексті IoT, великі дані можуть включати дані від численних сенсорів, пристроїв, лог-файлів, соціальних мереж та інших джерел.

З огляду на значну кількість даних, які збирають пристрої Інтернету речей, постає необхідність у використанні технологій обробки та аналізу великих обсягів інформації, відомих як Big Data. У контексті IoT, Big Data стає ключовим аспектом безпеки, оскільки включає в себе обробку і зберігання величезних обсягів даних, зібраних від мільйонів підключених пристроїв.

IoT генерує значну кількість різноманітних даних, які можуть містити інформацію про фізичний стан пристроїв, їхнє місцезнаходження, параметри навколишнього середовища, а також поведінкові та операційні дані. Ці дані, як правило, є високочастотними, різноманітними за своєю природою та обсягом. Для ефективного управління та аналізу таких даних необхідні потужні обчислювальні ресурси та передові аналітичні методи, що забезпечують інтеграцію, зберігання, обробку та візуалізацію інформації в реальному часі.

Великі Дані також відіграють важливу роль у розробці моделей прогнозування та оптимізації для IoT. Наприклад, аналіз даних від сенсорів може допомогти виявити тенденції та аномалії, що сприяє покращенню оперативної ефективності та прийняттю рішень на основі даних. Завдяки аналітиці Big Data можна виявляти приховані закономірності та передбачати майбутні події, що дозволяє здійснювати проактивне обслуговування пристроїв IoT, оптимізувати витрати ресурсів та підвищувати загальну продуктивність системи.

Більшість даних, що генеруються IoT, є суттєвими для функціонування системи, а також містять конфіденційну та особисту інформацію користувачів. Оскільки ці дані можуть бути предметом кібератак, захист великих обсягів даних в IoT стає надзвичайно важливим завданням.

Застосування штучного інтелекту (ШІ) для захисту даних в IoT може включати в себе розробку алгоритмів аналізу та виявлення аномалій у великих наборах даних. ШІ може автоматизувати процеси моніторингу, виявлення вразливостей і реагування на потенційні загрози безпеці в реальному часі. Крім того, за допомогою ШІ можна розробляти інтелектуальні системи захисту, які навчаються на основі зібраних даних про попередні кібератаки і виявляють нові загрози безпеці. Такий підхід дає змогу створювати більш адаптивні та ефективні системи захисту в IoT.

Для забезпечення надійного захисту даних в IoT необхідно застосовувати багатошарові методи безпеки, які включають шифрування даних, аутентифікацію користувачів, контроль доступу, а також постійний моніторинг і аудит систем. Аналіз даних за допомогою технологій Big Data дозволяє виявляти підозрілі активності та потенційні загрози на ранніх стадіях, що підвищує рівень захищеності системи в цілому.

У висновку, взаємозв'язок між Big Data та IoT є критично важливим для ефективного управління та захисту даних. Інтеграція технологій Big Data у сферу IoT сприяє покращенню якості обслуговування, підвищенню рівня безпеки та оптимізації ресурсів, що в сукупності забезпечує стійке та безпечне функціонування систем Інтернету речей.

1.1.3 Штучний інтелект: методи навчання та застосування в IoT

Штучний інтелект (ШІ) − це галузь комп'ютерних наук, що ставить перед собою завдання створення систем, які можуть виконувати завдання, які зазвичай потребують людського інтелекту. Основна ідея полягає в тому, щоб надати

комп'ютерам здатність «мислити», «вирішувати проблеми» та «навчатися» аналогічно людям.

Основні способи навчання ШІ:

− Машинне навчання (Machine learning) − метод, за допомогою якого комп'ютерні системи вчаться на основі даних, удосконалюючи свої алгоритми на основі досвіду.

− Підкріплювальне навчання (Reinforcement learning) − система навчається шляхом спроб і помилок, отримуючи винагороди за правильні рішення.

− Навчання з учителем (Supervised learning) − система навчається на основі позначених даних, де кожен приклад має вхідні та вихідні значення.

− Навчання без учителя (Unsupervised learning) − система шукає структури в даних без попередньо зазначених прикладів.

− Глибоке навчання (Deep learning) − підвид машинного навчання, що використовує багатошарові нейронні мережі для аналізу великих обсягів даних і виявлення складних патернів.

ШІ використовує різні методи, включаючи МН, обробку природної мови, комп'ютерний зір та інші, для створення інтелектуальних систем, здатних виконувати високорівневі завдання, схожі на ті, що виконує людина, і які не можуть бути повноцінно автоматизовані традиційними методами. Таким чином, ШІ здатний вирішувати складні завдання, приймаючи рішення самостійно на основі знань, отриманих у процесі навчання. Деякі системи можуть продовжувати навчатися під час своєї повноцінної роботи, що робить їх ще більш ефективними.

1.1.3.1 Штучний інтелект та кібербезпека

Штучний Інтелект (ШІ) відіграє важливу роль у сфері кіберзахисту, де швидка та ефективна реакція на кіберзагрози є критично важливою. Його використовують для автоматизації пошуку аномалій у системах та їх усунення, що робить ШІ потужним інструментом для захисту в ІТ-просторі.

ШІ є ключовим об'єктом, що виконує корисне навантаження, підвищуючи рівень кібербезпеки систем на рівні з людиною. Один з варіантів застосування таких

систем полягає у виявленні кіберзагроз через аналіз великих обсягів даних та виявлення аномальної активності, що може вказувати на потенційні загрози.

ШІ також допомагає передбачати наступні кібератаки, аналізуючи попередні інциденти та шаблони загроз. Цей функціонал є одним з найпотужніших інструментів, що демонструє корисність ШІ у сфері кіберзахисту, оскільки він може перекрити роботу групи спеціалістів за швидкістю та продуктивністю, за умови достатніх ресурсів та якісного навчання моделі.

Не менш корисною є автоматизація відповіді на кібератаки, що включає блокування шкідливого трафіку та видалення загроз. Це може здійснюватися через блокування доступу несанкціонованих користувачів чи заражених пристроїв, а також інші форми, залежно від структури мережі.

Що стосується підвищення безпеки користувачів, ШІ може запобігати фішинговим атакам та атакам соціальної інженерії. Такі атаки можуть призвести до витоку даних або фінансових втрат для користувачів, а також до зараження комп'ютерів шкідливим програмним забезпеченням, що може поширюватися на інші пристрої в мережі, як це було у випадку з WannaCry у 2017 році і це лише один аспект з можливих з якими може допомогти впровадження ШІ в систему безпеки [1].

Загалом, застосування ШІ у кіберзахисті дозволяє підвищити ефективність виявлення, прогнозування та відповіді на кіберзагрози, забезпечуючи високий рівень безпеки для користувачів та організацій.

1.1.3.2 Використання штучного інтелекту в кібербезпеці інтернету речей

Оскільки інтернет речей - це область, де велика кількість підключених пристроїв збирає, обробляє та взаємодіє з даними в реальному часі. Застосування Штучного Інтелекту особливо у цій сфері може значно підвищити рівень кібербезпеки цієї галузі, забезпечуючи виявлення, запобігання та відповідь на потенційні загрози.

Системи штучного інтелекту можуть аналізувати великі обсяги даних, зібраних від підключених пристроїв IoT, для виявлення аномальної активності, яка може свідчити про кіберзагрози або вразливості.

Машинне навчання може використовуватися для створення моделей, які виявляють вразливі місця у пристроях та мережах IoT, допомагаючи у запобіганні можливих атак.

Як і в випадку з стандартними мережами, тут так само ШІ мають функціонал захисту від кібератак, системи штучного інтелекту можуть автоматично виявляти та заблокувати шкідливий трафік, направлений на підключені пристрої IoT, за допомогою аналізу мережевого трафіку та патернів атак.

Машинне навчання в даному випадку може використовуватися для розробки алгоритмів, на яких буде базуватись ШІ, вони виявляють атаки та вразливості у реальному часі, навчаючись на прикладах попередніх інцидентів.

Відносно прогнозування ризиків та реагування на них, це працює так само як і на звичайних мережах.

Штучний інтелект може використовуватися для аналізу даних та прогнозування можливих кіберзагроз, що дозволяє приймати запобіжні заходи та готуватися до потенційних інцидентів.

Машинне навчання допомагає у розробці систем автоматизованого реагування на кібератаки, забезпечуючи швидку та ефективну відповідь на загрози для пристроїв та мереж IoT, тим чином що максимально вдосконалює модель нейронної мережі під час процесу її навчання.

У висновку до такого варіанту підвищення рівня безпеки мережі можно констатувати що застосування штучного інтелекту для аналізу мережевого трафіку та виявлення вразливостей може значно підвищити загальний рівень кібербезпеки в IoT мережах.

Застосування штучного інтелекту у області кібербезпеки інтернету речей дозволяє створити ефективні та інтелектуальні системи, які забезпечують надійний захист від кіберзагроз для підключених пристроїв та мереж.

1.1.3.3 Практичні приклади використання бізнесом

Так як штучний інтелект стає все більш важливим інструментом для захисту від кібератак у сучасному цифровому світі. Багато компаній вже використовують ШІ для виявлення, блокування та прогнозування загроз. Нижче наведено деякі приклади реального використання штучного інтелекту компаніями для кібербезпеки.

Перший приклад це Darktrace.

Darktrace - це компанія, яка використовує технології штучного інтелекту для виявлення загроз кібербезпеці в реальному часі. Їх платформа використовує алгоритми машинного навчання для аналізу мережевого трафіку та виявлення аномальної активності, що може вказувати на кібератаки або внутрішні загрози.

Технологія що вони використовують - Enterprise Immune System для виявлення аномальної активності в мережі, як можно зрозуміти з самої назви, моделює роботу імунної системи живої істоти для виявлення потенційної загрози, система може автоматично реагувати на неї шляхом застосування захисних заходів, таких як блокування підозрілих підключень або ізоляція скомпрометованих пристроїв від мережі [2]. Крім того, система може генерувати повідомлення для спеціалістів з кібербезпеки або адміністраторів мережі, щоб вони могли вжити відповідних заходів у разі потреби. Такий підхід дозволяє не тільки виявляти загрози, але і реагувати на них швидко і ефективно, зменшуючи можливість виникнення серйозних наслідків від кібератак.

Базуючись на заяві розробників, дана система допомагає скоротити час на виявлення аномалії на 92% і вивільнити людські команди для більш стратегічної роботи.

Окрім цього Enterprise Immune System має гиганську кількість функцій до всіх стандартних програм та сервісів що зазвичай використовує бізнес при роботі, однак ми не будемо розглядати так як це не є важливою частиною висвітлювальної теми.

Другий приклад це Cylance.

Компанія Cylance використовує штучний інтелект, CylancePROTECT для розробки антивірусного програмного забезпечення нового покоління, яке виявляє та блокує загрози на основі поведінкового аналізу[3]. Їх система використовує алгоритми машинного навчання для виявлення вразливостей та аномальної активності, що дозволяє попереджати кібератаки до їх виникнення.

Їх система є мультиплатформленою, тобто її можно використовувати навіть у мобільному пристрої.

ШІ Watson від компанії IBM.

IBM Watson for Cyber Security використовує штучний інтелект для аналізу великих обсягів даних про кіберзагрози та виявлення нових патернів атак. Його система використовує машинне навчання для автоматичного аналізу безлічі даних та ідентифікації потенційних загроз[4].

Сам ШІ Watson є універсальним, створена IBM модель нейронної системи вирішує безліч проблем в різних сферах, тому назвати його повноцінним вирішенням як мінімум для IoT систем я не можу.

Ці приклади демонструють, як компанії використовують штучний інтелект для підвищення ефективності своїх систем кібербезпеки та захисту від кібератак. Отже застосування штучного інтелекту дозволяє автоматизувати процеси виявлення, аналізу та реагування на загрози, що забезпечує більш високий рівень безпеки для користувачів та організацій і дане рішення не є експериментальним його готові впроваджувати бізнеси.

1.2 Огляд літератури та аналіз сучасного стану проблеми

1.2.1 Загальні аспекти захисту інформації в мережах IoT

На сьогодні через тенденцію швидкого розвитку технологій, концепція мереж Інтернету речей стала ключовою складовою інформаційного суспільства. IoT забезпечує зв'язок між фізичними пристроями та Інтернетом, що дозволяє збирати, обробляти та обмінюватися даними без прямої людської участі. Однак, разом зі

зростанням популярності IoT з'являються серйозні питання щодо безпеки та конфіденційності даних, які ці мережі обробляють.

Основні аспекти захисту інформації в мережах IoT включають:

− Автентифікація та авторизація, це забезпечення того, що доступ до пристроїв та даних отримують тільки авторизовані користувачі та пристрої. Це дозволяє зменшити ризик несанкціонованого доступу та забезпечити безпеку даних [5].

− Захист даних під час передачі та зберігання шляхом використання криптографічних методів. Шифрування гарантує, що навіть у разі перехоплення даних вони залишаться недоступними для зловмисників.

− Використання методів виявлення та запобігання різним типам кібератак, таким як DDoS атаки, зломи, перехоплення даних тощо. Це допомагає забезпечити стабільну та безпечну роботу мережі IoT [6].

− Забезпечення того, що особисті дані користувачів залишаються конфіденційними і не потрапляють до небажаних рук. Конфіденційність є важливим аспектом для збереження довіри користувачів до IoT.

Це є основою безпеки і не тільки для мереж IoT, однак, через те, що часто не дотримуються ці правила, або через вразливості в пристроях, виникають серйозні проблеми. Це лише підкреслює необхідність дотримання та покращення цих аспектів для уникнення проблем з безпекою. Наприклад, нещодавно стався витік даних у компанії Fujitsu, де хакери отримали доступ до конфіденційної інформації через вразливість в їх мережі, що лише підтверджує важливість надійного захисту в мережі [7]. Конкретніше спричинило це шкідливе програмне забезпечення, яким було інфіковано декілька комп'ютерів співробітників що мали доступ до мережі компанії.

1.2.2 Виклики безпеки в мережах IoT

Дослідження, проведене Акіл-ур-Рехманом та співавторами, відображає актуальний стан наукової думки щодо проблем безпеки та приватності в мережах

IoT. Вони визначають основні загрози та ризики, що виникають у зв'язку з розширенням використання IoT, і надають важливі вказівки для подальших досліджень у цій галузі [8].

Багато пристроїв IoT мають обмежені ресурси для забезпечення повного захисту, що робить їх вразливими до атак. Недостатня обчислювальна потужність та пам'ять обмежують можливості впровадження складних методів захисту.

Через недостатній рівень захисту існує ризик витоку конфіденційних даних. Це може призвести до серйозних наслідків для користувачів, включаючи фінансові втрати та порушення приватності.

Можливість використання IoT для шпигунства та незаконного збирання інформації. Пристрої можуть бути використані для несанкціонованого збору даних про користувачів. Це створює ризики для конфіденційності та безпеки особистих даних.

Вразливості мереж IoT можуть призвести до серйозних наслідків для критичних систем, таких як енергетичні мережі, транспортні системи тощо. Це може мати катастрофічні наслідки для суспільства та економіки.

Ці виклики вказують на необхідність розробки нових та вдосконалення існуючих методів захисту інформації в мережах IoT. Важливо враховувати специфічні вимоги та обмеження пристроїв IoT при розробці цих методів, щоб забезпечити ефективний захист.

1.2.3 Сучасні методи та засоби захисту інформації в мережах IoT

На сьогодні існує безліч методів та засобів захисту інформації в мережах IoT.

Наприклад шифрування даних, за допомогою використання сучасних криптографічних методів для захисту даних під час передачі та зберігання. Це включає використання алгоритмів, таких як AES, RSA, та ECC, які забезпечують високу ступінь захисту даних [9].

Тому слід розібрати що означають дані абревіатури:

− AES (Advanced Encryption Standard) − симетричний алгоритм шифрування, який використовується для захисту даних завдяки своїй високій швидкості та стійкості до атак. AES підтримує ключі довжиною 128, 192 та 256 біт.

− RSA (Rivest-Shamir-Adleman) − асиметричний криптографічний алгоритм, що використовується для безпечної передачі даних. RSA забезпечує безпеку завдяки складності факторизації великих простих чисел і зазвичай застосовується для шифрування ключів та цифрових підписів.

− ECC (Elliptic Curve Cryptography) − асиметричний алгоритм шифрування, що базується на алгебраїчній структурі еліптичних кривих над скінченними полями. ECC забезпечує аналогічний рівень безпеки, як і RSA, але з меншими розмірами ключів, що робить його більш ефективним для використання в обмежених обчислювальних ресурсах пристроїв IoT.

− IDS(Intrusion Detection System) − за допомогою програмних та апаратних засобів для виявлення та реагування на підозрілі активності в мережі. IDS допомагають виявляти аномалії та потенційні загрози у реальному часі.

Що є достатньо серйозним заходом безпеки що бере на себе частину роботи інженера з безпеки або адміністратора мережі.

Але якщо говорити про найпростіші та найефективніші заходи для поліпшення рівня безпеки мережі то перше місце посідає саме аутентифікація та авторизація.

Його принцип роботи це предоставлення доступу до пристроїв та даних тільки авторизованим користувачам. Це включає використання методів багатофакторної аутентифікації, біометричних даних та інших технологій.

Однак оскільки ідеального пристрою та програми з точки зору безпеки, що являє собою ще і складну та водночас корисну систему, що проводить спілкування з іншими системами, не може існувати тому для того щоб забезпечити високий рівень безпеки для такого пристрою чи програми достатньо його «підтримувати», що означає регулярні оновлення програмного забезпечення, встановлення останніх оновлень та патчів для усунення відомих вразливостей. Регулярні оновлення забезпечують актуальність та безпеку програмного забезпечення.

Також не треба забувати про базову, для кожного адміністратора мережі що відповідає за безпеку, річь - використання мережевих екранувань (Firewall), це те що представляє захист мережі від несанкціонованого доступу за допомогою фільтрації трафіку. Firewalls допомагають контролювати та обмежувати доступ до мережевих ресурсів [9].

1.2.4 Проблеми існуючих методів захисту

Незважаючи на наявність багатьох методів захисту, існують певні проблеми та обмеження.

Обмежені ресурси пристроїв, багато IoT пристроїв мають низьку обчислювальну потужність та обмежену пам'ять, що ускладнює впровадження складних методів захисту. Це призводить до необхідності розробки легких та ефективних алгоритмів захисту.

Сумісність та стандартизація, різноманітність пристроїв та протоколів ускладнює забезпечення універсального захисту. Відсутність загальноприйнятих стандартів безпеки створює труднощі в інтеграції різних систем.

Віддалений доступ, здійснення віддаленого доступу до IoT пристроїв через Інтернет може бути критичним з точки зору безпеки, якщо не вжиті відповідні заходи захисту. Віддалений доступ підвищує ризик атак та несанкціонованого доступу.

Складність управління, зростаюча кількість IoT пристроїв ускладнює їхнє централізоване управління та моніторинг. Це вимагає розробки ефективних методів управління та моніторингу для забезпечення безпеки [10].

Незважаючи на ці проблеми, важливо продовжувати розробляти та вдосконалювати методи захисту, щоб забезпечити безпеку та конфіденційність даних у мережах IoT.

1.3 Основні принципи безпеки в мережах Інтернету речей

У цьому розділі розглянуті основні принципи, які слід враховувати для забезпечення безпеки в мережах Інтернету речей. З огляду на виявлені проблеми та загрози, що існують у IoT-системах, наступні принципи мають велике значення для забезпечення ефективного захисту:

− Принцип мінімізації атакованості(Attack Surface Minimization), менша кількість вразливостей у системі зменшує ризик атак. Розробники мають мінімізувати атакованість системи, обмежуючі доступ до критичних ресурсів та скорочуючи потенційні шляхи атак.

− Принцип захисту доступу(Access Control), контроль доступу до системи є ключовим аспектом безпеки. Необхідно ефективно управляти правами доступу, використовувати сильні методи аутентифікації та авторизації, щоб гарантувати доступ тільки авторизованим користувачам або пристроям.

− Принцип шифрування(Encryption), шифрування даних на всіх етапах їхнього обміну допомагає захистити конфіденційні дані від несанкціонованого доступу. Використання сильних алгоритмів шифрування є важливим аспектом забезпечення безпеки в мережах IoT.

− Принцип надійності та стійкості (Resilience), IoT-системи повинні бути стійкими до різноманітних загроз та витоків даних. Розробники мають передбачати можливі сценарії збоїв та розробляти заходи для їхнього виявлення та відновлення.

− Принцип постійного моніторингу та виявлення загроз(Continuous Monitoring and Threat Detection), постійний моніторинг системи дозволяє вчасно виявляти потенційні загрози та реагувати на них. Використання засобів виявлення аномальної поведінки та загроз дозволяє ефективно виявляти та запобігати можливим атакам.

Дослідження, проведене Акіл-ур-Рехманом та співавторами, відображає актуальний стан наукової думки щодо проблем безпеки та приватності в мережах IoT. Вони визначають основні загрози та ризики, що виникають у зв'язку з

розширенням використання IoT, і надають важливі вказівки для подальших досліджень у цій галузі [8].

Обмежені ресурси пристроїв, багато пристроїв IoT мають обмежені ресурси для забезпечення повного захисту, що робить їх вразливими до атак. Недостатня обчислювальна потужність та пам'ять обмежують можливості впровадження складних методів захисту.

Ризик витоку конфіденційних даних, через недостатній рівень захисту існує ризик витоку конфіденційних даних. Це може призвести до серйозних наслідків для користувачів, включаючи фінансові втрати та порушення приватності.

Шпигунство та незаконний збір інформації, пристрої можуть бути використані для несанкціонованого збору даних про користувачів. Це створює ризики для конфіденційності та безпеки особистих даних.

Вразливості в критичних системах, вразливості мереж IoT можуть призвести до серйозних наслідків для критичних систем, таких як енергетичні мережі, транспортні системи тощо. Це може мати катастрофічні наслідки для суспільства та економіки.

Ці виклики вказують на необхідність розробки нових та вдосконалення існуючих методів захисту інформації в мережах IoT. Важливо враховувати специфічні вимоги та обмеження пристроїв IoT при розробці цих методів, щоб забезпечити ефективний захист.

2 АНАЛІЗ ЕФЕКТИВНОСТІ ЗАХИСНИХ ЗАХОДІВ ТА РЕАКЦІЇ НА КІБЕРЗАГРОЗИ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ ТА ОГЛЯД СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

У цьому розділі проводиться детальний аналіз функціонування та безпеки мереж Інтернету речей. Проводячи огляд фактичних даних та результатів аналізу, ми розглянемо різні аспекти безпеки в IoT-системах та намагатимемося зрозуміти їх вплив на сучасні технологічні середовища.

У першому підрозділі ми проведемо детальний аналіз частоти та типів кібератак на системи IoT, розглянемо використання експлойтів та оцінимо ефективність існуючих захисних заходів. У другому підрозділі ми вивчимо функціонування бази дослідження протягом періоду не менше двох років, а також проаналізуємо особливості та вразливості мереж IoT. У третьому підрозділі ми зосередимося на тлумаченні отриманих результатів та формулюванні висновків, які дозволять нам краще зрозуміти стан безпеки в мережах Інтернету речей та надати рекомендації щодо подальших досліджень у цій області.

Цей розділ відіграє важливу роль у розумінні складнощів та викликів, з якими стикаються системи IoT, а також дозволить нам зосередитися на покращенні безпеки цих систем у майбутньому.

2.1 Фактологічна інформація та аналіз результатів

Цей підрозділ присвячений аналізу фактів та результатів досліджень у сфері безпеки в мережах Інтернету речей. У підрозділі було проведено аналіз досліджень з безпеки в мережах Інтернету речей. Дані досліджень вказують на стійке зростання кількості підключених пристроїв, що призводить до збільшення обсягу даних і ризику кібератак. Найпоширенішими вразливостями систем IoT є недостатній рівень шифрування даних, використання слабких паролів та відсутність регулярних оновлень програмного забезпечення. Не зважаючи на застосування сучасних

методів захисту, IoT-пристрої залишаються вразливими до атак через швидкий розвиток нових загроз. Це свідчить про необхідність постійного вдосконалення методів захисту та впровадження новітніх технологій для забезпечення безпеки в мережах Інтернету речей.

2.1.1 Світова тенденція в сфері IoT

В світі вже який рік кількість IoT девайсів росте, разом з цим збільшується і кількість систем що базуються на даних елементах, дана тенденція стосується багатьох сфер бізнесу, серед яких найбільшу частину займає користувацька сфера, іншими словами сфера побуту людини.

Базуючись на інформації за минулі роки та інформації що базуються на прогнозі до 2025 року, кількість підключень девайсів до системи інтернет і в подальшому буде збільшуватися від року в рік, і ця тенденція буде зберігатися і в подальшому [11]. Що означає і рост ринку даного напрямку.

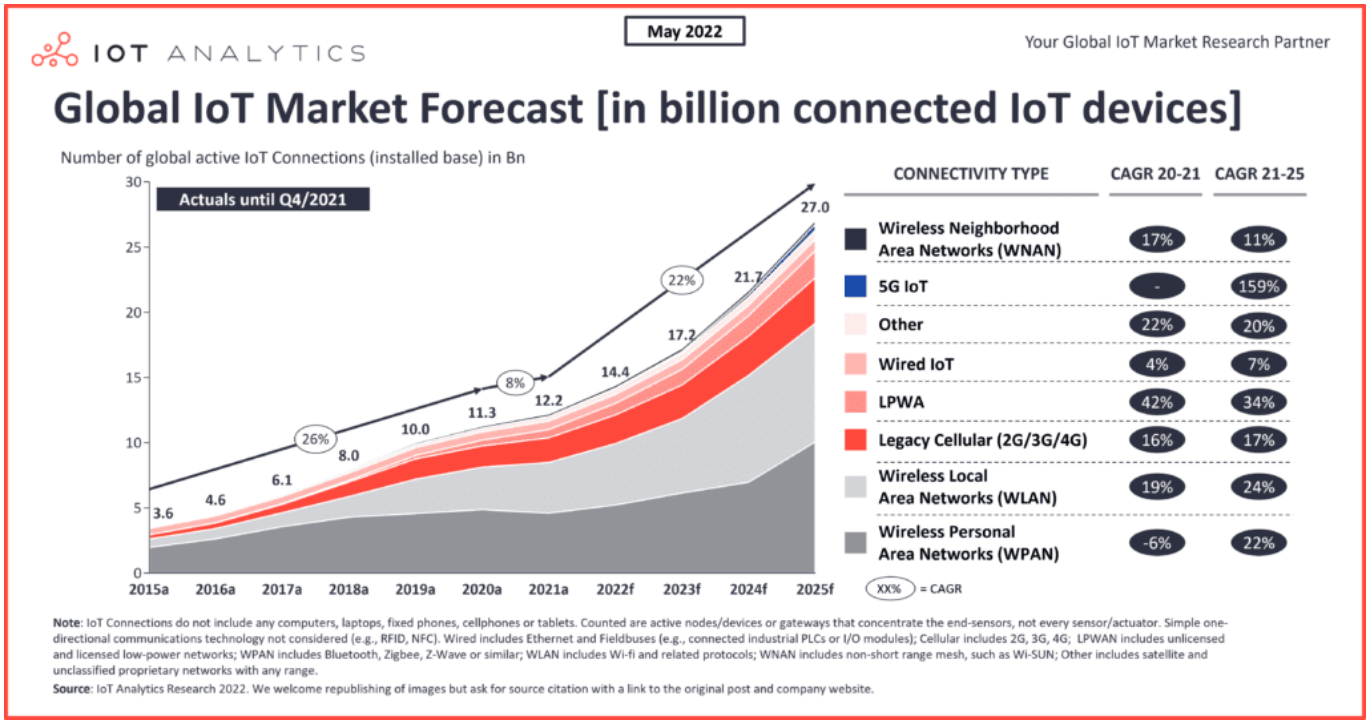


Рис. 2.1 Прогноз маркету IoT девайсів [12]

На сьогоднішній день в світі постійно з'являються державні або приватні ініціативи для поліпшення життя та/або для підвищення ефективності процесів промислового сектору або для домашнього використання.

Однак великий процент таких проектів закінчують своє існування тільки через одну основну причину, це проблема з безпекою.І процесі інтеграції пристроїв та систем пристроїв до структур в яких вони не були передбачені виникає велика кількість проблем, однак найкритичніша серед них це проблема безпеки. Розглянемо такі випадки не гіпотетично, а з реальних проектів у світі.

Базою даних прикладів буде стаття «Захист персональних даних в сфері Інтернет речей» [13].

Почнемо з випадком у Нідерландах, де був відхилений проект по створенню інтелектуальних систем електромереж на основі «розумних» лічильників, який в теорії крім підвищення рівня комфорту людей привів до підвищення рівня автоматизації міста, що в свою чергу стало б позитивним прецедентом для майбутніх проектів такого формату. Однак він все ж був відхилений на підставі того що був шанс того що збір актуальної інформації про рівень споживання електроенергії, та зберигання цієї інформації і використання її для подальшого аналізу може призвести до того що ця інформація буде вкрадена зловмисниками для розкриття способу життя людини, зокрема коли ця людина знаходиться в квартирі, а коли ні, на основі використання електроенергії.

Ця ситуація гіпотетичним витоком даних може бути може здатися просто не приемною, однак проблеми з безпекою IoT девайсів можуть бути більш деструктивними та небезпечними для життя, тому розглянемо інший приклад того як проблеми з безпекою можуть потенційно призвести до серйозної шкоди, як метеріальної так і здоров'ю [14].

Класифікується як IoT і системи автомобіля що підключені до інтернету, тому обговоримо інцидент у липні 2015 року. «Білі» хакери продемонстрували можливість дистанційного взлому бортового комп’ютера, автомобіля Jeep Cherokee 2014. Ці дослідними змогли відключити систему маніпуляції коробкою передач та заблокувати тормоза. Саме ця праця призвела до того що компанія Fiat Chrysler була

вимушена виправляти цю вразливість у понад 1,4 млн автомобілів, що призвело як до збитків так і до зменшення рівня довіри людей до безпеки «розумних» систем в автомобілях. В тому ж році були і інші випадки знаходження критичних вразливостей в автомобілях і інших виробників, що могли призвести як до смертельної ситуації так і до банальної крадіжки автомобіля. У висновку більшість вразливостей було усунено і ці прецеденти підштовхнули рівень безпеки, однак це підвищило рівень недовіри до цієї технології що в свою чергу зменшило її популяризацію публічну, через що фінансування розвитку цієї технології потенційно зменшилось

Щодо більш небезпечних ситуацій, у медицинському обладнанні може використовуватися інтернет зв'язок, однак більшість лікарів проти цього, через небезпеку хакерських атак. Наприклад, кардіолог одного з колишніх віце-президентів США наполягав щоб його пацієнт мав кардіостимулятор без функції Wi-Fi контролю. Так як за його словами, це могли б використати хакери для замаху на життя цього політика.

Усі ці конкретні випадки описують стуацию у всій сфері IoT.

Іншими словами весь час через низький рівень захисту IoT елементів, впливає на розповсюдженість та популярність цієї технології, саме тому розвиток захищеності в даній сфері такий необхідний елемент для процвітання цього напрямку та більшої інтеграції нього у наше життя.

2.1.2 Виявлення та аналіз вразливостей систем IoT

У цьому підрозділі проведено детальне дослідження вразливостей систем Інтернету речей. Виявлено та проаналізовано основні проблеми, що виникають у зв'язку з недоліками в безпеці IoT.

Один із провідних інструментів аналізу кібербезпеки IoT сегменту - це вивчення частоти та типів кібератак, що спрямовані на системи IoT. Відносно тенденцій кількості кібератак саме на IoT системи або системи що тічно пов’язані з ними, наразі тенденція присутня на зростанні объему таких випадків, згідно з

піврічним оновленням звіту SonicWall про кіберзагрози за 2023 рік, за перші шість місяців 2023 року кількість шкідливих програм для Інтернету речей зросла на 37% у всьому світі, що призвело до 77,9 мільйона атак, порівняно з 57 мільйонами атак за перші шість місяців 2022 року [15].

Цього року в Північній Америці кількість атак зменшилася на 3%, але в Азії та Латинській Америці спостерігалося тризначне зростання - 170% і 164% відповідно. Що стосується країн з найбільшим максимумом і та мінімум кібератак на цей сектор, то кількість атак на IoT в Індії зросла на приголомшливі 311%, а в Німеччині знизилася на 30%.

Що стосується показників галузей, то хороша новина полягає в тому, що в державному управлінні та освіті кількість атак скоротилася на 73%, у фінансах та охороні здоров'я - на 60%, і лише в роздрібній торгівлі спостерігається зростання на 13%.

Прикладом кібератаки на IoT може бути атака типу DDoS (розподілена відмова в обслуговуванні) що є різновид хакерської атаки, яка перевантажує пропускний канал, порушуючи роботу сервісу, яка є дуже ефективною у перекриванні роботи пристроїв IoT та призводить до втрати доступу для легітимних користувачів, такий тип атаки також називають «флудом», цей термін в контексті кібербезпеки використовується для опису атак, які спрямовані на переповнення цільової системи або мережі великою кількістю запитів або даних, зазвичай штучно згенерованими. Інші типи атак, такі як віруси та програми вимагачі, також широко розповсюджені та мають серйозний вплив на безпеку мереж IoT.

Перелік основних видів «флуду» можна подати так [16].

Атаки на базі протоколу ICMP:

− Smurf-атака, найпростіший і найбільш примітивний спосіб «флуду», при якому зловмисник відправляє широкомовний запит ICMP ECHO-REQUEST з IP-адресою жертви в якості відправника, що призводить до отримання жертвою запитів ICMP ECHO-REPLY від усіх хостів-отримувачів.

Атаки на базі TCP протоколу:

− SYN flood.

− PSH flood.

− ACK flood.

Атаки на базі протоколу UDP:

− UDP flood, атака, при якій заповнюються випадковими байтами UDP-пакети з подальшим їх відправленням на обчислювальний ресурс жертви.

− Атака з використанням протоколу Generic Routing Encapsulation (GRE).

− DRDoS (розподілений відбивний відмова в обслуговуванні). Ця атака полягає в перенаправленні відповідей жертви на власну IP-адресу.

− DNS flood, специфічний випадок попередньої атаки, що полягає в завантаженні 53 порту сервера DNS запитами про його доменне ім'я або IP-адресу фіктивного домена, що призводить до залучення всіх ресурсів сервера на пошук запису, якого не існує.

Атака на базі протоколу HTTP - це досить простий різновид DoS/DDoS атак, при якому відправляються невеликі за розміром HTTP GET або POST запити, наповнені випадковими байтами, на об’єкт атаки.

Окрім «флуду» є ще цілий перелік способів атаки на IOT системи такі як:

− Атаки на пристрої безпеки, зловмисники можуть скористатися відомими вразливостями в програмному забезпеченні пристроїв IoT або скерувати атаку на слабко захищені мережеві точки. Вони можуть використовувати збої безпеки, які дозволяють отримати несанкціонований доступ до пристроїв або отримати конфіденційну інформацію.

− Викрадення даних, зловмисники можуть використовувати шкідливе програмне забезпечення або методи соціальної інженерії для отримання доступу до конфіденційної інформації, що передається між пристроями IoT. Це може включати особисті дані користувача, медичну інформацію або комерційну інтелектуальну власність.

− Маніпулювання фізичними пристроями, зловмисники можуть намагатися використати фізичний доступ до пристроїв IoT для виконання несанкціонованих дій, таких як зміна налаштувань, встановлення шкідливого програмного забезпечення або видалення даних.

− Атаки на мережевий рівень, зловмисники можуть перехоплювати або змінювати трафік між пристроями IoT та іншими мережевими пристроями або серверами, що може призвести до витоку конфіденційної інформації або зміни взаємодії між пристроями.

− Фізичні атаки, вони можуть включати фізичну руйнівну дію на пристрої IoT, таку як злам або знищення пристроїв, що може призвести до втрати даних або перерви в роботі мережі.

Велика кількість вразливостей в системах IoT зазвичай є наслідком невиконання рекомендацій та недосконалості в самий системі. Наприклад, використання стандартних паролів на пристроях, недоліки у прошивці, а також недостатня автентифікація можуть викликати серйозні проблеми. Зловмисники активно використовують ці вразливості, використовуючи експлойти(комп'ютерна програма, або просто «шкідливе програмне забезпечення», частина програмного коду або послідовність команд, задача якого за допомогою вразливості в програмному забезпеченні для того щоб розпочати атаки на комп'ютерну систему.), щоб отримати доступ до систем та даних, а також використовувати їх у шкідливих цілях.

2.1.3 Оцінка ефективності захисних заходів та реакції на кіберзагрози

У цьому підрозділі проведено оцінку ефективності захисних заходів та реакції на кіберзагрози у мережах Інтернету речей.

Elimination (Усунення)

Усунення є найбільш ефективним рівнем захисту, оскільки повністю видаляє джерело загрози або вразливості. У контексті кібербезпеки усунення може включати в себе видалення застарілого або небезпечного програмного забезпечення, відключення небезпечних служб або функцій, та ліквідацію шкідливих компонентів у мережі.

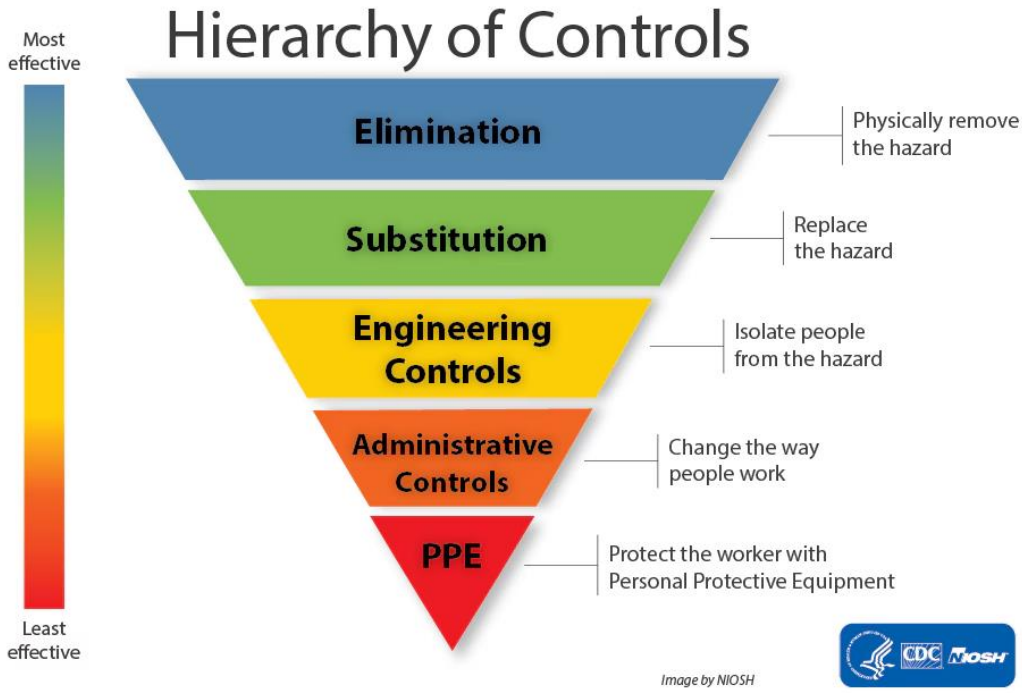


Рис. 2.2 Візуалізація ієрархії рівнів захисту [17]

– Чим представляє собою цей рівень, видалення всіх потенційно небезпечних елементів з IoT-системи.

– Що в ньому міститься/як функціонує, наприклад, видалення небезпечних або скомпрометованих IoT-пристроїв з мережі, застосування патчів для усунення вразливостей у програмному забезпеченні.

– Як він підвищує рівень безпеки, усунення джерела загрози зменшує потенційні шанси для атакуючих використати ці вразливості, тим самим забезпечуючи максимальний рівень захисту.

Substitution (Замінення)

Замінення менш безпечних елементів на більш безпечні альтернативи. Це може включати заміну небезпечного програмного забезпечення або обладнання на більш безпечні аналоги.

– Чим представляє собою цей рівень, заміна небезпечних елементів на безпечніші.

− Що в ньому міститься/як функціонує, наприклад, заміна старих протоколів зв'язку на більш сучасні та захищені, використання безпечних сертифікатів для аутентифікації.

− Як він підвищує рівень безпеки, підвищення безпеки досягається шляхом впровадження більш надійних і перевірених рішень, що знижує ризики компрометації системи.

Engineering Controls (Інженерні заходи)

Інженерні заходи включають в себе проектування системи таким чином, щоб запобігти або обмежити доступ до вразливих елементів. Це може включати в себе застосування міжмережевих екранів, систем виявлення вторгнень, та інших технічних засобів контролю.

− Чим представляє собою цей рівень, впровадження технічних засобів для запобігання загрозам.

− Що в ньому міститься/як функціонує, використання міжмережевих екранів (файрволів), систем виявлення вторгнень (IDS), розмежування мережевих сегментів.

− Як він підвищує рівень безпеки, зменшує можливість несанкціонованого доступу та знижує ризик поширення атак по мережі.

Administrative Controls (Адміністративні заходи)

Адміністративні заходи включають в себе розробку і впровадження політик, процедур та інструкцій для підвищення рівня безпеки. Це можуть бути політики управління доступом, навчання співробітників, регулярний аудит безпеки та інші організаційні заходи.

− Чим представляє собою цей рівень, встановлення правил і процедур для підвищення безпеки.

− Що в ньому міститься/як функціонує, політики управління доступом, навчання персоналу з питань безпеки, регулярні аудити та перевірки безпеки.

− Як він підвищує рівень безпеки, забезпечує правильне використання технічних засобів і знижує ризик людських помилок.

Personal Protective Equipment (PPE) (Особисті захисні засоби)

У контексті кібербезпеки особисті захисні засоби можуть включати використання засобів захисту інформації, таких як антивірусне програмне забезпечення, засоби шифрування, двофакторна аутентифікація та інші персональні заходи безпеки.

− Чим представляє собою цей рівень, використання засобів захисту інформації для окремих користувачів.

− Що в ньому міститься/як функціонує, антивірусне ПЗ, шифрування даних, двофакторна аутентифікація, використання VPN.

− Як він підвищує рівень безпеки, захищає індивідуальних користувачів та їх пристрої, знижуючи ризик компрометації через особисті вразливості.

Оцінка ефективності захисних заходів та реакції на кіберзагрози в IoT-системах є критично важливим аспектом забезпечення безпеки. Застосування ієрархії контролю, яка включає усунення, замінення, інженерні, адміністративні заходи та особисті захисні засоби, дозволяє забезпечити всебічний захист IoT-систем. Кожен рівень має свої переваги та функціонує для підвищення загального рівня безпеки, знижуючи ризики компрометації та підвищуючи стійкість до кіберзагроз. Такий підхід забезпечує надійну та комплексну систему захисту, здатну протистояти сучасним викликам у сфері кібербезпеки.

2.2 Аналіз ефективності захисних заходів та реакції на кіберзагрози в мережах Інтернету речей

Аналіз різних систем Інтернету речей показав, що більшість з них мають обмежені можливості виявлення кіберзагроз. Згідно з дослідженням, компанії Gartner понад 80% організацій впровадили Інтернет речей, і майже 20% організацій виявили атаку на основі IoT за останні три роки [18]. Проте менше третини IT-директорів впевнені, що їхні служби інформаційної безпеки можуть надійно оцінити та зменшити ризики, пов'язані з Інтернетом речей.
Що означає доволі велику недовіру до захищеності IoT систем.

Деякі системи Інтернету речей мають реакцію на загрози, проте це зазвичай вимагає втручання операторів систем. З особистих спостережень можу заявити шо

доволі велика частина компаній мають автоматичні системи захисту від кіберзагроз, однак кількість компаній що покладаються тільки на ручне втручання при виникненні кіберзагрози, не менша ніж кількість компаній що використовують автоматичні рішення.

Багато систем Інтернету речей застосовують обмежений набір заходів безпеки. Згідно з інформацією з звіту на стан 2020 року 98% процентів IoT пристроїв не шифрують дані які передають/обробляють, а на стан 2019 рік процент нешифрованого трафіку був в межах 91% [19][20].

Не варто вважати, що дані дослідження повноцінно передають точний відсоток або весь спектр проблеми, але можна точно сказати, що з шифруванням і IoT сфері є серйозні проблеми.

Потенційно ця проблема пов'язана з ним що підключені пристрої часто швидко виводяться на ринок виробниками, які допускають доволі очевидні, але здебільшого легко запобіжні помилки в процесі проектування, через те що банально не планують великий рівень безпеки у таких системах через те що зачасту вважається що такі системи можуть містити критичні дані, однак зачасту навіть глибоко технічна інформація може використовуватися злочинцями для шантажу або більш серйозних злочинів. Потім їх охоче купують підприємства, які часто не беруть ці помилки до уваги, і розгортають у своїх мережах. Звідти зловмисники знаходять їх за допомогою простого пошуку shodan і знаходять легку точку проникнення на підприємство.

І все ж - незалежно від стану безпеки - Інтернет речей нестримно зростає.

Багато операторів систем Інтернету речей не мають достатньої підготовки для реагування на кіберзагрози, в особливості якщо її складність вища за стандартні методи, які хакери використовують в більшості випадків. Для поліпшення кількості позитивних випадків відбиття кібератак, компанії повинні регулярно проводити тренінги та курси для актуалізації навичок адміністраторів IOT мереж

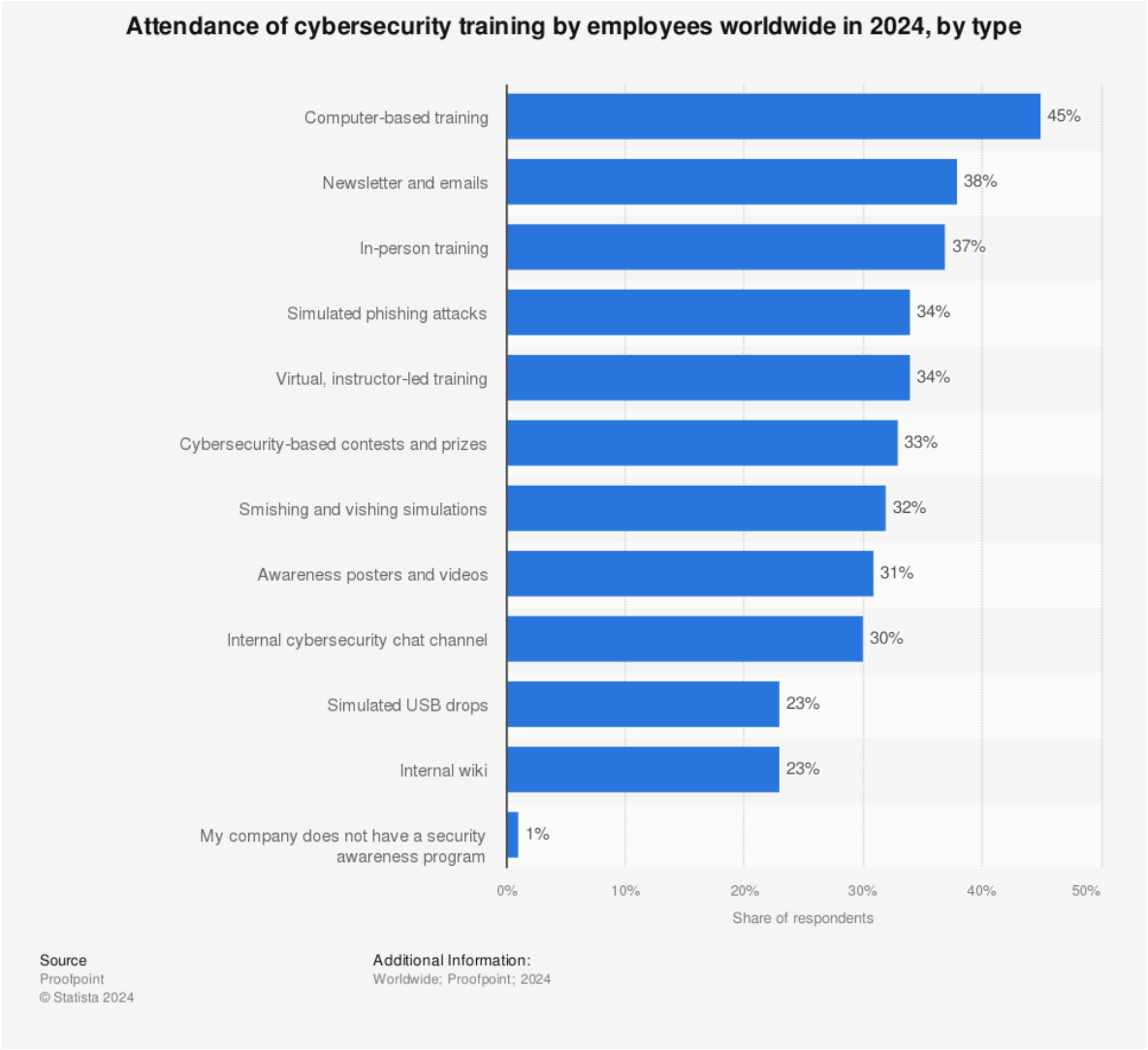


Рис. 2.3 Діаграма відвідування працівниками тренінгів з кібербезпеки в усьому світі по типам тренінгу[21]

Базуючись на даній статистиці менше половини робітників відвідують тренінги що відносяться до кібербезпеці, але ця статистика відноситься до кожного працівника компаній, а не тільки тих хто безпосередньо впливає на безпеку, тому ці цифри не такі критичні як може здатися. Однак все одно нам недоступна інформація про регулярність чи не регулярність таких подій.

На основі оцінки поточного стану безпеки можна передбачити подальші інциденти в мережах Інтернету речей. Згідно зі звітом, кількість кібератак на системи Інтернету речей очікується зрости на 300% до 2025 року відносно 2015 року та збитки від кібератак становитимуть близько 10,5 трильйонів доларів США

щорічно [22]. Це свідчить про те, що з ростом використання технологій Інтернету речей та збільшенням кількості підключених пристроїв, ймовірність кібератак також зростатиме. Відповідно, можна зробити висновок, що зростання ринку сфери Інтернету речей буде супроводжуватися збільшенням частоти та кількості кібератак на ці системи.

Покупець IoT девайсів може і самостійно підвищити захищеність, навіть не маючі знань та навичок в цій сфері, є рекомендації до можуть допомогти в цьому По-перше придбання IoT-пристроїв у авторитетних брендів, які приділяють велику увагу безпеці, а також реалізація заходів безпеки всередині пристроїв до їх поширення на ринку.

По-друге застосування політики складності паролів і використання багатофакторної автентифікації (MFA), коли це доступно.

По-третє необхідно переконатися, що на підключених пристроях встановлено новітнє програмне забезпечення, і підтримуйте працездатність пристроїв, це мінімізує шанс того що зловмисних зможе скористатися вразливістю якщо вона буде знайдена.

Також важливо впровадження профілів мережевого доступу з нульовим рівнем довіри для підключених пристроїв.

Для користувачів що інтегрують системи IoT у іншу інфраструктуру рекомендується робити поділ мереж для IT і IoT, якщо це можливо [23].

Аналіз показав, що безпека в мережах Інтернету речей потребує вдосконалення. Для підвищення рівня захищеності важливо розробляти та впроваджувати ефективні заходи безпеки, підвищувати кваліфікацію персоналу та вдосконалювати процедури реагування на кіберзагрози.

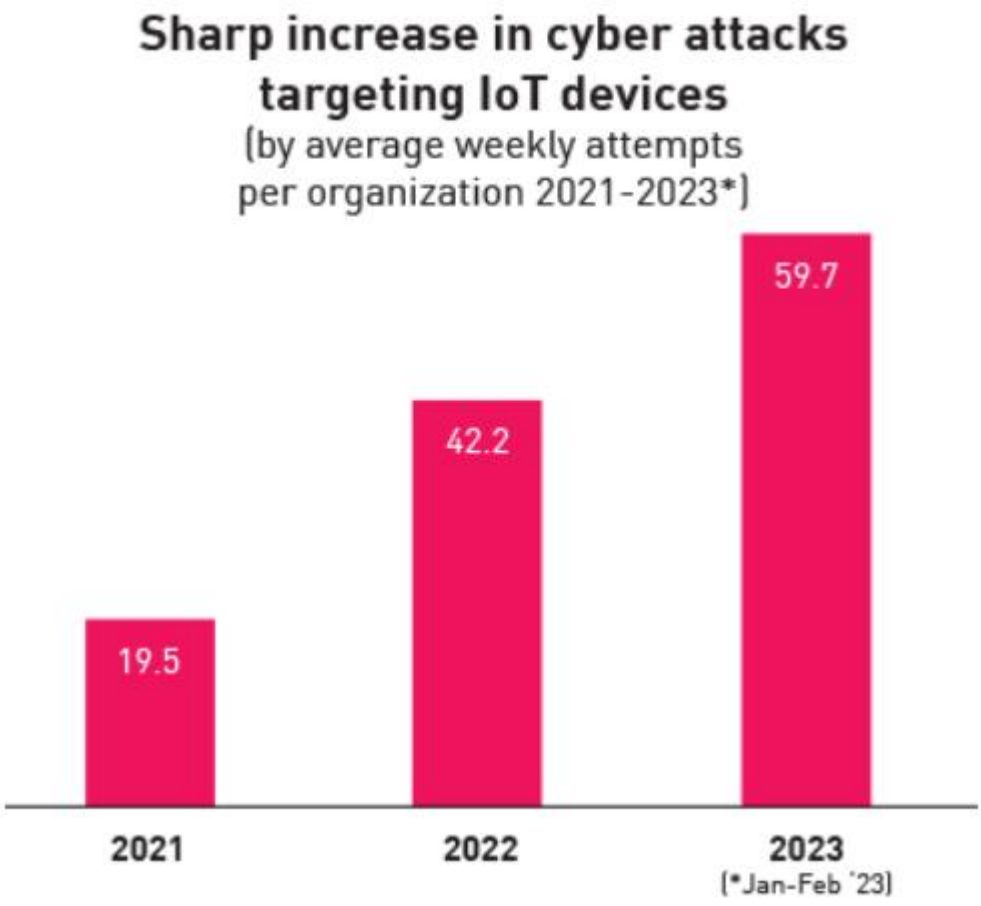


Рис. 2.4 Усереднена кількість інцидентів кібератак в тиждень на компанію що спрямовані на IoT девайси [23]

В результаті аналізу ми виявили, що кібератаки на системи IoT стають все більш поширеними, використовуючи різноманітні методи, такі як DDoS-атаки, експлойти вразливостей та інші.

Велика кількість вразливостей у системах IoT є основною причиною їхньої низької безпеки, і зловмисники активно використовують цю можливість для здійснення атак.

Неспроможність ефективно реагувати на кіберзагрози та виявлення їхнього прогресу ставить під загрозу безпеку мереж IoT і вимагає від нас пошуку нових підходів до захисту. Для цього варто звернутися до новітніх технологій, таких як штучний інтелект, який може надати додаткові інструменти та можливості для виявлення та запобігання кібератакам.

2.3 Дослідження шляху розробки ШІ

Для того щоб точніше розуміти можливості штучного інтелекту в області кібербезпеки нам треба дослідити процес створення абстрактного прототипу ШІ. За допомогою цього простіше зрозуміти які обмеження мають такі системи та можливості.

2.3.1 Процес збору даних

Для проведення збору даних для навчання системи штучного інтелекту в галузі кібербезпеки можна використовувати різні джерела та методики.

Журнали подій або логи, системи кібербезпеки зазвичай ведуть журнали подій, у яких фіксуються різні дії та події, що відбуваються в інформаційній системі. Ці логи можуть містити дані про спроби злому, аномальну поведінку користувачів, мережевий трафік та інші аспекти безпеки. Тому їх можуть використовувати як масиви даних для тренування моделі ШІ.

Дані сенсорів і датчиків, у системах Інтернету речей дані збираються з різних сенсорів і датчиків, встановлених у пристроях. Конкретніше ці дані можуть містити інформацію про температуру, вологість, рух та інші параметри, які можуть бути використані для виявлення аномалій і кібератак. Маючи інформацію про те які значення штатні для тих чи інших видів IoT-девайсів ШІ може навчитися підмічати аномалії в роботі сенсорів/датчиків, або проблеми з передачею даних від них, для того щоб мати можливість виявити можливих несанкціонованих втручань.

Збір пакетів мережевого трафіку, для аналізу мережевих загроз і атак можна збирати пакети мережевого трафіку, що проходять через мережу. Ці дані можуть бути використані для створення базиса для навчання ШІ, та в подальшому задля виявлення атак, ідентифікації шкідливого програмного забезпечення та аналізу поведінки мережевих пристроїв.

Дані про користувацьку активність, інформація про дії користувачів в інформаційній системі також може бути корисною для навчання системи

кібербезпеки. Це охоплює дані про вхід у систему, активність на сайті, використання застосунків тощо, для того щоб в майбутньому штучний інтелект мав можливість відрізняти які дії для користувачів є нормою, а які можуть свідчити про недоброчесність намірів чи того що з мережею контактує не людина, а программа.

Дані про конфігурацію та вразливості, інформація про конфігурацію системи та відомі вразливості також може бути використана для навчання системи ШІ знаходити й усувати вразливості. Так як ще не можливо при умові що ШІ немає інформації про те як працює система в цілому, розгорнутий аналіз є неможливим.

Усі ці дані можуть бути зібрані за допомогою спеціалізованих засобів збору даних, таких як сенсори, моніторингові системи, аналітичні інструменти тощо. Після збору дані можуть бути піддані обробці, за для структурування чи додавання інформації конкретно для ШІ, та аналізу перед використанням їх для навчання системи ШІ.

Дані для навчання це дуже важливий елемент, що буде впливати на успішність ШІ, тому зазвичай вони проходять багато рівнів обробки для того щоб ітогом модель навчалася тільки на вірних та не пошкоджених даних, що в свою чергу призводить до зниження кількості помилок.

2.3.2 Відбір найуспішнішої моделі

Відбір найкращої моделі машинного навчання є ключовим етапом у процесі розроблення алгоритму, який має досягти певних цілей. Ось кілька кроків, які можуть допомогти в проведенні цього відбору:

− Чітке визначення мети завдання машинного навчання є першим кроком. Це допоможе визначити, які метрики та характеристики моделі важливі для досягнення цієї мети.

− Вибір метрик, які найкращим чином відображають якість моделі для конкретного завдання. Наприклад, для завдань класифікації(коли ми хочемо віднести дані до певних категорій або класів) це можуть бути точність, повнота, F1-мера(метрика, яка використовується для оцінки точності моделей машинного

навчання, особливо в задачах класифікації) тощо. завдань класифікації (коли ми хочемо передбачити чисельне значення на основі наявних даних) - середня абсолютна помилка, коефіцієнт детермінації(статистическая мера, которая показывает, насколько хорошо модель регрессии соответствует данным) та інші.

− Вибір алгоритмів це наступний можливий крок, в процесі дослідження різних алгоритмів машинного навчання, які підходять для конкретного завдання. Це може включати в себе класичні методи, такі як лінійна регресія і метод найближчих сусідів, а також більш складні алгоритми, наприклад як випадковий ліс, градієнтний бустінг і нейронні мережі.

Лінійна регресія - це базовий метод регресійного аналізу, який використовується для моделювання залежності між змінними. Алгоритм намагається знайти пряму лінію, яка найкраще описує зв'язок між незалежними змінними (вхідними даними) та залежною змінною (цільовим значенням).

KNN - це простий і ефективний алгоритм класифікації та регресії, який використовує відстані між точками даних для передбачення класу або значення нової точки на основі найближчих до неї сусідів.

Випадковий ліс - це ансамблевий метод навчання, що використовує множину рішень дерев для класифікації або регресії. Кожне дерево в лісі створюється на основі випадкової вибірки даних, і кінцеве рішення приймається голосуванням всіх дерев.

Градієнтний бустінг - це метод ансамблевого навчання, який створює модель за допомогою послідовного навчання слабких моделей, таких як дерева рішень, де кожна наступна модель коригує помилки попередньої.

Крос-валідація, використовуючи цей метод для оцінки продуктивності кожної моделі на різних підмножин даних. Це дає змогу оцінити, наскільки модель узагальнюється на нові дані й уникнути перенавчання.

Гіперпараметри це - параметри моделі машинного навчання, які налаштовуються до початку процесу навчання і залишаються незмінними під час навчання. Вони зазвичай не пов'язані безпосередньо з даними і не налаштовуються в процесі навчання моделі, а скоріше визначають структуру або поведінку моделі. Для

конкретної моделі їх підбирають зазвичай за допомогою методів оптимізації, як Grid Search(метод налаштування гіперпараметрів, який систематично перебирає всі можливі комбінації заданого набору параметрів для визначення оптимальних значень) або випадковий пошук(метод налаштування гіперпараметрів, який випадковим чином вибирає комбінації параметрів з визначеного діапазону). Це надає змогу знайти комбінацію гіперпараметрів, яка забезпечує найкращу продуктивність моделі.

Порівняння результатів, зрівняв продуктивність різних моделей на основі обраних метрик. Вибирають модель з найкращою продуктивністю і роблять висновки про її придатність для даного завдання.

Після вибору найкращої моделі перевіряють її продуктивність на відкладеній вибірці, яка не використовувалася в процесі навчання. Це допоможе оцінити, наскільки добре модель узагальнюється на нові дані.

Проведення ретельного і систематичного аналізу різних моделей машинного навчання дає змогу вибрати найкращу модель для конкретного завдання і досягти оптимальних результатів.

2.3.3 Процес навчання моделі

Навчання моделі в машинному навчанні відбувається так, спочатку необхідно підготувати дані для навчання моделі.

Цей етап охоплює:

− збір даних

− очищення

− перетворення

− поділ на навчальний і тестовий набори

Далі проводиться вибір типу моделі, яка найкраще підходить для цього завдання на основі машинного навчання. Це може бути класифікація(класифікування даних), регресія(на основі даних що маємо генеруємо

ті до яких можемо дійти базуючить на тих що маємо), кластеризація(метод групування об'єктів даних на основі їхньої подібності) або інші методи.

Визначення функції втрат(математичні вирази, які вимірюють, наскільки добре модель передбачає цільову зміну на основі вхідних даних), яку будуть мінімізувати в процесі навчання моделі. Це може бути середньоквадратична помилка(різниця між передбаченими значеннями моделі та істинними значеннями в наборі даних) для завдань регресії або крос-ентропія(міра відстані між двома розподілами ймовірностей, функція втрат) для завдань класифікації.

Налаштування параметрів, використовують початковий набір даних для налаштування параметрів моделі таким чином, щоб мінімізувати обрану функцію втрат. Це зазвичай відбувається шляхом ітеративного процесу, званого оптимізацією, під час якого параметри моделі змінюються таким чином, щоб поліпшити її продуктивність.

Далі йде оцінка продуктивності моделі на тестовому наборі даних, який не використовувався в процесі навчання. Це дає змогу оцінити, наскільки добре модель узагальнюється на нові дані й уникнути перенавчання.

Налаштування гіперпараметри моделі,можливі варіанти − швидкість навчання, кількість прихованих шарів у нейронній мережі або глибина дерев у випадковому лісі, щоб поліпшити її продуктивність.

Після навчання моделі йде процес аналізу її на реальних даних і проведіть валідацію результатів. Це дасть змогу переконатися, що модель працює коректно і відповідає очікуванням.

Можливі також і додаткові кроки, які як регуляризація та оптимізація, щоб поліпшити продуктивність моделі та уникнути перенавчання.

Навчання моделі в машинному навчанні - це ітеративний процес, який вимагає ретельного аналізу даних, вибору підходящої моделі та параметрів, а також оцінки результатів для досягнення оптимальної продуктивності.

2.3.4 Процес тестування моделі

Тестування моделі в машинному навчанні є важливим етапом, що допомагає оцінити її продуктивність та здатність узагальнювати нові дані.

На початковому етапі тестування важливо підготувати окремий набір даних, який не використовувався в процесі навчання моделі. Цей набір даних повинен бути репрезентативним і відповідати реальним умовам, в яких модель буде працювати. Це дозволяє об'єктивно оцінити її продуктивність.

Наступним кроком є застосування моделі до тестового набору даних. Модель використовується для прогнозування цільових змінних або класифікації об'єктів у тестовому наборі. Отримані передбачення зберігаються для подальшого аналізу.

Для оцінки продуктивності моделі необхідно порівняти передбачені значення з фактичними значеннями цільової змінної. Це дозволяє обчислити різні метрики, такі як:

− Середня абсолютна помилка (MAE) - показує середню різницю між передбаченими і фактичними значеннями.

− Середня квадратична помилка (MSE) - дає змогу оцінити середню квадратичну різницю між передбаченими і фактичними значеннями.

− Точність, повнота, F1-міра - використовуються для оцінки класифікаційних моделей, показують, наскільки точно модель класифікує об'єкти.

Потім починається процес аналізу, щоб зрозуміти, наскільки добре модель справляється з поставленим завданням. Якщо метрики показують незадовільні результати, можливо, модель потребує додаткового налаштування або поліпшення.

У разі незадовільної продуктивності модель може бути вдосконалена через ітераційний процес.

Це може включати:

− Зміну параметрів моделі.

− Додавання або видалення ознак.

− Вибір іншого алгоритму навчання.

− Інші заходи для поліпшення результатів.

Тестування моделі є критичним етапом у розробці та оцінці моделей машинного навчання. Воно допомагає виявити сильні та слабкі сторони моделі, а також оцінити її здатність узагальнювати нові дані.

2.3.5 Процес імплементації моделі

Імплементація в контексті штучного інтелекту відноситься до процесу створення конкретної реалізації моделі або алгоритму, що був розроблений у рамках дослідження або проектування.

Цей процес включає в себе кілька етапів.

Перш за все, потрібно вибрати платформу або мову програмування, на якій буде реалізовано модель. Це може бути Python з бібліотеками машинного навчання, такими як TensorFlow, PyTorch, scikit-learn та інші, або інші мови програмування, такі як Java, C++ тощо.

Написання коду, який реалізує обраний алгоритм машинного навчання або модель ШІ. Це передбачає створення класів, функцій і методів, які реалізують логіку моделі, включно з навчанням, прогнозуванням та оцінкою продуктивності.

Тестування, після написання коду модель має бути протестована на тестових даних, щоб переконатися, що вона працює коректно і дає очікувані результати. Тестування допомагає виявити помилки або недоліки в реалізації та виправити їх.

Після тестування модель може знадобитися оптимізувати для поліпшення продуктивності або ефективності. Це може включати в себе оптимізацію алгоритмів, поліпшення швидкості роботи моделі, зменшення споживання ресурсів тощо.

Після завершення розроблення модель має бути інтегрована в систему або застосунок, де її використовуватимуть для вирішення конкретного завдання. Це може включати в себе створення API для взаємодії з моделлю, інтеграцію з базами даних, веб-серверами та іншими компонентами системи.

Імплементація моделі ШІ вимагає не тільки технічних навичок програмування, а й розуміння принципів роботи моделі, її особливостей та вимог до конкретного

завдання. Це багатоступеневий процес, що потребує значних зусиль і часу для успішної реалізації.

2.3.6 Процес постпродакшену

Функція моніторингу та підтримки в контексті штучного інтелекту відіграє ключову роль у забезпеченні ефективної роботи системи ШІ та підтримки її продуктивності.

Моніторинг продуктивності моделі, це безперервне відстеження роботи моделі ШІ, її продуктивності та точності передбачень. Моніторинг дозволяє виявляти аномалії або зміни в роботі моделі, які можуть вимагати втручання або перенавчання.

Аналіз даних і зворотний зв'язок, зібрані в процесі роботи моделі дані аналізуються, а результати надаються розробникам або дослідникам. Це допомагає покращити модель, виявити помилки або недоліки в її роботі та вжити заходів для їх виправлення

Оптимізація та налаштування параметрів, моніторинг дозволяє оптимізувати параметри моделі, такі як гіперпараметри або архітектура моделі, для підвищення її продуктивності та точності. Це може включати зміну параметрів навчання, вибір інших алгоритмів або архітектур моделей.

Керування даними і ресурсами, функція моніторингу та підтримки також включає управління даними, використовуваними для навчання і тестування моделі, і управління обчислювальними ресурсами, необхідними для роботи моделі. Це може охоплювати масштабування ресурсів, управління пам'яттю і процесорним часом тощо.

Розв'язання проблем і обробка відмов, у разі виникнення проблем або збоїв у роботі моделі ШІ функція моніторингу та підтримки дає змогу швидко виявити й виправити проблеми, а також вжити заходів для запобігання їхньому виникненню в майбутньому.

Загалом, функція моніторингу та підтримки відіграє важливу роль у забезпеченні надійної та ефективної роботи системи ШІ, а також у безперервному поліпшенні її продуктивності та точності.

2.3.7 Висновки та рекомендації

Після огляду всього шляху від розробки до впровадження моделей штучного інтелекту, варто зазначити, що цей процес має безліч аспектів, де неточності або обмеження можуть вплинути на якість моделі. Серед основних проблем можна виділити:

− Невірні або неповні дані під час навчання моделі можуть призвести до неправильних результатів або зниження точності передбачень.

− Недостатнє розуміння проблеми або неправильний вибір алгоритму можуть негативно вплинути на продуктивність моделі.

− Використання застарілих або неефективних бібліотек та інструментів може уповільнити процес навчання та впровадження моделі.

− Недоліки в знаннях або навичках розробників можуть спричинити помилки на будь-якому етапі розробки, навчання чи впровадження моделі.

− Некоректна інтеграція моделі в робоче середовище може призвести до зниження її ефективності або викликати збої в роботі системи.

Незважаючи на ці потенційні проблеми, штучний інтелект залишається потужним інструментом, який дійсно допомагає у багатьох сферах. Використання ШІ значно підвищує ефективність і точність процесів, а при поєднанні з експертними знаннями людини, результати можуть бути вражаючими. Системи ШІ можуть оптимізувати робочі процеси, зменшувати витрати і підвищувати якість прийняття рішень, що робить їх незамінними в сучасному світі.

Тому можно составили такі рекомендації.

Завжди необхідно перевіряти і очищати дані перед їх використанням для навчання моделі, щоб уникнути неточностей і помилок.

Треба проводити детальний аналіз проблеми і ретельно вибирайте алгоритми, які найкраще підходять для її вирішення.

Використовувати необхідно сучасні інструменти і бібліотеки для розробки і впровадження моделей ШІ.

Якщо ви керуєте компанію то інвестування в навчання і підвищення кваліфікації розробників, зменшить вплив негативного аспекту людського фактора.

Також необхідне регулярне тестування і моніторинг моделей після їх впровадження, щоб забезпечити їх ефективність і вчасно виявляти та виправляти проблеми.

Інтеграція ШІ у робочі процеси вимагає уваги до деталей на кожному етапі, але з належним підходом і підготовкою, це може значно покращити результати і сприяти інноваціям у різних галузях.

3 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ: АНАЛІЗ, МЕТОДИ ТА РЕКОМЕНДАЦІЇ

3.1 Основні проблеми безпеки в мережах IoT

У процесі аналізу сучасного стану мереж IoT стало очевидно, що існують численні проблеми, які перешкоджають забезпеченню належного рівня безпеки. Ці проблеми стосуються як технічних аспектів, так і організаційних факторів, що створює складні виклики для захисту IoT-систем. Однією з найбільш поширених проблем є те, що багато розробників не дотримуються стандартних рекомендацій з безпеки. Це часто пов'язано з прагненням швидше вивести продукт на ринок, ігноруючи важливі аспекти безпеки. Наприклад, розробники можуть використовувати недостатньо захищені протоколи передачі даних або залишати заводські налаштування без змін, що робить пристрої вразливими для атак. Як результат, такі мережі стають легкою мішенню для зловмисників.

Передача даних по бездротових мережах становить значну загрозу, оскільки ці дані можуть бути перехоплені за допомогою спеціального обладнання. Наприклад, зловмисники можуть використовувати методи прослуховування (sniffing) для отримання конфіденційної інформації. Бездротові мережі часто використовують слабкі методи шифрування або взагалі не шифрують дані, що дозволяє зловмисникам легко отримати доступ до чутливої інформації.

Інтеграція IoT з іншими мережами, такими як IT-інфраструктури компаній, підвищує рівень небезпеки, оскільки вразливості в одній мережі можуть поширитися на інші системи. Зокрема, якщо IoT-пристрій вразливий до атак, зловмисники можуть використати його як точку входу для атак на інші частини мережі. Це може призвести до компрометації критично важливих даних та систем компанії.

Багато IoT-пристроїв мають обмежені обчислювальні потужності та пам'ять, що ускладнює впровадження стандартних методів шифрування та аутентифікації. Це обмежує можливості захисту та робить ці пристрої більш вразливими до атак.

Зловмисники можуть використовувати слабкі місця цих пристроїв для проведення атак, таких як DoS (Denial of Service) або маніпуляція даними.

Багато IoT-пристроїв не отримують регулярних оновлень програмного забезпечення, що призводить до накопичення вразливостей, які можуть бути використані зловмисниками. Відсутність механізмів автоматичного оновлення або складність процесу оновлення призводить до того, що пристрої залишаються вразливими протягом тривалого часу.

Багато IoT-пристроїв не мають достатніх засобів для аутентифікації користувачів та управління доступом. Це може призвести до несанкціонованого доступу до пристроїв та даних. Наприклад, використання слабких або заводських паролів значно підвищує ризик компрометації пристроїв. Зловмисники можуть використовувати ці вразливості для отримання доступу до конфіденційних даних або керування пристроями.

Наразі немає єдиних глобальних стандартів безпеки для IoT-пристроїв, що призводить до різнорідності підходів до захисту. Кожен виробник використовує власні методи та протоколи, що ускладнює інтеграцію та забезпечення належного рівня безпеки в змішаних мережах. Це створює додаткові труднощі для управління безпекою та збільшує ризики.

Зловмисники можуть використовувати методи соціальної інженерії та фішинг для отримання доступу до IoT-систем. Це включає обман користувачів з метою отримання конфіденційної інформації або доступу до пристроїв. Наприклад, зловмисники можуть надсилати підроблені повідомлення або створювати фальшиві веб-сайти для збору даних про користувачів.

Основні проблеми безпеки в мережах IoT є комплексними та вимагають всебічного підходу до їх вирішення. Важливо дотримуватися стандартних рекомендацій з безпеки, впроваджувати надійні методи шифрування та аутентифікації, регулярно оновлювати програмне забезпечення пристроїв та забезпечувати управління доступом. Інтеграція IoT-пристроїв з іншими мережами повинна проводитися з урахуванням можливих вразливостей та ризиків. Крім того,

необхідно розробляти єдині стандарти безпеки для IoT, які б забезпечували належний рівень захисту для всіх пристроїв та мереж.

3.2 Найбільш ефективні методи захисту інформації в IoT

Для захисту IoT мереж існують кілька ефективних методів. Одним з найважливіших є ізоляція мережі. Якщо мережа спроектована як ізольована система, ризик значних збитків у разі зламу значно знижується. Наприклад, ізольована мережа водопостачання не зможе вплинути на інші критичні інфраструктури.

Також важливо використовувати надійні паролі та двофакторну аутентифікацію, щоб забезпечити захист від несанкціонованого доступу. Цей метод доповнює шифрування даних, яке гарантує, що навіть у разі перехоплення даних вони залишаться недоступними для зловмисників. Шифрування може бути реалізовано за допомогою алгоритмів, таких як AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), та ECC (Elliptic Curve Cryptography), які забезпечують високий рівень захисту.

Інтеграція штучного інтелекту (ШІ) також може суттєво підвищити безпеку мереж IoT. Системи ШІ можуть автоматично виявляти аномалії та несанкціонований доступ, реагувати на загрози та виявляти нетипове поведінку користувачів. Наприклад, сервіси, як Enterprise Immune System, використовують алгоритми ШІ для аналізу мережевого трафіку та виявлення аномалій, що дозволяє оперативно реагувати на потенційні атаки.

3.3 Використані методи машинного навчання для виявлення загроз

Машинне навчання є важливим інструментом у виявленні загроз в IoT мережах. Системи машинного навчання здатні аналізувати великі обсяги даних, виявляючи патерни та аномалії, що можуть свідчити про потенційні загрози. Нижче розглянемо основні методи машинного навчання, які використовуються для виявлення загроз в IoT.

Одним з ефективних методів виявлення загроз є аналіз нетипової поведінки користувачів. Машинне навчання дозволяє створювати моделі поведінки користувачів на основі історичних даних. Якщо користувач раптово починає завантажувати великі обсяги даних у незвичайний час або виконує дії, які не відповідають його типовій поведінці, система може визначити це як аномалію і сигналізувати адміністратора про можливу загрозу. Для цього можуть використовуватися такі алгоритми, як кластеризація (k-means clustering), яка розбиває дані на групи на основі їх схожості. Цей метод визначає центри кластерів і розподіляє дані таким чином, щоб мінімізувати відстань між точками даних та центрами кластерів, що допомагає виявляти нетипову поведінку. Інший підхід — методи аномалійного виявлення (One-Class SVM), що спеціалізуються на виявленні аномалій, навчаючись на даних, що відносяться до нормальної поведінки. Відхилення від цієї поведінки розглядаються як потенційні аномалії або загрози.

Виявлення аномалій у мережевому трафіку є ще одним важливим методом. Алгоритми машинного навчання можуть швидко аналізувати великі обсяги мережевих даних, виявляючи відхилення від нормального стану. Наприклад, алгоритми глибокого навчання, такі як рекурентні нейронні мережі (RNN, Recurrent Neural Networks) та довго-короткочасна пам'ять (LSTM, Long Short-Term Memory), використовуються для обробки послідовних даних. RNN враховують контекст попередніх елементів у послідовності, що дозволяє їм виявляти аномалії в часі, що корисно для аналізу мережевого трафіку. LSTM, з іншого боку, здатні зберігати інформацію на тривалий час, що робить їх ефективними для виявлення довгострокових залежностей і аномалій у мережевому трафіку.

Методи класифікації також широко використовуються для виявлення загроз в IoT. Алгоритми, такі як дерева рішень (Decision Trees), випадкові ліси (Random Forest) та метод опорних векторів (SVM, Support Vector Machine), навчаються розпізнавати, до якого класу належить новий зразок даних. Дерева рішень є моделлю, яка використовує деревоподібну графічну структуру для прийняття рішень. Кожен вузол дерева представляє вибір атрибуту даних, а кожна гілка — результат цього вибору, що робить їх простими у візуалізації та інтерпретації.

Випадкові ліси є ансамблевим методом, що об'єднує кілька дерев рішень для підвищення точності і зменшення ризику переобучення. Метод опорних векторів (SVM) знаходить гіперплощину, що максимально розділяє зразки різних класів, що є ефективним для високовимірних даних.

Баєсові мережі (Bayesian Networks) використовуються для ймовірнісного виявлення загроз, враховуючи взаємозв'язки між різними подіями та поведінковими патернами. Баєсові мережі моделюють складні залежності між змінними за допомогою графічних структур, де вузли представляють змінні, а ребра — їх залежності. Цей підхід дозволяє проводити індуктивні висновки та виявляти загрози, аналізуючи ймовірності певних подій.

Методи навчання без учителя (Unsupervised Learning), такі як автокодери (Autoencoders) та генеративно-змагальні мережі (GANs, Generative Adversarial Networks), також знаходять застосування у виявленні загроз в IoT. Автокодери є нейронними мережами, що навчаються стискати дані (кодування) і потім відновлювати їх до початкового стану (декодування). Якщо відновлені дані значно відрізняються від оригінальних, це може свідчити про наявність аномалій. Генеративно-змагальні мережі складаються з двох мереж — генератора і дискримінатора. Генератор створює синтетичні дані, а дискримінатор намагається відрізнити їх від реальних даних, що покращує здатність моделі виявляти аномалії.

Ансамблеві методи (Ensemble Methods), такі як градієнтний бустинг (Gradient Boosting) та стекінг (Stacking), об'єднують кілька моделей машинного навчання для підвищення точності та надійності виявлення загроз. Градієнтний бустинг послідовно створює нові моделі для корекції помилок попередніх моделей. Кінцевий результат є комбінацією всіх моделей, що покращує загальну точність. Стекінг комбінує прогнози кількох моделей за допомогою метамоделі, яка навчається на виходах кількох базових моделей, що дозволяє враховувати їхні слабкі та сильні сторони для покращення загальної продуктивності.

Таким чином, використання методів машинного навчання для виявлення загроз в IoT мережах дозволяє значно підвищити ефективність захисту, забезпечуючи своєчасне виявлення та реагування на потенційні загрози.

Комплексний підхід, що включає аналіз нетипової поведінки, виявлення аномалій у мережевому трафіку, методи класифікації, баєсові мережі, методи навчання без учителя та ансамблеві методи, забезпечує високий рівень захищеності IoT інфраструктури.

3.4 Приклади успішної інтеграції ШІ в системи безпеки IoT

Одним із найяскравіших прикладів успішної інтеграції ШІ в систему безпеки є Enterprise Immune System від компанії Darktrace. Ця система використовує машинне навчання та алгоритми штучного інтелекту для виявлення аномалій у поведінці мережі. Підхід Darktrace імітує роботу імунної системи людини, що дозволяє швидко виявляти та реагувати на загрози, навіть якщо вони є новими або невідомими. Enterprise Immune System аналізує поведінкові патерни пристроїв та користувачів, виявляючи відхилення, які можуть свідчити про кібератаку. Це дозволяє забезпечити проактивний захист мереж IoT, адаптуючись до нових загроз у реальному часі.

CylancePROTECT від компанії Cylance є ще одним прикладом успішної інтеграції ШІ у системи безпеки IoT. Цей продукт використовує алгоритми машинного навчання для запобігання кібератакам. Ця система ШІ здатна виявляти та блокувати шкідливі програми і атаки без необхідності у постійному оновленні сигнатур. Система аналізує характеристики файлів і програм, що дозволяє визначати потенційні загрози на основі їх поведінкових ознак. Завдяки цьому підходу, CylancePROTECT забезпечує високий рівень захисту для пристроїв IoT, мінімізуючи ризик компрометації системи.

IBM Watson for Cyber Security використовує потужності когнітивних обчислень та аналізу великих обсягів даних для виявлення потенційних загроз. Watson обробляє великі масиви інформації з різних джерел, включаючи блоги, наукові статті, новини та інші ресурси, для ідентифікації нових та невідомих загроз. Система також здатна проводити глибокий аналіз інцидентів, визначаючи кореляції між різними подіями та виявляючи складні атаки. Завдяки цьому IBM Watson for

Cyber Security забезпечує розширений рівень захисту мереж IoT, дозволяючи виявляти загрози, які могли б залишитися непоміченими традиційними методами.

Ці приклади демонструють, як інтеграція ШІ у системи безпеки IoT може значно підвищити рівень захищеності мереж та пристроїв. Використання передових технологій ШІ дозволяє не тільки ефективно виявляти та реагувати на загрози, але й проактивно запобігати потенційним атакам, забезпечуючи стійке та безпечне функціонування Інтернету речей. Ці розробки ведуться на рівні інтерпрайс так як їх створили доволі великі компанії, для заробітку, якій вони отримують, що зайвий раз опосередковано доказує перспективність та затребуваність цієї технології вже на даний момент часу.

3.5 Рекомендації щодо поліпшення стандартів безпеки в IoT

Встановлення строгих стандартів безпеки для всіх мереж IoT є необхідним для зниження ризиків кібератак. Для досягнення цього необхідно застосовувати комплексний підхід, який охоплює як технічні, так і організаційні аспекти.

По-перше, важливо впроваджувати сучасні методи шифрування, такі як AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman) та ECC (Elliptic Curve Cryptography), для забезпечення захисту даних. Ці методи шифрування дозволяють забезпечити високий рівень безпеки, навіть у випадку компрометації окремих пристроїв. Важливо також використовувати криптографічні протоколи, такі як TLS (Transport Layer Security), для забезпечення безпечного обміну даними між пристроями IoT.

Крім того, слід впроваджувати багатофакторну аутентифікацію (MFA) для підвищення рівня захищеності доступу до пристроїв та мереж IoT. Це може включати використання паролів, біометричних даних, а також додаткових засобів аутентифікації, таких як одноразові коди чи апаратні токени.

Не менш важливим є підвищення обізнаності користувачів та адміністраторів щодо важливості дотримання стандартів безпеки. Проведення регулярних навчальних заходів та тренінгів допоможе сформувати культуру безпеки та підвищити рівень захищеності мереж IoT. Користувачі повинні бути обізнані про

основні загрози, методи захисту, а також про важливість регулярного оновлення програмного забезпечення.

Постійний моніторинг мереж та регулярне оновлення програмного забезпечення є ключовими для забезпечення безпеки мереж IoT. Автоматизовані системи моніторингу можуть виявляти аномальні дії та потенційні загрози в реальному часі, що дозволяє оперативно реагувати на можливі атаки. Регулярні оновлення програмного забезпечення та прошивок пристроїв забезпечують захист від відомих вразливостей та знижують ризик успішних атак.

Використання штучного інтелекту (ШІ) для виявлення та реагування на загрози може значно покращити безпеку, дозволяючи швидко реагувати на потенційні атаки. ШІ−системи можуть аналізувати великі обсяги даних, виявляти аномалії та передбачати можливі загрози на основі історичних даних. Впровадження технологій машинного навчання та глибокого навчання дозволяє створювати адаптивні системи захисту, які постійно вдосконалюються та підлаштовуються під нові загрози.

Окрім технічних заходів, важливо розробити чіткі політики безпеки та процедури для управління ризиками в мережах IoT. Це включає визначення ролей та обов'язків, регулярні аудити безпеки, а також створення планів реагування на інциденти. Політики безпеки повинні враховувати специфіку IoT та забезпечувати комплексний підхід до захисту даних та інфраструктури.

На завершення, впровадження стандартів безпеки в IoT є складним і багатогранним завданням, яке потребує постійного вдосконалення та адаптації до нових загроз. Комплексний підхід, що включає використання сучасних технологій шифрування, багатофакторної аутентифікації, постійного моніторингу, застосування ШІ, а також підвищення обізнаності користувачів, дозволить значно підвищити рівень захисту мереж IoT та забезпечити їх безпечне функціонування.

3.6 Загальні висновки та рекомендації

На основі проведеного дослідження можна зробити висновок, що забезпечення безпеки мереж IoT є складним завданням, яке потребує комплексного підходу. Виявлені численні проблеми безпеки, такі як недотримання стандартних рекомендацій, вразливість бездротової передачі даних, обмежені ресурси пристроїв IoT, відсутність регулярних оновлень та патчів, проблеми з аутентифікацією та управлінням доступом, відсутність єдиних стандартів безпеки, а також ризики, пов'язані з соціальною інженерією та фішингом, підкреслюють необхідність ретельного аналізу та планування заходів безпеки.

Недотримання стандартних рекомендацій з безпеки є поширеною проблемою, оскільки багато розробників прагнуть швидше вивести продукт на ринок, ігноруючи важливі аспекти безпеки, що робить IoT-пристрої легкою мішенню для зловмисників. Передача даних по бездротових мережах може бути перехоплена зловмисниками, що загрожує витоком конфіденційної інформації, особливо коли застосовуються слабкі методи шифрування. Інтеграція IoT-пристроїв з іншими мережами, такими як корпоративні IT-інфраструктури, підвищує загальний рівень небезпеки, оскільки вразливості в IoT-пристроях можуть поширитися на інші системи.

Обмежені ресурси пристроїв IoT, зокрема недостатні обчислювальні потужності та пам'ять, ускладнюють впровадження надійних методів захисту, що підвищує їх вразливість до атак. Відсутність регулярних оновлень та патчів для багатьох IoT-пристроїв призводить до накопичення вразливостей, які можуть бути використані зловмисниками. Проблеми з аутентифікацією та управлінням доступом, зокрема використання слабких або заводських паролів, недостатні засоби для аутентифікації, підвищують ризик несанкціонованого доступу. Відсутність єдиних стандартів безпеки ускладнює інтеграцію та забезпечення належного рівня безпеки в змішаних мережах.

Соціальна інженерія та фішинг залишаються значними загрозами, оскільки зловмисники використовують ці методи для отримання доступу до IoT-систем.

Встановлення строгих стандартів безпеки є необхідним для зменшення різнорідності підходів та забезпечення надійного захисту. Інтеграція штучного інтелекту для виявлення та реагування на загрози, зокрема використання методів машинного навчання для ідентифікації підозрілих дій та швидкого реагування на них, може значно підвищити рівень безпеки.

Постійний моніторинг та оновлення програмного забезпечення є критично важливими для закриття вразливостей. Автоматичні системи оновлення можуть спростити цей процес та забезпечити своєчасне впровадження необхідних змін. Навчання користувачів та адміністраторів щодо безпекових ризиків та методів їх запобігання є ключовим фактором у забезпеченні безпеки мереж IoT. Це включає проведення тренінгів та інформаційних кампаній.

Застосування багаторівневих методів захисту, таких як шифрування даних, аутентифікація, управління доступом, моніторинг та реагування на інциденти, дозволяє створити комплексний підхід до безпеки. Впровадження адаптивних систем безпеки, які можуть динамічно змінювати свої налаштування в залежності від поточних загроз, забезпечує більш високий рівень захисту та швидке реагування на нові виклики.

Забезпечення безпеки мереж IoT є складним та багатоаспектним завданням, яке потребує інтеграції сучасних технологій, постійного моніторингу та регулярного оновлення. Встановлення строгих стандартів безпеки, використання штучного інтелекту для виявлення та реагування на загрози, навчання користувачів та адміністраторів, а також впровадження багаторівневих методів захисту дозволить значно знизити ризики кібератак та забезпечити належний рівень захисту для мереж IoT. Це є критично важливим у сучасному світі, де кількість підключених пристроїв постійно зростає.

ВИСНОВКИ

Проведене дослідження методів захисту інформації в мережах Інтернету речей (IoT) дозволило досягти важливих результатів, які мають значний вплив на розуміння та покращення безпеки в цій сфері. Було встановлено, що процес створення Штучного Інтелекту (ШІ) включає кілька критичних етапів, і кожен з них може суттєво вплинути на якість кінцевої моделі. Неправильні дані для навчання, помилки в проектуванні або впровадженні можуть значно знизити ефективність системи. ШІ продемонстрував себе як потужний інструмент у кіберзахисті, зокрема, для виявлення кіберзагроз, прогнозування атак та автоматизації відповідних заходів. Здатність аналізувати великі обсяги даних і виявляти аномалії допомагає забезпечувати високий рівень безпеки.

Рекомендується впроваджувати системи ШІ для підвищення рівня кібербезпеки в мережах IoT, особливо в критичних інфраструктурах. Для забезпечення актуальності та ефективності моделей ШІ необхідно постійно оновлювати їхні дані для навчання. Після впровадження системи ШІ необхідний постійний моніторинг її продуктивності та оптимізація параметрів для підтримки високого рівня безпеки.

ШІ в кібербезпеці мереж IoT має великий потенціал для подальшого розвитку. Зокрема, розвиток адаптивних моделей, які можуть самостійно навчатися та вдосконалювати свої можливості під час роботи, є перспективним напрямом. Проведене дослідження підтвердило доцільність і ефективність використання ШІ для вирішення завдань кібербезпеки в мережах IoT, забезпечуючи високий рівень захисту для організацій та їхніх користувачів.

ПЕРЕЛІК ПОСИЛАНЬ

1. WannaCryhttps [Електроний ресурс]://uk.wikipedia.org/wiki/WannaCry
2. Darktrace Launches Enterprise Immune System Version 4 [Електроний ресурс]: https://darktrace.com/news/darktrace-launches-enterprise-immune-system-version-4
3. CylanceENDPOINT Powered by Cylance AI [Електроний ресурс]: https://www.blackberry.com/us/en/products/cylance-endpoint-security/cylance-endpoint
4. Watson [Електроний ресурс]: https://www.ibm.com/blogs/nordic-msp/category/watson/
5. XIAOHUI, Xu. Study on security problems and key technologies of the internet of things. In: 2013 International conference on computational and information sciences. IEEE, 2013. p. 407-410.
6. BUTUN, Ismail; ÖSTERBERG, Patrik; SONG, Houbing. Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 2019, 22.1: 616-644.
7. Tech giant Fujitsu says it was hacked, warns of data breach [Електроний ресурс]: https://techcrunch.com/2024/03/18/fujitsu-tech-giant-hacked-customer-data-breach/
8. Aqeel-ur-Rehman, S. U. R., Khan, I. U., Moiz, M., & Hasan, S. (2016). Security and privacy issues in IoT. International Journal of Communication Networks and Information Security (IJCNIS), 8(3), 147-157.
9. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A. (2015). «Security, privacy and trust in Internet of Things: The road ahead.» Computer Networks.
10. Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., Qiu, D. (2014). «Security of the Internet of Things: perspectives and challenges.» Wireless Networks
11. Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025 [Електроний ресурс]: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-

worldwide/#:~:text=The%20total%20installed%20base%20of,that%20are%20expected%20in%202021.

12. Поширені атаки на IoT та захист від них [Електроний ресурс]: https://corewin.ua/blog/attacks-on-iot-how-protect/
13. Баранов, О. А., & Брижко, В. М. (2016). Захист персональних даних в сфері Інтернет речей. Інформація і право, (2 (17)), 85-91
14. КАК В 2015 ГОДУ БЫЛ ВЗЛОМАН ИНТЕРНЕТ ВЕЩЕЙ [Електроний ресурс]: https://igate.com.ua/news/12342-kak-v-2015-godu-byl-vzloman-internet-veshhej
15. 2024 SONICWALL CYBER THREAT REPORT [Електроний ресурс]: https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf
16. ОЦІНКА ВРАЗЛИВОСТІ ПРИСТРОЇВ «ІНТЕРНЕТУ РЕЧЕЙ» К. О. Кіфорчук1, М. В. Грайворонський1 [Електроний ресурс]: https://core.ac.uk/download/pdf/132192673.pdf
17. About Hierarchy of Controls [Електроний ресурс]: https://www.cdc.gov/niosh/hierarchy-of-controls/about/?CDC_AAref_Val=https://www.cdc.gov/niosh/topics/hierarchy/default.html
18. IoT Security Primer: Challenges and Emerging Practices [Електроний ресурс]: https://www.gartner.com/en/doc/iot-security-primer-challenges-and-emerging-practices
19. 2020 Unit 42 IoT Threat Report [Електроний ресурс]: https://unit42.paloaltonetworks.com/iot-threat-report-2020/
20. Study: Most enterprise IoT transactions are unencrypted [Електроний ресурс]: https://www.networkworld.com/article/967419/study-most-enterprise-iot-transactions-are-unencrypted.html
21. Attendance of cybersecurity training by employees worldwide in 2024, by type [Електроний ресурс]: https://www.statista.com/statistics/1376495/cybersecurity-training-use-employees-worldwide-by-type/

22. Exploring The Explosive Growth Of The Cybersecurity Market [Електроний ресурс]: https://bluetree.digital/cybersecurity-market-growth/
23. The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally [Електроний ресурс]: https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/

Державний університет інформаційно-комунікаційних технологій

Кафедра Інженерії програмного забезпечення автоматизованих систем

Державна атестаційна робота кваліфікаційного рівня бакалавр на тему:

«Дослідження методів захисту інформації в мережах іот»

на здобуття освітнього ступеня бакалавра
зі спеціальності 126 Інформаційні системи та технології
освітньо-професійної програми Інформаційні системи та технології

Виконав(ла): Андреєв Я.О ІСД-41
Науковий керівник роботи:
Жидка О.В.

Київ - 2024

Актуальність теми: Забезпечення безпеки мереж IoT є надзвичайно актуальною проблемою через зростання кількості підключених пристроїв та пов'язаних з ними кіберзагроз

Наукова новизна: полягає у розробці практичних пропозицій та рекомендацій, які можуть бути впроваджені для покращення безпеки в цій галузі.

Об`єкт дослідження: мережі Інтернету речей (IoT)

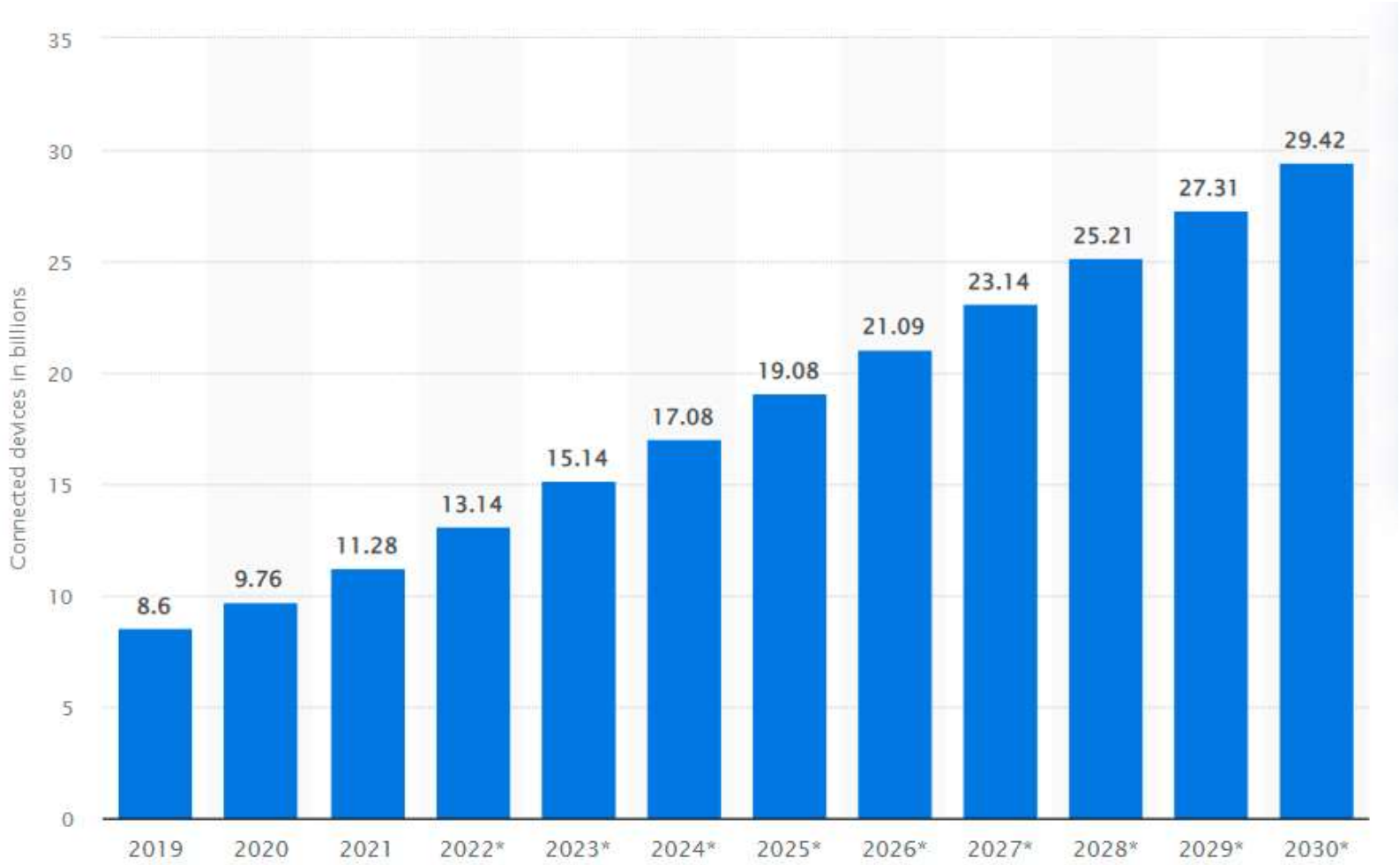
Предмет дослідження: методи забезпечення безпеки мереж IoT із застосуванням штучного інтелекту

Мета дослідження: дослідження методів забезпечення безпеки мереж Інтернету речей (IoT) із використанням штучного інтелекту (ШІ) та оцінка їх ефективності.

Завдання дослідження:

1. Проведення аналізу сучасних проблем безпеки мереж IoT
2. Аналіз ефективності захисних заходів у мережах IoT
3. Рекомендації та висновки щодо поліпшення безпеки мереж IoT

Тема та актуальність роботи



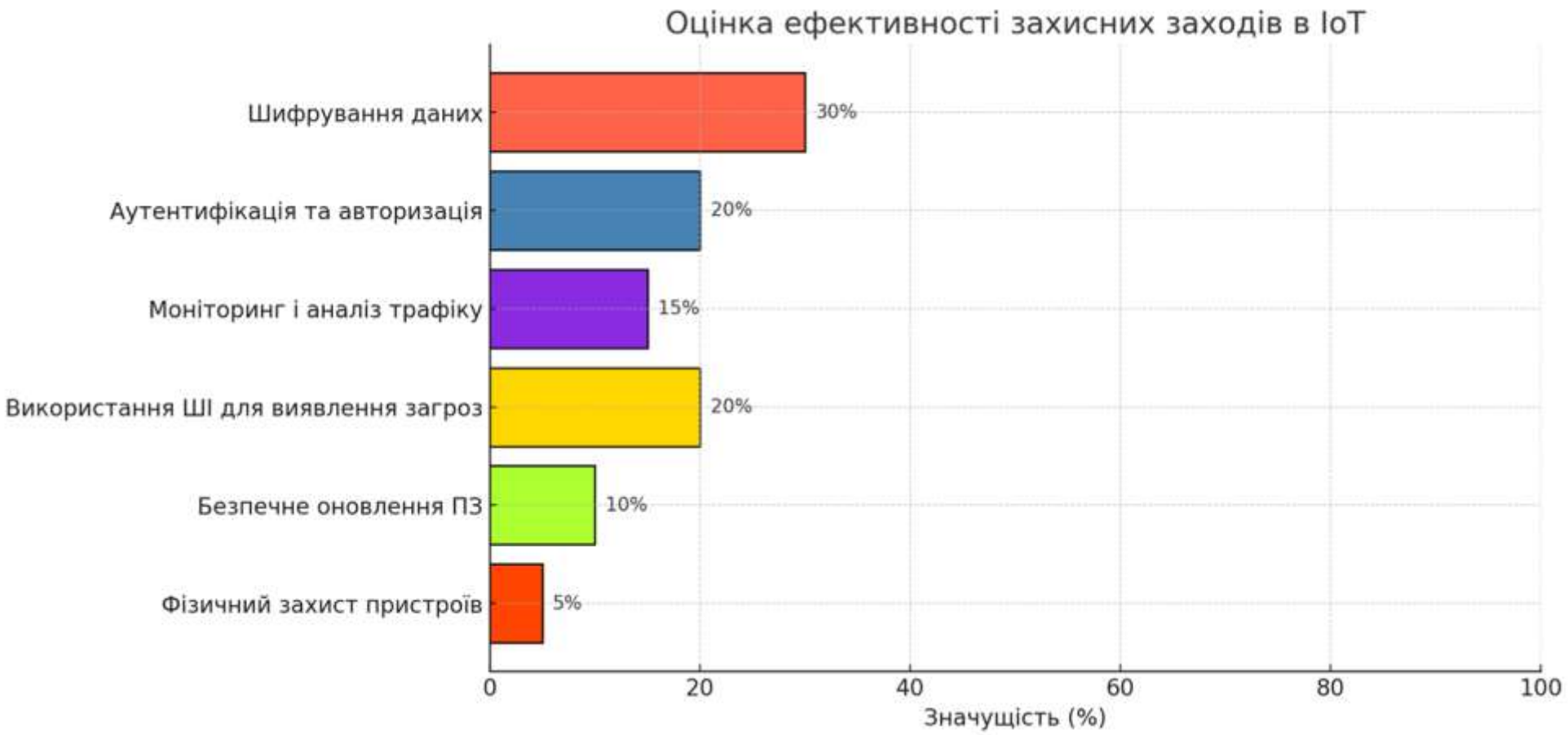
Що таке IoT?

Його ринок

Проблеми

Аналіз вразливостей в IoT

Оцінка ефективності захисних заходів



Рішення для підняття рівня безпеки

Мінімальне: Використання стандартних підходів

Шифрування даних: Захист інформації при передачі та зберіганні.
Аутентифікація та авторизація: Контроль доступу до пристроїв та даних.
Моніторинг і аналіз трафіку: Виявлення підозрілої активності та загроз.
Безпечне оновлення ПЗ: Регулярне оновлення прошивки та ПЗ для усунення вразливостей.
Фізичний захист пристроїв: Запобігання несанкціонованому фізичному доступу до пристроїв IoT.

Максимальне: Використання інноваційних підходів

ШІ для виявлення та реагування на загрози: Автоматичне виявлення аномалій та реагування на загрози в реальному часі.
Машинне навчання для прогнозування загроз: Аналіз поведінки мережі та передбачення можливих атак.
Big Data для підвищення ефективності захисту: Обробка великого обсягу даних для виявлення складних шаблонів загроз.
Блокчейн для безпеки транзакцій: Надійний та незмінний облік дій та транзакцій в мережах IoT.

Висновки

- Досліджено та виявлено основні проблеми безпеки в мережах IoT, показано світові тенденції, проаналізовано методи захисту, простежено еволюцію безпеки, окреслено та виокремлено ефективні методи машинного навчання та інтеграції ШІ, визначено рекомендації для покращення стандартів і обґрунтовано комплексний підхід до зниження ризиків кібератак.

- Апробація:

Андреєв Я.О. “Застосування штучного інтелекту та машинного навчання для захисту від піратства”. Тези доповіді на V Міжнародно науково-технічній конференції «сучасний стан та перспективи розвитку iot» .

Андреєв Я.О. “Захист великих обсягів даних у мережах IoT: виклики та можливості Big Data аналізу”. Тези доповіді на Всеукраїнську науково-технічна конференція «Застосування програмного забезпечення в інформаційно-комунікаційних технологіях».