DOI: https://doi.org/10.26642/ten-2024-2(94)-174-179
УДК 004.75

О.О. Шелуха, к.т.н.
Державний університет «Житомирська політехніка»
Д.М. Квашук, к.е.н., доц.
Національний авіаційний університет
К.О. Супруненко, студентка
Державний університет «Житомирська політехніка»

Дворівнева система захисту домашньої IoT-мережі

У статті розглянуто проблеми захисту домашніх IoT-мереж, зокрема, шляхи забезпечення безпеки під час передачі даних у системах, побудованих на основі мікроконтролерів ESP32. Зважаючи на збільшення кількості пристроїв IoT, актуальність розробки надійних засобів захисту зростає. Адже використання незахищених каналів передачі може спричинити витік даних, несанкціонований доступ або інші кібератаки. Запропонована архітектура з використанням алгоритму AES для локальних мережевих з'єднань та SSL/TLS для передачі даних на зовнішній MQTT-брокер надає кількарівневий захист від потенційних загроз.

У роботі запропоновано застосування автоматичної ротації AES-ключів, що дозволяє уникнути ризиків, пов'язаних із компрометацією ключів за тривалого використання. Завдяки інтеграції з Telegram-ботом користувачі отримують сповіщення про інциденти або потенційні загрози, що підвищує зручність взаємодії із системою та забезпечує швидку реакцію на події. Система дозволяє підтримувати високу конфіденційність передачі інформації в домашній IoT-мережі та водночас не потребує значних обчислювальних ресурсів, що є важливим для обмежених можливостей IoT-пристроїв.

У процесі дослідження проведено аналіз існуючих методів захисту IoT-мереж, їх переваг і недоліків, а також запропоновано підхід на основі зберігання та автоматичного розповсюдження ключів через MQTT-брокер. Це дозволяє централізовано управляти криптографічними параметрами та забезпечує їх доступність для всіх пристроїв мережі, підвищуючи таким чином рівень захищеності IoT-системи.

Ключові слова: *інтернет речей (IoT); захист IoT-мереж; контролер ESP32; MQTT-брокер; кібербезпека; симетричний алгоритм блочного шифрування AES128; легковагова криптографія; граничні обчислення; Edge Computing.*

Актуальність теми. Сучасний розвиток технологій Інтернету речей (IoT) змінює підхід до побудови інфраструктур у різних сферах життя, таких як домашня автоматизація, промислові системи, «розумні» міста, медицина та аграрний сектор. Зростання кількості IoT-пристроїв та широке впровадження мережевих рішень, що об'єднують ці пристрої, вимагає підвищення рівня захищеності даних та безпеки підключених мереж. Без належного захисту IoT-системи можуть бути вразливими до кіберзагроз, що створює серйозні ризики для користувачів, зокрема, ризики витоку приватної інформації, несанкціонованого доступу до систем управління пристроями та втрати цілісності даних.

Розробка захищеної архітектури IoT є особливо актуальною у домашніх умовах, де приватність користувачів має бути надійно захищена. Багато сучасних розумних будинків використовують IoT-сенсори та пристрої для моніторингу й управління кліматом, освітленням, безпекою, але ці системи часто стають мішенню для кібератак через недостатній захист каналів передачі даних.

У цьому контексті використання шифрування для локальних мереж (наприклад, AES) та захищених протоколів передачі (SSL/TLS) є актуальним підходом для створення стійкої до загроз системи. Крім того, автоматична ротація ключів шифрування значно підвищує рівень захисту, знижуючи ризик компрометації системи у разі тривалого використання одного і того ж ключа. Цей підхід особливо корисний для IoT-мереж, де часто використовуються обмежені ресурси з невеликою обчислювальною потужністю, як у випадку контролерів ESP32.

Окрім аспектів безпеки, актуальність дослідження цієї теми визначається зростаючими потребами у швидкій та гнучкій обробці даних, які надходять з IoT-пристроїв. Інтеграція IoT-систем з хмарними сервісами та системами обробки повідомлень (наприклад, через Telegram-боти) дозволяє користувачам своєчасно отримувати інформацію про події та реагувати на зміни в системі в режимі реального часу. Це важливо для зручності користувача та ефективного управління домашнім господарством.

Отже, розробка безпечних IoT-систем із захищеними каналами передачі даних, використанням протоколів шифрування та іншими механізмами захисту IoT-рішень робить дослідження актуальним.

Аналіз останніх досліджень та публікацій, на які спираються автори. У [1] авторами описується система, основним завданням якої є захист домашньої мережі IoT-пристроїв, за допомогою використання методів глибокої перевірки пакетів, що захоплюються спеціально створеним honeypot та відповідно переміщення портів для ускладнення ідентифікації зловмисниками відкритих портів. Такий метод зручний для досліджень, але, по-перше, вимагає постійної уваги з боку користувача та достатньої його кваліфікації для аналізу трафіка, виявлення та реагування на загрози, по-друге, така система є достатньо вимогливою до ресурсів, що також сильно знижує можливості застосування висвітленої системи для домашньої мережі.

У [2] авторами висвітлюється методика тестування вразливостей на основі ройового інтелекту для аналізу вразливостей, виявлення та ліквідації загроз IoT-мережі завдяки паралельній діяльності декількох алгоритмів тестування системи на проникнення. Цей метод дозволяє швидше знаходити вразливості порівняно із лінійними алгоритмами, проте вимагає складного налаштування, потреби в потужних обчислювальних ресурсах і, відповідно, через великий об'єм трафіка може негативно вплинути на продуктивність мережі.

У [3] авторами широко оглянуто різноманітні IoT-пристрої як домашнього, так промислового рівнів, висвітлено переваги автономізації пристроїв та підкреслено високу безпеку IoT-мереж під час використання криптографічних протоколів та їх адаптації до каналів передачі даних IoT-пристроїв. Як недолік багатьох пристроїв наведено наявність недосконалих механізмів захисту паролів або взагалі відсутність модулів шифрування в прошивках IoT-пристроїв. Також як один із критичних недоліків підкреслено незахищений канал зв'язку (HTTP).

Авторами дослідження [4] розглянуто проблеми з безпекою передачі даних при взаємодії між IoT-пристроями, висвітлено новітні методи та алгоритми шифрування даних для забезпечення безпеки IoT.

У [5] розглянуто модель легковагової криптографії (Lightweight Cryptography) для IoT-пристроїв, що дозволяє враховувати обмеженість обчислювальних ресурсів та пам'яті у таких пристроях, при достатньо великому об'ємі даних, що оброблюються та передаються до вищих рівнів IoT-системи на прикладі камери відеоспостереження. Також підкреслено, що застосування великих ключів та їх періодичне оновлення робить метод шифрування достатньо стійким до проникнення. А втім, продовженням зазначених переваг є недоліки, викликані обмеженістю ресурсів IoT-пристрою, збільшення затримок при великому трафіку та нестабільності мережі.

У [6] детально розглянуто методи атак на найбільш популярні протоколи передачі даних в IoT, таких як DNS, HTTP та MQTT. Зібрано статистичні дані, на основі яких розроблено метод ансамблевого навчання з використанням декількох методів машинного навчання, а саме дерева рішень, наївного баєсовського алгоритму та штучної нейронної мережі. Запропонований авторами ансамблевий метод передбачає більш високу швидкість визначення атак та меншу кількість помилкових спрацювань порівняно з кожним із зазначених методів окремо. Проте зазначений метод має і свої недоліки під час застосування в домашній IoT-мережі: високі вимоги до обчислювальних ресурсів системи, що може бути проблемою для слабких домашніх IoT-пристроїв, складність налаштування такого захисту для пересічного користувача, і відповідно необхідність в зборі та підготовці даних для навчання, а також певна тривалість навчання такої системи. Отже, така система хоча і здається надійною, але краще підходить для промислових або професійних пристроїв, які мають достатні обчислювальні потужності для аналізу даних, спеціально підготовлених фахівців та набори даних, що зможуть реалізувати процес навчання та впровадження зазначеного ансамблевого методу в IoT-систему.

У [7] авторами проведено дослідження ландшафту кібербезпеки домашніх IoT-пристроїв та систем. Наведено аналіз найбільш типових методів атаки на IoT-мережу та побудовано моделі аналізу ризиків, що дозволяють спростити вибір стратегії захисту від кожної з атак. Проте в роботі не висвітлено конкретного рішення, а лише певні рекомендації, які можна використовувати для захисту системи IoT-пристроїв пересічного користувача, впровадження яких вимагає відповідної кваліфікації та досвіду.

Якщо у зазначених вище роботах розглядалися методи захисту лише домашньої мережі IoT-пристроїв, то у роботах [8, 9] автори розглянули методи виявлення вже скомпрометованих систем.

Так у роботі [8] автори зайшли з іншої сторони до виявлення вразливостей домашньої IoT-мережі – використання Shodan API для виявлення публічної доступності власних пристроїв та перевірки їх на вразливості, що дозволяє швидко виявляти загрози та захищати пристрої від потенційних атак. Проте зазначена методика одночасно є і недоліком, оскільки виявлення ризиків у цьому випадку є залежним від сторонніх сервісів, що може вплинути на час реакції на загрози та надійність системи в цілому.

Відповідно в [9] автори розглянули методи виявлення вже заражених систем, що підключені за домашнім NAT, до того як вони почнуть спричиняти проблеми. За допомогою засобів машинного навчання авторами запропоновано виявляти підозрілий трафік всередині мережі та запропоновано декілька алгоритмів його аналізу. Таке рішення спрямоване не стільки на домашнього користувача, скільки на провайдера і дозволить йому виявляти проблеми навіть у зашифрованому трафіку, але це, відповідно, містить в собі загрозу конфіденційності клієнтів, вимагатиме додаткових витрат на

встановлення програмних та апаратних агентів для аналізу та збору даних, а також достатньо сильно буде навантажувати мережу і викликати затримки. Також така система буде дуже чутливою до якості навчання машинних алгоритмів.

Підсумовуючи проведений вище аналіз, можна зробити висновок, що для домашньої мережі, де користувач не має достатніх навичок для аналізу даних систем моніторингу та налаштування відповідних систем захисту мережі, оптимальною є парадигма граничних обчислень (Edge computing), коли на граничних IoT-пристроях виконується обробка зібраної інформації та налаштовується шифрований канал зв'язку із сервером, для взаємодії в середині IoT-системи, та система зберігання оброблених даних на випадок недоступності мережі.

Таким чином, існує нагальна потреба у розробці спеціалізованих рішень на основі окремих IoT-пристроїв, які б забезпечували як автономне виконання своїх функцій, так і захищений зв'язок через центральний серверний вузол. Це своєю чергою сприятиме підвищенню ефективності та безпеці домашньої IoT-мережі шляхом оптимізації режимів роботи IoT-пристроїв.

Метою дослідження є вивчення можливості створення захищеної домашньої IoT-мережі, як з можливістю створення додаткового захисту каналу комунікації через локальний вебсервер криптографічними методами, на якому буде відбуватися шифрування каналів зв'язку між центральним вузлом та окремими граничними пристроями, так і побудувати захищений канал напряму з користувачем через сервіс обміну повідомлень Telegram. Така методика подвійного криптографічного захисту дозволить підвищити конфіденційність домашньої мережі IoT-пристроїв, а методика дублювання каналів комунікації дозволить забезпечити доступність системи для користувача.

Викладення основного матеріалу. Для створення домашньої IoT-мережі існує багато різних пристроїв. В деяких роботах [10, 11] авторами розглядається декілька приладів, зручних для використання в домашніх умовах, але і пропонується створення власних IoT-пристроїв на базі процесорів ESP32. Проте зазначені в роботах розробки не враховують висвітлену в цій роботі потребу в захисті каналів передачі даних, а лише відображають напрацювання за конкретними розробками – вимірювання мікроклімату [10] та камери фотофіксації для системи датчика руху [11].

Основна ідея цього дослідження полягає в розробці єдиної IoT-мережі, яка не лише об'єднає окремі пристрої в єдину систему, а й висвітлить аспект захисту каналів обміну даними між граничними пристроями, центральним вебсервером та користувачем, і забезпечення можливості автономного функціонування окремих елементів системи при втраті зв'язку між ними та сервером. Також важливим нюансом є система взаємодії з користувачем, як через візуалізацію на вебсервері, так і напряму через повідомлення в сервісі обміну повідомленнями Telegram. Схема функціонування системи відображено на рисунку 1.

Розроблювана система має забезпечити зручний доступ до управління пристроями, моніторингу їх стану та автоматизації завдань у межах домашньої IoT-мережі. Основним елементом системи буде вебсервер на основі мікроконтролера ESP32, який слугуватиме як інтерактивний інтерфейс для користувачів, дозволяючи їм легко контролювати освітлення, кліматичні системи, охоронні пристрої та інші елементи IoT-середовища. Крім того, для забезпечення безпеки системи будуть впроваджені додаткові методи захисту даних, що дозволяє знизити ризики несанкціонованого доступу та захистити конфіденційність користувачів.

Для створення ефективної домашньої IoT-мережі як граничний пристрій також використовується контролер ESP32, оснащений модулями Wi-Fi та Bluetooth, що дозволяє легко інтегрувати пристрої в бездротову мережу та керувати ними дистанційно. Завдяки підтримці різних протоколів зв'язку ESP32 може взаємодіяти з багатьма сенсорами та пристроями, а також має значну кількість доступних бібліотек, що спрощує процес розробки додаткових програмних модулів. Граничні компоненти системи містять різноманітні сенсори та датчики для збору даних про температуру, вологість, рух, а також камеру для відеоспостереження. Так датчики температури й вологості забезпечують точний моніторинг кліматичних параметрів, датчики руху фіксують активність у зоні покриття, а камера ESP32-CAM дозволяє не лише робити знімки, але й вести відеотрансляцію. Це додає можливість системі виконувати важливі функції моніторингу та забезпечення безпеки, і дозволяє користувачу оперативно реагувати на будь-які зміни або інциденти. Уся зібрана інформація передається на вебсервер для подальшої обробки й аналізу. Система також дозволить налаштовувати сценарії автоматизації, що сприяє ефективнішому використанню енергії та підвищує зручність управління, додаючи гнучкість і безпеку в роботі з домашньою IoT-мережею.

Архітектура безпеки запропонованої IoT-мережі (рис. 1) полягає у використанні двох основних компонентів: використання захищеного SSL/TLS-з'єднання з зовнішніми компонентами та застосування шифрування каналів зв'язку між граничними пристроями та вебсервером в середині внутрішньої Wi-Fi-мережі за допомогою простого алгоритму AES128.

Особливістю цієї архітектури є використання MQTT-брокера для централізованого управління ключами та їх розповсюдження на всі пристрої в мережі. У цьому випадку брокер генерує та зберігає нові ключі, передаючи їх локальному серверу, який своєю чергою надсилає ключі граничним пристроям.

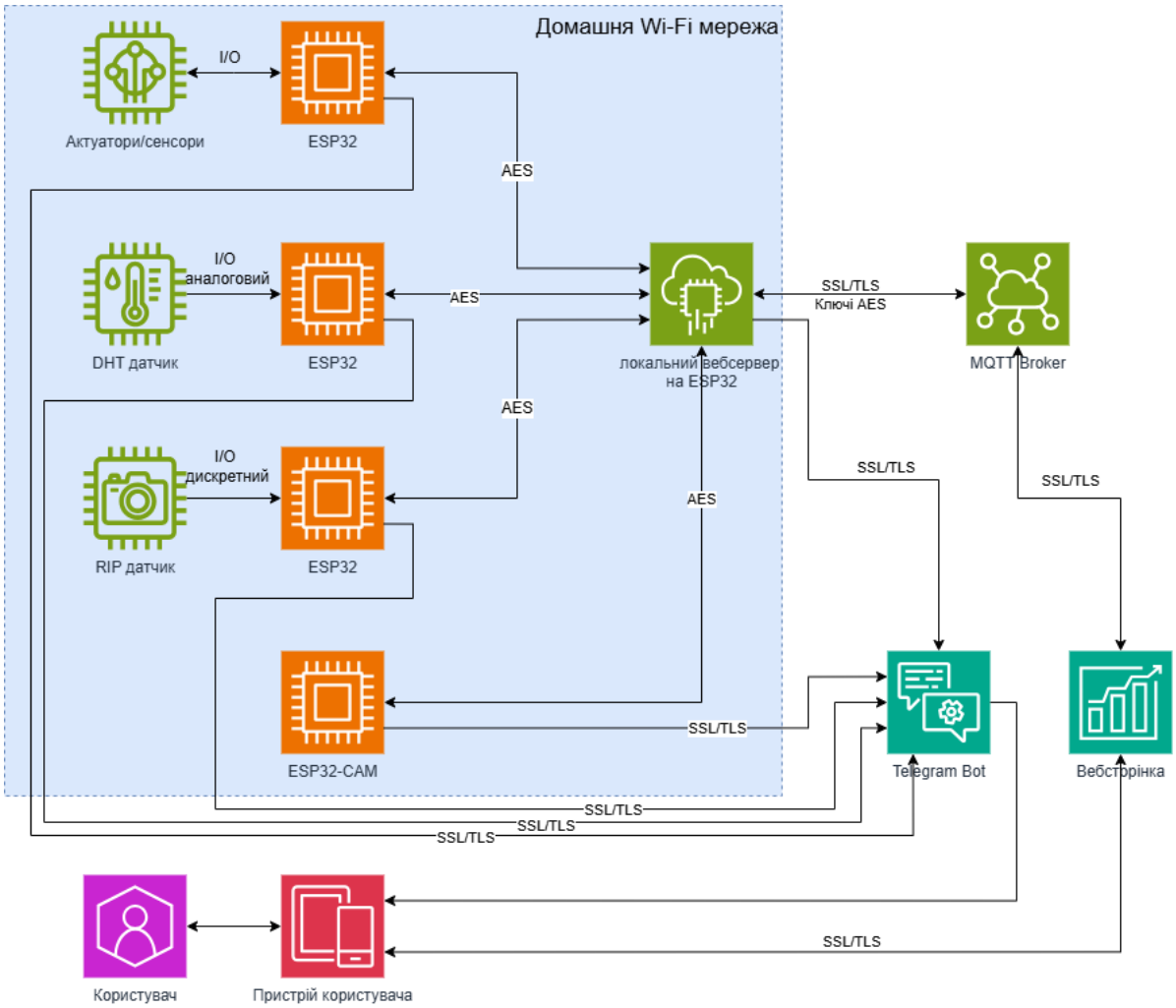

Рис. 1. Архітектура запропонованої IoT-мережі з візуалізацією захисту каналів зв'язку

Розглянемо основні етапи функціонування цієї системи:

1. Генерація ключів на MQTT-брокері. Брокер може періодично генерувати нові ключі AES (наприклад, раз на добу) і публікувати їх на спеціальному каналі MQTT (наприклад, keys/update). Важливо налаштувати брокер на підтримку захищеного з'єднання (SSL/TLS) для передачі ключів;

2. Отримання ключів локальним сервером. Локальний сервер підписується на канал keys/update на MQTT-брокері. Після публікації нового ключа брокером контролер локального сервера отримує повідомлення з ключем і зберігає його в локальній пам'яті для подальшого розповсюдження на граничні пристрої;

3. Локальний сервер надсилає нові ключі на кожен граничний пристрій;

4. Після отримання ключа кожен граничний пристрій оновлює ключ шифрування та використовує його для шифрування / дешифрування даних.

Після оновлення ключів усі граничні пристрої можуть використовувати новий ключ для шифрування та дешифрування даних, переданих між ними та сервером.

Для розробки системи захисту використовувалися з використанням бібліотек Wi-Fi для створення Wi-Fi з'єднання, WiFiClientSecure для створення захищеного (SSL/TLS) з'єднання з віддаленими сервісам, а також між мікроконтролерами в середині IoT-мережі, AESLib, Base64 та Crypto для забезпечення додаткового шифрування каналів передачі даних. Так AESLib виконує шифрування та дешифрування, що забезпечує конфіденційність даних при передачі, а Base64 використовується для кодування шифрованих даних у текстовий формат для зручної передачі. Бібліотека Crypto додає додаткові криптографічні функції, такі як хешування та HMAC, для перевірки цілісності й автентичності даних.

Також для покращення гнучкості та адаптованості система підтримує можливість отримання та виконання фрагментів коду з хмари для оновлення або розширення функціоналу. Це дозволяє легко оновлювати ПЗ та додавати нові функції без необхідності фізичного доступу до пристроїв. Додатково реалізовано інтеграцію з Telegram-ботом для своєчасного інформування про інциденти. Так за

виникнення тривоги з датчика руху або отримання аномальних температурних відхилень пристрої можуть ініціювати з'єднання з Telegram-ботом та надіслати усі необхідні дані користувачу у вигляді повідомлення, що дозволяє швидко реагувати на зміни й підтримувати високий рівень безпеки.

Отже, запропонована система є надійним та безпечним рішенням для створення локальної IoT-мережі. Зокрема, використання різнорівневої архітектури захисту дозволяє захистити приватні дані користувача, при цьому зберігаючи високий рівень функціональності та зручності.

Висновки та перспективи подальших досліджень. У цій роботі розглянуто процес захисту IoT-системи для моніторингу й управління домашніми пристроями, яка базується на контролерах ESP32, інтегрованих із MQTT-брокером. Основна увага приділена забезпеченню безпеки на всіх етапах передачі даних: від збирання інформації до передачі на центральний сервер і до користувача. Запропонована архітектура використовує кілька рівнів захисту, враховуючи шифрування AES для локальних з'єднань та SSL/TLS для комунікації з MQTT-брокером та сервісом обміну повідомлень Telegram, що дозволяє знизити ризики несанкціонованого доступу до пристроїв, а також забезпечити цілісність та доступність даних у мережі. Так автоматична ротація AES-ключів, запроваджена в системі, дозволяє додати додатковий рівень безпеки, зменшуючи ймовірність компрометації застарілих ключів. Інтеграція з Telegram-ботом забезпечує оперативне отримання сповіщень користувачем, що підвищує зручність взаємодії із системою та дозволяє швидко реагувати на потенційні загрози.

У майбутніх дослідженнях доцільно буде розглянути використання вдосконалених методів аутентифікації, таких як багатофакторна верифікація для доступу до пристроїв та даних IoT-системи ззовні. Це дозволить додатково захистити систему від несанкціонованого доступу навіть при компрометації окремих елементів мережі. Також подальше вдосконалення системи може враховувати оптимізацію енергоспоживання, зокрема для пристроїв, що працюють від акумуляторів, що дозволить розширити застосування IoT-рішень в умовах обмеженого доступу до живлення.

Список використаної літератури:

1. *Vincentius M.* Fending off IoT-hunting attacks at home networks / *M.Vincentius, C.Qiang, B.Theophilus* // Proceedings of the 2nd Workshop on Cloud-Assisted Networking (CAN '17). – NY, USA : Association for Computing Machinery New York, 2017. – P. 67–72. DOI: 10.1145/3155921.3160640.
2. Security Awareness in Smart Homes and Internet of Things Networks through Swarm-Based Cybersecurity Penetration Testing / *T.Schiller, B.Caulkins, A.Wu, S.Mondesire* // Information. – 2023. DOI: 10.3390/info14100536.
3. Security analysis on consumer and industrial IoT devices / *J.Wurm, K.Hoang, O.Arias and other* // 21st Asia and South Pacific Design Automation Conference (ASP-DAC). – 2016. – P. 519–524. DOI: 10.1109/ASPDAC.2016.7428064.
4. *Garg P*. Analysis of cryptographic encryption algorithm design to Secure IoT Devices: A review / *P.Garg, D.K. Singh* // Materials Today: Proceedings. – 2021. DOI: 10.1016/j.matpr.2021.06.240.
5. *Al-Husainy M.A.F.* Secure and Lightweight Encryption Model for IoT Surveillance Camera / *M.A.F. Al-Husainy, B.Al-Shargabi*. – 2020. DOI: 10.30534/ijatcse/2020/143922020.
6. *Moustafa N*. An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things / *B.Turnbull, K.Choo* // IEEE Internet of Things Journal. – 2019. – № 6. – P. 4815–4830. DOI: 10.1109/JIOT.2018.2871719.
7. *James F*. IoT Cybersecurity based Smart Home Intrusion Prevention System / *F.James* // 3rd Cyber Security in Networking Conference (CSNet). – 2019. – P. 107–113. DOI: 10.1109/CSNet47905.2019.9108938.
8. Defensive Programming for Smart Home Cybersecurity / *M.Rossi, R.Greca, L.Iovino and other* // A 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – 2020. – P. 600–605. DOI: 10.1109/EuroSPW51379.2020.00087.
9. A novel approach for detecting vulnerable IoT devices connected behind a home NAT / *Y.Meidan, V.Sachidananda, H.Peng and other* // Computers and Security. – 2020. – Vol. 97. DOI: 10.1016/j.cose.2020.101968.
10. *Коренівська О.Л.* Аспекти побудови систем моніторингу параметрів мікроклімату в навчальних аудиторіях / *О.Л. Коренівська, В.Б. Бенедицький, Т.М. Нікітчук* // Технічна інженерія. – 2022. – No. 2 (90). – P. 136–143. DOI: 10.26642/ten-2022-2(90)-136-143.
11. *Андрєєв О.В.* Комбінована система сигналізації на базі ESP32CAM / *О.В. Андрєєв, О.Дубина, Т.М. Нікітчук* // Технічна інженерія. – 2022. – No. 2 (90). – P. 131–135. DOI: 0.26642/ten-2022-2(90)-131-135.

References:

1. Vincentius, M., Qiang, C. and Theophilus, B. (2017), «Fending off IoT-hunting attacks at home networks», *Proceedings of the 2nd Workshop on Cloud-Assisted Networking (CAN '17)*, Association for Computing Machinery New York, NY, USA, pp. 67–72, doi: 10.1145/3155921.3160640.
2. Schiller, T., Caulkins, B., Wu, A. and Mondesire, S. (2023), «Security Awareness in Smart Homes and Internet of Things Networks through Swarm-Based Cybersecurity Penetration Testing», *Information*, doi: 10.3390/info14100536.
3. Wurm, J., Hoang, K., Arias, O. et al. (2016), «Security analysis on consumer and industrial IoT devices», *21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, pp. 519–524, doi: 10.1109/ASPDAC.2016.7428064.
4. Garg, P. and Singh, D.K. (2021), «Analysis of cryptographic encryption algorithm design to Secure IoT Devices: A review», *Materials Today: Proceedings*, doi: 10.1016/j.matpr.2021.06.240.

5. Al-Husainy, M.A.F. and Al-Shargabi, B. (2020), «Secure and Lightweight Encryption Model for IoT Surveillance Camera», doi: 10.30534/ijatcse/2020/143922020.
6. Moustafa, N., Turnbull, B. and Choo, K. (2019), «An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things», *IEEE Internet of Things Journal*, No. 6, pp. 4815–4830, doi: 10.1109/JIOT.2018.2871719.
7. James, F. (2019), «IoT Cybersecurity based Smart Home Intrusion Prevention System», *3rd Cyber Security in Networking Conference (CSNet)*, pp. 107–113, doi: 10.1109/CSNet47905.2019.9108938.
8. Rossi, M., Greca, R., Iovino, L. et al. (2020), «Defensive Programming for Smart Home Cybersecurity», *A 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW*), pp. 600–605, doi: 10.1109/EuroSPW51379.2020.00087.
9. Meidan, Y., Sachidananda, V., Peng, H. et al. (2020), «A novel approach for detecting vulnerable IoT devices connected behind a home NAT», *Computers and Security*, Vol. 97, doi: 0.1016/j.cose.2020.101968.
10. Korenivska, O., Benedytskyi, V. and Nikitchuk, T. (2022), «Aspekty pobudovy system monitorynhu parametriv mikroklimatu v navchalnykh audytoriiakh», *Tekhnichna inzheneriia*, No. 2 (90), pp. 136–143, doi: 10.26642/ten-2022-2(90)-136-143.
11. Andreiev, O.V., Dubyna, O. and Nikitchuk, T. (2022), «Kombinovana syctema syhnalizatsii na bazi ESP32CAM», *Tekhnichna inzheneriia*, No. 2 (90), pp. 131–135, doi: 10.26642/ten-2022-2(90)-131-135.

Шелуха Олексій Олегович – кандидат технічних наук, доцент Державного університету «Житомирська політехніка».

https://orcid.org/0000-0002-6088-8262.

Наукові інтереси:

– комп'ютерні системи та мережі;
– Інтернет речей;
– системи автоматизованого управління та інформаційно-вимірювальні системи.

E-mail: kkik_shoo@ztu.edu.ua.

Квашук Дмитро Михайлович – кандидат економічних наук, доцент, доцент Національного авіаційного університету.

https://orcid.org/0000-0002-4591-8881.

Наукові інтереси:

– інформаційно-вимірювальні системи;
– електроніка.

E-mail: dmytro.kvashuk@npp.nau.edu.ua.

Супруненко Катерина Олександрівна – студентка Державного університету «Житомирська політехніка».

https://orcid.org/0009-0007-1149-8333.

Наукові інтереси:

– Інтернет речей;
– захист інформації в комп'ютерних системах та мережах.

E-mail: suprunenko.kateryna07@gmail.com.

Shelukha O.O., Kvashuk D.M., Suprunenko K.O.

Two-level home IoT network protection system

The article discusses the problems of protecting home IoT networks, in particular, ways to ensure security during data transmission in systems built on the basis of ESP32 microcontrollers. Due to the growing number of IoT devices, the relevance of developing reliable security tools increases, because the use of unprotected transmission channels can lead to data leaks, unauthorized access or other cyber attacks. The proposed architecture using the AES algorithm for local network connections and SSL/TLS for data transfer to an external MQTT broker provides multi-level protection against potential threats.

The paper suggests the use of automatic rotation of AES keys, which avoids the risks associated with key compromise during prolonged use. Thanks to integration with the Telegram bot, users receive notifications about incidents or potential threats, which increases the convenience of interacting with the system and provides a quick response to events. The system allows you to maintain high confidentiality of information transmission in your home IoT network and at the same time does not require significant computing resources, which is important for the limited capabilities of IoT devices.

In the course of the study, the analysis of existing methods of protecting IoT networks, their advantages and disadvantages is carried out, and an approach based on storing and automatically distributing keys through an MQTT broker is proposed. This allows you to centrally manage cryptographic parameters and ensures their availability for all network devices, thus increasing the level of security of the IoT system.

Keywords: Internet of Things (IoT); IoT network protection; ESP32 controller; MQTT broker; cybersecurity; AES128 symmetric block encryption algorithm; lightweight cryptography; limit computing; Edge Computing.

Стаття надійшла до редакції 27.09.2024.