Дзядик Володимир,
студент 2 курсу
Галицький фаховий коледж імені В'ячеслава Чорновола
Тернопільської міської ради Тернопільської області
Посвятовська О.Б.
спеціаліст вищої категорії, викладач-методист
Галицький фаховий коледж імені В'ячеслава Чорновола
Тернопільської міської ради Тернопільської області
helgaposv@gmail.com

БЕЗПЕКА В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ ЯК АКТУАЛЬНА СКЛАДОВА ЇХ ЯКІСНОГО ФУНКЦІОНУВАННЯ

Анотація

В публікації розглянуто питання безпеки в системах Інтернету речей (IoT), які є важливою складовою сучасного цифрового світу. Проаналізовано основні загрози безпеці IoT, методи їх запобігання та перспективи розвитку захищених технологій. Розглянуто проблеми аутентифікації, шифрування, сегментації мереж в забезпеченні безпеки.

Ключові слова: Інтернет речей, кібербезпека, шифрування, штучний інтелект.

Вступ

Інтернет речей (IoT) є сучасною технологією, що забезпечує взаємодію пристроїв через Інтернет, дозволяючи їм автоматично обмінюватися даними та виконувати різні функції без втручання людини. Популярність цієї технології зростає, але разом із тим підвищується ризик кібератак. З огляду на це питання безпеки IoT є надзвичайно актуальним.

Мета і завдання публікації є аналіз основних загроз у безпеці, визначення методів їх запобігання та розгляд перспектив підвищення рівня захищеності IoT-пристроїв.

Основними завданнями є:

- дослідити види кібератак на IoT;
- проаналізувати слабкі місця безпеки IoT-пристроїв;
- визначити ефективні методи забезпечення захисту;
- розглянути перспективи розвитку безпечних технологій IoT.

Виклад основного матеріалу

Інтернет речі (IoT) є однією з ключових технологій сучасного цифрового світу, що активно впроваджується в різні сфери життєдіяльності, включаючи промисловість, медицину, транспорт і побут. Взаємозв'язок розумних пристроїв через Інтернет дозволяє автоматизувати процеси, збирати та аналізувати великі обсяги даних, а також підвищувати ефективність систем управління. Проте, стрімке розширення мережі IoT супроводжується численними ризиками, пов'язаними з кібербезпекою, що потребують ретельного аналізу та розробки ефективних механізмів захисту пристроїв[1]. Питання кібербезпеки пристроїв IoT напряму залежить від кількості пристроїв (Рисунок 1).

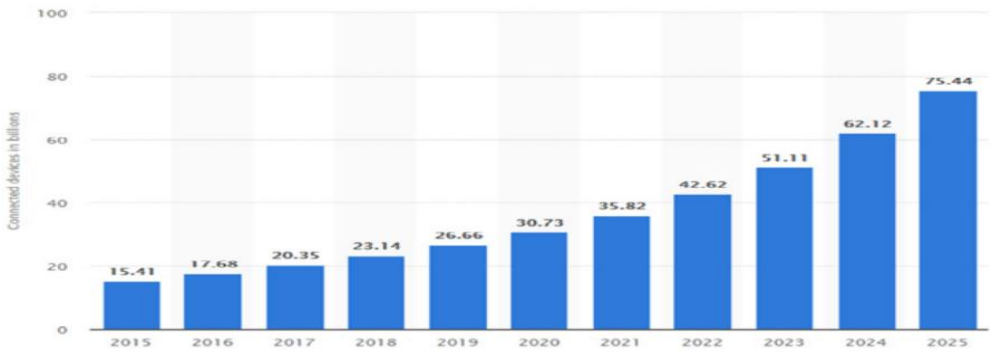


Рисунок 1. Кількість IoT пристроїв

Однією з основних загроз для безпеки IoT є кібератаки на пристрої зі слабким шифруванням та наявність вразливостей. Зловмисники можуть використовувати слабкі паролі, вразливості програмного забезпечення або недостатній рівень шифрування для отримання несанкціонованого доступу до пристроїв. Це може призвести до перехоплення конфіденційної інформації, маніпуляції даними або навіть управління критично важливими системами. Відомий випадок атаки на сервіс Dyn у 2016 році показав, що заражені IoT-пристрої можуть бути використані для масштабних DDoS-атак [2], що виводять з ладу великі інтернет-ресурси. Крім того, хакери можуть використовувати компрометовані пристрої для шпигунства, підміни даних або поширення шкідливого програмного забезпечення.

Ще однією серйозною проблемою є незахищеність самих пристроїв. Багато виробників прагнуть скоротити час виходу продукту на ринок, нехтуючи заходами кібербезпеки. Це призводить до того, що IoT-пристрої мають обмежені можливості щодо автентифікації користувачів, зберігають паролі у відкритому вигляді або використовують застарілі алгоритми шифрування. Відсутність регулярних оновлень і патчів лише посилює проблему, залишаючи пристрої вразливими до нових типів атак. Також багато IoT-пристроїв працюють у відкритих мережах без належного контролю доступу, що робить їх легкою мішенню для зловмисників.

Важливим питанням є також ризик витоку персональних даних. IoT-пристрої часто обробляють інформацію про місцезнаходження користувачів, їхні фінансові операції, стан здоров’я та інші конфіденційні відомості. Якщо ці дані потрапляють до рук зловмисників, це може призвести до фінансових втрат, порушення приватності та навіть фізичної небезпеки. Наприклад, хакери можуть отримати доступ до розумного замка або системи відеоспостереження, що відкриває можливості для крадіжок та інших злочинів. Також витік медичних даних може використовуватися для шантажу або шахрайських схем.

Щоб забезпечити належний рівень безпеки IoT, необхідно впроваджувати комплексні заходи захисту. Насамперед це стосується автентифікації та шифрування. Оскільки пристрої часто енергозалежні асиметричні алгоритми шифрування не використовуються для постійного зв’язку з сервером керування. Натомість використовуються симетричні алгоритми з «достатнім» рівнем шифрування, котрі не використовують багато ресурсів при їх застосуванні (Таблиця 1).

Таблиця 1 – Широко вживані симетричні алгоритми шифрування для пристроїв IoT

Шифр	Розмір блоку (біт)	Розмір ключа (біт)	Рівень безпеки
AES	128	128	0.70
LBlock	64	80	0.72
PRESENT	64	80	0.84
PRINCE	64	128	0.83
RC5	64	128	0.90

Використання двофакторної аутентифікації, та впровадження сучасних криптографічних алгоритмів, таких як AES-256, а також сертифікатів безпеки SSL/TLS дозволяє значно знизити ризик несанкціонованого доступу. Крім того, важливим є регулярне оновлення програмного забезпечення, що дає змогу закривати відомі вразливості та протидіяти новим загрозам. Додатково варто використовувати унікальні паролі для кожного пристрою, оскільки стандартні паролі, встановлені виробником, є основною мішенню для атак.

Одним із ефективних методів підвищення безпеки є сегментація мережі. Виділення окремої мережі для IoT-пристроїв дозволяє обмежити доступ до них з основної мережі та мінімізувати можливі ризики компрометації. Додатковим механізмом є впровадження блокчейн-технологій [3], що забезпечують децентралізоване та захищене зберігання даних. Завдяки неможливості підробки інформації блокчейн може бути використаний для перевірки автентичності пристроїв та безпечної передачі команд між ними. Також блокчейн може застосовуватися для створення безпечних журналів подій, що дозволяє швидко виявляти та аналізувати підозрілі дії в системі.

Штучний інтелект відіграє дедалі важливішу роль у забезпеченні безпеки IoT. Машинне навчання дозволяє аналізувати поведінку пристроїв у режимі реального часу, виявляти аномальні дії та своєчасно реагувати на потенційні загрози. Алгоритми штучного інтелекту можуть автоматично блокувати підозрілі запити, запобігаючи кібератакам ще до їхнього виконання. Крім того, AI може використовуватися для аналізу трафіку в мережах IoT, що дозволяє швидко ідентифікувати підозрілі дії та запобігати їхньому розвитку.

У 2025 році експерти прогнозують зростання загроз для IoT через активне впровадження 5G-мереж, що створюють нові точки входу для зловмисників. Особливо вразливими залишаються пристрої «розумного міста», які керують критично важливою інфраструктурою. Для підвищення безпеки очікується посилене регулювання галузі та впровадження нових технологій, таких як Zero Trust Architecture (ZTA), яка передбачає постійну перевірку кожного підключеного пристрою. Додатково набувають популярності технології кібербезпеки на основі поведінкового аналізу, які використовують AI для відстеження аномальних дій та вчасного реагування на потенційні загрози.

Безпека IoT є не просто технічним викликом, а важливим чинником, що визначає ефективність і надійність цієї технології. Впровадження комплексних заходів захисту, зокрема шифрування, автентифікації, використання AI та блокчейн-технологій, дозволить зробити Інтернет речей безпечнішим. Для досягнення цього необхідна спільна робота виробників, користувачів та

державних органів, спрямована на створення надійного цифрового середовища. Оскільки IoT продовжує зростати, зростатимуть і виклики щодо його безпеки, тому важливо завчасно впроваджувати відповідні механізми захисту, щоб уникнути масштабних загроз у майбутньому.

Висновок

Безпека Інтернету речей відіграє важливу роль у його стабільному функціонуванні. Використання сучасних методів, таких як шифрування, багатофакторна аутентифікація, блокчейн і штучний інтелект, допомагає знизити ризики кібератак і витоку даних. Однак загрози постійно змінюються, тому необхідний комплексний підхід до захисту IoT. Важливо, щоб виробники, користувачі та регулятори співпрацювали задля створення надійного середовища, адже це впливає на безпеку та ефективність цифрових технологій у майбутньому.

Список використаних джерел

1. Голод Ю.В., Гарматюк В.Р., Волос І.П. Мережеві атаки на інтернетречей. Матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2023. – С. 39-42.

2. Дзівак О.А., Мачуляк М.В., Волос І.П. Фізичні атаки на мережі інтернет-речей. Матеріали науково-практична конференція молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2023), Тернопіль, 2023. – С. 100-102.

3. Яцків Н. Г. Перспективи використання технології блокчейн у мережі інтернет речей / Н. Г. Яцків, С. В. Яцків // Науковий вісник НЛТУ України. - 2016. - Вип. 26.8. - С. 381-387. - Режим доступу: http://nbuv.gov.ua/UJRN/nvnltu_2016_26.

Довгалюк Олена Олегівна
учениця 10-В класу
Тернопільська спеціалізована школа І-ІІІ ступенів №3
з поглибленим вивченням іноземних мов
Тернопільської міської ради Тернопільської області
Рудяк Юрій Аронович
доктор технічних наук, професор,
завідувач кафедри медичної фізики
Тернопільського національного медичного університету
м. Тернопіль
dovgalyuk.olena@icloud.com

ПОЄДНАННЯ ЕЛЕМЕНТІВ ТЕОРІЇ ХАОСУ ТА DATA SCIENCE ДЛЯ ЗБІЛЬШЕННЯ ЕФЕКТИВНОСТІ МЕДИЧНИХ ПРОГНОЗІВ

Анотація

У роботі запропоновано поєднання підходів теорії хаосу та Data Science для отримання довгострокових прогнозів результатів лікування (включаючи оцінку