

Ю. О. Якович^{1✉}, А. Н. Поликанин¹

Использование технологий квантового шифрования в системах контроля управления доступом

¹ Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
e-mail: yakovich.yury@yandex.ru

Аннотация. Развитие квантовых вычислений создает угрозу для криптографической защиты систем контроля управления доступом (СКУД), основанной на алгоритмах RSA и ECC. Цель статьи – анализ применения квантового распределения ключей (QKD) для защиты каналов связи в СКУД. Рассмотрены протокол BB84 и стандарты постквантовой криптографии NIST. На основе анализа практических проектов (Южная Корея, Великобритания) обоснована многоуровневая архитектура защиты: использование QKD на уровне «контроллер–сервер» и постквантовых алгоритмов на нижних уровнях. Гибридный подход обеспечивает устойчивость к угрозе «сначала собери, потом расшифруй» без полной замены инфраструктуры.

Ключевые слова: квантовая криптография, квантовое распределение ключей, система контроля управления доступом, СКУД, BB84, постквантовая криптография, защита каналов связи

Y. O. Yakovich^{1✉}, A. N. Polikanin¹

Application of Quantum Encryption Technologies in Access Control Systems

¹ Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: yakovich.yury@yandex.ru

Abstract. The development of quantum computing poses a threat to the cryptographic protection of access control systems (ACS) based on RSA and ECC algorithms. This article analyzes the use of quantum key distribution (QKD) to secure communication channels in ACS. The BB84 protocol and NIST post-quantum cryptography standards are considered. Based on an analysis of practical projects (South Korea, UK), a multi-layered security architecture is substantiated: the use of QKD at the controller-server level and post-quantum algorithms at the lower levels. This hybrid approach ensures resilience to the "assemble first, then decrypt" threat without completely replacing the infrastructure.

Keywords: quantum cryptography, quantum key distribution, access control system, BB84, post-quantum cryptography, communication channel protection

Введение

Актуальность исследования обусловлена развитием квантовых вычислений, угрожающих безопасности криптографических протоколов СКУД. Криптографическая защита в СКУД реализуется на уровнях: идентификатор–считыватель (AES-128), считыватель–контроллер (OSDP), контроллер–сервер [1, 2]. Алгоритм Шора способен скомпрометировать RSA и ECC [3]. К середине 2030-х годов квантовые компьютеры нарушат безопасность классического шифрования; правительства

ряда стран устанавливают 2030–2035 гг. как срок миграции на квантово-устойчивые алгоритмы [4]. Дополнительную угрозу представляет стратегия «harvest now, decrypt later». Квантовое распределение ключей (QKD) – метод передачи ключей, безопасность которого основана на законах квантовой физики [5].

Цель статьи – анализ возможностей применения QKD для защиты каналов связи между элементами СКУД и обоснование архитектурного подхода к интеграции. Задачи: анализ уязвимостей криптографии СКУД; обзор протоколов QKD и стандартов NIST; систематизация практических примеров; разработка рекомендаций по интеграции.

Задачи: анализ уязвимостей криптографии СКУД; обзор протоколов QKD и стандартов NIST; систематизация практических примеров; разработка рекомендаций по интеграции.

Методы и материалы

Исследование выполнено методом аналитического обзора научных публикаций и стандартов за 2020–2026 гг. Базу составили статьи из журналов *Advances in Optics and Photonics*, *ACM Computing Surveys*, *Advanced Photonics*, документы NIST, ETSI, ITU-T, документация ID Quantique, Toshiba, Cisco.

Базовым протоколом QKD является BB84 (Беннет, Брассар, 1984 г.) [6]. Его безопасность основана на принципе неопределенности Гейзенберга и теореме о запрете клонирования квантовых состояний. Отправитель (Алиса) кодирует биты в поляризационных состояниях одиночных фотонов, используя два неортогональных базиса: прямолинейный (0° , 90°) и диагональный (45° , 135°). Получатель (Боб) случайно выбирает базис измерения. После передачи стороны сравнивают базисы по открытому каналу и отбрасывают несовпавшие результаты. Оставшиеся биты формируют секретный ключ [7].

Ключевое свойство протокола – обнаружение перехвата: измерение фотона злоумышленником неизбежно вносит ошибки. Уровень ошибок оценивается по QBER; при QBER выше $\sim 11\%$ канал считается скомпрометированным. Для формирования итогового ключа применяются процедуры согласования информации и усиления секретности [5, 7].

Наряду с BB84 развиваются протоколы на основе непрерывных переменных (CV-QKD), кодирующие информацию в амплитуде и фазе когерентных импульсов. Их преимущество – совместимость с существующим оптоволоконным и стандартными детекторами. В 2026 г. исследователи из Университета Падуи продемонстрировали интегральный приемник на стеклянной платформе (3,2 Мбит/с на 9,3 км, QRNG 42,7 Гбит/с) [8].

В августе 2024 г. NIST утвердил стандарты постквантовой криптографии: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), предназначенные для замены RSA и ECC [9]. Организациям рекомендовано начать миграцию на новые алгоритмы.

Результаты и обсуждение

Анализ практических проектов подтверждает зрелость QKD для защиты каналов связи. ID Quantique и SK Broadband развернули квантово-защищенную

сеть в Южной Корее (48 ведомств, 800 км) с непрерывным обновлением ключей [10]. BT, Toshiba и HSBC создали в Лондоне квантово-защищенную банковскую сеть; HSBC первым применил QKD совместно с PQC для защиты торгового терминала при моделировании валютной сделки на 30 млн евро [11].

Cisco разработала интерфейс SKIP для доставки квантовых ключей в IPsec и MACsec, поддерживаемый более чем десятью производителями [12]. Deutsche Telekom и Juniper Networks протестировали квантово-защищенное MACsec-шифрование по ETSI API [10]. В Китае QKD защищает каналы управления энергосетей, в Швейцарии – каналы передачи электоральных данных. Toshiba и NEC реализовали QKD с мультиплексированием по одному оптоволокну [11].

На основании анализа предлагается многоуровневая архитектура защиты каналов СКУД с использованием QKD (рис. 1). Модель включает: ML-KEM на уровне идентификатор-считыватель; симметричное шифрование с квантовыми ключами на уровне считыватель-контроллер; ротацию ключей через QKD на уровне контроллер-сервер.

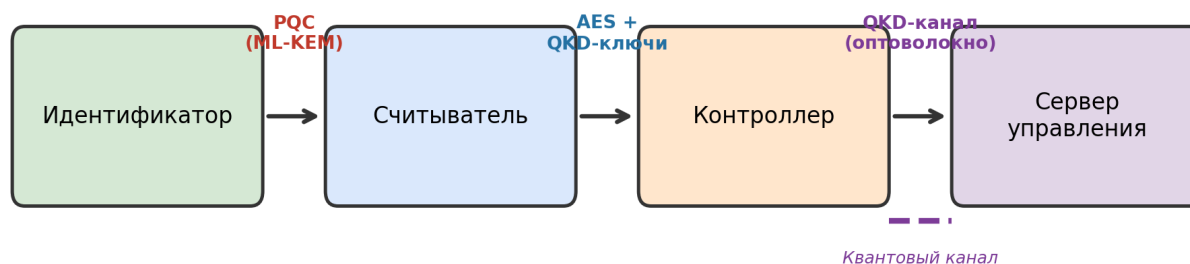


Рис. 1. Многоуровневая архитектура защиты каналов СКУД с использованием QKD

Внедрение QKD сопряжено с ограничениями: дальность – 100–150 км без ретрансляторов [7]; стоимость высока, хотя рынок растет. QKD требует предварительной аутентификации и подвержена атакам на оборудование, однако стандарты ISO/IEC 23837, ETSI ISG QKD, ITU-T серии 380х последовательно устраняют уязвимости [5].

Заключение

В соответствии с целью и задачами проведен анализ применения QKD для защиты каналов СКУД. Установлено, что RSA и ECC уязвимы перед квантовыми атаками, тогда как AES сохраняет устойчивость при надежном распределении ключей.

Обзор протоколов BB84 и CV-QKD показал, что QKD достигли уровня практического применения. Систематизация проектов (сети в Южной Корее, Великобритании; интерфейсы SKIP и ETSI QKD) подтверждает возможность шифрования каналов на существующей инфраструктуре.

Обоснована многоуровневая архитектура защиты СКУД: QKD на уровне контроллер–сервер, постквантовые алгоритмы NIST (FIPS 203–205) на уровне конечных устройств. Гибридный подход обеспечивает устойчивость СКУД к квантовым угрозам без полной замены инфраструктуры. Дальнейшие исследования направлены на разработку прототипа СКУД с модулем QKD.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. – М. : Горячая линия – Телеком, 2020. – 272 с.
2. Стасенко Л. Применение методов шифрования в СКУД // Системы безопасности. – 2022. – URL: https://www.aktivsb.ru/statii/primenenie_metodov_shifrovaniya_v_skud.html (дата обращения: 20.03.2026).
3. Shor P. W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science. – IEEE, 1994. – P. 124–134.
4. World Economic Forum. Quantum-Safe Migration: An Opportunity to Modernize Cryptography. – 2026. – URL: <https://www.weforum.org/stories/2026/01/quantum-safe-migration-cryptography-cybersecurity/> (дата обращения: 20.03.2026).
5. Pirandola S., Andersen U. L., Banchi L. et al. Advances in Quantum Cryptography // Advances in Optics and Photonics. – 2020. – Vol. 12, № 4. – P. 1012–1236.
6. Bennett C. H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Theoretical Computer Science. – 2014. – Vol. 560. – P. 7–11.
7. Mehic M., Niemiec M., Rass S. et al. Quantum Key Distribution: A Networking Perspective // ACM Computing Surveys. – 2020. – Vol. 53, № 5. – P. 1–41.
8. Avesani M. et al. Glass-based integrated quantum coherent receiver for CV-QKD and QRNG // Advanced Photonics. – 2026. – Vol. 8, № 2. – DOI: 10.1117/1.AP.8.2.026003.
9. NIST. Post-Quantum Cryptography FIPS Approved: FIPS 203, 204, 205. – 2024. – URL: <https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved> (дата обращения: 20.03.2026).
10. ID Quantique. Quantum Key Distribution: Integrated Solutions. – 2026. – URL: <https://www.idquantique.com/quantum-safe-security/integrated-solutions/> (дата обращения: 20.03.2026).
11. Building Resilient Security in the Age of Quantum Computing // ISACA Journal. – 2025. – Vol. 6. – URL: <https://www.isaca.org/resources/isaca-journal/issues/2025/volume-6/> (дата обращения: 20.03.2026).
12. Cisco. Quantum Key Distribution and the Path to Post-Quantum Computing. – 2025. – URL: <https://blogs.cisco.com/security/quantum-key-distribution-and-the-path-to-post-quantum-computing> (дата обращения: 20.03.2026).

© Ю. О. Якович, А. Н. Поликанин, 2026