УДК 004.056.55

АДАПТИВНОЕ КВАНТОВО-УСТОЙЧИВОЕ ШИФРОВАНИЕ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Дементьев Н.В.
специалист, Воронежский государственный университет
(Воронеж, Россия)

ADAPTIVE QUANTUM-RESISTANT ENCRYPTION FOR ARTIFICIAL INTELLIGENCE-BASED INFORMATION SYSTEMS

Dementyev N.V.
specialist degree, Voronezh state university (Voronezh, Russia)

Аннотация

В статье рассматривается концепция адаптивного квантово-устойчивого шифрования (АКУШ), ориентированного на защиту данных в интеллектуальных информационных системах, подверженных угрозам квантовых вычислений. Описаны основные принципы реализации АКУШ, его роль в различных сферах применения, таких как автономные транспортные системы, медицинские платформы и финансовые сети. Рассматривается взаимодействие ключевых компонентов системы, таких как модули оценки контекста, предсказания угроз, выбора шифрования, криптоконтейнера и модуля обратной связи. Приводится анализ эффективности адаптивного шифрования в реальных сценариях и обсуждаются перспективы развития технологий, включая интеграцию с методами машинного обучения и гибридными вычислительными архитектурами. В статье также подчеркивается значимость адаптивного подхода для обеспечения безопасности данных в условиях постоянно меняющихся угроз.

Ключевые слова: адаптивное квантово-устойчивое шифрование, постквантовая криптография, интеллектуальные информационные системы, машинное обучение, квантовые вычисления, защита данных, распределённые системы, финансовые сети, медицинские платформы, автономные транспортные системы.

Abstract

This article discusses the concept of adaptive quantum-resistant encryption (AQRE), designed to protect data in intelligent information systems vulnerable to quantum computing threats. The main principles of implementing AQRE are described, along with its role in various application fields such as autonomous transportation systems, medical platforms, and financial networks. The interaction of key system components, such as the context evaluation, threat prediction, encryption selection modules, cryptographic container, and feedback module, is also explored. The article analyzes the effectiveness of adaptive encryption in real-world scenarios and discusses the future development of technologies, including integration with machine learning methods and hybrid computational architectures. The importance of an adaptive approach for ensuring data security in the face of constantly evolving threats is emphasized.

Keywords: adaptive quantum-resistant encryption, post-quantum cryptography, intelligent information systems, machine learning, quantum computing, data security, distributed systems, financial networks, medical platforms, autonomous transportation systems.

Введение

В условиях стремительного развития квантовых вычислений традиционные криптографические методы подвергаются риску утраты устойчивости. Квантовые алгоритмы, такие как алгоритм Шора, способны за полиномиальное время взламывать широко используемые схемы асимметричного шифрования, основанные на факторизации или логарифмических задачах. Это ставит под угрозу безопасность не только государственных и корпоративных информационных систем, но и архитектур искусственного интеллекта (ИИ), оперирующих чувствительными данными. Современные информационные системы, функционирующие на базе ИИ, требуют высокоадаптивных механизмов защиты, способных учитывать динамику угроз, а также особенности самообучающихся алгоритмов. Применение статичных схем шифрования в подобных средах ведёт к значительным уязвимостям при переходе на новые вычислительные парадигмы. В связи с этим необходима разработка алгоритмов, обладающих квантовой устойчивостью, способных к адаптивному функционированию в средах с переменной архитектурой и загрузкой. Цель настоящего исследования - разработка концепции адаптивного квантово-устойчивого шифрования, предназначенного для применения в интеллектуальных информационных системах. Предполагается интеграция механизмов постквантовой криптографии с элементами машинного обучения для динамической адаптации параметров шифрования в реальном времени.

Основная часть

Развитие квантовых вычислений коренным образом меняет парадигму обеспечения информационной безопасности. Наиболее уязвимыми оказываются классические криптографические схемы, основанные на факторизации и дискретных логарифмах, чья стойкость теряет актуальность в условиях появления квантовых алгоритмов, таких как Шора и Гровера. Угроза становится особенно значимой для интеллектуальных информационных систем, использующих самонастраивающиеся модели и обрабатывающих критические данные в режиме реального времени. Такие системы нуждаются в шифровании, способном не только обеспечивать высокий уровень стойкости, но и адаптироваться к изменяющимся условиям эксплуатации - включая тип данных, контекст использования, нагрузку на систему и характер угроз. Постквантовая криптография (PQC), развивающаяся в рамках инициативы NIST по стандартизации устойчивых алгоритмов, предоставляет математически обоснованные решения, стойкие к квантовому взлому. Однако большинство схем PQC остаются статичными по своей природе: они предполагают фиксированные параметры, не учитывающие специфику ИИ-сред. Напротив, адаптивное квантово-устойчивое шифрование предполагает внедрение механизмов самонастройки криптографических протоколов в зависимости от контекста. Это может включать динамическое переключение между алгоритмами, масштабирование параметров в ответ на изменение угроз, а также интеграцию методов машинного обучения для прогнозирования атакующих воздействий и оптимизации конфигурации защиты [1].

Ниже представлен фрагмент кода на языке python, реализующий концепцию адаптивного выбора алгоритма PQC в зависимости от типа данных и уровня угрозы, определяемого предварительно обученной моделью. Архитектура построена с расчётом на встраивание в распределённую ИИ-среду с динамическим изменением условий:

```
class AdaptiveEncryptor:
    def __init__(self, threat_model):
        self.threat_model = threat_model  # ML-модель оценки угроз

    def select_scheme(self, data_type, context_features):
        risk_score = self.threat_model.predict(context_features)

        if data_type == "stream" and risk_score < 0.4:
            return self.use_NTRU()
        elif data_type == "archive" or risk_score >= 0.7:
```

```
            return self.use_Kyber()
        else:
            return self.use_SABER()

    def use_NTRU(self):
        print("Используется схема NTRU-HRSS")
        # Загрузка и вызов реализаций шифрования
        return "NTRU"

    def use_Kyber(self):
        print("Используется схема Kyber-1024")
        return "Kyber"

    def use_SABER(self):
        print("Используется схема SABER")
        return "SABER"

# Пример использования
# Предположим, модель возвращает уровень угрозы на основе контекста (0 - низкий, 1 - критический)
mock_threat_model = lambda features: 0.65  # Подставная модель для демонстрации

encryptor = AdaptiveEncryptor(threat_model=mock_threat_model)
chosen_scheme = encryptor.select_scheme(data_type="archive", context_features={"region": "cloud", "load": "high"})
```

Представленный подход позволяет обеспечить не только гибкость криптографической защиты, но и её соответствие текущему уровню угрозы и типу данных, обрабатываемых ИИ-системой. Ключевым преимуществом такой архитектуры является снижение вероятности избыточных вычислительных затрат в ситуациях с пониженной угрозой при сохранении полной стойкости в критических условиях.

Эффективное внедрение адаптивного квантово-устойчивого шифрования в интеллектуальные информационные системы требует четко структурированной архитектуры, обеспечивающей постоянный обмен данными между модулями анализа, шифрования и принятия решений. Архитектура должна учитывать специфику распределённых сред, в которых ИИ-модули и криптографические компоненты могут находиться на разных узлах вычислительной сети, в том числе в облаке или на периферийных устройствах. Ключевыми элементами данной архитектуры выступают: Модуль оценки контекста - осуществляет сбор телеметрии, включая характеристики трафика, нагрузку на систему, тип обрабатываемых данных, и результаты анализа угроз. Модуль предсказания угроз - на основе машинного обучения формирует прогноз уровня угрозы, включая вероятность целенаправленных атак, перебора или попыток внедрения зловредных пакетов. Модуль выбора шифрования - адаптивно выбирает и активирует одну из заранее определённых схем PQC в зависимости от входных параметров, минимизируя затраты на шифрование и одновременно соблюдая необходимый уровень безопасности. Криптоконтейнер - выполняет шифрование и дешифрование в соответствии с выбранной схемой, обеспечивает журналирование операций и защиту ключей. Модуль обратной связи - возвращает в цикл обучения информацию о результатах работы выбранного алгоритма, что позволяет корректировать модели угроз и адаптировать поведение системы в долгосрочной перспективе.

Эта архитектура обеспечивает не только гибкость и адаптивность, но и способность к самообучению и оптимизации на основе накопленных данных. Важным аспектом является способность системы к динамическому реагированию на изменения в угрозах и условиях эксплуатации. Каждый модуль взаимодействует с другими через четко определённые

интерфейсы, что позволяет поддерживать устойчивость системы даже в условиях сбоя или возникновения новых угроз.

Система адаптивного квантово-устойчивого шифрования должна быть интегрирована с существующими механизмами защиты данных, такими как средства обнаружения вторжений (IDS), а также с протоколами защиты в сетях передачи данных, что обеспечивает комплексную защиту на всех уровнях архитектуры [2]. Например, модуль выбора шифрования может использовать результаты работы системы IDS для уточнения выбора шифра в зависимости от текущего уровня угроз. Кроме того, архитектура должна учитывать требования к производительности. Модуль обратной связи играет важную роль в оптимизации работы системы. На основе информации о производительности алгоритмов шифрования и их применимости в разных сценариях, система может адаптировать параметры для улучшения скорости обработки без ущерба для безопасности. Это особенно важно в реальных сценариях использования, таких как беспилотные транспортные средства или автоматизированные медицинские системы, где задержка в обработке данных может привести к критическим последствиям.

Технологии машинного обучения, интегрируемые в систему, могут также использоваться для предсказания появления новых типов атак, что даёт возможность заранее подготовиться к их возможному возникновению. Например, использование алгоритмов, способных идентифицировать аномальные паттерны в трафике и действиях пользователей, помогает минимизировать риски, связанные с неизвестными или ранее не предусмотренными уязвимостями. Таким образом, успешная реализация адаптивного квантово-устойчивого шифрования в интеллектуальных системах требует комплексного подхода к проектированию, который включает не только выбор устойчивых к квантовому взлому алгоритмов, но и обеспечение их гибкости и способности адаптироваться к изменениям угроз и условий эксплуатации.

Оценка эффективности применения адаптивного квантово-устойчивого шифрования в интеллектуальных системах: анализ производительности и устойчивости к угрозам

Эффективность адаптивного квантово-устойчивого шифрования в интеллектуальных информационных системах определяется рядом факторов, среди которых основными являются криптографическая стойкость, производительность системы и её способность адаптироваться к изменениям угроз. Эти параметры играют ключевую роль при выборе конкретных алгоритмов шифрования для различных типов данных и уровней угроз. Важно отметить, что в интеллектуальных системах, использующих ИИ и машинное обучение, требуется быстрое и динамичное шифрование, которое не нарушает процессов принятия решений в реальном времени [3].

Для объективной оценки различных алгоритмов PQC и их применения в реальных условиях, важно провести сравнение производительности, криптостойкости и адаптивности. Таблица 1 содержит сравнительный анализ нескольких популярных постквантовых алгоритмов с учётом их производительности в реальных системах с переменной нагрузкой и угрозами. Рассматриваются такие показатели, как время шифрования, потребление памяти, устойчивость к квантовым атакам и возможность адаптации в условиях изменяющихся данных и угроз.

Таблица 1

Сравнительный анализ постквантовых алгоритмов шифрования по ключевым параметрам

Алгоритм	**Время шифрования (мс)**	**Память (МБ)**	**Квантовая устойчивость**	**Адаптивность**	**Пригодность для реального времени**
Kyber-1024	12.4	3.5	Высокая	Средняя	Частичная
NTRU-HRSS-701	10.1	2.8	Средняя	Высокая	Высокая

SABER	15.9	4.2	Высокая	Средняя	Средняя
BIKE	22.3	5.0	Средняя	Высокая	Частичная

Сравнительный анализ в таблице 1 показывает, что алгоритм NTRU-HRSS-701 обладает наилучшим балансом между производительностью, адаптивностью и устойчивостью к угрозам. Этот алгоритм является оптимальным выбором для динамически изменяющихся ИИ-сред, где важно минимизировать время шифрования и эффективно использовать вычислительные ресурсы. Kyber-1024 и SABER, несмотря на более высокую криптостойкость, показывают более высокое потребление памяти и времени, что ограничивает их использование в системах реального времени с высокой нагрузкой. BIKE имеет высокую устойчивость к угрозам, однако из-за высокой вычислительной нагрузки его применение ограничено в реальных приложениях.

Реализация адаптивного квантово-устойчивого шифрования в распределённых ИИ-системах: вызовы и решения

Интеллектуальные системы, использующие распределённую архитектуру, требуют продвинутых решений для защиты данных, поскольку их компоненты могут находиться на различных узлах вычислительной сети [4]. В таких системах важны не только эффективное шифрование, но и способность адаптироваться к изменяющимся условиям с минимальными задержками. Адаптивное квантово-устойчивое шифрование идеально подходит для таких систем, поскольку оно позволяет динамически менять параметры шифрования в зависимости от типа данных и уровня угроз.

Ключевыми элементами этой системы являются следующие модули:

- **Модуль оценки контекста** - собирает данные о трафике и нагрузке, а также анализирует угрозы.
- **Модуль предсказания угроз** - на основе машинного обучения прогнозирует уровень угроз и идентифицирует потенциальные атаки.
- **Модуль выбора шифрования** - адаптивно выбирает подходящую схему PQC, оптимизируя баланс между безопасностью и производительностью.
- **Криптоконтейнер** - выполняет шифрование и дешифрование в соответствии с выбранной схемой, управляет ключами.
- **Модуль обратной связи** - отправляет данные о результатах работы системы в цикл обучения для корректировки алгоритмов.

Внедрение АКУШ в распределённые ИИ-системы сталкивается с несколькими вызовами, среди которых необходимость обеспечения независимости узлов при сохранении целостности данных и минимизации времени отклика [5]. Модули шифрования и дешифрования должны быть синхронизированы для обеспечения непрерывной работы всей системы (рис. 1). Использование интерфейсов программирования приложений (API) помогает гибко интегрировать и адаптировать алгоритмы шифрования на разных уровнях системы, обеспечивая их быструю настройку в зависимости от текущих угроз.

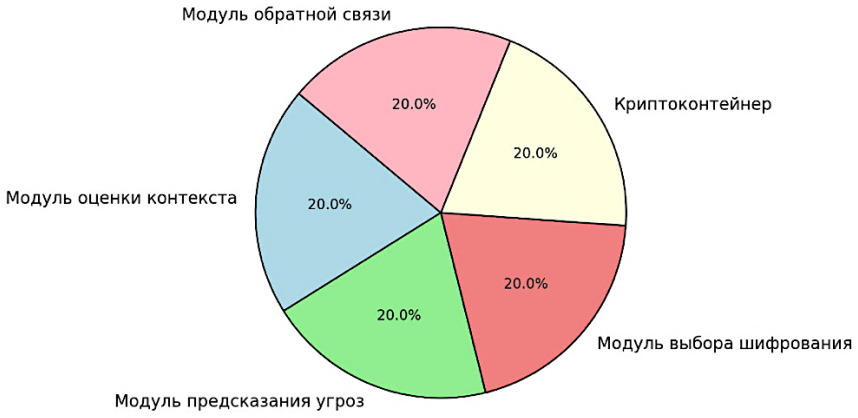

Рисунок 1. Архитектура реализации адаптивного квантово-устойчивого шифрования в распределённой ИИ-системе

Реализация адаптивного квантово-устойчивого шифрования в распределённых ИИ-системах обеспечивает высокую степень безопасности данных при минимизации задержек и вычислительных затрат. Интеграция таких компонентов, как модуль оценки контекста, модуль предсказания угроз, модуль выбора шифрования, криптоконтейнер и модуль обратной связи, позволяет гибко и динамично адаптировать криптографическую защиту в зависимости от текущих угроз и условий работы системы [6]. Это обеспечивает как высокую устойчивость к квантовым атакам, так и эффективное функционирование в реальном времени. Использование интерфейсов программирования приложений позволяет эффективно интегрировать шифрование на разных уровнях распределённой системы, обеспечивая её безопасность и производительность без потери гибкости.

Применение адаптивного квантово-устойчивого шифрования в реальных сценариях: защита данных в автономных системах, медицинских и финансовых приложениях

В условиях роста применения интеллектуальных систем, таких как автономные транспортные средства, медицинские платформы и финансовые сети, безопасность данных становится важнейшим приоритетом. Адаптивное квантово-устойчивое шифрование предоставляет решения для защиты данных, которые должны быть не только защищены от квантовых атак, но и обработаны в реальном времени с минимальной задержкой.

В автономных транспортных системах, где данные обрабатываются с высокой скоростью и в условиях динамически изменяющейся среды, важно быстро реагировать на потенциальные угрозы. Использование АКУШ позволяет динамически изменять параметры шифрования, обеспечивая защиту данных без замедления работы системы [7].

Медицинские платформы, которые обрабатывают персональные данные пациентов, требуют высокой степени защиты от возможных атак, а также соблюдения стандартов конфиденциальности. Здесь также необходимо учитывать низкие задержки в обработке данных, что делает АКУШ идеальным решением для таких приложений.

Финансовые сети сталкиваются с огромным количеством транзакций, которые требуют высокой скорости обработки и одновременно должны быть защищены от различных угроз. Адаптивное шифрование позволяет минимизировать риски, связанные с кражей данных или манипуляциями с транзакциями, при этом не нарушая быстродействие системы.

На рисунке 2 представлена диаграмма, иллюстрирующая, как адаптивное квантово-устойчивое шифрование может быть интегрировано в эти реальные сценарии для защиты данных.

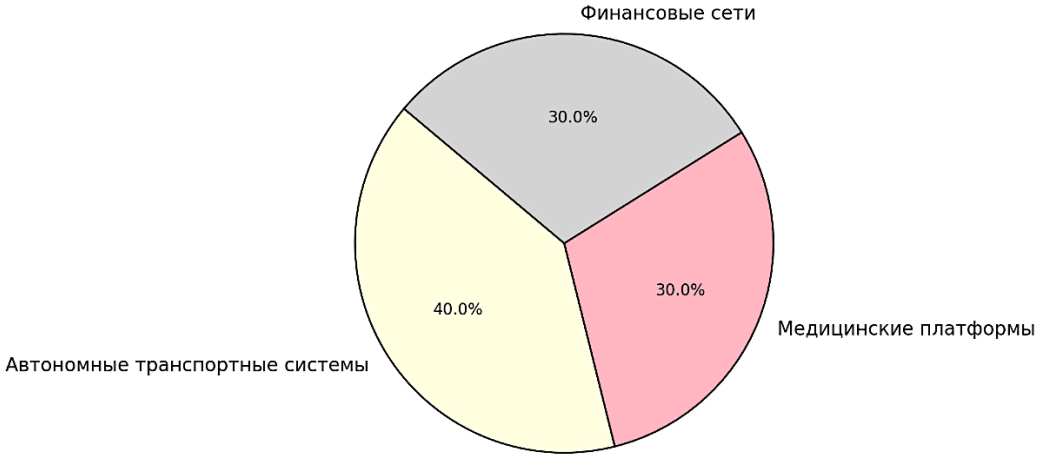

Рисунок 2. Применение адаптивного квантово-устойчивого шифрования в реальных сценариях

Диаграмма показывает распределение применения адаптивного квантово-устойчивого шифрования в ключевых сферах, таких как автономные транспортные системы, медицинские платформы и финансовые сети. Наибольшую долю занимает защита данных в автономных транспортных системах, что подчёркивает важность быстродействующего шифрования в динамически изменяющихся условиях. За этим следуют медицинские платформы и

финансовые сети, для которых также требуется высокая степень защиты данных [8]. Применение АКУШ в этих сферах помогает эффективно балансировать между безопасностью данных и производительностью системы, минимизируя риски при обработке и передаче критичных данных в реальном времени.

Перспективы развития адаптивного квантово-устойчивого шифрования в интеллектуальных системах: будущее и инновации

С развитием квантовых вычислений и усилением угроз, связанных с возможностью взлома традиционных криптографических алгоритмов, адаптивное квантово-устойчивое шифрование будет играть всё более важную роль в обеспечении безопасности интеллектуальных информационных систем. В ближайшие годы ожидается дальнейшее развитие как теоретических основ, так и практических методов реализации постквантовых криптографических решений, которые смогут поддерживать защиту данных в условиях квантовых вычислений.

Одной из перспективных тенденций является развитие квантово-устойчивых алгоритмов с учётом машинного обучения. Эти алгоритмы будут не только защищать от квантовых атак, но и адаптироваться к новым типам угроз, прогнозируемым на основе анализа больших данных. Внедрение машинного обучения в процесс выбора и настройки алгоритмов шифрования откроет новые возможности для повышения эффективности защиты данных в реальном времени.

Другим важным направлением является интеграция адаптивного шифрования в гибридные системы, использующие как традиционные вычисления, так и квантовые технологии. Разработка гибридных архитектур, где элементы ИТ-систем будут использовать как классические, так и квантово-устойчивые алгоритмы шифрования в зависимости от ситуации, обеспечит максимальную безопасность данных без значительных потерь в производительности [9].

Особое внимание следует уделить интероперабельности между различными криптографическими модулями и стандартами. С ростом числа различных приложений и систем, использование унифицированных интерфейсов для адаптивных криптографических решений позволит улучшить взаимодействие между различными компонентами инфраструктуры и обеспечить более гибкую настройку в условиях быстро меняющихся угроз.

Не менее важным направлением является повышение устойчивости алгоритмов к новым типам атак, включая атаки на сам процесс шифрования, а также атаки на инфраструктуру хранения и распространения ключей. Совершенствование методов защиты ключей, в том числе использование многоуровневых систем защиты, станет важной частью будущих технологий в области адаптивного шифрования.

Таким образом, будущее адаптивного квантово-устойчивого шифрования состоит в его интеграции в интеллектуальные системы с учётом новых технологий, таких как квантовые вычисления и машинное обучение, и в разработке решений, которые обеспечат высокий уровень безопасности данных в условиях постоянно изменяющихся угроз и технологических изменений.

Заключение

Адаптивное квантово-устойчивое шифрование представляет собой важный шаг в обеспечении безопасности данных в условиях стремительного развития квантовых вычислений. Его способность динамически адаптироваться к изменяющимся условиям и угрозам, а также эффективно взаимодействовать с интеллектуальными системами, делает его ключевым элементом защиты данных в современных распределённых системах. Применение АКУШ в таких критичных сферах, как автономные транспортные системы, медицинские платформы и финансовые сети, подчеркивает его важность для защиты данных в реальном времени при минимальных задержках.

Постоянное развитие постквантовой криптографии и её интеграция с методами машинного обучения и гибридными вычислительными архитектурами откроют новые возможности для повышения безопасности данных. Важно отметить, что адаптивное

шифрование не только защищает от квантовых атак, но и позволяет оперативно реагировать на изменения угроз, что особенно актуально для динамично развивающихся ИТ-систем.

В будущем ожидается дальнейшее совершенствование алгоритмов и технологий, направленных на обеспечение устойчивости к новым типам атак и улучшение процесса управления ключами. Интеграция АКУШ в интеллектуальные системы станет неотъемлемой частью обеспечения комплексной безопасности данных, предоставляя новые возможности для защиты критической информации в условиях быстро меняющегося технологического ландшафта.

Из этого следует, что адаптивное квантово-устойчивое шифрование станет основой для создания более защищённых, устойчивых и эффективных информационных систем, способных справляться с вызовами будущего.

Список литературы

1. Singh S., Kumar D. Enhancing cyber security using quantum computing and artificial intelligence: A review // algorithms. 2024. Vol. 4. No. 3.
2. Arumugam S.K., Kumari S., Tiwari S., Tyagi A.K. Quantum Computing for Next-Generation Artificial Intelligence-Based Blockchain // Quantum Computing. Auerbach Publications. 2025. P. 251-267.
3. Taherdoost H., Le T.V., Slimani K. Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review // Cryptography. 2025. Vol. 9. No. 1. P. 17.
4. Thirupathi L., Akshaya B., Reddy P.C., Harsha S.S., Reddy E.S. Integration of AI and Quantum Computing in Cyber Security // Integration of AI, Quantum Computing, and Semiconductor Technology. IGI Global. 2025. P. 29-56.
5. Qadri S., Malik J.A., Shah H., Raza M.A., Alsanoosy T., Saleem M. Innovating with Quantum Computing Approaches in Block-Chain for Enhanced Security and Data Privacy in Agricultural IoT Systems // Computational Intelligence in Internet of Agricultural Things. Cham: Springer Nature Switzerland. 2024. P. 339-370.
6. Khatoon A., Riaz R. Quantum Computing Impacts on Smart City Cybersecurity Through Resilient Defense Framework: Quantum Computing Impacts on Resilient Cybersecurity Frameworks for Smart Cities // Ubiquitous Technology Journal. 2025. Vol. 1. No. 1. P. 23-31.
7. Nair M.M., Deshmukh A., Tyagi A.K. Artificial intelligence for cyber security: Current trends and future challenges // Automated Secure Computing for Next-Generation Systems. 2024. P. 83-114.
8. Hasan K.F., Simpson L., Baee M.A.R., Islam C., Rahman Z., Armstrong W., McKague M.A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies // IEEE Access. 2024. Vol. 12. P. 23427-23450.
9. Olutimehin A.T. Advancing cloud security in digital finance: AI-driven threat detection, cryptographic solutions, and privacy challenges // Cryptographic Solutions, and Privacy Challenges. 2025.