Авторлар туралы мәліметтер

Тұрсынхан Саятұлы Жылқыбаев – IT технологиялар кафедрасының оқытушысы; Шәкәрім университеті, Қазақстан Республикасы; e-mail zhitosya@mail.ru.

Александр Дмитриевич Золотов* – техника ғылымдарының кандидаты, IT технологиялар кафедрасының қауымдастырылған профессоры; Шәкәрім университеті, Қазақстан Республикасы; e-mail azol64@ mail.ru.

Бақытгүл Қадырханқызы Көпабаева – IT технологиялар кафедрасының докторанты; Шәкәрім университеті, Қазақстан Республикасы; e-mail kbahyt_73@mail.ru.

Наркен Қайрулайұлы Алғазинов – техника ғылымдарының магистрі, «Электротехника және автоматтандыру» кафедрасының аға оқытушысы, Торайғыров университеті; e-mail: narkenalgazinov@gmail.com.

Дінмұхамед Асқарұлы Жұмағажинов – IT технологиялар кафедрасының АУ 101 тобының студенті; Шәкәрім университеті, Қазақстан Республикасы; e-mail zhumagazhinov1970@mail.ru.

Габит Жумабаевич Шүйтенов – педагогика ғылымдарының кандидаты, доцент, стратегия және цифрландыру бойынша проректор; Esil university; Қазақстан; e-mail: g.shuitenov@mail.ru. ORCID: https://orcid.org/0000-0003-1042-0415.

Information about the authors

Tursinkhan Sayatuly Zhylkybayev – lecturer at the Department of IT Technologies; Shakarim University, Republic of Kazakhstan; e-mail zhitosya@mail.ru.

Alexander Dmitrievich Zolotov* – Candidate of Technical Sciences, Associate Professor of the Department of IT Technologies; Shakarim University, Republic of Kazakhstan; e-mail azol64@ mail.ru.

Bakhytgul Kadyrkhanovna Kopabayeva – PhD student of the Department of IT Technologies; Shakarim University, Republic of Kazakhstan; e-mail kbahyt_73@mail.ru.

Narken Kairulayevich Algazinov – Master of Technical Sciences, Senior Lecturer at the Department of Electrical Engineering and Automation, Toraigyrov University; e-mail: narkenalgazinov@gmail.com.

Dinmukhamed Askarovich Zhumagazhinov – student of AU 101 group of the Department of IT Technologies; Shakarim University, Republic of Kazakhstan; e-mail: zhumagazhinov1970@mail.ru.

Gabit Shuitenov – Candidate of Pedagogical Sciences, Associate Professor, Vice-Rector for Strategy and Digitalization of Esil University, Republic of Kazakhstan; e-mail: g.shuitenov@mail.ru. ORCID: https://orcid.org/0000-0003-1042-0415.

Поступила в редакцию 21.04.2025
Поступила после доработки 29.04.2025
Принята к публикации 30.04.2025

https://doi.org/10.53360/2788-7995-2025-2(18)-8

МРНТИ: 81.93.29

К.М. Сагиндыков[1], Д.Ж. Сатыбалдина[2], Ф.Б. Тебуева[3], Т.А. Айдынов[1], А.К. Шайханова[*]
[1]Евразийский национальный университет им. Л.Н. Гумилева,
010000, Республика Казахстан, г. Астана, улица К. Сатпаева, 2
[2]ТОО "KazHackStan", 010000, Республика Казахстан, г. Астана, проспект Мангилик Ел, 54
[3]ФГАОУ ВО «Северо-Кавказский федеральный университет»,
355017, Российская Федерация, г. Ставрополь, ул. Пушкина, 1
*e-mail: shaikhanova_ak@enu.kz

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ ПЛАТФОРМ И ПРОТОКОЛОВ ИНТЕРНЕТА ВЕЩЕЙ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Аннотация: *В работе представлены результаты исследования безопасности распространенных платформ и протоколов Интернета вещей на основе анализа известных баз данных уязвимостей, а также практического эксперимента по аудиту сети устройств Интернета вещей с использованием современных методов тестирования на проникновение. Реализован алгоритм сбора и извлечения релевантных данных из базы Common Vulnerabilities and Exposures (CVE). Разработан веб-интерфейс интерактивной CVE таблицы, который реализует задачи обработки и представления больших объемов данных в удобном и наглядном формате. Анализ проведен для выявления наиболее критичных уязвимостей, которые должны быть минимизированы новым протоколом аутентификации устройств Интернета вещей и для формирования конкретных требований к протоколу, направленных на минимизацию выявленных уязвимостей. В*

ходе тестирования беспроводных сетей на проникновение были выявлены критические уязвимости в исследованных устройствах Интернета вещей и беспроводной сети LoRaWAN. В результате исследований получен датасет, включающий список уязвимостей систем Интернета вещей, извлеченных из CVE глоссария с описанием векторов атак и критичности по шкале Common Vulnerability Scoring System (CVSS), сформулированы рекомендации по устранению уязвимостей.

Ключевые слова: *атака, Интернет вещей, кибербезопасность, протокол, уязвимость, тестирование на проникновение (пентестинг).*

1 Введение

Технологии Интернета вещей (Internet of Things, IoT) обеспечивают новые возможности для удаленного мониторинга и управления распределенными киберфизическими системами. Имея несомненные достоинства (низкую стоимость, невысокие требования по энергопотреблению, возможность подключения к беспроводной сети и передачи данных на большие расстояния), IoT-устройства одновременно обладают рядом недостатков, снижающих возможности безопасного использования (ограничения по памяти, невозможность реализации продвинутых криптографических алгоритмов) [1]. IoT-системы подвергаются эксплуатации злоумышленниками, поскольку многие устройства поставляются с небезопасными настройками по умолчанию или содержат удаленно эксплуатируемый код [2]. Дополнительные проблемы безопасности связаны с необходимостью взаимодействия различных технологий и протоколов, что усложняет обеспечение их защиты [3], а также с развертыванием IoT-продуктов в небезопасных или уязвимых средах [4, 5].

Особый интерес вызывает безопасность протоколов беспроводной связи маломощных широкополосных сетей (Low-Power Wide-Area Network, LPWAN). Среди них значительную популярность приобрел протокол LoRaWAN (Long-Range Wide-Area Network), основанный на технологии радиомодуляции LoRa. Востребованность LoRaWAN обусловлена низким энергопотреблением, возможностью масштабирования и территориально распределенного подключения устройств и низкой стоимостью реализации различных IoT- приложений [5]. Тем не менее, в работе [6] показано, что стек протоколов LoRaWAN имеет серьёзные проблемы безопасности, подтвержденные проведением ряда успешных атак в контролируемой среде.

В связи с этим актуальной задачей является анализ уязвимостей IoT устройств, используемых ими программного обеспечения и протоколов беспроводных сетей протоколов, и разработка подходов к повышению безопасности киберфизических систем. Настоящая работа направлена на решение этой задачи путем систематического анализа известных уязвимостей, зарегистрированных в базе Common Vulnerabilities Exposures (CVE), а также проведением практическим тестированием IoT-систем на проникновение на примере системы мониторинга качества воздуха, поддерживающие передачу данных по протоколу LoRaWAN.

Цель исследования состояла в выявлении критических уязвимостей программного обеспечения, встроенного ПО и сетевых протоколов, используемых для реализации киберфизических систем, и формулировке требований для разработки новых схем аутентификации IoT-устройств, минимизирующих выявленные риски. В ходе исследований был разработан алгоритм сбора и извлечения релевантной информации из базы CVE, что позволило выявить наиболее значимые угрозы для. Для удобства работы с извлеченными данными создан алгоритм и код для реализации веб-интерфейса интерактивной таблицы CVE, упрощающего анализ и визуализацию больших объемов информации. Полученные результаты, включающие датасет уязвимостей, описание векторов атак и практические рекомендации по повышению безопасности, могут использоваться специалистами и разработчиками для улучшения защищенности IoT-систем.

2 Методы исследования

2.1 Анализ уязвимостей на основе обработки данных общеизвестных баз

2.1.1 Сбор данных

На первом этапе исследований был использован открытый код на языке Python [7] для анализа уязвимостей на основе данных национального института стандартов и технологий США (National Vulnerability Database, NVD) отнесенных к глоссарию общих уязвимостей и воздействий (Common Vulnerabilities and Exposures, CVE) с указанием критичности по шкале CVSS (Common Vulnerability Scoring System) [8].

Основные этапы работы *Алгоритма 1 для сбора данных о современных уязвимостях программного обеспечения* описаны ниже.

Загрузка и проверка данных о CVE с сайта NVD: скрипт автоматически скачивает .zip-архивы файлов описания уязвимостей, сохраненных в формате JSON, и проверяет целостность данных через сопоставление контрольных сумм SHA256.

Проверка и обновление локального кэша данных: для уменьшения количества повторных загрузок реализована систему кэширования метаданных, при каждом запуске скрипта производится проверка наличия новых данных или обновлений, используя информацию о контрольных суммах (рис. 1); если изменения найдены, соответствующий файл загружается заново, иначе если данные актуальны, загрузка пропускается.

Распаковка архивов с CVE: скачанные файлы в формате ZIP автоматически распаковываются, чтобы получить доступ к содержимому JSON; для этого был разработан модуль (рис. 2), который открывает архивы, читает их содержимое и сохраняет его в соответствующие файлы для дальнейшей обработки.Обработка и извлечение релевантных данных из JSON файлов: для каждого CVE-объекта извлекается информация о его уникальном идентификаторе (ID), дате публикации, дате последнего обновления, описании, а также метрики CVSS версии 2. Если CVSS версии 2 для уязвимости отсутствует, запись отбрасывается.

```python
# Проверяются метаданные
def nvd_definition_check():
    regex=re.compile('(?<=sha256:)([A-Z0-9]{64})')
    cache = load_cache_definitions()

    if not path.exists('nvd'):
        makedirs('nvd')

    r = requests.get('https://nvd.nist.gov/vuln/data-feeds#JSON_FEED')
    all_meta = re.findall("nvdcve-1.1-[0-9a-z]*\.meta",r.text)

    for meta in tqdm(all_meta):
        r_file = requests.get("https://static.nvd.nist.gov/feeds/json/cve/1.1/" + meta, stream=True)
        hash=regex.findall(r_file.text)[0]
        if meta in cache and path.exists('nvd_cache.json'):
            if cache[meta]!=hash:
                download_json(meta)
                cache[meta]=hash
            else:
                continue
        else:
            cache[meta]=hash
            download_json(meta)
    save_cache_definitions(cache)
```

Рисунок 1 – Код проверки и обновления локального кэша данных

```python
# распаковываются данные - json
def unzip_cve():
    if not path.exists('data'):
        makedirs('data')
    files = [f for f in listdir('nvd/') if re.match(r'nvdcve-1.1-[0-9a-z]*\.json\.zip', f)]
    files.sort()
    print('\n',"Vykdomas duomenų išarchyvavimas:")
    for file in tqdm(files):
        archive = zipfile.ZipFile(join("nvd/", file), 'r')
        jsonfile = archive.open(archive.namelist()[0])
        cve_dict = json.loads(jsonfile.read())
        with open('data/'+file+'.json', 'w', encoding='utf-8') as f:
            json.dump(cve_dict, f, ensure_ascii=False, indent=4)
        jsonfile.close()
```

Рисунок 2 – Код распаковки архивов с CVE

Проверка на наличие эксплуатируемых уязвимостей (Exploited Vulnerabilities): реализована проверка уязвимости на наличие в каталоге эксплуатируемых уязвимостей, опубликованном Агентством по кибербезопасности и инфраструктуре США (Cybersecurity and Infrastructure Security Agency, CISA). Для этого загружается файл CSV с сайта CISA, содержащий список известных эксплуатируемых уязвимостей, и сверяем каждую запись CVE с этим списком. Если уязвимость найдена в списке, она помечается как эксплуатируемая с добавлением соответствующей информации.

Конвертация данных в факты для последующего анализа: код реализует конвертацию данных CVE в формат фактов (рис. 3). Каждая уязвимость представляется в виде факта, который содержит всю релевантную информацию: идентификатор CVE, описание, даты, данные CVSS (метрики, вектор атаки, оценки сложности и влияния), статус

эксплуатируемости, а также список продуктов, подверженных уязвимости. Факты формируются на основе шаблона (deftemplate), который был разработан для этой задачи.

```
(MAIN::vulnerability
  (id "CVE-2021-34527")
  (publishedDate "2021-07-01")
  (lastModifiedDate "2021-07-07")
  (description "A remote code execution vulnerability exists when the Windows
  (cpe23Uri "cpe:2.3:a:microsoft:windows_10:*:*:*:*:*:*:*:*")
  (vectorString "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:C/A:C")
  (accessVector "NETWORK")
  (accessComplexity "LOW")
  (authentication "NONE")
  (confidentialityImpact "COMPLETE")
  (integrityImpact "COMPLETE")
  (availabilityImpact "COMPLETE")
  (baseScore 10.0)
  (severity "HIGH")
  (exploitabilityScore 3.9)
  (impactScore 10.0)
  (known_exploited "YES")
  (date_added_to_known_exploited "2021-07-02")
  (affected_products "Microsoft Windows 10")
)
```

Рисунок 3 – Пример факта, который генерируется скриптом для каждой уязвимости

Вывод результатов и ошибок: для удобства отслеживания хода выполнения скрипта было реализовано детализированное логирование. Все успешно конвертированные факты сохраняются в отдельный файл, а записи с ошибками – в файл с описанием причин их отбраковки.

2.1.2 Создание веб- интерактивной таблицы для анализа уязвимостей CVE

После загрузки всех данных CVE (описанной в разделе 2.1.1) реализован собственный алгоритм и код создания интерактивной таблица для поиска, фильтрации и сортировки данных о CVE с возможностью отображения данных из внешнего источника. Использованы следующие библиотеки и фреймворки:

- Bootstrap 5 для стилизации таблиц и общего дизайна интерфейса;
- DataTables для работы с данными в табличном формате, эта библиотека предоставляет функции сортировки, поиска, фильтрации и обработки данных;
- jQuery для упрощения работы с DOM-элементами и управления событиями;
- Highlight.js для реализации подсветки поисковых запросов в таблице.

Алгоритм 2 создания интерактивной таблицы уязвимостей программного обеспечения состоит из следующих этапов.

Создание структуры HTML: основная HTML-структура включает в себя заголовок, контейнер для таблицы и футер. Таблица была создана с использованием классов Bootstrap для стилизации, а ее содержимое было подготовлено для интеграции с DataTables. Столбцы таблицы включают следующие категории (рис. 4): CVE_Year (год регистрации уязвимости), CVE_Name (идентификатор уязвимости), CVE_Description (описание уязвимости), CVE_GitHub (ссылка на соответствующий GitHub репозиторий), CVE_References (ссылка на внешние ресурсы).

CVE_Year	CVE_Name	CVE_Description	CVE_GitHub	CVE_References
2024	CVE-2024-8517	SPIP before 4.3.2, 4.2.16, and 4.1.18 is vulnerable to a command injection issue. A remote and unauthenticated attacker can execute arbitrary operating system commands by sending a crafted multipart file upload HTTP request.	https://github.com/fkie-cad/nvd-json-data-feeds	No PoCs from references.
2024	CVE-2024-8509	A vulnerability was found in Forklift Controller. There is no verification against the authorization header except to ensure it uses bearer authentication. Without an Authorization header and some form of a Bearer token, a 401 error occurs. The presence of a token value provides a 200 response with the requested information.	https://github.com/fkie-cad/nvd-json-data-feeds	No PoCs from references.
2024	CVE-2024-8480	The Image Optimizer, Resizer and CDN – Sirv plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'sirv_save_prevented_sizes' function in all versions up to, and including, 7.2.7. This makes it possible for authenticated attackers, with Contributor-level access and above, to exploit the 'sirv_upload_file_by_chunks_callback' function, which lacks proper file type	https://github.com/fkie-cad/nvd-json-data-feeds	No PoCs from references.

Рисунок 4 – Основная структура таблица

Инициализация DataTables: при загрузке HTML-страницы инициализируется библиотека DataTables. Были заданы следующие настройки таблицы:

- dom (определение структуры таблицы, добавление фильтров и кнопок управления столбцами);
- paging (включение постраничной навигации);
- processing (включение индикатора загрузки для обработки данных);
- responsive (обеспечение адаптивности таблицы на разных устройствах);

- buttons (добавление кнопки для управления видимостью столбцов, опция «colvis»);
- deferRender (отложенная отрисовка для повышения производительности).

Фильтрация данных в таблице: реализованы функции фильтрации данных по мере ввода текста, а также были добавлены текстовые поля в нижней части таблицы, которые позволяли пользователю искать данные в каждом столбце отдельно (рис. 5).

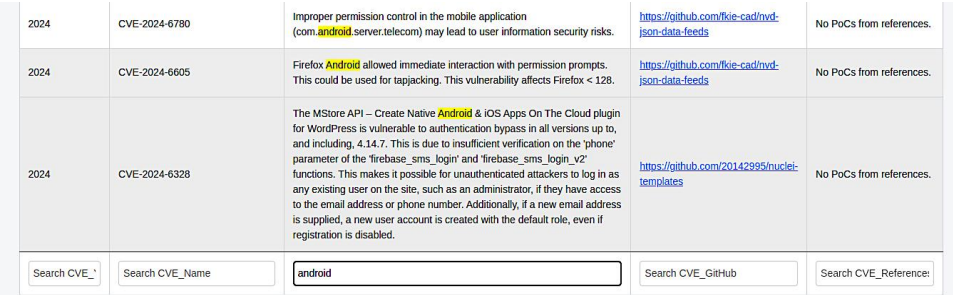

Рисунок 5 – Подсветка поисковых запросов в интерактивной таблице

Добавление индикатора загрузки: для улучшения пользовательского опыта при загрузке данных создана простая система индикации загрузки – блок #overlay с вращающимся спиннером, который отображался до полной инициализации таблицы. Этот блок автоматически исчезал, когда данные были загружены, и таблица была полностью отрисована.

Добавление подсветки поисковых запросов: добавлена функция подсветки введенных в поле поиска слов в результатах таблицы с использованием библиотеки jquery.highlight.js. При вводе ключевого слова в поле поиска, таблица обновляется, и совпадающие слова подсвечиваются в желтый цвет для более легкой идентификации результатов поиска (рис. 5).

2.1.3 Методика анализа данных в сгенерированной интерактивной таблице CVE

Для аналитики данных глоссария общих уязвимостей и воздействий CVE, собранных автоматизированным способом по алгоритму 1 и структурированных в интерактивной таблице согласно алгоритму 2, использованы статистические методы обработки данных. Реализация этих методов позволяет извлечь полезную информацию с использованием выделенных ключевых слов и выявить основные уязвимости, касающиеся платформ и протоколов Интернета вещей.

Список ключевых слов для выделения уязвимостей, соответствующей области исследований представлен в таблице 1 с распределением по пяти классам.

Таблица 1 – Перечень ключевых слов для выделения уязвимостей области исследования

№ п/п	Наименование класса	Ключевые слова
1	Беспроводные технологии и протоколы	Wi-Fi (802.11), Bluetooth, BLE, NFC, Near Field Communication, Cellular Networks, 4G, LTE, 5G, Zigbee, Z-Wave, LoRa, WiMax, Mesh, Ad-hoc, WPA3 (Wi-Fi Protected Access 3), WPA2 (Wi-Fi Protected Access 2), WEP
2	Виды атак	Evil Twin Attack, Man-in-the-Middle (MITM) Attack, Deauthentication Attack, Rogue Access Point, Packet Sniffing, Brute Force Attack, ARP Spoofing, KRACK Attack (Key Reinstallation Attack), Bluetooth Hacking, Signal Jamming
3	Криптографические аспекты	Encryption Protocols, AES, RSA, ECC, Public Key Infrastructure, PKI, End-to-End Encryption, Hash Functions, SHA, MD5, Digital Certificates, Diffie-Hellman Key Exchange, TLS, SSL, Elliptic Curve Cryptography, ECC
4	Методы тестирования и анализа безопасности	Penetration Testing, Pentest, Vulnerability Scanning, Wireless Network Auditing, Packet Analysis, Traffic Analysis, Fuzzing, Side-Channel Attacks, Cryptanalysis, Reverse Engineering
5	Инструменты для тестирования уязвимостей сетей и устройств Интернета вещей	Aircrack-ng, Kismet, Wireshark, tcpdump, Metasploit, Nmap, Burp Suite, SDR, Bettercap, Reaver, Zanti, NetHunter

2.2 Инструменты и методика практического эксперимента

Методы и инструменты тестирования на проникновение (penetration testing, пентестинг) представляют собой перспективный и необходимый подход для оценки защищенности систем Интернета вещей, особенно учитывая ограниченность традиционных мер безопасности при выявлении новых угроз. В рамках исследования применялись техники этичного хакинга, позволяющие квалифицированным специалистам моделировать реальные сценарии атак, заранее выявлять уязвимости и своевременно устранять обнаруженные проблемы безопасности [9].

В качестве тестовой сети в эксперименте исследована система мониторинга качества воздуха на основе трех прототипов мультисенсорной газоаналитической системы с передачей данных по беспроводной сети LoRaWAN [10], разработанные в НИИ ИБ и криптологии НАО «Евразийский национальный университет им. Л.Н. Гумилева» в рамках выполнения проекта грантового финансирования (AP14872171). В таблице 2 представлены основные этапы эксперимента, а в таблице 3 описан использованный инструментарий тестирования на проникновение.

Таблица 2 – Этапы аудита безопасности IoT-устройств и сетей LoRaWAN и WLAN

№ п\п	Наименование этапа	Описание
1	Планирование и подготовка	Определение целей и объема тестирования. Получение необходимых разрешений. Подготовка инструментов
2	Сбор информации	Идентификация устройств и сетей. Сканирование портов и сервисов. Анализ открытых источников (OSINT, Shodan)
3	Анализ уязвимостей	Использование автоматизированных сканеров. Поиск известных уязвимостей.
4	Эксплуатация уязвимостей	Попытки получить несанкционированный доступ. Эскалация привилегий
5	Отчетность	Документирование найденных уязвимостей. Предложение мер по устранению.

Таблица 3 – Перечень использованных инструментов и программных средств

№ п\п	Объект тестирования	Инструменты и программные средства
1	IoT-устройства (прототипы мультисенсорной газоаналитической системы)	Nmap, OpenVAS, Nessus, Metasploit Framework
2	сети LoRaWAN	SDR (HackRF), LoRaWAN Sniffer Tools, LoRaWAN-frame-decoder, GNU Radio

3 Результаты исследований

В целях создания классификации типов уязвимостей интерактивной веб-таблице из сформированного файла были выполнены следующие действия:

- для извлечения данных о типах уязвимостей используется поле problemtype по признаку классификации (CVE_Type);
- проведен подсчет количества уязвимостей каждого типа (табл. 5);
- для визуализации классификации данных построена круговая диаграмма распределения уязвимостей по типам (рис. 7).

Таблица 5 – Результаты подсчет количества уязвимостей каждого типа

Тип уязвимости (CVE_Type)	**Частота**	**Описание**
NVD-CVE-noinfo	30406	Информация не предоставлена
NVD-CVE-Other	29128	Другая неопределенная уязвимость
CVE-79	25419	Межсайтовый скриптинг
CVE-119	11350	Неправильное ограничение операций в пределах буфера памяти
CVE-787	10280	Ошибка записи за пределами выделенного блока
CVE-89	10163	SQL инъекция
CVE-20	8909	Неправильная проверка ввода
CVE-200	6632	Раскрытие конфиденциальной информации неавторизованному субъекту
CVE-22	5594	Обход пути, открывает доступ к файлам и директориям

CVE-125	5453	Чтение за пределами выделенного блока
CVE-264	5206	Неправильное назначение разрешения
CVE-352	4917	Межсайтовая подделка запроса
CVE-416	4183	Некорректное использование динамической памяти после ее освобождения
CVE-78	3113	Некорректная нейтрализация команд
CVE-94	3084	Внедрение кода.
CVE-287	3060	Неправильная аутентификация.
CVE-862	2978	Отсутствует авторизация.
CVE-476	2783	Разыменование указателя NULL.
CVE-399	2543	Ошибки управления ресурсами.
CVE-310	2440	Криптографические проблемы
CVE-190	2238	Целочисленное переполнение или циклический возврат
CVE-120	2039	Переполнение буфера.
CVE-434	1926	Неограниченная загрузка файлов

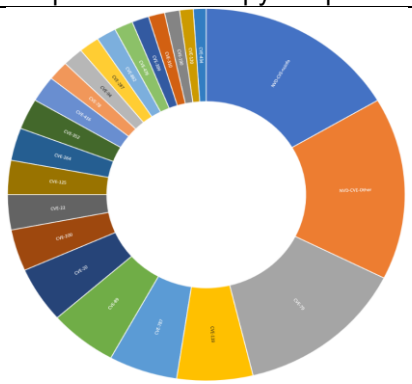

Рисунок 7 – Количественное распределение уязвимостей по типам

В сетях LoRaWAN удалось перехватить пакеты, содержащие незашифрованные данные. Это указывает на недостаточную защиту передаваемой информации и позволяет злоумышленникам получать доступ к конфиденциальным данным. Также была выявлена возможность проведения Replay-атак из-за ограниченной длины счётчика в поле FRMPayload, составляющей всего 16 бит. Эта уязвимость позволяет злоумышленнику перехватывать пакеты, ждать переполнения счётчика и повторно отправлять их, что может привести к нарушению работы сети или отказу в обслуживании.

Кроме того, определено, что использование метода активации ABP (Activation By Personalization) повышает уязвимость сети, так как этот метод не обеспечивает достаточную защиту от подобных атак. Главным недостатком метода ABP является его повышенная уязвимость к криптоаналитическим атакам. Поскольку ключи остаются постоянными, их компрометация предоставляет злоумышленникам длительный доступ к сети без необходимости повторного получения ключей.

4 Обсуждение научных результатов

Анализ полученных результатов показал, что следующие типы уязвимостей из представленных в таблице 7 являются критическими для обеспечения безопасности протоколов в сетях устройств Интернета вещей (IoT):

- CVE-287, проблемы с проверкой подлинности IoT-устройств являются критическими, так как позволяют злоумышленнику осуществлять несанкционированный доступ или управление устройствами;
- CVE-862, отсутствие корректной авторизации также дает возможность злоумышленникам свободно взаимодействовать с IoT-устройствами, что существенно снижает безопасность всей сети;
- CVE-310, уязвимости в реализации криптографических механизмов могут привести к компрометации передаваемых данных и нарушению конфиденциальности и целостности сообщений;
- CVE-20, неправильная проверка ввода позволяет злоумышленнику отправлять специально подготовленные команды, вызывающие сбои в работе устройств или выполнение вредоносного кода;

– CVE-200, уязвимость приводит к утечкам данных, критически важных в IoT-системах, особенно в средах, где передается чувствительная информация.

Таким образом, приоритетными для обеспечения защищённости IoT-протоколов и систем являются уязвимости, связанные с аутентификацией, авторизацией, криптографией и обработкой данных.

В ходе проведённого пентестинга были выявлены серьезные уязвимости в IoT-устройствах и беспроводных сетях LoRaWAN. В частности, в IoT-устройствах были обнаружены устройства со стандартными паролями и устаревшими версиями программного обеспечения, что значительно снижает их защиту и делает их лёгкими мишенями для атак. В сетях LoRaWAN удалось перехватить пакеты с зашифрованными данными и выявить уязвимость, связанную с ограниченной длиной счётчика в поле FRMPayload. Эта уязвимость позволяет злоумышленникам осуществлять Replay-атаки, что может привести к нарушению работы сети или отказу в обслуживании. Дополнительно, использование метода активации ABP было определено как фактор, повышающий уязвимость сети, что подчеркивает необходимость использования более безопасных методов активации.

5 Заключение

В настоящей работе проведен комплексный анализ критических уязвимостей программного обеспечения и сетевых протоколов, используемых в киберфизических системах Интернета вещей. Полученные результаты позволили определить наиболее значимые типы угроз, требующие приоритетного внимания при разработке механизмов защиты IoT-устройств. Практические испытания (пентестинг) выявили серьёзные уязвимости в устройствах IoT и беспроводных сетях LoRaWAN. Были обнаружены устройства со стандартными паролями и устаревшим ПО, существенно снижающие их защищённость. Дополнительно была выявлена уязвимость, связанная с перехватом незашифрованных пакетов данных и ограниченной длиной счётчика FRMPayload, что открывает возможность осуществления атак, приводящих к отказу в обслуживании.

Будущие исследования будут направлены на разработку эффективной схемы аутентификации устройств Интернета вещей, использующей физически неклонируемые функции, которые позволяют существенно повысить уровень защищенности устройств и предотвратить ряд существующих атак.

Список литературы

1. Evaluating critical security issues of the IoT world: Present and future challenges / M. Frustaci et al // IEEE Internet of things journal. – 2017. – V.5, № 4. – P. 2483-2495.
2. Goranin N. A Bibliometric Review of Intrusion Detection Research in IoT: Evolution, Collaboration, and Emerging Trends / N. Goranin, S.K. Hora, H.A. Čenys // Electronics. – 2024. – Vol. 13. – P. 3210. https://doi.org/10.3390/electronics13163210.
3. Advancing IoT Security: A Review of Intrusion Detection Systems Challenges and Emerging Solutions / T. Zhukabayeva et al // Proceeding of the 11th International Conference on Software Defined Systems. – 2024. – P. 115-122.
4. A method of vulnerability analysis in wireless internet of things networks for smart city infrastructures / T. Zhukabayeva et al // Scientific Journal of Astana IT University. – 2024. – Vol. 20. – P. 48-61.
5. Comprehensive Vulnerability Analysis and Penetration Testing Approaches in Smart City Ecosystems / T. Zhukabayeva et al // Proceeding of the 8th International Symposium on Innovative Approaches in Smart Technologies. – 2024. – P.1-6.
6. Security vulnerabilities in LoRaWAN / X. Yang et al // Proceeding of the Third International Conference on Internet-of-Things Design and Implementation. – 2018. – P. 129-140.
7. Automated Conversion of CVE Records into an Expert System, Dedicated to Information Security Risk Analysis, Knowledge-Base Rules / D. Benetis et al // Electronics. – 2024. – Vo. 13. – P. 2642. https://doi.org/10.3390/electronics13132642.
8. Kühn P. Common vulnerability scoring system prediction based on open source intelligence information sources / P. Kühn, D.N. Relke, C. Reuter // Computer Security. – 2023. – Vol. 131. – P. 103286.
9. Ethical hacking for IoT: Security issues, challenges, solutions and recommendations / J.P.A. Yaacoub et al // Internet of Things and Cyber-Physical Systems. – 2023. – V. 3. – P. 280-308.

10. An IoT-based Air Pollution Monitoring System for Smart City / A. Aubakirov et al // Proceedings of 4th IEEE International Conference on Computer Systems. – 2024. – P. 156-161.

Информация о финансировании: *Данное исследование финансируется Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP 26198843).*

К.М. Сагиндыков[1], Д.Ж. Сатыбалдина[2], Ф.Б. Тебуева[3], Т.А. Айдынов[1], А.К. Шайханова[1]*
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
010000, Қазақстан Республикасы, Астана қ., Қ. Сәтпаев көшесі, 2
[2]KazHackStan, ЖШС, 010000, Қазақстан Республикасы, Астана қ., Мәңгілік Ел даңғылы, 54
[3]Солтүстік Кавказ федералды университеті,
355017, Ресей Федерациясы, Ставрополь қ., Пушкин көшесі, 1
*e-mail: shaikhanova_ak@enu.kz

ИНТЕРНЕТ ЗАТТАРЫ ПЛАТФОРМАЛАРЫ МЕН ПРОТОКОЛДАРЫНЫҢ ОСАЛДЫҚТАРЫН РҰХСАТСЫЗ ЕНУГЕ СЫНАУ ӘДІСТЕРІН ПАЙДАЛАНЫП ЗЕРТТЕУ

Бұл мақалада танымал Интернет заттары (IoT) платформалары мен протоколдарының қауіпсіздігіне қатысты зерттеулердің нәтижелері ұсынылған. Зерттеу танымал осалдықтар деректер базасын талдау және ену сынағының заманауи әдістерін қолдана отырып, IoT құрылғыларының желісін тәжірибелік аудиттеу арқылы жүргізілді. Common Vulnerabilities and Exposures (CVE) деректер базасынан өзекті мәліметтерді жинау және шығарып алуға арналған алгоритм әзірленді. Үлкен көлемдегі деректерді өңдеуге және көрнекі, пайдалануға ыңғайлы түрде ұсынуға мүмкіндік беретін интерактивті CVE кестесінің веб-интерфейсі жасалды. Талдау барысында IoT құрылғыларының жаңа аутентификация протокол мен оңтайландырылып ең маңызды осалдықтар анықталып, осы осалдықтарды жоюға бағытталған нақты талаптар қалыптастырылды. Сымсыз желілерді рұхсатсыз енуге сынау барысында IoT құрылғылары мен LoRaWAN сымсыз желілерінде маңызды осалдықтар анықталды. Зерттеу нәтижесінде IoT жүйелерінің осалдықтарының тізімі қамтылған деректер жинағы жасалды, әрбір осалдыққа қатысты шабуыл векторлары мен олардың Common Vulnerability Scoring System (CVSS) шкаласы бойынша критикалық деңгейі сипатталып, оларды жою бойынша практикалық ұсыныстар берілді.

Түйін сөздер: *шабуыл, Интернет заттары, киберқауіпсіздік, протокол, осалдық, ену сынағы (пентестинг).*

K. Sagindykov[1], D. Satybaldina[2], F. Tebueva[3], T. Aidynov[1], A. Shaikhanova[1]*
[1]L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Astana, 2 Satbayev Street
[2]KazHackStan LLP, 010000, Republic of Kazakhstan, Astana, Mangilik El Avenue, 54
[3]North Caucasus Federal University,
355017, Russian Federation, 1 Pushkin Street, Stavropol
*e-mail: shaikhanova_ak@enu.kz

INVESTIGATION OF VULNERABILITIES IN INTERNET OF THINGS PLATFORMS AND PROTOCOLS USING PENETRATION TESTING METHODS

The paper presents research findings related to the security of widespread Internet of Things (IoT) platforms and protocols, based on the analysis of existing vulnerability databases and practical penetration testing of IoT device networks using modern methods. An algorithm for collecting and extracting relevant data from the Common Vulnerabilities and Exposures (CVE) database has been developed. Additionally, a web interface for an interactive CVE table was created, facilitating the processing and visualization of large volumes of data in a convenient and clear format. The conducted analysis aimed to identify the most critical vulnerabilities that should be minimized through the introduction of a new authentication protocol for IoT devices and to define specific requirements for the protocol targeting identified vulnerabilities. During penetration testing of wireless networks, significant vulnerabilities were discovered in the examined IoT devices and the LoRaWAN wireless network. As a result, a dataset containing a list of IoT system vulnerabilities extracted from the CVE glossary, including descriptions of attack vectors and severity based on the Common Vulnerability Scoring System (CVSS), was compiled, along with practical recommendations for mitigating the vulnerabilities.

Key words: *attack, Internet of Things, cybersecurity, protocol, vulnerability, penetration testing (pentesting*).

Сведения об авторах

Каким Молдабекович Сагиндыков – кандидат технических наук, доцент кафедры «Информационная безопасность», Евразийский национальный университет имени Л.Н. Гумилева, г. Астана, Республика Казахстан; e-mail: sagindykov_km@enu.kz. ORCID: https://orcid.org/0000-0003-3315-798X.

Дина Жагыпаровна Сатыбалдина – кандидат физико-математических наук, ассоциированный профессор, ТОО «KazHackStan», г. Астана, Республика Казахстан; e-mail: satybaldina_dzh@enu.kz. ORCID: https://orcid.org/0000-0003-0291-4685.

Фариза Биляловна Тебуева – доктор физико-математических наук, профессор кафедры вычислительной математики и кибернетики, ФГАОУ ВО «Северо-Кавказский федеральный университет», г. Ставрополь, Российская Федерация; e-mail: ftebueva@nfcu.ru. ORCID: https://orcid.org/0000-0002-7373-4692.

Төлеген Айдынұлы Айдынов – докторант кафедры «Информационная безопасность», Евразийский национальный университет имени Л.Н. Гумилева, г. Астана, Республика Казахстан; e-mail: tolegen.ch@gmail.com. ORCID: https://orcid.org/0009-0005-3327-9719.

Айгуль Кайрулаевна Шайханова*– PhD, профессор кафедры «Информационная безопасность», Евразийский национальный университет имени Л.Н. Гумилева, г. Астана, Республика Казахстан; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Авторлар туралы мәліметтер

Каким Молдабекович Сагиндыков – техника ғылымдарының кандидаты, «Ақпараттық қауіпсіздік» кафедрасының доценті; Л.Н. Гумилев атындағы Еуразия ұлттық университеті КЕАҚ, Астана қ., Қазақстан Республикасы; e-mail: sagindykov_km@enu.kz. ORCID: https://orcid.org/0000-0003-3315-798X.

Дина Жагыпаровна Сатыбалдина – физика-математика ғылымдарының кандидаты, қауымдастырылған профессор, KazHackStan, ЖШС, Астана қ., Қазақстан Республикасы; e-mail: satybaldina_dzh@enu.kz. ORCID: https://orcid.org/0000-0003-0291-4685.

Фариза Биляловна Тебуева – физика-математика ғылымдарының докторы, есептеу математикасы және кибернетика кафедрасының профессоры, Солтүстік Кавказ федералды университеті, Ставрополь қ., Ресей Федерациясы; e-mail: ftebueva@nfcu.ru. ORCID: https://orcid.org/0000-0002-7373-4692.

Төлеген Айдынұлы Айдынов – «Ақпараттық қауіпсіздік» кафедрасының докторанты; Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан Республикасы; e-mail: tolegen.ch@gmail.com. ORCID: https://orcid.org/0009-0005-3327-9719.

Айгуль Кайрулаевна Шайханова* – PhD, «Ақпараттық қауіпсіздік» кафедрасының профессоры; Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан Республикасы; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Information about the authors

Kakim Sagindykov – Candidate of Technical Sciences, associate Professor of the Information Security Department, L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan; e-mail: sagindykov_km@enu.kz. ORCID: https://orcid.org/0000-0003-3315-798X.

Dina Satybaldina – Candidate of Physical and Mathematical Sciences, Associate Professor, KazHackStan LLP, Astana, Republic of Kazakhstan; e-mail: satybaldina_dzh@enu.kz. ORCID: https://orcid.org/0000-0003-0291-4685.

Fariza Tebueva – Doctor of Physical and Mathematical Sciences, Professor of the Computational Mathematics and Cybernetics Department, North-Caucasus Federal University, Stavropol, Russian Federation; e-mail: ftebueva@nfcu.ru. ORCID: https://orcid.org/0000-0002-7373-4692.

Tolegen Aydynov – PhD student of the Information Security Department, L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan; e-mail: tolegen.ch@gmail.com. ORCID: https://orcid.org/0009-0005-3327-9719.

Aigul Shaykhanova* – PhD, Professor of the Information Security Department; L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Поступила в редакцию 31.03.2025
Поступила после доработки 12.04.2025
Принята к публикации 14.04.2025