IQRO JURNALI , IQRO JOURNAL, ИКРО ЖУРНАЛИ
ISSN:2181-4341| wordlyknowledge.uz/index.php/iqro
Volume 22 Issue 01 IYUN 2026

МЕХАНИЗМЫ ЗАЩИТЫ И СИНХРОНИЗАЦИИ ДАННЫХ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ (IOT) В УСЛОВИЯХ НЕСТАБИЛЬНОГО СЕТЕВОГО СОЕДИНЕНИЯ

Джуманиязов Азизбек Ансатбаевич
Аймуратов Айдос Кобланбек угли
Джимова Жанар Таубековна
Нукусский государственный технический университет

Аннотация: В статье представлен комплексный анализ уязвимостей систем Интернета вещей (IoT) в условиях нестабильного сетевого соединения и предложена интегрированная архитектура безопасности на основе парадигмы «сохранение и передача» (store-and-forward). Разработанная система решает фундаментальные проблемы управления ключами и защиты данных в состоянии покоя при длительных обрывах связи. Экспериментальная валидация, проведенная на гибридном стенде с использованием реальных Android-устройств (Termux), SIEM Wazuh и Suricata IDS, доказывает высокую практическую эффективность архитектуры. Внедрение адаптивного легковесного криптографического алгоритма ASCON-128 обеспечивает снижение потребления оперативной памяти (RAM) до ~1 КБ, что в несколько раз эффективнее традиционных алгоритмов AES. Гибридная система обнаружения вторжений, использующая анализ временных окон, достигает 100% точности выявления атак типа DDoS и MITM, при этом уровень ложных срабатываний (False Positive) снижен до 0,01%.

Ключевые слова: Интернет вещей (IoT), кибербезопасность, прерывистая связь (DTN), адаптивная криптография, ASCON-128, система обнаружения вторжений (IDS), Store-and-Forward, оркестрация безопасности.

Введение. В эпоху цифровой трансформации технологии интернета вещей (IoT) стали неотъемлемой частью промышленности, сельского хозяйства и логистики. Однако значительная часть промышленных IoT-устройств, таких как датчики на трубопроводах или гидроэлектростанциях, функционирует в удаленных зонах, не имеющих постоянного и стабильного интернет-соединения. Традиционные программные решения безопасности, такие как TLS 1.3, MQTT+TLS или DTLS, требуют постоянного подключения к сети для инициализации сессий и обмена ключами в реальном времени. В условиях прерывистой связи такие протоколы либо полностью не функционируют, либо создают серьезные уязвимости. Для государств, реализующих масштабные программы цифровизации, таких как стратегия «Цифровой Узбекистан – 2030», обеспечение кибербезопасности критической инфраструктуры приобретает стратегическое значение. Вопросы безопасности IoT-систем активно исследуются международным научным сообществом. Мировые исследователи, такие как Г. Рестуччиа и Н. Гхарат, предлагают гибридные подходы, комбинирующие AES и ECC. Тем не менее, существующие коммерческие решения зачастую не способны обеспечить локальное офлайн-шифрование и требуют постоянной связи с облачными платформами.

Объект и предмет исследования. Объектом исследования выступают IoT-сенсоры, установленные в удаленных зонах с прерывистой связью, и система их взаимодействия с локальным сервером. Предметом исследования являются механизмы офлайн-шифрования данных в архитектуре "сохранение и передача", протоколы аутентификации пакетов и методы обнаружения аномалий на уровне локального сервера.

Цель и задачи исследования. Цель исследования — разработка и экспериментальная оценка интегрированной адаптивной системы безопасности на основе

архитектуры сохранения и передачи данных для IoT-устройств с ограниченными ресурсами, работающих в условиях прерывистой связи. Ключевые задачи включают:

- Классификацию специфических угроз в условиях прерывистой связи.
- Адаптацию легковесного алгоритма ASCON-128 для офлайн-шифрования и управления nonce.
- Разработку механизмов аутентификации и проверки целостности на уровне локального сервера.
- Создание ансамбля алгоритмов выявления аномалий (IDS) в реальном времени.
- Экспериментальное тестирование архитектуры на реальных аппаратных платформах.

Методология исследования. Экспериментальная среда была спроектирована как гибридная инфраструктура. В качестве IoT-сенсора использовалось реальное физическое устройство на базе Android (окружение Termux) с запущенным Python-скриптом шифрования. Физическое отключение Wi-Fi модуля устройства симулировало реалистичные обрывы связи. Сетевое взаимодействие и централизованный мониторинг обеспечивались системой Wazuh SIEM v4.14.3 и Suricata IDS v8.0.4, развернутыми в контейнерах Docker. Для моделирования целевых атак (DDoS SYN-flood, сканирование портов) применялась машина Kali Linux 2024 с инструментами hping3 и научным датасетом Edge-IIoTset.

Результаты исследования. Анализ угроз и стандартов. Системный анализ выявил три фундаментальные проблемы в условиях прерывистой связи: управление ключами в офлайн-режиме, безопасность данных в состоянии покоя (data-at-rest) в период их локального накопления, а также нарушение связности и хронологии при доставке пакетов. Существующие стандарты IETF (RFC 9171 и 9172) определяют общие спецификации для сетей DTN, но не предлагают легковесных реализаций для IoT.

Разработка пропозициональной интегрированной архитектуры. Для преодоления существующих ограничений предложена трехуровневая архитектура:

- **Уровень устройств (Device Layer):** Отвечает за сбор данных, их локальное шифрование и сохранение в офлайн-буфере (offline_buffer.json) при потере связи.
- **Сетевой уровень (Edge Gateway Layer):** Обеспечивает локальную фильтрацию трафика и выступает криптографическим терминатором.
- **Облачный уровень (Cloud Layer):** Реализует глобальную оркестрацию, управление ключами и централизованный мониторинг IDS.

Криптографический слой. В качестве базового стандарта был выбран легковесный криптографический алгоритм ASCON-128 (NIST SP 800-232), идеально подходящий для микроконтроллеров (например, ESP32). Алгоритм использует конструкцию «губка» и реализует механизм аутентифицированного шифрования (AEAD). Для защиты от атак повторного воспроизведения (Replay Attack) генерируется уникальный 16-байтовый nonce, состоящий из 8-байтовой временной метки (timestamp) и 8-байтового криптографически безопасного случайного числа.

Система обнаружения вторжений (IDS). Для проактивной защиты разработана гибридная распределенная система обнаружения вторжений. Важнейшей инновацией стало внедрение алгоритма «адаптивных временных окон» (temporal anomaly detection). Датчики программируются на выход в сеть в строго заданные интервалы (например, 08:00–08:15 и 20:00–20:15). Любой пакет, поступающий вне этого расписания, классифицируется системой Wazuh как экстремальная угроза (Level 14), что позволяет мгновенно блокировать поведенческие аномалии, даже если злоумышленник скрывает IP-адрес.

Экспериментальные результаты. Тестирование подтвердило высокую эффективность выбранных криптографических примитивов для ресурсно-ограниченных узлов.

Таблица 1

Сравнительный анализ потребления ресурсов криптографическими алгоритмами для IoT

Алгоритм	Длина ключа (бит)	Потребление RAM (КБ)	Скорость (Мбит/с)	Стандарт
ASCON-128	128	~0.3	~24	NIST SP 800-232
AES-128-GCM	128	~2.0	~18	NIST FIPS 197
ChaCha20-Poly1305	256	~0.5	~31	RFC 8439
AES-256-CCM	256	~3.0	~14	NIST SP 800-38C

Данные Таблицы 1 доказывают, что ASCON-128 требует в несколько раз меньше оперативной памяти по сравнению с традиционными реализациями AES, что критически важно для автономных датчиков, сохраняя при этом высокую пропускную способность.

В ходе симуляции потери связи (фаза OFFLINE) датчик успешно накопил 221 зашифрованный пакет. После восстановления сети (фаза ONLINE) все 221 пакетов были автоматически синхронизированы с сервером в хронологическом порядке без потерь (data loss). Сервер корректно присвоил им статус synced_from_offline, исключив ложное срабатывание системы на внезапный всплеск трафика.

Таблица 2

Показатели результативности системы обнаружения угроз (IDS)

Тип атаки (Уровень угрозы)	Обнаружено	Точность (Accuracy)	Ложные срабатывания (FP)
DDoS HTTP Flood (L12)	1 534	100%	0
MITM ARP Spoofing (L12)	617	100%	0
Port Scanning (L10)	1 494	100%	3
Временные аномалии (L14)	~1 800	100%	2

В Таблице 2 зафиксирована абсолютная результативность системы. При анализе более 66 000 сетевых событий система продемонстрировала 100% точность обнаружения целевых атак. Общее количество ложных срабатываний (False Positives) составило всего 10 инцидентов, что математически эквивалентно 0,01%. Уведомления об инцидентах и статусах подключения устройств доставляются оператору через Telegram-бота с задержкой всего 8–12 секунд. Сравнительный анализ с коммерческими решениями (AWS IoT, Azure Sphere) подтвердил уникальность разработанной open-source платформы, которая единственная предлагает одновременную интеграцию офлайн-шифрования, авто-синхронизации буфера и поведенческого анализа.

Заключение. В результате исследования успешно решена актуальная научно-техническая задача обеспечения кибербезопасности IoT-систем в условиях прерывистой связи. Теоретически обоснована и экспериментально доказана эффективность архитектуры «сохранение и передача». Использование легковесного алгоритма ASCON-128 гарантирует конфиденциальность и целостность данных в локальном буфере, а генерация уникальных nonce надежно защищает от атак повторного воспроизведения. Внедрение адаптивных временных окон в систему IDS позволило достичь 100% выявления аномалий при уровне ложных срабатываний всего 0,01%. Полученные

результаты обладают высокой практической ценностью и готовы к внедрению в реальные системы мониторинга в рамках стратегии «Цифровой Узбекистан – 2030».

Список литературы:

1. Гладких А. А. Основы современных криптографических систем и перспективы их развития : учебное пособие. – Ульяновск : УлГТУ, 2020. – 214 с.
2. Ли П. Архитектура интернета вещей / пер. с анг. М. А. Райтмана. – М.: ДМК Пресс, 2019. – 454 с.
3. Стратегия «Узбекистан – 2030» // Национальная база данных законодательства Республики Узбекистан «LexUZ on-line». – URL: https://lex.uz/docs/6600404#6605092.
4. Alanezi, K., Annapareddy, T., Khan, S. et al. An edge-based IDS for the IoT using combined ML and generative AI models. Peer-to-Peer Netw. Appl. 19, 24 (2026). URL: https://doi.org/10.1007/s12083-025-02174-7