УДК 004.056.5

Лянгузов Никита Алексеевич, студент факультета кибербезопасности, Санкт-Петербургский университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург

АНАЛИЗ СОВРЕМЕННЫХ МЕТОДОВ ЗАЩИТЫ СКУД ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Аннотация

Рассмотрены актуальные угрозы безопасности систем контроля и управления доступом (СКУД) и методы противодействия им. Сформирована матрица угроз и контрмер; проведён сравнительный анализ криптографических, биометрических и программно-аппаратных методов защиты по критериям надёжности, стоимости и сложности внедрения. Обоснован переход от устаревших стандартов RFID к защищённым протоколам. Рассмотрены концепции Zero Trust, облачные СКУД и видеоаналитика на основе ИИ.

Annotation

The paper analyses current threats to physical access control systems (ACS) and countermeasures. A threat-countermeasure matrix is constructed; cryptographic, biometric, and hardware-software protection methods are compared by reliability, cost, and implementation complexity. Migration from legacy RFID standards to secure protocols is substantiated. Zero Trust, cloud ACS, and AI-driven video analytics are discussed.

Ключевые слова: СКУД, несанкционированный доступ, RFID, биометрия, MFA, Zero Trust, OSDP, MIFARE DESFire, информационная безопасность.

Keywords: access control system, ACS, unauthorized access, RFID, biometrics, MFA, Zero Trust, OSDP, MIFARE DESFire, information security.

Системы контроля и управления доступом выступают первым рубежом защиты ресурсов организации. Я исхожу из того, что современные СКУД — это сложные сетевые программно-аппаратные комплексы, интегрированные с корпоративной инфраструктурой, видеоаналитикой и BMS [1]. Согласно отчётам Лаборатории Касперского, число атак на физическую инфраструктуру предприятий ежегодно растёт на 18 %, причём 34 % инцидентов связано с устаревшими стандартами идентификации, а 27 % — с отсутствием шифрования [2]. Требования ФСТЭК России и Федеральный закон № 187-ФЗ ужесточают нормы для объектов КИИ, что подтверждает актуальность моей работы [3].

Цель работы — систематизировать угрозы безопасности СКУД и провести сравнение методов защиты с выдачей практических рекомендаций.

Типовая СКУД включает пять уровней: идентификации (считыватели, биометрические терминалы), управления (контроллеры), исполнения (замки, турникеты), мониторинга (сервер, БД, АРМ оператора) и интеграции (корпоративная сеть) [4]. Каждый уровень имеет характерные уязвимости. Ключевой проблемой остаётся протокол Wiegand – де-факто стандарт отрасли с 40-летней историей, передающий данные идентификатора в открытом виде без аутентификации и шифрования [5]. Злоумышленник, получив физический доступ к кабелю между считывателем и контроллером, может перехватить и воспроизвести коды доступа. Протокол OSDP v2 устраняет эти недостатки за счёт взаимной аутентификации и шифрования AES-128, однако его доля в действующих инсталляциях не превышает 25–30 % [8].

В таблице 1 представлена матрица угроз СКУД с приоритетами устранения для типового корпоративного объекта.

Таблица 1 – Матрица угроз безопасности СКУД и контрмер

Вектор атаки	**Механизм реализации**	**Методы защиты**	**Приоритет**

Клонирование RFID	Считывание карт EM-4100, MIFARE Classic	MIFARE DESFire EV3, динамические ключи	Критический
Replay-атака на Wiegand	Перехват 26-битного кода	Переход на OSDP v2 с AES-шифрованием	Критический
MITM в сети	ARP-spoofing, перехват трафика контроллер–сервер	TLS 1.3, VLAN, 802.1X	Высокий
Атака на сервер СКУД	SQL-инъекция, брутфорс веб-интерфейса	WAF, MFA для администраторов, патч-менеджмент	Высокий
Tailgating	Проход вслед за авторизованным пользователем	Видеоаналитика, антипассбэк, турникеты	Высокий
Социальная инженерия	Фишинг учётных данных операторов	MFA, обучение персонала	Средний
Инсайдерские угрозы	Злоупотребление правами администратора	Принцип наименьших привилегий, UBA, журналы	Средний

Анализ матрицы показывает: критические угрозы (клонирование RFID, replay-атаки) устраняются относительно недорогой заменой стандарта карт и протокола, тогда как угрозы среднего приоритета требуют прежде всего организационных мер.

Карты EM-4100 не имеют криптозащиты и считываются с метра. MIFARE Classic использует взломанный CRYPTO-1: перебор 48-битного ключа занимает менее 200 мс [6]. MIFARE DESFire EV3 исключает клонирование за счёт AES-128/256, диверсификации ключей и Secure Messaging [13].

Двухфакторная аутентификация снижает риск компрометации на 99,9 % [10]. Связка «карта + PIN» оптимальна для большинства объектов, а «карта + биометрия» — для зон повышенной безопасности, но даёт ложный отказ (FRR). Я рекомендую адаптивную аутентификацию с резервным PIN [9]. Компрометация биометрии опасна невозможностью смены идентификатора, поэтому шаблоны следует хранить в HSM [11].

Распознавание лица требует liveness-проверки — мультиспектральные сенсоры дают точность 99,7 % [12].

Сегодня в 62 % взломов инфраструктуры СКУД служат точкой входа [7]. Я применяю изоляцию VLAN, TLS 1.3 и 802.1X [14]. Концепция Zero Trust («никогда не доверяй, всегда проверяй») предполагает непрерывную верификацию и микросегментацию, что критично для КИИ [17].

Сравнение методов по ключевым критериям приведено в таблице 2.

Таблица 2 – Сравнение методов защиты СКУД

Метод защиты	Нейтрализуемые угрозы	Надёжность	Стоимость	Сложность	Область применения
MIFARE DESFire EV3	Клонирование, replay	Высокая	Средняя	Низкая	Корпоративные объекты
Карта + PIN	Клонирование, кража карты	Высокая	Низкая	Низкая	Офисы, здания
Карта + биометрия	Клонирование, кража, tailgating	Очень высокая	Высокая	Средняя	Зоны огр. доступа
Распознавание лица	Tailgating, подмена личности	Высокая	Высокая	Средняя	Высокий поток людей
OSDP v2	Перехват, replay трафика	Высокая	Низкая	Низкая	Все инсталляции
VLAN + TLS 1.3	MITM, горизонт. распростр.	Высокая	Низкая	Средняя	Сетевой уровень
IDS/IPS + SIEM	Аномалии, многоэтапные атаки	Зависит от настройки	Высокая	Высокая	КИИ, крупные объекты
Zero Trust	Все внутренние угрозы	Очень высокая	Высокая	Очень высокая	КИИ, ЦОД, финансы

Облачные СКУД (ACaaS) растут на 14–17 % в год [15], обеспечивая централизованное управление распределёнными объектами. Критические риски – зависимость от канала связи и требования ФЗ-152 к хранению биометрических данных [16]. Мобильные идентификаторы на базе BLE/NFC реализуют MFA нативно через PIN или биометрию смартфона. Интеграция с видеоаналитикой на нейронных сетях позволяет детектировать tailgating с точностью до 97 % и вести поведенческий анализ в реальном времени [12].

Для обычных объектов я считаю минимально необходимыми: замену карт EM-4100/MIFARE Classic на DESFire EV3, переход на OSDP v2, MFA (карта + PIN) в зонах доступа, VLAN-изоляцию и централизованное журналирование. Для КИИ дополнительно требуется биометрия, Zero Trust, интеграция с SIEM/IDS/IPS и аудит по стандартам ФСТЭК России.

Ни один метод не является исчерпывающим; наибольший эффект достигается при их комплексном применении. Перспективное направление – разработка формальных моделей оценки защищённости СКУД и исследование устойчивости биометрических классификаторов к состязательным атакам.

Литература

1. Зайцев А. П., Шелупанов А. А., Мещеряков Р. В. Технические средства и методы защиты информации. [Электронный ресурс]. URL: https://www.techbook.ru/book.php?id_book=549 (дата обращения: 20.05.2026)
2. Лаборатория Касперского. Ландшафт угроз для систем промышленной автоматизации: отчёт за второе полугодие 2023 года. – М.: АО «Лаборатория Касперского», 2024. – 52 с.
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 20.05.2026)
4. Горбачёв О. В., Алексеев В. В. Системы контроля и управления доступом. Современные решения. – М.: Бастион, 2019. – 224 с.
5. Осипов Д. Л., Лосев С. А. Анализ уязвимостей протокола Wiegand в системах контроля доступа // Вопросы кибербезопасности. – 2021. – № 3 (43). – С. 54–62.
6. Жуков И. Ю., Петренко С. А. Методы клонирования RFID-идентификаторов и меры противодействия // Безопасность информационных технологий. – 2022. – Т. 29. – № 1. – С. 38–49.
7. ФСТЭК России. Методика оценки угроз безопасности информации. [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-

dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 20.05.2026)
8. Ассоциация предприятий безопасности. Обзор протоколов передачи данных в СКУД: Wiegand, RS-485, OSDP. – М.: АПБ, 2022. – 38 с.
9. Котенко И. В., Саенко И. Б. Многофакторная аутентификация в корпоративных информационных системах // Труды СПИИ РАН. – 2021. – Т. 20. – № 2. – С. 77–108.
10. Шелупанов А. А., Груздева Л. М., Рудницкий В. Н. Биометрические системы защиты информации. – М.: Горячая линия – Телеком, 2020. – 288 с.
11. Нестеров С. А. Информационная безопасность и защита информации. – СПб.: Лань, 2022. – 324 с.
12. Кузнецов А. А., Матюхин В. Г. Применение нейронных сетей в системах биометрической идентификации // Информационные технологии. – 2023. – № 2. – С. 94–103.
13. Сертификат соответствия ФСТЭК России № 4672. Средства защиты информации. Карты MIFARE DESFire EV3. – М.: ФСТЭК России, 2023.
14. ГОСТ Р 59547-2021. Защита информации. Мониторинг информационной безопасности. Общие положения. [Электронный ресурс]. URL: https://docs.cntd.ru/document/1200180385 (дата обращиния: 20.05.2026)
15. Ковалёв Д. В., Сизов А. Н. Облачные системы контроля доступа: архитектура и угрозы // Вопросы кибербезопасности. – 2023. – № 2 (54). – С. 71–82.
16. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 14.07.2022). [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 20.05.2026)
17. Петренко С. А., Симонов С. В. Управление информационными рисками. – М.: АйТи; ДМК Пресс, 2021. – 384 с.

Literature

1. Zaytsev A. P., Shelupanov A. A., Meshcheryakov R. V. Technical Means and Methods of Information Protection. [Electronic resource]. URL: https://www.techbook.ru/book.php?id_book=549 (accessed: 05/20/2026)

2. Kaspersky Lab. Threat Landscape for Industrial Automation Systems: Report for the Second Half of 2023. – Moscow: Kaspersky Lab JSC, 2024. – 52 p.
3. Federal Law No. 187-FZ of July 26, 2017 "On the Security of the Critical Information Infrastructure of the Russian Federation". [Electronic resource].
URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (acc essed: 05/20/2026)
4. Gorbachev O. V., Alekseev V. V. Access Control and Management Systems. Modern Solutions. – Moscow: Bastion, 2019. – 224 p.
5. Osipov D. L., Losev S. A. Analysis of Wiegand Protocol Vulnerabilities in Access Control Systems // Cybersecurity Issues. – 2021. – No. 3 (43). – P. 54–62.
6. Zhukov I. Yu., Petrenko S. A. Methods of Cloning RFID Identifiers and Countermeasures // Information Technology Security. – 2022. – Vol. 29. – No. 1. – P. 38–49.
7. FSTEC of Russia. Methodology for Assessing Information Security Threats. [Electronic resource]. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (accessed: 05/20/2026)
8. Association of Security Enterprises. Overview of Data Transfer Protocols in ACS: Wiegand, RS-485, OSDP. – Moscow: APB, 2022. – 38 p.
9. Kotenko I. V., Saenko I. B. Multi-factor Authentication in Corporate Information Systems // Proceedings of SPIIRAS. – 2021. – Vol. 20. – No. 2. – P. 77–108.
10. Shelupanov A. A., Gruzdeva L. M., Rudnitsky V. N. Biometric Information Protection Systems. – Moscow: Hotline – Telecom, 2020. – 288 p.
11. Nesterov S. A. Information Security and Information Protection. – St. Petersburg: Lan, 2022. – 324 p.
12. Kuznetsov A. A., Matyukhin V. G. Application of Neural Networks in Biometric Identification Systems // Information Technologies. – 2023. – No. 2. – P. 94–103.
13. FSTEC of Russia Certificate of Conformity No. 4672. Information Security Tools. MIFARE DESFire EV3 Cards. – Moscow: FSTEC of Russia, 2023.

14. GOST R 59547-2021. Information Protection. Information Security Monitoring. General Provisions. [Electronic resource]. URL: https://docs.cntd.ru/document/1200180385 (accessed: 05/20/2026)
15. Kovalev D. V., Sizov A. N. Cloud Access Control Systems: Architecture and Threats // Cybersecurity Issues. – 2023. – No. 2 (54). – P. 71–82.
16. Federal Law No. 152-FZ of July 27, 2006 "On Personal Data" (amended on July 14, 2022). [Electronic resource]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (accessed: 05/20/2026)
17. Petrenko S. A., Simonov S. V. Information Risk Management. – Moscow: IT; DMK Press, 2021. – 384 p.