INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 8.854 Volume 13, issue 05 (2026)

DEVELOPMENT OF ADAPTIVE ALGORITHMS FOR ENSURING IOT DATA SECURITY IN A DISCONNECTED COMMUNICATION ENVIRONMENT.

Babadjanov Elmurod Satimbaevich

(Nukus State Technical University)

Jumaniyazov Azizbek Ansatbaevich

(Nukus State Technical University)

https://doi.org/10.5281/zenodo.20186072

Abstract: This paper presents a comprehensive analysis of the vulnerabilities of cyber-physical production systems and proposes a comprehensive integrated security architecture for the Industrial Internet of Things (IIoT). The developed system is based on the paradigms of a Unified Trust Fabric, adaptive communication, and cross-layer intelligence. The paper explores the transition from fragmented, discrete security tools to an adaptive, centrally orchestrated ecosystem. Experimental validation conducted on a hybrid rig simulating multi-stage targeted attacks (APTs) using the MITRE ATT&CK for ICS matrix demonstrates the high practical effectiveness of these solutions. Implementation of an adaptive cryptographic stack based on ECC reduces power consumption at the edge by 4.3 times, and the hybrid intrusion detection system achieves a 96% APT attack detection rate. Automated orchestration reduces incident response time to 3.2 seconds while maintaining 99.98% operational availability.

Keywords: Industrial Internet of Things (IIoT), cybersecurity, adaptive cryptography, intrusion detection system (IDS), security orchestration, machine learning, MITRE ATT&CK

РАЗРАБОТКА АДАПТИВНЫХ АЛГОРИТМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ УСТРОЙСТВ IOT В СРЕДЕ ПРЕРЫВИСТОЙ СВЯЗИ.

Бабаджанов Элмурод Сатимбаевич

(Нукусский государственный технический университет)

Джуманиязов Азизбек Ансатбаевич

(Нукусский государственный технический университет)

Аннотация: В статье представлен исчерпывающий анализ уязвимостей киберфизических производственных систем и предложена комплексная интегрированная архитектура безопасности для промышленного Интернета вещей (IIoT). Разработанная система базируется на парадигмах единой фабрики доверия (Unified Trust Fabric), адаптивной связи и межуровневого интеллекта (Cross-Layer Intelligence). Рассматривается переход от фрагментированных дискретных средств защиты к адаптивной, централизованно оркестрируемой экосистеме. Экспериментальная валидация, проведенная на гибридном стенде с моделированием многоэтапных целевых атак (APT) по матрице MITRE ATT&CK for ICS, доказывает высокую практическую эффективность решений. Внедрение адаптивного криптографического стека на базе ECC обеспечивает снижение энергопотребления на периферии в 4,3 раза, а гибридная система обнаружения вторжений достигает коэффициента обнаружения APT-атак в 96%. Автоматизированная

оркестрация сокращает время реакции на инциденты до 3,2 секунд при сохранении 99,98% операционной доступности.

Ключевые слова: промышленный интернет вещей (IIoT), кибербезопасность, адаптивная криптография, система обнаружения вторжений (IDS), оркестрация безопасности, машинное обучение, MITRE ATT&CK.

Введение. Стремительное развитие технологий Интернета вещей (IoT) и их масштабное внедрение в промышленный сектор привели к формированию нового технологического уклада – Industrial Internet of Things (IIoT), который сегодня рассматривается как один из ключевых драйверов четвертой промышленной революции.[1] По оценкам аналитических агентств, к 2025 году количество подключенных промышленных устройств превысит 25 миллиардов, а объем мирового рынка IIoT достигнет сотен миллиардов долларов.[1] Данная трансформация объединяет интеллектуальные датчики, программируемые логические контроллеры (ПЛК), промышленные шлюзы и облачные платформы в единую цифровую экосистему.[1]

Однако глубокая взаимосвязанность элементов приводит к резкому расширению поверхности атаки. Угрозы в таких системах носят киберфизический характер: последствия атак могут включать физическое повреждение оборудования, остановку критической инфраструктуры и экологические инциденты.[1] Практика подтверждает актуальность проблемы инцидентами с BlackEnergy (2015), WannaCry (2017) и атакой на Colonial Pipeline (2021).[1] Для государств, реализующих масштабные программы цифровизации экономики, например, стратегию «Цифровой Узбекистан – 2030», обеспечение киберустойчивости приобретает стратегическое значение.[1]

Вопросы безопасности IIoT активно исследуются мировым научным сообществом. Значительный вклад в развитие криптографии для IoT внесли Г. Рестуччиа, Х. Чофениг и Э. Баччелли.[1] Н. Гхарат предложил гибридные схемы AES и ECC, а Л. Де Ла Кадена выявил уязвимости протокола MQTT к атакам MITM.[1] Проблематика IDS подробно рассмотрена А. Тхаккаром и Р. Лохией.[1] Однако большинство работ сосредоточено на изолированных аспектах, в то время как комплексные открытые архитектуры представлены недостаточно.[1] Коммерческие платформы (Azure Sphere, AWS IoT) частично решают задачу, но их закрытая архитектура формирует жесткую привязку к вендору (vendor lock-in), что критично для гетерогенных сред.[1]

Объект и предмет исследования. Объектом исследования выступают промышленные IIoT-системы как киберфизические комплексы, включающие распределенные устройства, контроллеры, шлюзы и облачные платформы.[1] Предметом исследования являются архитектурные модели, методы и механизмы обеспечения комплексной безопасности, ориентированные на интеграцию защитных решений в единую управляемую среду.[1]

Цель и задачи исследования. Цель исследования — повышение уровня киберустойчивости промышленных IoT-систем за счет разработки, теоретического обоснования и экспериментальной проверки интегрированной архитектуры безопасности.[1] Ключевые задачи включают: системный анализ угроз; проектирование компонентов архитектуры (адаптивного протокола, гибридной IDS, механизмов TEE, Security Orchestrator); реализацию программно-аппаратного прототипа и проведение экспериментальной оценки.[1]

Методология исследования. В работе использованы методы системного анализа, прикладной криптографии, машинного обучения и стендового моделирования. Экспериментальная среда была спроектирована как гибридная инфраструктура. Физический сегмент (OT-уровень) построен на базе Raspberry Pi 4 (имитация ПЛК и шлюзов) с модулями TPM 2.0 (Infineon OPTIGA) для аппаратного корня доверия, а также микроконтроллеров ESP32 (датчики и актуаторы).[1] Сетевое взаимодействие велось по протоколам OPC UA и MQTT. Виртуальный сегмент (IT-уровень) включал Security Orchestrator, Центр сертификации (CFSSL), корреляционный движок IDS, SIEM Wazuh и симулятор MiniCPS, генерирующий детерминированный трафик.[1] Методология моделирования угроз строго базировалась на матрице MITRE ATT&CK for ICS и включала атаки на канал связи, на устройства, на прикладной уровень и сложные многоэтапные атаки (APT).[1] Для атак использовались фреймворки Metasploit, bettercap, scapy, modbuspal.[1]

Результаты исследования. *Анализ угроз и стандартов.* Системный анализ показывает, что уязвимости присутствуют на всех уровнях. На уровне связи легковесные протоколы (MQTT, ZigBee, LoRaWAN) подвержены перехвату, фальсификации брокера и атакам replay.[1] На аппаратном уровне отсутствие Secure Boot и открытые порты JTAG/UART позволяют извлекать ключи и модифицировать прошивки.[1] Отраслевые стандарты, такие как серия IEC 62443, регламентируют модель «Зоны и Каналы» и вычисляют целевой уровень безопасности по формуле: $SL - T = f(\text{Последствия} \times \text{Вероятность} \times \text{Уязвимости})$.[1]

Тем не менее, стандарты описывают целевое состояние, а не методы технической реализации.

Разработка пропозициональной интегрированной архитектуры. Для решения проблемы фрагментации предложена архитектура, опирающаяся на принципы единого доверия (Unified Trust Fabric), адаптивной безопасной связи, межуровневого интеллекта (Cross-Layer Intelligence) и централизованной оркестрации (Orchestrated-Distributed Enforcement).[1] Логически она делится на три плоскости:

1. Плоскость данных и управления (Data & Control Plane).

2. Плоскость безопасности (Security Plane), объединяющая PKI, оркестратор и корреляционный движок IDS.[1]

3. Плоскость доверенного исполнения (Trusted Execution Plane), обеспечивающая аппаратный корень доверия, Secure Boot и Secure FOTA.[1]

Криптографический слой. В рамках архитектуры разработан адаптивный модульный протокол. Симметричное шифрование опирается на AES-128/256-GCM, который выполняет шифрование и контроль целостности параллельно с низкими задержками.[1] Асимметричная часть базируется на криптографии эллиптических кривых (ECC, secp256r1), обеспечивающей идеальную прямую секретность (ECDHE) и легковесную аутентификацию (ECDSA).[1]

Система обнаружения вторжений (IDS). Пассивной криптографии недостаточно, поэтому архитектура включает гибридную распределенную IDS.[1] На периферии работают легкие агенты с сигнатурным анализом (Snort).[1] На граничных шлюзах DPI и ML-модели

(Isolation Forest) выявляют аномалии техпроцесса. На центральном уровне корреляционный движок использует машинное обучение для выявления распределенных APT-атак (Lateral Movement).[1] Взаимодействие с Security Orchestrator позволяет автоматически реагировать на события (например, изолировать VLAN или менять cipher suite).

Экспериментальные результаты. Тестирование выявило критическое превосходство ECC над RSA для ресурсно-ограниченных узлов.

Таблица 1	**Время полного рукопожатия и session resumption для RSA и ECC**
Целевая платформа	Алгоритм / Кривая
ESP32	RSA-2048
ESP32	ECDSA P-256
Raspberry Pi 4	RSA-3072
Raspberry Pi 4	ECDSA P-384

Данные Таблицы 1 [1] доказывают, что использование ECDSA (P-256) на ESP32 сокращает время соединения в 4,5 раза и снижает энергопотребление в 4,3 раза по сравнению с устаревшим RSA-2048. Адаптивное переключение шифров с AES-128-GCM на AES-256-GCM занимает всего 195 мс на ESP32 и 22 мс на шлюзе, происходя без разрыва соединения.[1] Накладные расходы на сквозную задержку при этом составляют допустимые +20,8% (до 15,1 мс).[1]

Таблица 2	**Эффективность обнаружения атак**
Тип атаки (Сценарий)	Базовая конфигурация (DR / FPR)
Сканирование портов / Флудинг	98% / 2%

Нарушение логики протокола	40% / 5%
Аномалия уставок	10% / 15%
Многоэтапная APT-атака	15% / 1%

В Таблице 2 [1] зафиксирован колоссальный рост результативности. Базовый сигнатурный анализ слеп к поведенческим аномалиям (обнаружение 10%). Адаптивная гибридная система, интегрирующая контекстные данные, поднимает коэффициент обнаружения APT-атак (DR) до 96%, снижая ложные срабатывания (FPR) до 2,1%.[1]

Таблица 3	**Временные метрики IDS (TTD и TTR) по конфигурациям системы**
Метрика	Базовая конфигурация
Среднее время до обнаружения (TTD), с	4.8 (только известные атаки)
Среднее время до реагирования (TTR), с	>120 (ручное)
Медианное TTR для APT (полная цепочка), с	>300

Интеграция с Security Orchestrator (Таблица 3) [1] позволила радикально сократить среднее время реагирования (TTR) с более чем 120 секунд при ручном администрировании до автоматизированных 3,2 секунд. Оркестратор изолирует нарушителей и отзывает сертификаты быстрее, чем злоумышленник переходит к физическому воздействию. При этом за 720 часов непрерывного тестирования система показала $A_o = 99.98\%$ операционной доступности без незапланированных простоев.[1]

Сравнительный анализ показал, что традиционные средства обладают лишь частичным соответствием IEC 62443 и не могут выявить APT.[1] Коммерческие платформы (Azure Sphere) обеспечивают защиту, но вызывают сильную привязку к проприетарной экосистеме. Предложенная архитектура является полностью открытой, не привязана к

вендору и успешно поддерживает интеграцию унаследованных (legacy) систем за счет доверенных шлюзов-посредников.[1]

Заключение. В результате проведенного исследования решена значимая научно-техническая задача создания целостной архитектуры безопасности для промышленных сред IIoT. Теоретически обоснован и экспериментально подтвержден системный подход, где безопасность является не набором изолированных барьеров, а динамически управляемой системой.[1] Синергия адаптивной легковесной криптографии (ECC, AES-GCM), гибридного машинного обучения для поиска аномалий и автоматизированной оркестрации политик позволила поднять выявление целевых атак до 96% при практически мгновенном реагировании в 3,2 секунды. При этом система сохраняет 99,98% доступности критических сервисов. Полученные результаты имеют высокую практическую ценность для внедрения в реальных индустриальных сетях и полностью соответствуют стандартам IEC 62443.[1]

Список литературы:

1. Гетьман А. И., Горюнов М. Н., Мацкевич А. Г., Рыболовлев Д. А. Сравнение системы обнаружения вторжений на основе машинного обучения с сигнатурными средствами защиты информации // Труды ИСП РАН. – Т. 34. – № 5. – 2022. – С. 111–126.

2. Гладких А. А. Основы современных криптографических систем и перспективы их развития : учебное пособие. – Ульяновск : УлГТУ, 2020. – 214 с.

3. Закон Республики Узбекистан, от 15.04.2022 г. № ЗРУ-764 «О кибербезопасности» // Национальная база данных законодательства Республики Узбекистан «LexUZ on-line». – URL: https://lex.uz/ru/docs/5960609.

4. Зверев С. И. Безопасность IoT-устройств: угрозы и методы защиты // Актуальные исследования. 2025. – №19 (254). – Ч.I. – С. 12-14.

5. Карпов А. В. Введение в криптографию: Учебное пособие. – Казань: Казан. ун-т, 2024. – 128 с.

6. Ли П. Архитектура интернета вещей / пер. с анг. М. А. Райтмана. – М.: ДМК Пресс, 2019. – 454 с.

7. Назарова З. К. Анализ уровня развития кибербезопасности в Узбекистане // Raqamli iqtisodiyot (Цифровая экономика). – 2025. – № 10. – С. 517–523.

8. Попова И. А. Обнаружение аномалий в наборе данных с помощью алгоритмов машинного обучения без учителя isolation forest и local outlier factor // StudNet. 2020. №12. С. 1460–1470.

9. Рогов А. В. Сравнительный анализ методов шифрования данных: традиционные и современные подходы // Научные высказывания. 2025. №14 (82). С. 21–25.

10. Салаев А.К., Сатторов А.Ш., Хайитбоев У.С. Эффективность и безопасность криптографических алгоритмов на основе эллиптических кривых по сравнению с алгоритмом RSA // Universum: технические науки : электрон. научн. журн. 2025. 3(132). С. 23–27.

11. Старилов А. Д. Обзор криптографических алгоритмов в сетях интернета вещей // Молодой ученый. – 2024. – № 21 (520). – С. 94–96.

12. Стратегия «Узбекистан – 2030» // Национальная база данных законодательства Республики Узбекистан «LexUZ on-line». – URL: https://lex.uz/docs/6600404#6605092.

13. Фейзуллаев Р. Э. Сравнительный анализ режимов шифрования AES в мобильном мессенджере: переход от ECB к CBC и GCM // Вестник науки. 2025. №5 (86). С. 934–952.

14. 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