

Научная статья

УДК 004.421

<https://doi.org/10.31854/1813-324X-2025-11-3-119-128>

EDN:UMCIKU



Использование криптографических алгоритмов для создания временного пропуска за счет технологии генерации QR-кодов

Юлия Юрьевна Калинина✉, jilietka@mail.ru

Юлия Александровна Смирнова, got-22@mail.ru

Астраханский государственный университет им. В.Н. Татищева,
Астрахань, 414056, Российская Федерация

Аннотация

В современных условиях безопасность высших учебных заведений требует комплексного подхода, включающего как физическую защиту, так и кибербезопасность. С ростом числа студентов, преподавателей и посетителей, а также увеличением угроз, таких как терроризм, вандализм и кибератаки, актуальной задачей становится внедрение эффективных систем контроля доступа. Одним из перспективных решений является система мониторинга временных пропусков на основе QR-кодов, обеспечивающая не только ограничение несанкционированного доступа, но и сбор данных о передвижении лиц на территории учебного заведения. **Целью** данного исследования является разработка методики применения QR-кодов в системах контроля доступа высших учебных заведений с использованием современных криптографических алгоритмов, включая симметричное шифрование (AES-256), асимметричную криптографию на эллиптических кривых (ECC).

Сущность предлагаемого решения заключается в автоматизированной системе, включающей: электронные заявки на пропуск; автоматическую генерацию QR-кодов с зашифрованными данными; контроль сроков действия пропусков; мониторинг нарушений и интеграцию с Telegram-ботом для удобства пользователей. Принцип описанной методики **основан** на шифровании метаданных пропуска с последующей генерацией QR-кода, который может быть считан и проверен службой безопасности. Для обеспечения высокой степени защиты применяются алгоритмы AES-256 и ECC.

Научная новизна решения заключается в комбинированном использовании QR-кодов и современных криптографических методов, что обеспечивает высокий уровень безопасности и удобство применения в условиях высшего учебного заведения.

Теоретическая значимость работы состоит в разработке модели системы контроля доступа, адаптированной для образовательных учреждений, с учетом современных угроз и требований нормативных документов (например, Указа Президента РФ № 166 от 30.03.2022).

Практическая значимость подтверждается возможностью непосредственного внедрения системы в учебных заведениях. Решение позволяет не только повысить уровень безопасности, но и оптимизировать административные процессы за счет автоматизации выдачи пропусков и интеграции с мессенджером Telegram.

Ключевые слова: временные пропуска, контроль доступа, QR-код, шифрование AES-256, криптография на основе эллиптических кривых, автоматизация выдачи пропусков, комплексная безопасность, автоматизация выдачи пропусков

Ссылка для цитирования: Калинина Ю.Ю., Смирнова Ю.А. Использование криптографических алгоритмов для создания временного пропуска за счет технологии генерации QR-кодов // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 119–128. DOI:10.31854/1813-324X-2025-11-3-119-128. EDN:UMCIKU

Original article

<https://doi.org/10.31854/1813-324X-2025-11-3-119-128>

EDN:UMCIKU

Using Cryptographic Algorithms to Create a Temporary Pass Using QR Code Generation Technology

 Yulia Yu. Kalinina ✉, jilietka@mail.ru Yulia A. Smirnova, got-22@mail.ru

Tatishchev Astrakhan State University,
Astrakhan, 414056, Russian Federation

Annotation

In modern conditions, the security of higher education institutions requires an integrated approach, including both physical protection and cybersecurity. With the growing number of students, faculty, and visitors, as well as increasing threats such as terrorism, vandalism, and cyberattacks, the implementation of effective access control systems is becoming an urgent task. One of the promising solutions is a system for monitoring temporary passes based on QR codes, which ensures not only the restriction of unauthorized access, but also the collection of data on the movement of persons on the territory of the educational institution. **The purpose** of this study is to develop a methodology for using QR codes in access control systems of higher education institutions using modern cryptographic algorithms, including symmetric encryption (AES-256), asymmetric elliptic curve cryptography (ECC).

The essence of the proposed solution is an automated system that includes: electronic applications for admission; automatic QR code generation; codes with encrypted data; control of the validity period of passes; monitoring violations and integration with the Telegram bot for the convenience of users. The principle of the described technique is **based on** the encryption of the metadata of the pass, followed by the generation of a QR code that can be read and verified by the security service. AES-256 and ECC algorithms are used to ensure a high degree of protection.

The scientific novelty of the solution lies in the combined use of QR codes and modern cryptographic methods, which ensures a high level of security and ease of use in a university setting.

The theoretical significance of the work consists in developing a model of an access control system adapted for educational institutions, taking into account modern threats and requirements of regulatory documents (for example, Decree of the President of the Russian Federation No. 166 dated 30.03.2022).

The practical significance is confirmed by the possibility of direct implementation of the system in educational institutions. The solution allows not only to increase the level of security, but also to optimize administrative processes by automating the issuance of passes and integrating with the Telegram messenger.

Keywords: temporary passes, access control, QR code, AES-256 encryption, elliptic curve cryptography, pass issuance automation, integrated security, pass issuance automation

For citation: Kalinina Yu.Y., Smirnova Yu.A. Using Cryptographic Algorithms to Create a Temporary Pass Using QR Code Generation Technology. *Proceedings of Telecommunication Universities*. 2025;11(3):119–128. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-119-128. EDN:UMCIKU

Введение

Системы безопасности в высших учебных заведениях (вузах) являются одной из ключевых задач и, согласно ГОСТ Р 53704-2009 [1], требуют комплексного подхода, что предполагает объединение разнообразных технических средств и организационных мер для достижения оптимального уровня защиты.

Указанный стандарт регламентирует общие технические требования к системам безопасности, охватывающие видеонаблюдение, контроль доступа, пожарную и охранную сигнализацию, а также методы их испытаний и эксплуатации. В связи с увеличением числа студентов, преподавателей и посетителей, а также с ростом угроз безопасности, таких как

терроризм, вандализм и кибератаки, необходимость в эффективных системах безопасности становится все более актуальной. В условиях современного мира, где угрозы могут возникнуть в любой момент, создание безопасной образовательной среды становится приоритетом для всех учебных заведений.

Одним из важных аспектов обеспечения безопасности является контроль доступа, который можно реализовать через систему мониторинга временных пропусков. Эта система позволяет не только ограничить доступ к определенным зонам, но и отслеживать передвижение людей по территории учебного заведения. Внедрение современных технологий, таких как биометрические системы и электронные карты, значительно повышает уровень безопасности, позволяя быстро реагировать на потенциальные угрозы.

Важно отметить, что в связи с указом Президента РФ от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» вузы имеют возможность развивать отечественные решения в области безопасности, что не только обеспечивает систему защитой, но и способствует развитию местной экономики. Например, ряд университетов уже внедряет системы, разработанные российскими компаниями, что позволяет не только повысить уровень безопасности, но и поддержать отечественного производителя. Кроме того, важным элементом безопасности является обучение студентов и сотрудников правилам поведения в экстренных ситуациях. Проведение регулярных тренингов и семинаров по безопасности, а также информирование о возможных угрозах и способах их предотвращения способствует созданию более безопасной образовательной среды.

Комплексный подход к безопасности в вузах включает в себя не только технические решения, но и образовательные инициативы, направленные на повышение осведомленности и готовности всех участников учебного процесса. Это позволит создать безопасную и комфортную атмосферу для обучения и работы, что, в свою очередь, будет способствовать успешному развитию учебного заведения.

Проблематика безопасности в вузах

Вузы сталкиваются с различными угрозами, которые могут повлиять на безопасность студентов и сотрудников. Физические угрозы безопасности могут принимать различные формы и представляют собой серьезную опасность для студентов, преподавателей и инфраструктуры [2]. К числу таких угроз относятся терроризм, вандализм, физическое

насилие, кражи и грабежи, пожары и чрезвычайные ситуации.

В последние годы участились случаи *террористических актов* в учебных заведениях – как физические атаки, так и угрозы, связанные с взрывчатыми веществами. Важно, чтобы вузы имели четкие планы действий в случае возникновения таких ситуаций, включая эвакуацию и взаимодействие с правоохранительными органами.

Вандализм может проявляться в повреждении имущества, граффити и других формах разрушения. Это не только приводит к финансовым потерям, но и создает неблагоприятную атмосферу в учебном заведении. Необходимо проводить профилактические мероприятия и вовлекать студентов в поддержание порядка.

Конфликты между студентами, случаи буллинга и другие формы *физического насилия* могут негативно сказаться на учебном процессе и психоэмоциональном состоянии учащихся. Вузы должны иметь программы по предотвращению насилия и поддержке пострадавших.

С увеличением числа студентов и посетителей возрастает риск *краж и грабежей* на территории учебного заведения. Установка камер видеонаблюдения и присутствие охраны могут помочь в снижении этого риска.

Пожары, наводнения и другие природные катастрофы могут угрожать безопасности студентов и сотрудников. Крайне важно иметь в вузах планы по эвакуации и проводить регулярные тренировки для подготовки к таким ситуациям.

В контексте обеспечения безопасности в вузах необходимо руководствоваться рядом государственных стандартов, которые играют ключевую роль в создании надежных систем безопасности, способных эффективно реагировать на современные вызовы и угрозы. ГОСТ Р ИСО/МЭК 17799-2005 [3] предоставляет рекомендации по управлению информационной безопасностью, включая политики, процедуры и практики, направленные на защиту информации. ГОСТ 34.003-90 [4] устанавливает требования к автоматизированным системам, включая их разработку, внедрение и эксплуатацию, что способствует созданию надежных и безопасных систем, которые могут быть использованы для управления безопасностью в вузах.

Соблюдение описанных стандартов обеспечивает защиту как физической, так и цифровой инфраструктуры учебных заведений, способствуя созданию безопасной и комфортной атмосферы для работы и обучения, а также способствует повышению уровня осведомленности и готовности всех участников образовательного процесса, что, в свою очередь, будет способствовать эффективному

управлению угрозами и минимизации рисков, обеспечивая защиту данных и инфраструктуры.

Для эффективного управления физическими угрозами безопасности в вузах необходимо внедрение комплексных систем безопасности (КСБ). КСБ – это комплекс технических средств, защищающих жизнь и здоровье персонала и посетителей, предотвращающих несанкционированное проникновение на охраняемую территорию, обеспечивающих сохранность материальных ценностей [5]. В рамках предметной области акцент делается на технические вспомогательные средства, так как они представляют собой ключевой элемент в обеспечении безопасности, минимизируя человеческий фактор и повышая общую эффективность систем. Аспекты КСБ, рассматриваемые в исследовании, представлены на рисунке 1.



Рис. 1. Аспекты комплексной системы безопасности

Fig. 1. Aspects of the Integrated Security System

В современных реалиях безопасности вузов киберугрозы играют не менее важную роль, чем физические [6]. С увеличением зависимости от технологий и цифровых систем вузы сталкиваются с новыми вызовами, связанными с защитой информации, конфиденциальностью данных и обеспечением эффективного пропускного режима.

С ростом числа студентов и преподавателей, а также с распространением онлайн-обучения и удаленных рабочих мест, соответственно увеличивается доступ к различным данным и системам вузов. Атаки на информационные системы могут включать в себя фишинг, установку вредоносного ПО и DDoS-атаки. Киберпреступники нацеливаются на учебные заведения, чтобы получить доступ к личной информации студентов и сотрудников, финансовым данным, а также для осуществления шантажа и вымогательства. Для защиты от таких угроз вузам необходимо внедрять современные системы контроля доступа, которые обеспечивают не только физическую безопасность, но и защищают данные на уровне информационной системы.

Системы мониторинга временных пропусков становятся важным инструментом для предотвращения несанкционированного доступа как в физическую инфраструктуру учебного заведения, так и к его цифровым ресурсам.

Интеграция системы мониторинга временных пропусков

Наиболее эффективным инструментом для повышения безопасности является система генерации [7] и мониторинга временных пропусков. Данные системы позволяют контролировать доступ на территорию вуза и отслеживать передвижение людей, что особенно актуально в условиях увеличения числа студентов и сотрудников, а также растущих угроз безопасности.

Преимущества предлагаемой системы:

1) улучшение контроля доступа: система обеспечивает выдачу временных пропусков только тем лицам, которые имеют на это право, что значительно снижает риск несанкционированного проникновения на территорию вуза; это достигается за счет использования современных технологий идентификации, таких как бесконтактные карты и биометрические системы;

2) сбор данных о передвижении: система может фиксировать время и место входа и выхода пользователей, что позволяет анализировать потоки людей; это особенно полезно для выявления аномалий или подозрительного поведения, т. е. может помочь в предотвращении инцидентов;

3) автоматические уведомления о нарушениях: в случае попытки несанкционированного доступа система может автоматически предупреждать охрану или других ответственных лиц; это позволяет быстро реагировать на потенциальные угрозы и повышает общую безопасность;

4) аналитика и отчеты: система может предоставлять отчеты о перемещениях пользователей, что позволяет администрации вуза анализировать данные и принимать обоснованные решения для улучшения безопасности.

В рамках интеграции системы мониторинга временных пропусков следует выделить несколько ключевых компонентов, являющихся основополагающими для эффективности системы:

– электронные заявки на пропуск (модуль позволяет сократить бумажный документооборот и ускорить процесс оформления пропусков; пользователи могут подавать заявки через специальные электронные формы, что значительно упрощает процесс согласования);

– автоматизация выдачи пропусков (система обеспечивает автоматическую генерацию временных пропусков с необходимой информацией: ФИО, фотография, должность и данные транспортного

средства; это позволяет быстро и эффективно выдавать пропуск без необходимости ручного ввода данных);

- контроль сроков доступа (модуль контроля сроков доступа отслеживает актуальность пропускных документов и уведомляет ответственных лиц о необходимости их продления; если документы не были продлены вовремя, доступ автоматически блокируется, что предотвращает несанкционированный вход);

- управление нарушениями (система ведет реестр нарушителей и нежелательных посетителей, фиксируя случаи нарушения пропускного режима; это позволяет оперативно реагировать на инциденты и блокировать им доступ);

- личные кабинеты пользователей (система предоставляет личные кабинеты для пользователей и сотрудников отдела безопасности, что упрощает процесс заказа и продления пропусков; посетители могут самостоятельно управлять своими заявками, а сотрудники получают возможность проверять информацию без необходимости сбора множества документов);

- генерация пропуска (система автоматически генерирует пропуск посетителю, если его заявка не требует дополнительной проверки сотрудником службы безопасности в случае предоставления определенных прав; пропуском является QR-код, содержащий основную информацию о посетителе и обоснование легитимности нахождения на территории университета).

Данные компоненты образуют комплексную систему, позволяющую не только организовать упрощенный процесс выдачи временных пропусков, но и значительно повысить уровень безопасности в учебном заведении. Наглядное представление архитектуры системы представлено на рисунке 2. Внедрение этих модулей станет важным шагом к обеспечению эффективного контроля доступа и управлению пропускным режимом.

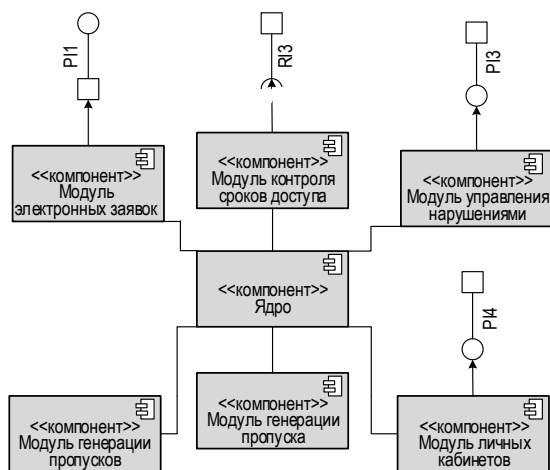


Рис. 2. Диаграмма компонентов UML

Fig. 2. UML Component Diagram

Использование QR-кодов в системе генерации временных пропусков

Современные технологии, такие как биометрические системы распознавания, карты доступа и многофакторная аутентификация, позволяют значительно увеличить уровень безопасности, что не только ограничивает доступ к ресурсам, но и защищает от потенциальных киберугроз, связанных с уязвимостями системы аутентификации и идентификации. Среди новейших технологий QR-коды являются эффективным и универсальным решением для генерации временных пропусков. QR-код (от англ. Quick Response code) – разновидность двумерных штриховых кодов, хранящий информацию в виде матрицы из черных и белых квадратов [8]. В отличие от традиционных штрих-кодов, могут хранить данные как горизонтально, так и вертикально, что позволяет поместить значительно больше информации, которая, как правило, представлена текстом, URL-адресами, контактной информацией и другими данными. QR-коды все чаще используются в качестве временных и разовых пропусков из-за простоты генерации, универсальности и совместимости с большим количеством современных устройств.

Основываясь на стандартах Российской Федерации, ключевым документом, определяющим технические требования к QR-кодам, является ГОСТ Р ИСО/МЭК 18004-2015 [9], который является полным аналогом международного ISO/IEC 18004 [10] и устанавливает единые требования к структуре кода, алгоритмам кодирования данных, методам коррекции ошибок и параметрам визуального представления. Стандарт регламентирует форматы данных, возможные версии кода, уровни коррекции ошибок, требования к размерам и алгоритмы маскирования. При этом ГОСТ не ограничивает сферы применения QR-кодов, что позволяет использовать их в различных областях.

Современные QR-коды можно разделить на несколько основных типов, в зависимости от структуры и максимального объема хранимой информации [11]:

- QR-код Модель 1 и Модель 2 – наиболее распространенный формат, поддерживающий кодирование до 7089 цифровых или 4296 буквенных символов (широко применяется в коммерческих и промышленных решениях);

- Micro QR – компактная версия, предназначенная для кодирования небольшого объема данных (до 35 цифровых символов); используются в условиях ограниченного пространства, например, при производстве и инвентаризации мелкогабаритных изделий, в том числе в машинном оборудовании;

- iQR-код – усовершенствованная версия, разработанная для увеличения плотности данных (до 40 тысяч цифровых символов) и поддержки как

квадратной, так и прямоугольной формы; данная особенность позволяет размещать большой объем информации в ограниченном пространстве);

– SQRC – визуально не отличается от классического формата QR-кода, но имеет функцию ограничения чтения, которая предотвращает доступ неавторизованных лиц к частной информации;

– Frame QR или рамочный код – формат, позволяющий разместить в центре QR-кода изображение или логотип компании.

В системах контроля и управления доступом использование QR-кодов Модели 2 для генерации временного пропуска обеспечивает максимальный баланс между размером изображения, объемом хранимых данных и надежностью считывания. Такой пропуск позволяет закодировать [12] *уникальный идентификатор* (случайно сгенерированный номер пропуска для однозначной идентификации пропуска) и *метаданные* (информацию о посетителе: ФИО, контактный номер, электронную почту, а также период действия пропуска, причину нахождения на охраняемой территории, уровень доступа, согласно разработанной матрице доступа).

Сгенерированный пропуск отображается на смартфоне посетителя и доступен весь период действия. При сканировании считывающим устройством QR-код расшифровывается, и ответственному лицу предоставляется возможность проверки легитимности доступа. Пример сформированного пропуска представлен на рисунке 3.



Рис. 3. Сформированный пропуск в виде QR-кода

Fig. 3. Generated Pass in the Form of a QR Code

Перед созданием QR-кода необходимо подготовить данные, которые будут в него закодированы:

1) зашифрованные данные – метаданные пропуска, зашифрованные с использованием расширенного стандарта шифрования с 256-битным ключом (AES-256);

2) зашифрованный симметричный ключ – ключ AES, зашифрованный с помощью шифрования на основе эллиптических кривых (ЕЕС);

3) дополнительные параметры – например, вектор инициализации (IV), используемый при шифровании AES, или метаданные для идентификации типа данных.

Полученные данные объединяются в единую строку или бинарный формат. Для удобства обработки их можно сериализовать, например, в формате JSON, или объединить в виде шестнадцатеричной строки. Далее, для генерации пропуска, можно использовать язык программирования Python и библиотеку qrcode, предоставляющую простой и гибкий интерфейс создания QR-кода и поддерживающую различные параметры, например размер, уровень коррекции ошибок и цветовое оформление.

QR-коды поддерживают несколько уровней коррекции ошибок, которые определяют, насколько устойчив код к повреждениям или искажениям: *L* (Low) – 7 % повреждений могут быть восстановлены; *M* (Medium) – 15 %; *Q* (Quartile) – 25%; *H* (High) – 30%.

Для систем контроля доступа рекомендуется использовать уровень коррекции ошибок не ниже *M*, чтобы обеспечить надежность считывания даже при частичном повреждении QR-кода.

Генерация QR-кода состоит из следующих шагов.

Шаг 1. Создание объекта QR-кода – инициализируется объект QR-кода с указанием параметров, таких как версия QR-кода, уровень коррекции ошибок и размер.

Шаг 2. Добавление данных – подготовленные зашифрованные данные добавляются в объект QR-кода.

Шаг 3. Генерация изображения – на основе добавленных данных создается изображение QR-кода. Это изображение может быть сохранено в файл или отображено на экране.

Шаг 4. Сохранение QR-кода в виде изображения (например, в формате PNG) для дальнейшего использования.

Шаг 5. Отправка QR-кода пользователю, которому необходимо предоставить доступ на территорию университета, с помощью Telegram-бота системы [13].

Генерация QR-кода является завершающим этапом в создании системы контроля доступа с использованием шифрования AES-256 и ЕЕС. QR-код позволяет удобно и безопасно передавать зашифрованные данные, которые могут быть расшифрованы и проверены на стороне сервера. Такой подход обеспечивает высокий уровень безопасности и надежности, что делает его идеальным решением для современных систем контроля доступа.

Варианты шифрования данных для генерации QR-кодов

Для повышения безопасности временных пропусков на основе QR-кодов важно использовать надежные и современные методы шифрования, такие как AES-256 и ЕЕС. Данные методы гарантируют, что закодированные в пропуска данные будут защищены от несанкционированного доступа, взлома и подделки, что гарантирует не только физическую, но и информационную безопасность при генерации пропусков.

AES-256 – симметричный алгоритм шифрования, широко используемый для защиты конфиденциальных данных [14]. Является одним из самых безопасных алгоритмов шифрования, что особенно важно для генерации пропусков, содержащих конфиденциальную информацию. Данный алгоритм также является предпочтительным для выбора при использовании QR-кода, как пропуска, так как:

- значительно упрощает процесс генерации и считывания пропуска – пара ключей заранее известна обеим сторонам процесса и ключ используется как для шифрования, так и для расшифровки данных;

- позволяет обрабатывать небольшие массивы данных, за счет работы с блоками объемом 128 бит, что важно для ограниченной вместимости QR-кода;

- скорость работы как на аппаратном, так и на программном уровне является достаточно высокой, что повышает производительность во время различных мероприятий или приемной кампании.

Для создания QR-кода с информацией о пропуске посетителя университета необходимо [15]:

- 1) сгенерировать случайный ключ, который будет использован для шифрования и расшифрования данных; длина ключа должна составлять 256 бит (32 байта);

- 2) преобразовать данные, необходимые для шифрования, в строку, а затем добавить отступы к полученной строке с помощью специальной функции для корректировки длины сообщения и корректной работы с блоками данных фиксированного размера (16 байт);

- 3) зашифровать данные с использованием сгенерированного ключа и режима шифрования, например, CBC (аббр. от англ. Cipher Block Chaining) – шифрование для симметричного блока с использованием механизма обратной связи; в процессе также генерируется вектор инициализации (IV) – произвольное число, используемое с ключом шифрования для повышения безопасности;

- 4) закодировать зашифрованные данные и вектор инициализации в формат base64 для удобства хранения, передачи и корректной обработки в текстовом формате;

- 5) создать QR-код на основе закодированного и зашифрованного сообщения с помощью выбранного программного решения.

При необходимости расшифровать данные пользователь сканирует QR-код и получает зашифрованные данные, а также – вектор инициализации (VI). Используя ключ шифрования, сообщение расшифровывается и восстанавливается исходное сообщение.

AES-256 является одним из самых безопасных методов шифрования, однако, если речь идет о высоком уровне безопасности при меньших размерах ключей и более эффективном использовании ресурсов, ЕЕС предпочтительнее [16].

ЕЕС – ассиметричный метод шифрования, основанный на алгебраической структуре эллиптических кривых над конечными полями для создания ключей. Может быть эффективно использован для генерации пропусков, представленных QR-кодом, сочетая безопасность, производительность и размер.

Для создания QR-кода с зашифрованной информацией необходимо [17] выполнить следующие действия:

- 1) выбрать эллиптическую кривую (это может быть стандартная кривая для шифрования), например, именованную кривую SECP256R1 и базовую точку G ;

- 2) сгенерировать случайное число d , выступающее в роли закрытого ключа (ключ, известный только администратору домена, использующийся для расшифровки информации в ассиметричном шифровании); число должно быть меньше порядка кривой n ;

- 3) вычислить открытый ключ Q с использованием базовой точки G по формуле: $Q = d * G$;

- 4) определить данные, необходимые в QR-коде (уникальный идентификатор и метаданные), и преобразовать их в подходящий для шифрования формат (например, в двоичный массив);

- 5) создать случайное число k , используемое в процессе шифрования в роли временного ключа;

- 6) вычислить точки C_1 и C_2 . $C_1 = k * G$ и $C_2 = k * Q + msg$, где msg – преобразованные данные для шифрования;

- 7) сформировать QR-код на основе зашифрованного сообщения; для формирования пропуска используется как C_1 , так и C_2 , для генерации с помощью конкатенации двух точек и последующего использования для расшифровки.

При расшифровке QR-кода сотрудник сканирует полученный пропуск, считывает закодированные как C_1 , так и C_2 , восстанавливает сообщение с помощью закрытого ключа по формулам $P_k = d * C_1$, и $msg = C_2 - P_k$.

Заключение

Безопасность в вузах является одной из ключевых задач, требующих комплексного подхода. С ростом числа студентов, преподавателей и посетителей, а также с увеличением угроз внедрение современных систем безопасности становится неотъемлемой частью обеспечения безопасной образовательной среды. Одним из эффективных решений является система мониторинга временных пропусков, которая позволяет не только контролировать доступ на территорию учебного заведения, но и отслеживать передвижение людей, оперативно реагируя на потенциальные угрозы.

Важным аспектом обеспечения безопасности является также обучение студентов и сотрудников правилам поведения в экстренных ситуациях. Регулярные тренинги, семинары и информирование о возможных угрозах помогают создать культуру безопасности, что является неотъемлемой частью комплексного подхода.

Использование QR-кодов в качестве временных пропусков представляет собой современный и универсальный подход, сочетающий в себе удобство, высокий уровень безопасности и эффективность. QR-коды позволяют хранить зашифрованные данные, такие как идентификатор пользователя, срок действия пропуска и другие метаданные, что обеспечивает защиту от несанкционированного доступа и подделки. Применение методов шифрования, таких как AES-256 и ECC, гарантирует высокий уровень конфиденциальности и целостности данных.

Новизна предлагаемого решения заключается в принципиально новом подходе к организации системы безопасности, основанном на интеграции QR-кодов с многоуровневой схемой верификации. В отличие от систем, использующих RFID-карты или бумажные носители, предлагаемая методика основывается на динамически генерируемых QR-кодах с усиленной защитой на базе алгоритмов криптографии, что обеспечивает не только надежную защиту от подделки, но и возможность оперативной корректировки параметров доступа в режиме реального времени. Параметры кодирования

изменяются в зависимости от уровня важности охраняемого объекта и основываются на матрице доступа [18].

Внедрение системы генерации временных пропусков на основе QR-кодов не только повышает уровень безопасности в вузах, но и упрощает процессы управления доступом. Автоматизация выдачи пропусков, контроль сроков действия, сбор данных и автоматические уведомления о нарушениях делают систему гибкой и адаптивной к различным сценариям использования. Предполагается, что внедрение описываемой методики может повысить безопасность в вузах на 30–40 %. Это связано с тем, что использование QR-кодов и современных методов шифрования позволяет снизить риск несанкционированного доступа и подделки пропусков. Кроме того, автоматизация процессов управления доступом и оперативное реагирование на потенциальные угрозы способствуют повышению эффективности системы безопасности.

С теоретической точки зрения, предлагаемая методика вносит значительный вклад в развитие методологии обеспечения безопасности в образовательных учреждениях и предлагает новую концепцию интеграции динамически генерируемых QR-кодов, что расширяет существующие подходы к управлению доступом и защите данных. Внедрение алгоритмов криптографии, таких как AES-256 и ECC, обеспечивает не только высокий уровень конфиденциальности и целостности данных, но и открывает новые перспективы для исследования в области информационной безопасности.

Таким образом, внедрение системы мониторинга временных пропусков на основе QR-кодов с использованием современных методов шифрования является важным шагом к созданию безопасной и комфортной образовательной среды. Это не только обеспечивает защиту от физических и киберугроз, но и способствует повышению эффективности управления доступом, что в конечном итоге положительно сказывается на репутации и успешном развитии учебного заведения.

Список источников

1. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования. М.: Стандартинформ, 2010.
2. Тимофеева О.А., Зайцев А.Н., Смурыгин А.В. Комплексное обеспечение безопасности образовательного учреждения как технология интегрированного обучения // V Международная научно-практическая конференция «Культура физическая и здоровье современной молодежи» (Воронеж, Российская Федерация, 15 сентября 2022 г.). Воронеж: Воронежский государственный педагогический университет, 2022. С. 216–220. EDN:DTHCAC
3. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. М.: Стандартинформ, 2006.
4. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. М.: Издательство стандартов, 1990.

5. Картамышев А.В., Маренчук Ю.А., Рожков С.Ю., Жук Е.А. Обеспечение комплексной безопасности образовательного учреждения // IX (66-я) ежегодная научно-практическая конференция Северо-Кавказского федерального университета «Актуальные проблемы инженерных наук» (Ставрополь, Российская Федерация, 04–29 апреля 2022 г.). Ставрополь: Северо-Кавказский федеральный университет, 2022. С. 277–281. EDN:QPBQJSJ
6. Загребина Е.И. К вопросу комплексной безопасности образовательных учреждений // Казанский педагогический журнал. 2015. № 1(108). С. 97–103. EDN:RXWADS
7. Калинина Ю.Ю. Разработка информационной системы автоматизации процесса создания временного пропуска на территорию Астраханского государственного университета им. В.Н. Татищева // VII Всероссийская научно-практическая конференция «Проблемы повышения эффективности научной работы в оборонно-промышленном комплексе России» (Знаменск, Российская Федерация, 11–12 апреля 2024 г.). Астрахань: Астраханский государственный университет им. В.Н. Татищева, 2024. С. 91–94. EDN:BQZIRB
8. QR Codes 101: A Beginner's Guide // QR-Code-Generator. URL: <https://ru.qr-code-generator.com/qr-code-marketing/qr-codes-basics> (Accessed 04 June 2025)
9. ГОСТ Р ИСО/МЭК 18004-2015. Информационные технологии. Автоматическая идентификация. Кодирование штриховое. Спецификация символа QR-код. М.: Стандартинформ, 2016.
10. ISO/IEC 18004:2015. Information technology – Automatic identification and data capture techniques – QR Code bar code symbology specification. Geneva: ISO, 2015.
11. Серебрякова С.Г. QR-код – будущее цифрового повествования? // XXIII Международный Балтийский коммуникационный форум «Вестник факультета социальных цифровых технологий» (Санкт-Петербург, Российская Федерация, 03–04 декабря 2021 г.). СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. С. 295–298. EDN:PHWWDE
12. Задорожный А.В. Использование QR-кода в процессе контроля посещаемости занятий // XI Международный молодежный форум «Образование. Наука. Производство» (Белгород, Российская Федерация, 01–20 октября 2019 г.). Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2019. С. 2928–2932. EDN:THNKCB
13. Калинина Ю.Ю., Смирнова Ю.А. Автоматизация процесса контроля доступа в университете с помощью Telegram-бота // V Международная научно-практическая конференция «Современные тенденции развития информационных технологий в научных исследованиях и прикладных областях» (Владикавказ, Российская Федерация, 25–26 апреля 2024 г.). Владикавказ: Северо-Кавказский горно-металлургический институт, 2024. С. 52–55. EDN:GBZBYA
14. Семенов С.Н., Сай С.В. Особенности алгоритма шифрования AES: Rijndael // Региональная научно-практическая конференция «ТОГУ-Старт: фундаментальные и прикладные исследования молодых» (Хабаровск, Российская Федерация, 12–16 апреля 2021 г.). Хабаровск: Тихоокеанский государственный университет, 2021. С. 345–350. EDN:AMLWHM
15. Волокитина Т.С. Программная реализация блочного шифрования с переменными ключами на основе шифра AES 256 // X Международный конкурс научно-исследовательских работ «Фундаментальные и прикладные научные исследования» (Уфа, Российская Федерация, 05 декабря 2022 г.). Уфа: Общество с ограниченной ответственностью "Научно-издательский центр "Вестник науки", 2022. С. 67–78. EDN:TMAWEA
16. Воробьев А.П., Кротова Е.Л., Воробьева Е.Ю. Преимущества криптографии на эллиптических кривых для решения задач аутентификации // Вестник УрФО. Безопасность в информационной сфере. 2024. № 2(52). С. 99–105. DOI:10.14529/secur240210. EDN:GZNHGR
17. Ольшевский В.К. Эллиптические кривые в современной криптографии // XVII Санкт-Петербургская международная конференция «Региональная информатика» (РИ-2020, Санкт-Петербург, Российская Федерация, 28–30 октября 2020 г.). Т. Часть 1. Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2020. С. 351–352. EDN:BJESRU
18. Калинина Ю.Ю., Смирнова Ю.А., Демина Р.Ю. Методика и алгоритм интеллектуальной поддержки принятия управленческих решений в системе генерации временных пропусков на Территорию высших учебных заведений // Вестник Тамбовского государственного технического университета. 2025. Т. 31. № 1. С. 70–80. DOI:10.17277/vestnik.2025.01.pp.070-080. EDN:NPFYUL

References

1. GOST R 53704-2009. *Complex and integrated security systems. General technical requirements*. Moscow: Standartinform 2010. (in Russ.)
2. Timofeeva O.A., Zaitsev A.N., Smurygin A.V. Comprehensive security of an educational institution as a technology of integrated learning. *Proceedings of the Vth International Scientific and Practical Conference on Physical culture and health of modern youth, 15 September, 2022, Voronezh, Russian Federation*. Voronezh: Voronezh State Pedagogical University Publ.; 2022. p.216–220. (in Russ.) EDN:DTHCAC
3. GOST R ISO/IEC 17799-2005. *Information technology. Code of practice for information security management*. Moscow: Standartinform Publ.; 2006. (in Russ.)
4. GOST 34.003-90. *Information technology. Set of standards for automated systems. Automated systems. Terms and definitions*. Moscow: Izdatelstvo standartov Publ.; 1990. (in Russ.)
5. Kartamyshev A.V., Marenchuk Yu.A., Rozhkov S.Y., Zhuk E.A. Ensuring the integrated security of an educational institution. *Proceedings of the IX (66th) Annual Scientific and Practical Conference of the North Caucasus Federal University on Actual Problems of Engineering Sciences, 04–29 April 2022, Stavropol, Russian Federation*. Stavropol: North Caucasus Federal University Publ.; 2022. p.277–281. (in Russ.) EDN:QPBQJSJ

6. Zagrebina E.I. To integrated safety educational organizations. *Kazan Pedagogical Journal*. 2015;1(108):97–103. (in Russ.) EDN:RXWADS
7. Kalinina Yu.Y. Development of an information system for automating the process of creating a temporary pass to the territory of the Astrakhan State University named after V.N. Tatishchev. *Proceedings of the VIIth All-Russian Scientific and Practical Conference on Problems of Increasing the Efficiency of Scientific Work in the Russian Military-Industrial Complex, 11–12 April 2024, Znamensk, Russian Federation*. Astrakhan: Astrakhan State University named after V.N. Tatishchev Publ.; 2024. p.91–94. (in Russ.) EDN:BQZIRB
8. QR-Code-Generator. QR Codes 101: A Beginner's Guide. URL: <https://ru.qr-code-generator.com/qr-code-marketing/qr-codes-basics> [Accessed 04 June 2025]
9. GOST R ISO/IEC 18004-2015. Information technology. Automatic identification. Bar coding. Encyclopedia of QR code symbols. Moscow: Stratinform; 2016. (in Russ.)
10. ISO/IEC 18004:2015. Information technology. Methods of automatic identification and data collection. Specification of QR codes and barcodes. Geneva: ISO; 2015.
11. Serebryakova S.G. Can QR-Code Become the Future of Digital Storytelling? *Proceedings of the XXIIIth International Baltic Communication Forum «Bulletin of the Faculty of Social Digital Technologies», 03–04 December 2021, St. Petersburg, Russian Federation*. St. Petersburg: The Bonch-Bruевич Saint Petersburg State University of Telecommunications Publ.; 2021. p.295–298. (in Russ.) EDN:PHWWDE
12. Zadorozhny A.V. The use of a QR code in the process of monitoring class attendance. *Proceedings of the XIth International Youth Forum "Education. Science. Production", 01–20 October 2019, Belgorod, Russian Federation*. Belgorod: Belgorod State Technological University named after V.G. Shukhov Publ.; 2019. p.2928–2932. (in Russ.) EDN:THNKCB
13. Kalinina Yu.Y., Smirnova Yu.A. Automation of the access control process at the university using a Telegram bot. *Proceedings of the Vth International Scientific and Practical Conference on Current Trends in the Development of Information Technologies in Scientific Research and Applied Fields, 25–26 April 2024, Vladikavkaz, Russian Federation*. Vladikavkaz: North Caucasus Mining and Metallurgical Institute Publ.; 2024. p.52–55. (in Russ.) EDN:GBZBYA
14. Semenov S.N., Sai S.V. Features of the AES: Rijndael encryption algorithm. *Proceedings of the Regional Scientific and Practical Conference «TOGU-Start: Fundamental and Applied Research of Young People», 12–16 April 2021, Khabarovsk, Russian Federation*. Khabarovsk: Pacific State University Publ.; 2021. p.345–350. (in Russ.) EDN:AMLWHM
15. Volokitina T.S. Software implementation of block encryption with variable keys based on the AES 256 cipher. *Proceedings of the Xth International Research Competition on Basic and Applied scientific Research, 05 December 2022, Ufa, Russian Federation*. Ufa: Nauchno-izdatelskii tsentr Vestnik nauki Publ.; 2022. p.67–78. (in Russ.) EDN:TMAWEA
16. Vorobyov A.P., Krotova E.L., Vorobyova E.Y. Advantages of cryptography on elliptic curves for solving authentication problems. *Bulletin of the Ural Federal District. Security in the Information Sphere*. 2024;2(52):99–105. (in Russ.) DOI:10.14529/secur240210. EDN:GZNHGR
17. Olshansky V.K. Elliptic curves in modern cryptography. *Proceedings of the XVIIth St. Petersburg International Conference «Regional Informatics (RI-2020)», 28–30 October 2020, St. Petersburg, Russian Federation, vol.1*. St. Petersburg: St. Petersburg Society of Informatics, Computer Technology, Communication and Control Systems Publ.; 2020. p.351–352. (in Russ.) EDN:BJESRU
18. Kalinina Yu.Y., Smirnova Yu.A., Demina R.Yu. A method and algorithm of intelligent decision-making support system for generation of temporary access passes to the territory of higher educational institutions. *Bulletin of Tambov State Technical University*. 2025;31(1):70–80. (in Russ.) DOI:10.17277/vestnik.2025.01.pp.070-080. EDN:NPFYUL

Статья поступила в редакцию 14.04.2025; одобрена после рецензирования 21.05.2025; принята к публикации 02.06.2025.

The article was submitted 14.04.2025; approved after reviewing 21.05.2025; accepted for publication 02.06.2025.

Информация об авторах:

КАЛИНИНА
Юлия Юрьевна

сотрудник кафедры информационных технологий Астраханского государственного университета им. В.Н. Татищева
 <https://orcid.org/0009-0009-8785-4634>

СМИРНОВА
Юлия Александровна

старший преподаватель кафедры информационных технологий Астраханского государственного университета им. В.Н. Татищева
 <https://orcid.org/0000-0002-3807-5062>

Авторы сообщают об отсутствии конфликтов интересов.

The authors declare no conflicts of interests..