його поведінку та наочним способом дослідити поведінку рідини в трубопроводі. На основі рівняння Пуазейля побудовано графіки розподілу швидкості рідини як уздовж радіуса, так і в поперечному перерізі труби. Результати моделювання мають практичну цінність для фахівців аграрної галузі, зокрема при проектуванні систем зрошення, де важливо забезпечити рівномірну подачу води.

Список використаних джерел

1. Переваги крапельного зрошення в агрономії. *Landlord*. URL: https://landlord.ua/agrolife-en/perevagi-vikoristannya-krapelnogo-zroshennya-v-agronomiyi/ (дата звернення 04.05.2025).

2. Дяденчук А. Ф., Шквиря В. В. Формування інформаційно-математичної компетентності здобувачів вищої освіти в загальному курсі фізики. *Інженерні та освітні технології*. 2022. Т. 10, № 1. С. 30-41.

3. Коробко І. В. Визначення запізнення в передачі тиску імпульсними трубками вимірювальних перетворювачів витрати газу, які базуються на методі змінного перепаду тиску. *Вісник Національного технічного університету України" Київський політехнічний інститут". Серія: Приладобудування*. 2012. Вип. 43. С. 95-100.

Науковий керівник: *Дяденчук А. Ф., к.т.н., доцент кафедри ВМФ Таврійського державного агротехнологічного університету імені Дмитра Моторного.*

БЕЗПЕКА ІО-Т ПРИСТРОЇВ: ВИКЛИКИ ТА РІШЕННЯ
Ціль сталого розвитку №9: Інновації та інфраструктура

Тронько С. О. hanna.hesheva@tsatu.edu.ua
Таврійський державний агротехнологічний університет імені Дмитра Моторного

У сучасному світі технологій Інтернет речей (IoT) став невід'ємною частиною цифрової трансформації різних галузей. Однак зростаюча кількість підключених пристроїв створює безпрецедентні виклики для кібербезпеки. Дослідження показують, що кількість вразливостей в IoT-системах стрімко зростає, а методи атак стають все складнішими, включаючи ботнети, програми-вимагачі та цільові кібератаки. Особливу занепокоєність викликає інтеграція штучного інтелекту з IoT (AIoT), що одночасно створює нові можливості та ризики. Ця стаття досліджує ключові виклики безпеки IoT-пристроїв, аналізує наявні вразливості та пропонує сучасні підходи до їх вирішення, включаючи технології шифрування, блокчейн, удосконалені методи автентифікації та комплексні стратегії кібербезпеки.

Вступ до проблематики IoT-безпеки

Інтернет речей (IoT) трансформує наш світ, з'єднуючи мільярди пристроїв у єдину мережу для збору, обміну та аналізу даних. З розвитком IoT, його еволюція призвела до появи концепції AIoT – інтеграції штучного інтелекту з інтернетом речей, що розширює функціональні можливості підключених пристроїв [1]. Однак ця еволюція супроводжується значними викликами у сфері кібербезпеки. Важливість забезпечення безпеки IoT-пристроїв зумовлена кількома чинниками. По-перше, ці пристрої збирають, обробляють та передають величезні обсяги даних, серед яких можуть бути конфіденційні особисті дані або критично важлива виробнича інформація. По-друге, IoT-пристрої часто

стають мішенню для кіберзлочинців через їхні вразливості та можливість використання як плацдарму для атак на більш захищені системи. По-третє, в таких галузях як охорона здоров'я, транспорт чи промисловість, компрометація IoT-систем може призвести не лише до фінансових втрат, але й до фізичних загроз для людей [1]. Сучасні дослідження вказують на експоненційне зростання кількості IoT-пристроїв, що призводить до суттєвого розширення поверхні для кібератак. З інтеграцією штучного інтелекту в IoT-системи, виникають як нові можливості для посилення безпеки, так і нові вразливості, які потребують ретельного аналізу та розробки ефективних стратегій захисту.

Ключові виклики безпеки IoT-пристроїв

Технічні виклики та вразливості

Серед найкритичніших технічних викликів безпеки IoT-пристроїв визначається проблема слабких, легко вгадуваних або апаратно закодованих паролів. Багато IoT-пристроїв постачаються із заводськими паролями, які користувачі часто не змінюють, що робить їх легкою мішенню для кіберзлочинців [3]. Крім того, деякі виробники вбудовують незмінні паролі безпосередньо у прошивку пристроїв, що унеможливлює їх зміну навіть свідомими користувачами.

Незахищені мережеві сервіси становлять ще один суттєвий виклик. IoT-пристрої часто мають відкриті порти та сервіси, які можуть бути використані для несанкціонованого доступу. Відсутність належного шифрування при передачі даних робить їх вразливими до перехоплення та модифікації сторонніми особами [2]. Особливо небезпечним є те, що багато IoT-пристроїв не підтримують сучасні протоколи шифрування через обмеження обчислювальних ресурсів. Незахищені інтерфейси, як веб-портали керування або мобільні додатки, часто містять вразливості, які дозволяють зловмисникам отримати контроль над пристроями. Ці вразливості можуть включати слабкі методи автентифікації, відсутність перевірки введених даних або недостатній захист сеансів користувачів [2]. При цьому компрометація одного пристрою може призвести до ланцюгової реакції в мережі IoT через горизонтальне переміщення зловмисників.

Проблеми конфіденційності та контролю доступу

IoT-пристрої збирають значні обсяги даних, часто без належного інформування користувачів про характер та обсяг цього збору. Недостатній захист конфіденційності може призвести до витоку особистої інформації, починаючи від звичок користувачів і закінчуючи даними про здоров'я або місцезнаходження [2]. Такі витоки можуть мати серйозні наслідки для приватності та безпеки осіб. Слабкі механізми автентифікації та контролю доступу є ще одним суттєвим викликом. Багато IoT-пристроїв не підтримують багатофакторну автентифікацію або детальне розмежування прав доступу, що ускладнює захист від несанкціонованого доступу [2]. Це особливо критично для промислових IoT-систем, де компрометація може призвести до порушення виробничих процесів або створення небезпечних умов. Проблеми із захистом API (Application Programming Interface) також становлять значний ризик для IoT-систем. Незахищені або недостатньо захищені API можуть дозволити зловмисникам отримати доступ до даних або функціональності IoT-пристроїв через легітимні канали взаємодії [2]. Часто розробники нехтують належним тестуванням безпеки API, що призводить до вразливостей, які можуть бути використані зловмисниками.

Основні загрози для IoT-систем

Програми-вимагачі та цільові атаки

Програми-вимагачі (ransomware) стали значною загрозою для IoT-середовища. Ці шкідливі програми шифрують дані або блокують функціональність пристроїв, вимагаючи викуп за відновлення доступу [2]. У контексті IoT така атака може мати катастрофічні наслідки, особливо для критичних систем, таких як медичне обладнання або системи промислової автоматизації. Цільові атаки на IoT-пристрої часто проводяться з метою промислового шпигунства, саботажу або крадіжки інтелектуальної власності. Такі атаки зазвичай ретельно плануються з урахуванням специфіки цільової організації та

використовуваних нею IoT-систем [2]. Цільові атаки можуть залишатися непоміченими протягом тривалого часу, завдаючи значної шкоди компаніям. Особливо небезпечними є просунуті постійні загрози (Advanced Persistent Threats, APT), які характеризуються тривалим перебуванням у системі, збором інформації та поступовим розширенням доступу. В контексті IoT такі загрози можуть використовувати вразливості пристроїв для проникнення в мережу та подальшого руху до більш критичних систем [2].

Фізичні загрози та ризики шпигунства

На відміну від традиційних IT-систем, IoT-пристрої часто розміщуються у фізично доступних місцях, що створює додаткові ризики безпеки. Несанкціонований фізичний доступ до IoT-пристроїв може дозволити зловмисникам модифікувати апаратне забезпечення, встановлювати шкідливе програмне забезпечення або викрадати конфіденційні дані [2]. Такі фізичні атаки можуть бути особливо небезпечними через складність їх виявлення традиційними системами безпеки. Шпигунство та підслуховування становлять ще одну серйозну загрозу, особливо для IoT-пристроїв, оснащених засобами запису аудіо та відео. Скомпрометовані розумні колонки, камери спостереження або інші пристрої з можливостями запису можуть перетворитися на інструменти для стеження за користувачами та збору конфіденційної інформації [2]. Це створює ризики як для приватних осіб, так і для організацій, де через такі пристрої може відбуватися витік комерційних таємниць або стратегічної інформації. Загрози фізичній безпеці можуть виникати, коли IoT-пристрої керують критичними системами, такими як медичне обладнання, системи контролю доступу або промислові установки. Компрометація таких пристроїв може призвести до фізичних ушкоджень, створення небезпечних умов або загрози життю людей [2]. Це робить безпеку IoT-пристроїв питанням не лише інформаційної безпеки, але й фізичної безпеки.

Стратегії та рішення для забезпечення безпеки

Технічні заходи захисту

Ефективне забезпечення безпеки IoT-пристроїв вимагає комплексного технічного підходу. Шифрування даних у стані спокою та під час передачі є одним із фундаментальних заходів, який захищає від несанкціонованого доступу та перехоплення інформації [1]. Для IoT-пристроїв важливо використовувати ефективні алгоритми шифрування, які можуть працювати з обмеженими обчислювальними ресурсами без суттєвого впливу на продуктивність. Посилення механізмів автентифікації є критично важливим для запобігання несанкціонованому доступу. Впровадження багатофакторної автентифікації, використання сертифікатів та токенів безпеки, а також унікальних, складних паролів для кожного пристрою значно підвищують рівень захисту [2]. Особливо важливо забезпечити можливість зміни заводських паролів та регулярне оновлення облікових даних.

Сегментація мережі та використання мікросегментації допомагають ізолювати IoT-пристрої від критичних систем та обмежити горизонтальне переміщення зловмисників у разі компрометації окремих пристроїв [1]. Реалізація безпечних шлюзів IoT дозволяє централізовано керувати з'єднаннями між IoT-пристроями та іншими мережами, забезпечуючи додатковий рівень захисту.

Управління вразливостями та оновленнями

Регулярне сканування та оцінка вразливостей IoT-систем є важливим елементом стратегії безпеки. Це дозволяє виявляти потенційні вразливості до того, як вони будуть використані зловмисниками, та вживати відповідних заходів для їх усунення [1]. Для ефективного сканування IoT-пристроїв необхідно використовувати спеціалізовані інструменти, адаптовані до особливостей таких систем.

Забезпечення безпечного та автоматизованого процесу оновлення програмного забезпечення IoT-пристроїв є критичним для підтримки їх безпеки. Механізми оновлень повинні включати перевірку цілісності оновлень, шифрування каналів передачі та можливість відкату у разі проблем [2]. Важливо також розробити стратегію для роботи з

застарілими пристроями, які більше не отримують оновлень безпеки.

Управління життєвим циклом IoT-пристроїв повинно включати чіткі процедури для безпечного виведення з експлуатації пристроїв, включаючи видалення чутливих даних та відкликання облікових даних [2]. Це запобігає використанню застарілих пристроїв як векторів атаки на мережу.

Список використаних джерел

1. Khan S. & Herrmann P. (2020). Future developments in standardisation of cyber risk in the Internet of Things (IoT). arXiv preprint arXiv:1903.04428.
2. Jooby. Прогноз тенденцій розвитку Інтернету речей у 2025 році.
3. USP-LTD. Як працює Інтернет речей: суть технології та її застосування в світі.
4. ITCCI. Огляд рішень з апаратної безпеки кінцевих пристроїв туманних обчислень в мережах Інтернету речей.
5. ITCE. Засоби захисту Internet of Things в корпоративній комп'ютерній мережі.

Науковий керівник: *Гешева Г. В., асистент кафедри комп'ютерних наук Таврійського державного агротехнологічного університету імені Дмитра Моторного.*

ЗАСТОСУВАННЯ GOOGLE ТАБЛИЦЬ ДЛЯ ВЕДЕННЯ СТАТИСТИКИ ЕНЕРГОСПОЖИВАННЯ В ПОБУТІ

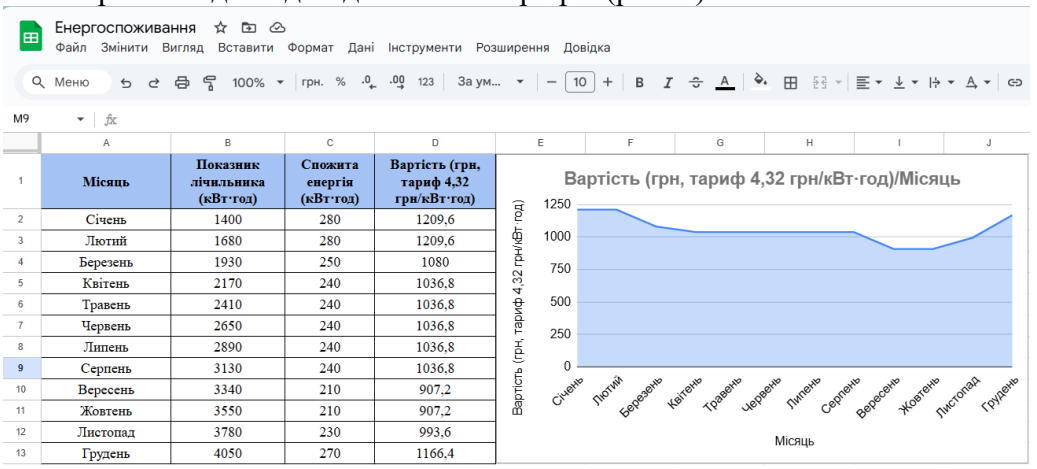
Ціль 12: Відповідальне споживання

Устименко А. Ю. kitamorro@gmail.com
Таврійський державний агротехнологічний університет імені Дмитра Моторного

У сучасних умовах зростання тарифів на електроенергію важливо раціонально використовувати енергоресурси навіть у побуті. Більшість користувачів не веде регулярного обліку енергоспоживання, що призводить до неефективного використання електроенергії та зайвих витрат. Одним з доступних способів контролю енергоспоживання є ведення регулярної статистики. Завдяки Google Таблицям можна створити просту, але зручну систему обліку без необхідності встановлення додаткового програмного забезпечення.

Мета роботи полягала в побудові системи моніторингу електроспоживання з використанням Google Таблиць, а також аналіз споживання та виявлення тенденцій або перевитрат.

Для контролю витрат електроенергії щотижня впродовж року до Google Таблиці вносилися дані електролічильника. Завдяки використанню вбудованих формул, таких як SUM, AVERAGE та IF, система автоматично розраховувала спожиту електроенергію (кВт·год) та її вартість відповідно до чинних тарифів (рис. 1).



	Місяць	Показник лічильника (кВт·год)	Спожита енергія (кВт·год)	Вартість (грн, тариф 4,32 грн/кВт·год)
2	Січень	1400	280	1209,6
3	Лютий	1680	280	1209,6
4	Березень	1930	250	1080
5	Квітень	2170	240	1036,8
6	Травень	2410	240	1036,8
7	Червень	2650	240	1036,8
8	Липень	2890	240	1036,8
9	Серпень	3130	240	1036,8
10	Вересень	3340	210	907,2
11	Жовтень	3550	210	907,2
12	Листопад	3780	230	993,6
13	Грудень	4050	270	1166,4