УДК 004.056:[004.738.5:338.46] DOI: 10.31673/2412-4338.2024.020515

Гайдур Галина Іванівна
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0003-0591-3290

Шулімова Дар'я Денисівна
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0002-9557-990X

Бойко Анна Олександрівна
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0001-3709-6283

Постніков Єгор Ігорович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0000-4358-928X

МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

***Анотація**: Інтернет речей вважається новим етапом розвитку Інтернету, на якому відбувається обмін даними між фізичними об'єктами, підключеними до мережі, і кожен пристрій може самостійно взаємодіяти та встановлювати зв'язки з мільярдами інших речей. IoT дозволяє людям виконувати різні завдання віддалено, що полегшить життя в майбутньому.*

У статті враховано особливості цієї технології, а також важливість розробки планів на випадок надзвичайних ситуацій щодо відновлення після потенційних кібератак у сфері Інтернету речей. Особлива увага приділяється ролі державних органів у забезпеченні кібербезпеки Інтернету речей, включаючи розробку нормативно-правових актів та співпрацю з приватним сектором і науковими установами.

Інтернет речей охоплює широкий спектр процесів: обчислення, зв'язок, час і дані. Як ці функції функціонують як єдина система з використанням комерційно доступних компонентів, які можна придбати будь-де за низькою ціною та в невеликих кількостях. Оскільки кількість пристроїв IoT продовжує зростати, очікується, що їх кількість досягне позначки в 36 мільярдів та відбудеться багато великих змін. Ринок IoT стрімко зростає, відкриваючи величезний бізнес-потенціал для постачальників послуг зв'язку, галузей і підприємств.

Стаття висвітлює існуючі підходи до цієї проблеми та їх переваги та недоліки. Надається огляд інноваційних стратегій та моделей забезпечення кібербезпеки, зокрема нова модель, яка поєднує в собі кращі практики та інноваційні рішення. Детально розглядаються складові цієї моделі, такі як заходи з контролю доступу, шифрування даних, моніторинг мережі та виявлення вторгнень. Особлива увага приділяється стратегіям співпраці з виробниками пристроїв IoT для успішного впровадження запропонованої моделі в практику. В заключенні наголошується на постійному вдосконаленні та адаптації забезпечення кібербезпеки відповідно до зростаючих загроз та розвитку технологій IoT.

***Ключові слова:** кібербезпека, Інтернет речей, нормативно-правове забезпечення, IoT, математична модель, програмний код.*

Haidur Halyna
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0003-0591-3290

Shulimova Daria
State University of Information and Communication Technologies, Kyiv
ORCID 0009-0002-9557-990X

Boiko Anna
State University of Information and Communication Technologies, Kyiv
ORCID 0009-0001-3709-6283

Postnikov Ehor
State University of Information and Communication Technologies, Kyiv
ORCID 0009-0000-4358-928X

THE MODEL OF PROVIDING CYBER SECURITY OF THE INTERNET OF THINGS

Abstract: *The Internet of Things is considered to be a new stage in the development of the Internet, where physical objects connected to the network exchange data, and each device can independently interact and establish connections with billions of other things. The Internet of Things allows people to perform various tasks remotely, which will make life much easier in the future.*

This article explores the specifics of the technology and the importance of developing contingency plans to recover from potential IoT cyberattacks. Special attention will be paid to the role of government entities in ensuring the security of IoT networks, including the development of regulations and cooperation with the private sector and academic institutions.

The Internet of Things encompasses a variety of steps: computational, communication-based, temporal and data-based. How these functions as a single system utilizing commercially available components that can be purchased easily and at a low cost. As the number of IoT devices continues to increase, it is expected to have a total of 36 billion members and significant changes will occur. The IoT market is expanding rapidly, this will allow communication service providers, industries and companies to have a large potential for revenue.

The article discusses existing approaches to this issue and their benefits and drawbacks. A general description of innovative cybersecurity strategies and approaches is presented, including a new combination of practical strategies and innovative solutions. Components of the model, including access control, data encryption, network monitoring, and intrusion detection, are detailed in depth. Particular attention is devoted to partnerships with IoT device manufacturers in order to successfully apply the proposed model in real life. The conclusion states that cyber security should be constantly improved and altered in response to the increasing dangers and the development of IoT technologies.

Keywords: *cyber security, Internet of Things, legal framework, IoT, mathematical model, software code.*

1. Вступ.

Інтернет речей (IoT) надзвичайно швидко перетворюється на ключовий елемент сучасних технологічних інфраструктур, проникаючи у різноманітні сфери життя користувачів, від побутових пристроїв до промислових систем. Зростання обсягів підключених пристроїв зумовлює неабияке підвищення продуктивності та зручності, однак це також викликає серйозні виклики у сфері кібербезпеки. Відомо, що із розвитком технологій зростає і кількість потенційних загроз для безпеки мережі IoT, які можуть мати негативні наслідки для інфраструктури та приватності користувачів.

У зв'язку з цим виникає необхідність вдосконалення моделей забезпечення кібербезпеки для Інтернету речей. Поточні підходи до кіберзахисту виявляються недостатніми у боротьбі зі зростаючими загрозами, оскільки технологічний ландшафт постійно еволюціонує. Із цією метою пропонується дослідження моделі забезпечення кібербезпеки IoT, яка б враховувала сучасні виклики та здатна була ефективно запобігати й виявляти загрози для безпеки підключених пристроїв[1].

У статті розглянуто існуючі підходи до забезпечення кібербезпеки в контексті IoT, проаналізовано їх переваги та недоліки, а також представлено модель забезпечення кібербезпеки Інтернету речей, яка базується на сучасних технологіях та кращих практиках в цій області. Робота спрямована на розробку комплексного підходу до кіберзахисту IoT, що враховуватиме специфіку цього сегменту технологій та забезпечить ефективний захист від ризиків інформаційної безпеки.

2. Постановка проблеми.

Впровадження заходів кібербезпеки для Інтернету речей відрізняється від стандартних заходів кібербезпеки. Кожен пристрій може стати точкою входу для зловмисників, які можуть використовувати їх для отримання несанкціонованого доступу до мережі чи виконання зловмисних дій. Ця проблема загрожує не лише приватності та безпеці користувачів, а також може мати серйозні наслідки для інфраструктури та функціонування систем, які залежать від IoT. Також потрібні вдосконалені нормативно-правові акти, які будуть регулювати правові аспекти кібербезпеки в IoT та міжнародні стандарти. Таким чином, ефективне забезпечення кібербезпеки в мережі IoT стає критично важливим завданням у сучасному технологічному середовищі.

3. Виклад основного матеріалу.

Інтернет речей (Internet of Things) – це мережева концепція, що складається з взаємопов'язаних фізичних пристроїв з вбудованими датчиками і програмним забезпеченням, які дозволяють передавати і обмінюватися інформацією між фізичними та комп’ютерними системами в автоматизованому режимі, використовуючи стандартні протоколи зв'язку. Крім датчиків, пристрої також можуть бути з'єднані між собою в дротові або бездротові мережі. Дані взаємопов'язані пристрої можуть зчитувати і приводити в дію, програмувати та ідентифікувати, а використання інтелектуальних інтерфейсів робить втручання людини непотрібним[2].

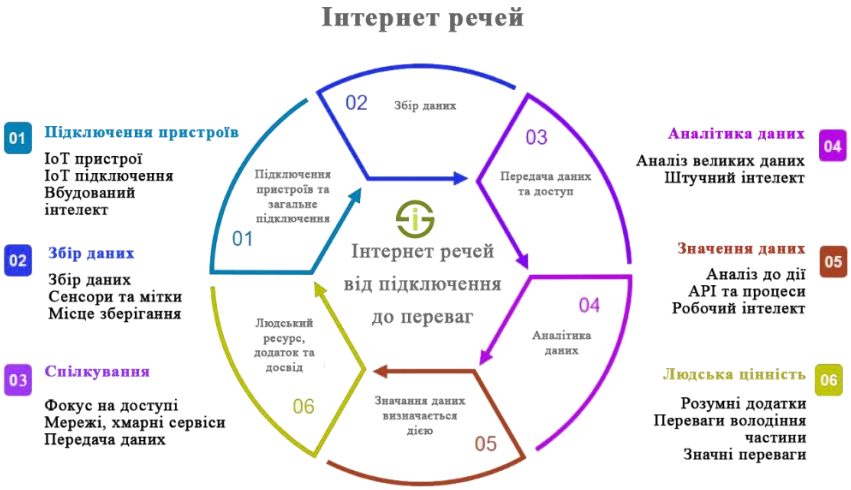

Рис. 1. Середовище Інтернету речей

IoT мають безліч різних сфер застосування:

1. Смарт-будинок: Управління освітленням, опаленням, кондиціонером, безпековими камерами та іншими системами вдома за допомогою смартфону або голосового асистента.
2. Смарт-автомобіль: Системи моніторингу та діагностики автомобілів, навігація, безпека на дорозі та автопілоти.
3. Смарт-міста: Вимірювання якості повітря, управління затратами на енергію та світлофорами, публічний транспорт та сміттєві системи.
4. Охорона: Системи відеоспостереження (IP-камери зможуть ідентифікувати людей за обличчям, транспортні засоби за номером, збирати статистику та повідомляти правоохоронні органи про порушення), сигналізації та безпеки приміщень.
5. Медицина: Відстеження стану пацієнтів, носимі медичні пристрої, які передають дані лікарям (Онлайн-платформа «Київстар» «Центр управління Інтернетом речей» допомагає медичним компаніям дистанційно керувати SIM-картами в розумних пристроях).
6. Енергетика: Моніторинг та управління електромережами, акумуляторами та розподілом енергії (У країнах Європи використовують окремий термін Internet of Energy).
7. Екологія: Моніторинг довкілля, включаючи рівень забруднення повітря, води та грунту.

8. Виробництво (IIoT): Відстеження робочих процесів, підвищення продуктивності, попередження витрат та обслуговування обладнання.

9. Смарт-сільське господарство: Моніторинг та автоматизація поливу, вирощування та збір даних про врожайність, контроль стану тварин та птахів.

Таблиця 1

Положення про безпеку, пов'язані з IoT

Положення, №	Назва	Тлумачення
1	Відсутність універсальних паролів за замовчуванням	Паролі повинні бути унікальні для кожного пристрою. Також доцільне використання багатофакторної автентифікації, наприклад використання пароля та одноразовий пароль.
2	Впровадження процесів керування звітами про вразливість	В сферу Інтернету речей потрібно впроваджувати CVD (набір процесів для роботи з розкриттям інформації про потенційну безпеку, вразливості та підтримку усунення цих вразливостей)
3	Оновлення програмного забезпечення	Рекомендується постійно оновлювати все програмне забезпечення.
4	Збереження конфіденційних параметрів безпеки	Конфіденційні параметри безпеки повинні надійно зберігатися на пристрої.
5	Безпека спілкування	Пристрої IoT мають підтримувати безпечний зв'язок із використанням безпеки транспортного рівня (TLS) або полегшеної криптографії (LWC) і завжди використовувати найновіші версії. Це означає, що конфіденційні дані мають бути зашифровані під час передачі, а ключами потрібно безпечно керувати.
6	Мінімізування можливості для атаки	Всі пристрої та служби повинні працювати за «принципом найменших привілеїв». Це один із найважливіших принципів, пов'язаний із якістю коду, оскільки дефекти програмного забезпечення або вразливі місця коду є вразливостями, якими користуються зловмисники.
7	Забезпечення цілісності програмного забезпечення	IoT-пристрій повинен перевіряти власне програмне забезпечення. Якщо виявлено несанкціоновану зміну програмного забезпечення, пристрій повинен повідомляти користувача та/або адміністратора.
8	Забезпечення безпеки персональних даних	Персональні дані повинні бути захищені за допомогою найкращої практики криптографії.
9	Стійкість системи до збоїв	Стійкість повинна бути вбудована в пристрої та служби IoT, беручи до уваги можливість відключень мереж передачі даних та електроенергії.
10	Телеметричні дані системи	Телеметричні дані потрібно перевіряти на можливі аномалії безпеки.
11	Спрощення видалення даних користувача	Користувачам повинні бути надані такі функції, щоб дані користувачів можна було легко стерти.
12	Спрощення установки та обслуговування пристроїв	Встановлення та обслуговування IoT-пристрою повинно включати мінімальну кількість рішень користувача та повинні бути зручні у використанні.
13	Перевірка введених даних	IoT-пристрій повинен перевіряти дані, які вводить користувач або були отримані при передачі між мережами в службах і пристроях.

Нормативно-правове забезпечення

У 2020 році Технічний комітет з кібербезпеки (TC CYBER)[3] опублікував ETSI EN 303 645, новий стандарт з кібербезпеки в Інтернеті речей [4]; EN 303 645 був розроблений Національною організацією зі стандартизації на основі специфікації ETSI TS 103 645 (До розробки було залучено більше зацікавлених сторін і зрештою рішення було вдосконалено). Цей новий стандарт є результатом співпраці між промисловістю, науковими колами та урядом.

ETSI EN 303 645 визначає 13 положень про безпеку, пов'язану з Інтернетом речей та супутніми послугами (Табл.1). Продукти Інтернету речей включають інтелектуальні охоронні та пожежні датчики, камери відеоспостереження, дитячі іграшки та радіоняні, розумні будинки, охоронну сигналізацію та інші продукти, пов'язані з безпекою. Новий стандарт з кібербезпеки також містить п'ять положень про захист даних для споживачів Інтернету речей.

Поки що, ETSI EN 303 645 вважається єдиним стандартом, який представляє єдину досяжну мету для виробників і зацікавлених сторін у сфері Інтернету речей. Багато організацій вже побудували свої продукти та схеми сертифікації на основі ETSI EN 303 645 та його попередника TS. Це показує, як один стандарт може підтримувати багато схем довіри і забезпечувати гнучкість сертифікації, зберігаючи при цьому провідний світовий рівень кібербезпеки. В Україні питання кібербезпеки в IoT регулюється Конституцією України та зазначеними законами. В майбутньому дотримання цього стандарту може стати обов'язковим.

Також потрібно забезпечити захист персональних даних користувачів Інтернет речей [5]. В Україні питання крадіжки персональних даних регулюється низкою законів на законодавчому рівні. Наприклад, відповідно до Закону України "Про захист персональних даних" (стаття 12) [6], збір персональних даних є одним з елементів процесу їх обробки, що передбачає діяльність, пов'язану з підбором або упорядкуванням відомостей про фізичних осіб (тобто власників персональних даних, суб'єктів персональних даних). Так і суб'єкти повинні бути проінформовані про склад і зміст інформації, що збирається, їхні права у зв'язку з цим, мету збору та інших суб'єктів, які отримують персональні дані. Крім того, стаття 32 Конституції України [5] піднімає питання захисту та обробки персональних даних інших осіб, згідно з якою не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди.

Якісним нормативно-правовим актом, що має найбільше відношення до захисту персональних даних та кібербезпеки в цьому відношенні, є правовий регламент про захист персональних даних в Інтернеті, відомий як GDPR (The General Data Protection Regulation), що набув чинності 25.05.2018 року. Всі учасники мережі, які беруть участь у зборі, зберіганні та обробці персональних даних, повинні дотримуватися даних правил.

Окрім забезпечення чіткого правового спрямування для захисту користувачів IoT, варто також застосувати підходи технічного та соціального впливу, а саме:

1) Забезпечувати дотримання та захист прав людини в Інтернеті та запобігати дискримінації користувачів.

2) Забезпечити правову визначеність, прозорість і зручність розуміння норм і правових актів для кожного жителя країни.

3) Удосконалити та забезпечити реалізацію законодавства про захист прав споживачів, пов’язаних з використанням обладнання в системі Інтернету речей [8].

4. Математична модель вразливості в IoT.

Математичні моделі вразливості в Інтернеті речей є важливим інструментом для аналізу, передбачення та управління кібербезпекою. Вони допомагають оцінювати ризики, пов'язані з імовірністю виникнення вразливостей у системах IoT. Аналіз безпеки на основі математичних моделей дозволяє розуміти вплив конкретних вразливостей на загальний стан безпеки системи. Крім того, такі моделі допомагають ідентифікувати ключові ризики та визначити стратегії для їх мінімізації. Прогнозування наслідків вразливостей забезпечує можливість передбачати потенційні загрози та вживати відповідних заходів безпеки. На основі аналізу

математичних моделей можна оптимізувати заходи безпеки, забезпечуючи ефективність захисту систем IoT.

Основні рекомендації для запобігання кібератакам та зменшення ризику для компанії згідно звіту української організації Corewin[7]:

1. Моніторинг усіх пристроїв: Спеціалісти з захисту інформації повинні знати точну кількість використовуваних IoT-пристроїв звітувати про положення їх захисту, проводити постійний моніторинг та аналіз.
2. Сегментація мережі: Поділ мережі на ізольовані зони (сегменти) дозволяє підвищити безпеку мережі та оптимізувати її продуктивність. Обмеження поверхні атаки для зловмисника дозволяє зменшити збитки компанії.
3. Встановлення надійних паролів: Пароль повинен бути унікальним для кожного пристрою та бути стійким до підбору.
4. Захист пристроїв на фізичному рівні: Фізичний захист пристроїв є надзвичайно важливим, оскільки доступність пристроїв для зовнішніх осіб може призвести до фізичного втручання зловмисників. Це може стати причиною отримання несанкціонованого доступу до пристроїв або завантаження в них шкідливого програмного забезпечення.
5. Оновлення програмного забезпечення: Оновлення прошивки можуть містити виправлення існуючих програмних вразливостей пристрою, що значно покращує загальний рівень безпеки в Інтернеті речей. Для забезпечення безпеки рекомендується використовувати автоматизовані системи аналізу прошивки пристроїв, які дозволяють контролювати версійність і завжди мати найновішу безпечну версію прошивки[9].

Математичну модель можна записати таким чином:

$$L = (m + s + r + p + u) - (I + N),$$

де L – рівень загрози для компанії, m – моніторинг за IoT- пристроями, s – рівень сегментації мережі, r – надійність паролів для IoT-пристроїв, p – рівень фізичного захисту, u - оновлення програмного забезпечення, I – задіяні ресурси для кібератаки, N – кількість компонентів атаки.

Ця математична модель дає змогу оцінити рівень ризику в залежності від захищеності всіх компонентів IoT-пристроїв та складності кібератаки. Для великої кількості IoT-пристроїв та кібератак цю математичну модель можна змінити таким чином:

$$L = \sum_{i=1}^{n} m(x)s(x)r(x)p(x)u(x) - \sum_{j=1}^{m} I(y)N(y).$$

5. Лістинг коду для захисту IoT.

Для кращого розуміння методів захисту Інтернету речей від кібератак та можливі прогалини у системі безпеки, у статті наведений приклад коду, направлений на захист IoT.

Приклад простого коду на мові програмування Python для реалізації базових заходів безпеки, таких як використання хешування паролів. Хешування пароля – це процес перетворення пароля у фіксований набір символів (хеш), який зазвичай є безумовним.

Hashlib – це модуль в мові програмування Python, що надає можливість використовувати різні хеш-функції. За допомогою hashlib можна обчислювати хеші для різних об’єктів.

Ключовою особливістю хеш-функцій є те, що вони повинні бути чіткими та незворотними. Це означає, що для великої кількості вхідних даних потрібно отримати фіксований, але унікальний хеш.

```python
import hashlib

class IoTDevice:
    def __init__(self, device_id, password):
        self.device_id = device_id
        self.password_hash = self.hash_password(password)

    def hash_password(self, password):
        # Використовуємо хеш-функцію для збереження паролю у вигляді хешу
        hashed_password = hashlib.sha256(password.encode()).hexdigest()
        return hashed_password

    def authenticate(self, entered_password):
        # Перевіряємо, чи введений пароль відповідає збереженому хешу паролю
        entered_password_hash = self.hash_password(entered_password)
        return entered_password_hash == self.password_hash

# Приклад використання
device = IoTDevice(device_id="example_device", password="secure_password")

# Введення користувача для перевірки аутентифікації
user_input_password = input("Enter the device password: ")

if device.authenticate(user_input_password):
    print("Authentication successful!")
else:
    print("Authentication failed.")
```

Рис. 2. Приклад використання модулю hashlib

Таблиця 2

Алгоритми хешування

Алгоритм хешування	Розмір,біт	Опис
MD5	128	Використовується менше через вразливості до колізій. Ситуація, коли хеш-функція дає однаковий результат для різних вхідних даних, називається колізією.
SHA-1	160	Вважається вразливим до колізій і не рекомендується для застосування в криптографічних задачах.
HA-2	256	Більш досконала версія SHA-1.
SHA-3	Залежить від обраного варіанту(224,256,384,512)	Новіший стандарт, призначений замінити SHA-2. Вважається безпечним.
Whirlpool	512	Розроблений для забезпечення безпеки та широкого спектру застосувань.
bcrypt	72	Був розроблений для хешування паролів. Включає в себе механізм “солі”, який володіє великою обчислювальною складністю, що ускладнює атаки методом перебору. “Сіль” – це випадкова частина даних, яка додається перед хешуванням до пароля.

```python
from flask import Flask, request, jsonify

app = Flask(__name__)

# Список зареєстрованих IoT-пристроїв
registered_devices = {"device1": "password1", "device2": "password2"}

def authenticate(device_id, password):
    # Перевіряємо, чи існує такий пристрій та вірний пароль
    return device_id in registered_devices and registered_devices[device_id] == password

@app.route('/data', methods=['POST'])
def handle_data():
    data = request.get_json()

    # Перевіряємо аутентифікацію перед обробкою даних
    if authenticate(data.get('device_id'), data.get('password')):
        result = {'status': 'success', 'message': 'Data received and processed.'}
    else:
        result = {'status': 'error', 'message': 'Authentication failed.'}

    return jsonify(result)

if __name__ == '__main__':
    app.run(debug=True)
```

Рис. 3. Створення невеликого веб- сервера з використанням бібліотеки Flask

Цей код використовує бібліотеку Flask для створення невеликого веб-сервера. Пристрій повинен надіслати запит POST на шлях "/data" за допомогою device_id та password. Сервер використовує функцію автентифікації для перевірки цих даних і обробляє дані, якщо автентифікація успішна. Flask – це простий фреймворк для розробки веб-додатків на мові програмування Python. Надає інструменти для створення веб-сайтів та веб-додатків з мінімальними зусиллями та обсягом коду.

```cpp
#include <iostream>
#include <unordered_map>
#include <string>
using namespace std;
class IoTDevice {
public:
    IoTDevice(const string& deviceID, const string& password):
        deviceID(deviceID), password(password) {}
    bool authenticate(const string& enteredPassword) const {
        return enteredPassword == password;
    }
private:
    string deviceID;
    string password;
};
int main() {
    // Список зареєстрованих IoT-пристроїв
    unordered_map<string, IoTDevice> registeredDevices;
    registeredDevices.emplace("device1", IoTDevice("device1", "password1"));
    registeredDevices.emplace("device2", IoTDevice("device2", "password2"));
    // Введення користувача для перевірки аутентифікації
    string deviceID;
    string enteredPassword;
    cout << "Enter device ID: ";
    cin >> deviceID;
    cout << "Enter device password: ";
    cin >> enteredPassword;
    // Перевірка аутентифікації
    if (registeredDevices.find(deviceID) != registeredDevices.end() &&
        registeredDevices[deviceID].authenticate(enteredPassword)) {
        cout << "Authentication successful!" << endl;
    }
    else {
        cout << "Authentication failed." << endl;
    }
    return 0;
}
```

Рис. 4. Приклад коду на мові C++ для перевірки автентифікації

Для порівняння наведено приклад схожого коду на мові програмування C++, в якому вводиться список зареєстрованих IoT-пристроїв та відбувається перевірка автентифікації.

Хешування паролів є критично важливим елементом забезпечення безпеки в інформаційних системах. Воно дозволяє перетворити паролі користувачів на незрозумілі хеш-значення, які важко або навіть неможливо перетворити назад у початковий пароль. Це забезпечує додатковий захист для облікових записів, оскільки навіть у випадку порушення безпеки і отримання доступу до бази даних хешованих паролів, зловмисникам буде вкрай важко відновити початкові паролі. Такий підхід мінімізує ризик зламу облікових записів та зберігає конфіденційність паролів користувачів. Щоб підвищити безпеку, рекомендується використовувати сучасні алгоритми хешування та вимагати складних паролів з великою кількістю символів[10].

6. Висновки.

Методи захисту Інтернеті речей (IoT) є надзвичайно важливою та актуальною проблемою через розповсюдження IoT систем у сучасному житті. Зростання кількості підключених пристроїв та систем потребує належного захисту від кіберзагроз, оскільки ця інфраструктура стає все більш вразливою. Головні висновки про кібербезпеку в IoT полягають у такому:

1. Масовість підключених пристроїв створює безліч точок входу для потенційних загроз.
2. Зловмисники використовують IoT для атак, крадіжок даних та інших злочинів, що включають атаки на пристрої, мережі та сервери.
3. Збільшена кількість пристроїв, які збирають особисті дані, може призвести до порушень приватності та незаконного використання цих даних.
4. Брак загальних стандартів та регулювань у сфері кібербезпеки ускладнює захист інфраструктури та даних.
5. Організації повинні розробити та впровадити практичні стратегії кібербезпеки для захисту систем IoT.
6. Навчання та освіта користувачів важливі для виявлення та запобігання кіберзагрозам.
7. Системи IoT повинні бути постійно моніторені та оновлювані для захисту від нових загроз і вразливостей.

Для забезпечення безпечної та надійної інфраструктури IoT необхідно вдосконалювати технології та співпрацювати на всіх рівнях, від виробників пристроїв до користувачів. Без цього інтернет речей може стати джерелом серйозних кіберзагроз та порушень приватності.

Список використаної літератури

1. Alkunidry D., Alhuwaysi S., Alharbi R. Security Threads and IoT Security. Journal of Computer and Communications. 2023. Т. 11, № 09. С. 76–83. (дата звернення: 11.03.2024).
2. Editorial: Security and Privacy in Internet of Things / J. M. de Fuentes та ін. Mobile Networks and Applications. 2018. Т. 24, № 3. С. 878–880. (дата звернення: 11.03.2024).
3. ETSI EN 303 645 V2.1.1 (2020-06). CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. Чинний від 2020-06-19. Вид. офіц. 2020. 34 с.
4. Новий стандарт кібербезпеки IoT. Worldvision – інтернет магазин систем безпеки. URL: https://worldvision.com.ua/poyavilsya-novyy-globalnyy-standart-interneta-veshchey-dlya-kiberbezopasnosti/ (дата звернення: 13.03.2024).
5. Філінович В. В. Кібербезпека та інтернет речей: правовий аспект. Цивільне і трудове право. 2020. Т. 4, № 57. С. 122–125.
6. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 15.03.2024).
7. Діденко Д. Поширені атаки на IoT та захист від них. Corewin. URL: https://corewin.ua/blog/attacks-on-iot-how-protect/ (дата звернення: 15.03.2024).
8. ETSI EN 303 645 for IoT Security - Onward Security, a DEKRA company. Onward Security Corp. URL: https://www.onwardsecurity.com/en/lab_security-detail/ETSIEN303645/ (дата звернення: 20.03.2024).

9. Pickavet H. Why IoT Security Is So Critical | TechCrunch. TechCrunch. URL: https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/ (дата звернення: 19.03.2024).

10. Security of IoT Devices / E. Buenrostro та ін. Journal of Cyber Security Technology. 2018. Т. 2, № 1. С. 1–13. (дата звернення: 20.03.2024).

References

1. Alkunidry D., Alhuwaysi S., Alharbi R. Security Threads and IoT Security. Journal of Computer and Communications. 2023. Vol. 11, No. 09. P. 76–83. (accessed 11/03/2024).

2. Editorial: Security and Privacy in Internet of Things / J. M. de Fuentes and others. Mobile Networks and Applications. 2018. Vol. 24, No. 3. P. 878–880. URL: https://doi.org/10.1007/s11036-018-1150-8 (date of access: 11/03/2024).

3. ETSI EN 303 645 V2.1.1 (2020-06). CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements. Valid from 2020-06-19. Kind. officer 2020. 34 p.

4. The new IoT cybersecurity standard. Worldvision is an online store of security systems. URL: https://worldvision.com.ua/poyavilsya-novyy-globalnyy-standart-interneta-veshchey-dlya-kiberbezopasnosti/ (access date: 03/13/2024).

5. Filinovych V.V. Cybersecurity and the Internet of Things: Legal Aspect. Civil and labor law. 2020. Vol. 4, No. 57. P. 122–125.

6. On the protection of personal data: Law of Ukraine dated June 1, 2010 No. 2297-VI: as of October 27 2022 URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (access date: 03/15/2024).

7. Didenko D. Common attacks on IoT and protection against them. Corewin. URL: https://corewin.ua/blog/attacks-on-iot-how-protect/ (access date: 03/15/2024).

8. ETSI EN 303 645 for IoT Security - Onward Security, a DEKRA company. Onward Security Corp. URL: https://www.onwardsecurity.com/en/lab_security-detail/ETSIEN303645/ (access date: 03/20/2024).

9. Pickavet H. Why IoT Security Is So Critical | TechCrunch. TechCrunch. URL: https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/ (accessed 03/19/2024).

10. Security of IoT Devices / E. Buenrostro and others. Journal of Cyber Security Technology. 2018. Vol. 2, No. 1. P. 1–13. (access date: 03/20/2024).