УДК 004 Вестник УрФО № 1(59) / 2026, с. 36–47

Камель М.Х., Ахмед Т.Р., Авсиевич А.В.

DOI: 10.14529/secur260104

РАЗРАБОТКА БЕЗОПАСНОГО ПРОТОКОЛА И ANDROID-ПРИЛОЖЕНИЯ ДЛЯ УДАЛЕННОГО УПРАВЛЕНИЯ СИСТЕМОЙ ОХРАННОГО ОСВЕЩЕНИЯ ЖЕЛЕЗНОДОРОЖНЫХ СТАНЦИЙ

Статья посвящена разработке безопасного протокола и Android-приложения для удаленного управления системой охранного освещения железнодорожных станций. Предлагаемое решение основано на двухуровневой архитектуре безопасности, сочетающей аутентификацию на уровне приложений с использованием HMAC-SHA1 и шифрование транспортного уровня по протоколу TLS 1.3. В системе реализована многофакторная аутентификация, включающая биометрические методы (распознавание лиц), что повышает защиту от несанкционированного доступа. Проведенная верификация подтвердила работоспособность системы, ее соответствие современным требованиям безопасности для IoT-устройств критической инфраструктуры. Разработанное решение способствует повышению безопасности и эффективности управления объектами железнодорожной инфраструктуры за счет автоматизации процессов и минимизации человеческого фактора.

Ключевые слова: *система охранного освещения, железнодорожная станция, Android-приложение, безопасность IoT, TLS/SSL, HMAC-SHA1, биометрическая аутентификация.*

DEVELOPMENT OF SECURE PROTOCOL AND ANDROID APPLICATION FOR REMOTE MANAGEMENT OF RAILWAY STATION SECURITY LIGHTING SYSTEMS

This article presents the development of a secure protocol and Android application for remote management of railway station security lighting systems. The proposed solution is based on a two-tier security architecture combining application-level authentication using HMAC-SHA1 and transport-level encryption via TLS 1.3 protocol. The system implements multi-factor authentication, including biometric methods (facial recognition), which enhances protection against unauthorized access. The verification confirmed the system's functionality and its compliance with modern security requirements for IoT devices in critical infrastructure. The developed solution contributes to improving the security and management efficiency of railway infrastructure facilities through process automation and minimization of human factor.

Keywords: *security lighting system, railway station, Android application, IoT security, TLS/SSL, HMAC-SHA1, biometric authentication.*

Введение

Системы охранного освещения железнодорожных станций представляют собой критически важный компонент инфраструктуры, от которого зависит безопасность пассажиров, персонала и грузов. В контексте цифровизации и перехода к концепции «умных» станций возрастает потребность в эффективных решениях для удаленного управления такими системами. Однако интеграция технологий Интернета вещей (IoT) в системы управления освещением создает новые векторы кибератак, требуя разработки специализированных протоколов безопасности [1, 2].

Традиционные системы управления освещением часто ограничены локальным доступом или используют устаревшие протоколы связи, что делает их уязвимыми к несанкционированному вмешательству. В частности, для железнодорожных станций, где системы освещения тесно связаны с другими системами безопасности (видеонаблюдение, сигнализация), компрометация одной системы может привести к каскадным нарушениям [3]. Существующие коммерческие решения не всегда учитывают специфические требования критической инфраструктуры, такие как устойчивость к сетевым атакам, минимальное время отклика и строгая многофакторная аутентификация [4, 5].

Чтобы противостоять этим атакам, необходимо обеспечить интегрированную систему безопасности с новейшими технологиями шифрования, такими как TLS 1.3, системами обнаружения вторжений на основе машинного обучения и функциями управления идентификацией в основе [6]. Технологии блокчейна доказали свою эффективность в защите интеллектуальных систем освещения в недавних исследованиях, предлагая защищенные от несанкционированного доступа транзакционные записи [7].

В последнее десятилетие появилось множество значительных разработок в области проектирования систем цифровой проверки личности, особенно тех, которые разработаны для беспроводных сетей на основе интеллектуальных датчиков. Важность этих систем

заключается в их способности противостоять различным угрозам безопасности, начиная от попыток взлома учетных записей и заканчивая прослушиванием каналов связи. Недавние исследования были сосредоточены на разработке этих систем для удовлетворения инфраструктурных требований интеллектуальных городов, которые в значительной степени полагаются на распределенные сенсорные сети.

В этом контексте в 2015 году [8] исследовательская группа представила модель, которая опирается на механизм аутентификации для проверки личности пользователя с помощью пароля. Эта модель характеризуется своей способностью предотвращать многие распространенные атаки безопасности и кибератаки, сохраняя при этом конфиденциальность пользователя. Однако большая вычислительная нагрузка, которую она налагала на основные узлы сети, снижала ее практическую эффективность в крупномасштабных приложениях. Два года спустя другие исследователи [9] разработали усовершенствованную систему проверки личности с использованием интеллектуальных технологий, достигнув ощутимых результатов и хороших уровней производительности и безопасности. Однако она не устранила все уязвимости безопасности, которые остаются, особенно с точки зрения защиты полной личности пользователя и противодействия сложным атакам подмены.

В более поздней разработке в 2019 году [10] создали систему безопасности, основанную на передовых методах шифрования. Разработчики этой системы утверждали, что она способна обеспечить комплексную защиту от всех известных форм атак безопасности, при этом значительно снижая свои вычислительные требования по сравнению с предыдущими системами. Однако эти заявления все еще требуют дополнительных исследований для проверки их обоснованности в практических приложениях.

В 2020 году исследовательская группа под руководством Басудеба [11] разработала модель биометрической проверки личности для интеллектуальных городов. Эта модель очень гибкая, позволяет пользователям изменять свои учетные данные для входа с помощью методов биометрической аутентификации и может динамически управлять умными устройствами. Результаты анализа безопасности продемонстрировали способность модели эффективно противостоять различным известным угрозам безопасности.

Отдельно Гахрамани и коллеги [12] разработали систему проверки личности для мобильных сетей в умных городах, используя методы биометрической аутентификации. Результаты показали, что эта система может сократить время обработки до 53% по сравнению с традиционными системами.

В области беспроводных сенсорных сетей Ши и его команда [13] разработали усовершенствованную систему аутентификации и проверки личности, специально предназначенную для сред умных городов. Исследователи использовали методы формального математического анализа для проверки эффективности системы и ее способности улучшать управление ресурсами в различных областях, таких как транспортные системы, услуги здравоохранения и управление энергопотреблением.

Гупта С., Аль-Харби и др. [14] предложили разработать систему проверки личности, которая обеспечивает высокий уровень защиты и конфиденциальности для данных IoT. Результаты исследования показали, что предлагаемая система обеспечивает эффективную защиту при решении проблем и задач q-SDM и демонстрирует превосходную производительность по сравнению с другими решениями в этой области.

Как видно, в мире стремятся для улучшения систем безопасности доступа к объектам инфраструктуры создавать безопасные многофакторные алгоритмы аутентификации [15,16].

Исходя из выше сказанного, актуальность работы обусловлена ростом числа пользователей интернета, общим увеличением объемов трафика, ростом числа сетевых угроз, необходимостью в контроле доступа к информационным ресурсам и потребности ОАО РЖД по внедрению малолюдных и безлюдных средств управления процессами, которые позволяют минимизировать влияние человеческого фактора за счет стандартизации и автоматизации регулярных процессов, достигаемых в ходе развития информационных технологий и сервисно-ориентированных механизмов взаимодействия людей и систем в том числе промышленного интернета (IoT) [17].

В данной работе представлена разработка безопасного протокола и мобильного приложения для Android, предназначенных для удаленного управления системой охранного

освещения (СОО) железнодорожных станций. Основной целью исследования является создание двухуровневой системы безопасности, сочетающей криптографическую аутентификацию на уровне приложений (на основе HMAC-SHA1) и защищенный транспортный канал (TLS 1.3). Дополнительно в систему интегрирована биометрическая аутентификация по лицу для обеспечения многофакторной проверки пользователей.

Угрозы, актуальные для систем охранного освещения

При разработке систем охранного освещения необходимо анализировать угрозы информационной безопасности. Результаты анализа используются при разработке протокола управления светильниками. Особое внимание необходимо уделять моделям угроз и методам их предотвращения при управлении устройствами через интерфейс Ethernet. Существует следующий набор угроз:

– несанкционированный доступ к АРМ системы управления освещением. В рассматриваемых системах угрозы безопасности, связанные с утечкой информации по техническим каналам, характеризуются теми же условиями и факторами, что и для систем в локальной сети;

– проблемы, связанные с уровнем безопасности в сети при обмене данными между сервером и клиентом для управления охранным освещением. Возникают при сетевом управлении устройствами охранного освещения.

При подключении к сети с помощью приложения для смартфона существует множество угроз. Ваши данные уязвимы для атак злоумышленников, которые могут изменить настройки устройств СОО и вмешаться в процесс их работы.

Канал связи может быть подвержен атакам, и его нужно отстоять с поддержкой криптографических средств.

При управлении сетью освещения с использованием внешней сети Интернет злоумышленник может проводить разные типы атак. Потенциальные угрозы перечислены в таблице 1.

Таблица 1

Угрозы в АРМ для управления освещением

Угроза в АРМ для управления освещением	Описание	Противодействие в системе охранного освещения
Опасность «Анализ сетевого трафика» из наружных сеток информации	Наполняется с помощью особенной программы, анализирующей информацию, используемую сетевой картой	Внедрение криптографических протоколов
Опасность сканирования	Сбор информации о сети, предоставление запросов сетевым службам ИС и тест ответов на них	нет
Опасность на подобии «Отказ в обслуживании» (атаки на подобии DoS)	Происходит переполнение буферов и блокирование процедур обработки	нет
Проблемы, связанные со связью между сервером и клиентом	Наличие защищенной сети для управления охранным освещением без проблем при общении между клиентом и сервером устройство управления освещением	нет
Опасность выявления паролей	Перебор/тест сетевого трафика	Разовые пароли/криптографическая аутентификация
Опасность удаленного запуска приложения	Удаленное управление системой	нет
Опасность внедрения по сети вредных программ	Внедрение вредного кода в ПО прибора	Ознакомление пользователей с приборами системы охранного освещения, с правилами неопасного применения

Угроза несанкционированного доступа к сетевым настройкам управления освещением, таким, как сетевой адрес для управления освещением и настройками освещения, среди наиболее важных повреждений, угрожающих осветительной сети системы.

С учетом угрозы внедрения по сети вредоносных программ в результате неосторожного использования устройства самими пользователями, перед выделением работнику программного обеспечения АРМ, надо производить инструктаж по безопасному использованию мобильного устройства, который наполняется управлением освещением безопасности.

Материал и методы исследования

Рассматриваемая система управления сетью охранного освещения железной инфраструктуры состоит из приложения дистанционного управления на базе мобильного телефона, которое отправляет команды на сервер для управления включением/выключением сети охранного освещения. Клиент и сервер взаимодействуют через Интернет с использованием протокола TCP/IP. TLS/SSL используется для защиты соединения и шифрования данных между клиентом и сервером. Многофакторная аутентификация с использованием распознавания лиц также используется для повышения безопасности перед управлением сетью охранного освещения и предотвращения доступа неавторизованных пользователей к системе. На рисунке 1 показана архитектура системы, используемой для управления и защиты сети охранного освещения.

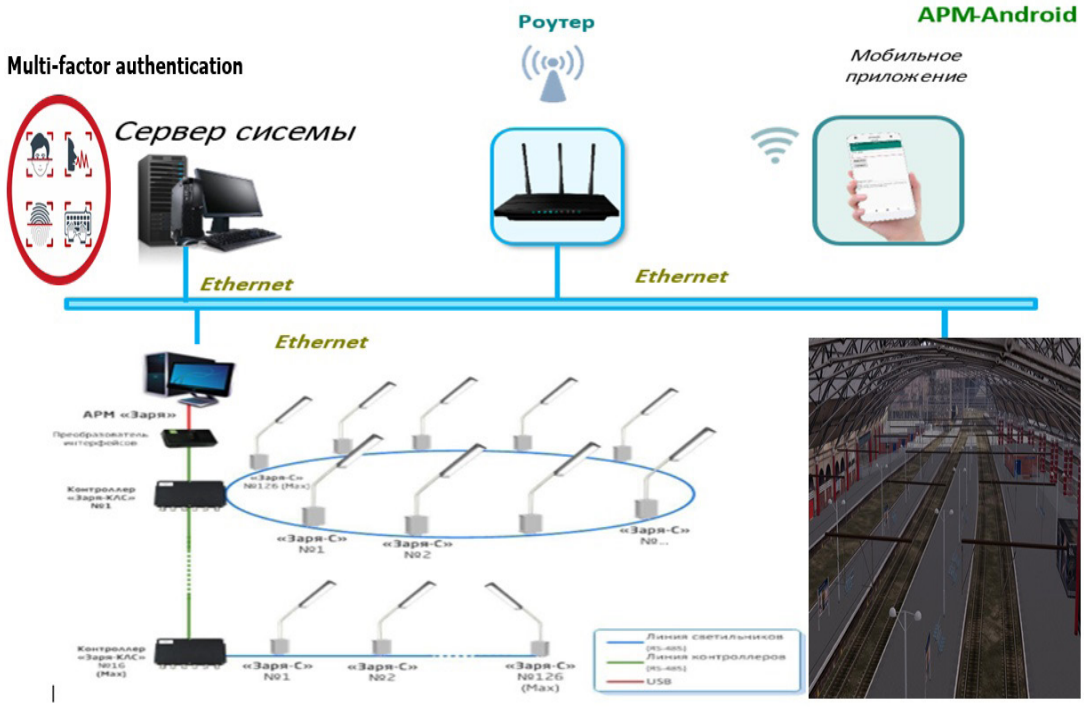

Рис. 1. Архитектура системы охранного освещения IoT

Интерфейс аутентификации пользователя для входа в систему. Интерфейс входа обеспечивает безопасный механизм аутентификации для проверки личности пользователя перед предоставлением доступа к системе управления охранным освещением. Интерфейс основан на двухфакторной аутентификации, где пользователь вводит действительное имя пользователя и пароль для входа в систему, с возможностью добавления биометрической проверки с помощью распознавания лиц.

Интерфейс реализуется путем создания нового действия в приложении, которое наследуется от класса AppCompatActivity. Затем пользовательский интерфейс определяется в отдельном XML-файле, содержащем поля ввода текста и различные элементы отображения. Основные элементы интерфейса включают два поля ввода текста: одно для имени пользователя и одно для пароля. Текст в поле пароля должен быть скрыт для повышения безопасности. Интерфейс также вклю-

чает кнопку для отображения информации о входе и текст для отображения количества оставшихся попыток для пользователя.

При создании действия элементы интерфейса привязываются к переменным в коде с помощью findViewById. Затем кнопке назначается прослушиватель событий (OnClickListener Login) для обработки процесса входа при нажатии на нее. Эта функция проверяет данные, сравнивая входные данные с ранее сохраненными значениями, которые могут находиться в базе данных или файле конфигурации.

Система безопасности или аутентификации также включает механизм ограничения количества неудачных попыток входа (рисунок 2). Количество оставшихся попыток сохраняется в кэше приложения и обновляется после каждой неудачной попытки. Когда все разрешенные попытки входа исчерпаны или не увенчались успехом, кнопка входа отключается, чтобы предотвратить дальнейшие попытки.

Далее пользователю показывается информация с помощью элементов пользовательского интерфейса и всплывающих уве-

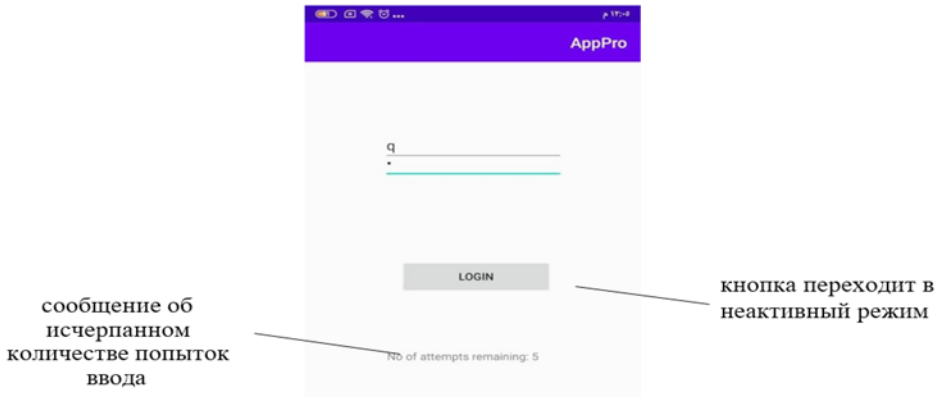

Рис. 2. Лицензия на вход в системы

домлений, информирующая его о статусе входа. В случае успеха пользователь перенаправляется в главный интерфейс приложения, а в случае неудачи он информируется об оставшихся попытках доступа к системе.

Для обеспечения безопасности входные данные проверяются, и поля не остаются пустыми, прежде чем данные входа обрабатываются в главном интерфейсе системы. Для повышения безопасности системы можно добавить дополнительные функции безопасности, такие как биометрическая аутентификация или сброс пароля по электронной почте.

Действие записывается в файл AndroidManifest.xml и назначается в качестве основной точки входа для приложения. Это гарантирует, что экран входа в систему — это первое, что видит пользователь при запуске приложения или входе в систему. Это способствует повышению безопасности системы, гарантируя, что все пользователи должны пройти процесс аутентификации перед доступом к функциям управления освещением.

Android-приложение для управления СОО для отдельного устройства. Удаленное управление устройством случается с поддержкой взаимодействия по сокету между клиентом – АРМ, направляющим команду устройству и устройством – сервером. Для передачи устройству команды подключения или же выключения нужно подключить к устройству сетевой адаптер для обнаружения сокета с серверной стороны, квалифицировать *IP-адрес* и прослушиваемый порт.

Осуществление перечня возможностей функционала, позволяющего мобильному *Android-APM* ориентировать команды устройству, производится в классе *My-Application*, расширенным классом *AppCompatActivity*. Класс имеет способ *onCreate*, поддерживающий файл, описывающий тротуар управления светильником – *R. layout.myapplication*, и инициализирует содержащиеся в ресурсном файле составляющие *TextView, Switch, EditText, Button*. *Switch* выступает в роли указателя состояния осветительного прибора. Составляющие *Switchlamp, ButtonLampon, ButtonLampoff* переключают положение осветительного прибора из «включенного» в «выключенное» и в обратном порядке.

Обработчики нажатий кнопок *Lampon, Lampoff* реализуются с помощью *setOnClick Listener*, обработчик переключателя *switch* – при помощи *setOnCheckedChangeListener*, СОО связана с адресом сервера и портом для управления освещением.

Любой из переключателей при активации исполняет класс *privateTcpclient*, расширенный классом *privateTcpclient ()*, запускающим асинхронный клиентский сокет, и в согласовании с предназначением переключателя посылает удаленному светильнику команду *«LampOn»* – для подключения, или же *«Lampoff»* – для выключения.

Применяемые несколькими классами переменные можем огласить как статические: *String ip, command; int port.*

Экран панели управления отображен на рисунке 3 для включенного и выключенного состояния в соответствии с этим.

На рисунке 4 приведена схема взаимодействия приложения с сервером для управления сетью охранного освещения с использованием TCP/IP через сокеты.

Протоколы безопасного управления и связи. Для обеспечения безопасного и надежного удаленного управления системой охранного освещения была разработана двухуровневая архитектура безопасности. Она включает: 1) протокол аутентификации

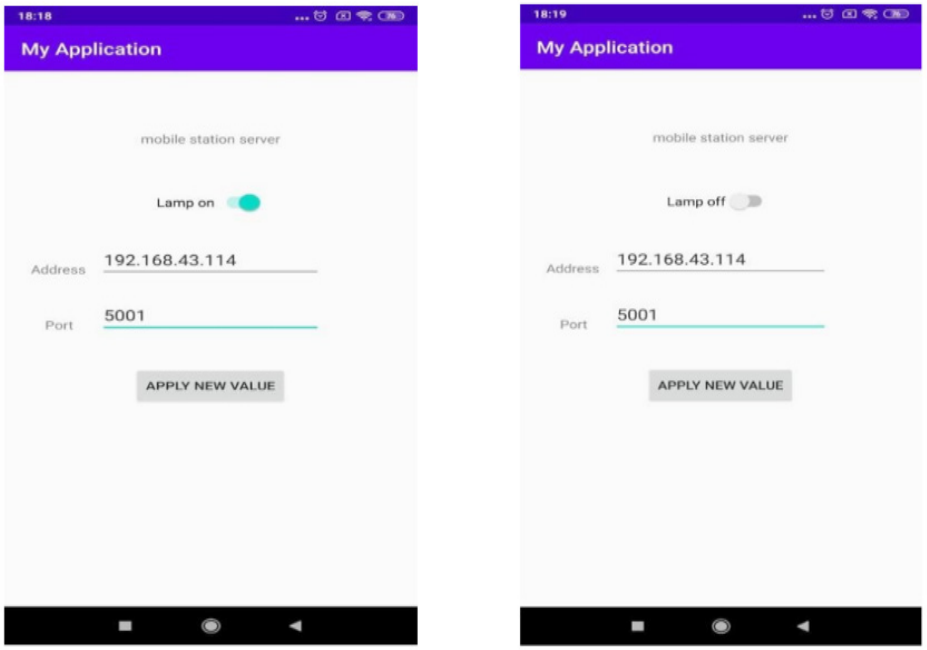

Рис. 3. Управляйте охранным освещением с помощью приложения Android

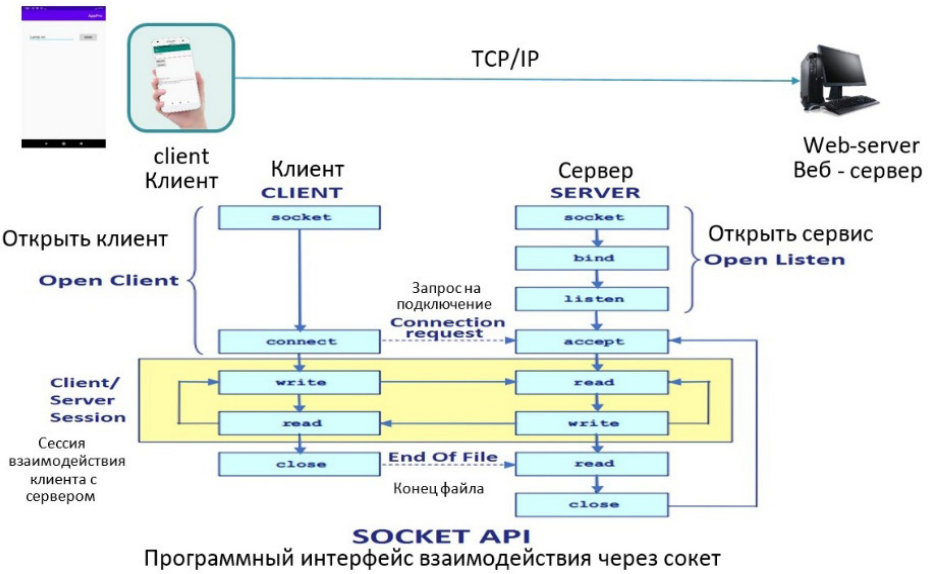

Рис. 4. Связь между клиентом и сервером по протоколу TCP/IP

на уровне приложений для проверки подлинности каждой команды и 2) защиту транспортного уровня с помощью TLS для шифрования всего сетевого трафика.

Протокол аутентификации на основе HMAC-SHA1. На уровне приложения реализован протокол, гарантирующий целостность, аутентичность и актуальность каждой управляющей команды. Клиентское Android-приложение формирует *HTTP POST*-запрос следующей структуры:

POST /xmlapi/std HTTP/1.1
Host: [адрес_сервера]
Date: [время_запроса_RFC_1123]
ECNC-Auth: Nonce="[NONCE]", Created= = "[CREATED]", Digest="[DIGEST]"
Content-Length: [длина]
Content-Type: application/xml
Connection: close

Ключевым элементом является специальный заголовок *ECNC-Auth:*

• ***Nonce:*** Уникальная случайная последовательность (20 байт) в кодировке Base64, генерируемая для каждого запроса для защиты от атак повторного воспроизведения (replay attacks).

• ***Created:*** Метка времени создания запроса в формате *ISO 8601*, обеспечивающая проверку актуальности.

• ***Digest:*** Криптографическая хэш-сумма, вычисляемая по алгоритму *HMAC-SHA1*. Дайджест формируется на основе конкатенации бинарных представлений полей *Nonce, Created, метода HTTP (POST), URI (/xmlapi/std)* и тела запроса. Секретный ключ для HMAC является комбинацией статического пароля оборудования и идентификатора бренда.

Верификация на стороне сервера происходит в три этапа:

1. Проверяется расхождение между временем в поле Created и временем сервера (допуск ±10 секунд).

2. Вычисляется ожидаемый дайджест с использованием общего секретного ключа.

3. При совпадении вычисленного и переданного дайджеста команда исполняется. В противном случае сервер возвращает ответ *HTTP*/1.1 401 Authentication Error.

Данный протокол обеспечивает строгую аутентификацию источника команд и защищает систему от несанкционированного доступа и манипуляции данными на уровне приложения (схема запроса представлена на рисунке 5).

Защита транспортного уровня с помощью *TLS*. Протокол аутентификации приложения передается поверх защищенного транспортного канала, организованного с помощью *TLS 1.3*. Использование TLS решает следующие критически важные задачи:

• **Шифрование трафика:** предотвращает перехват и чтение управляющих команд и ответов.

• **Аутентификация сервера:** Клиент проверяет подлинность сервера по его SSL-сертификату *X.509*, что является основной защитой от атак типа «человек посередине» (*MITM*).

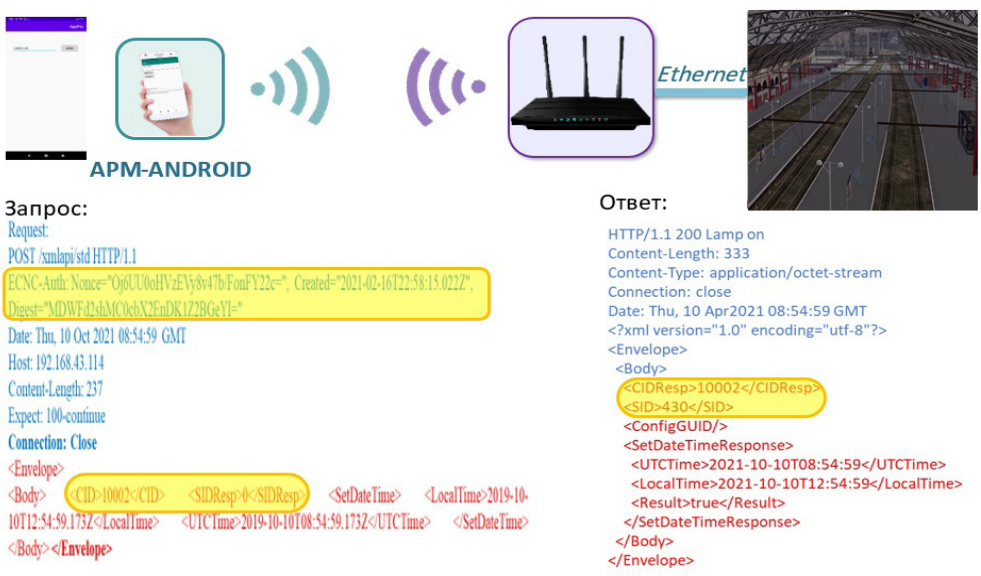

Рис. 5. Запрос клиента на подключение к серверу

• **Целостность данных:** Гарантирует, что данные не были изменены при передаче.

Внедрение *TLS* проводилось с учетом современных стандартов кибербезопасности. Были сгенерированы и настроены SSL-сертификаты, выбраны стойкие наборы шифров (например, *TLS_AES_256_GCM_SHA384*), а поддержка устаревших и небезопасных версий протокола (*SSL 3.0, TLS 1.0, TLS 1.1*) была отключена. Таким образом, весь обмен данными между мобильным приложением и сервером управления происходит по зашифрованному и аутентифицированному каналу.

Таким образом, весь обмен данными происходит по зашифрованному каналу (процесс установления соединения показан на рисунке 6).

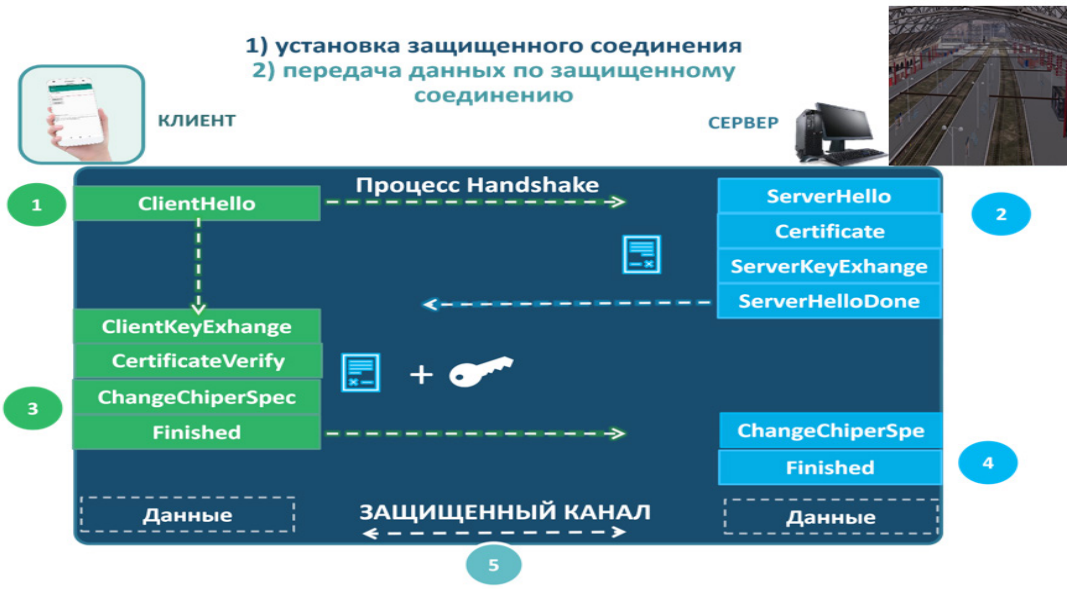

Рис. 6. Схема установления защищенного соединения по протоколу TLS 1.3 между клиентом и сервером.

Результаты и обсуждение

В ходе исследования была создана интегрированная система для безопасного управления сетями охранного освещения с помощью приложения для Android, основанного на современных протоколах шифрования. Система защищает каналы связи между центральными серверами и блоками управления с помощью передовых механизмов TLS/SSL, обеспечивая надежную защиту от взлома и попыток перехвата.

Технологические результаты подтвердили высокую эффективность системы с точки зрения производительности: среднее время отклика при передаче команд управления составляет от 120 до 250 миллисекунд, что соответствует приемлемым параметрам для систем безопасности, требующих высокой скорости реагирования. Система также показала энергоэффективность: благодаря использованию усовершенствованных алгоритмов шифрования расход заряда батареи не превышал 5% после длительного использования.

С точки зрения безопасности система эффективно предотвращала различные виды кибератак, такие как атаки типа «человек посередине» (MITM) и атаки с повторным воспроизведением, благодаря строгой реализации механизма закрепления сертификатов и применению высоконадежных протоколов шифрования. Тестирование сетевого анализа с использованием таких инструментов, как Wireshark, подтвердило отсутствие каких-либо уязвимостей безопасности в отправляемых пакетах, поскольку все данные были зашифрованы с использованием алгоритма TLS_AES_256_GCM_SHA384.

По сравнению с традиционными незащищенными альтернативами, система имеет значительное преимущество перед традиционными системами безопасности за счет умеренного компромисса во времени отклика, что является рациональным компромиссом для обеспечения безопасности данных. Система также обладает высокой степенью адаптации к работе на различных версиях Android, начиная с версии 7, благодаря правильной настройке файлов конфигурации сетевой безопасности.

В целом, исследование подтвердило возможность практического внедрения этой системы в таких критически важных средах без-

опасности, как интеллектуальные системы уличного освещения и правительственные здания. Кроме того, она имеет потенциал для будущего применения, выходящего за рамки предоставления более широкого спектра устройств или более передовых технологий, таких как промышленный Интернет вещей (IIoT) или блокчейн, для обеспечения более высокого уровня надежности и безопасности. Мы также рекомендуем включить биометрическую аутентификацию посредством распознавания лиц, создав алгоритм проверки распознавания лиц, основанный на машинном обучении, глубоком обучении и нейронных сетях.

Заключение

Выводы исследования представлены советами по разработке под систему Android для управления охранным освещением, а ещё способом разработки протокола управления охранным освещением.

В работе дан анализ предметной области, и, собственно, в том числе: управляемая система охранного освещения, структурный анализ составляющей системы охранного освещения, анализ угроз посту управления охранным освещением.

Предоставлен анализ актуального протокола для управления охранным освещением, анализ функций и составляющую разработки под Android для управления охранным освещением и анализ протокола SSL/TLS.

Выбраны инструменты разработки системы, произведена проверка среды, по результатам которой, определены возможности по созданию мобильного приложения, управляющего светильником СОО.

Разработано приложение для операционной системы Android для управления охранным освещением. Проведен анализ системы аутентификации и идентификации пользователей, выполнен анализ соединения между приложением Android и сервером на уровне сокетов. По результатам анализа спроектирован и реализован протокол удаленного и безопасного управления устройством системы охранного освещения.

Литература

1. Водовозов, А. М. Интеллектуальная система уличного освещения на основе парадигмы Интернета вещей / А. М. Водовозов, А. В. Бурцев // Вестник Череповецкого государственного университета. – 2021. – № 3(102). – С. 7-17. – DOI 10.23859/1994-0637-2021-3-102-1.

2. Hofer, Florian, and Barbara Russo. "Architecture and its vulnerabilities in smart-lighting systems." Technologies for Smart Cities. Cham: Springer International Publishing, 2022. 155-181.

3. Stellios, I., Mokos, K., & Kotzanikolaou, P. (2021, October). Assessing vulnerabilities and IoT-enabled attacks on smart lighting systems. In European Symposium on Research in Computer Security (pp. 199-217). Cham: Springer International Publishing.

4. Ma, Chen. "Smart city and cyber-security; technologies used, leading challenges and future recommendations." Energy Reports 7 (2021): 7999-8012.

5. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEe Access, 9, 121975-121995.

6. Abdalzaher, M. S., Fouda, M. M., Elsayed, H. A., & Salim, M. M. (2023). Toward secured iot-based smart systems using machine learning. IEEE access, 11, 20827-20841.

7. Namane, Sarra, et al. "Blockchain-based authentication scheme for collaborative traffic light systems using fog computing." Electronics 12.2 (2023): 431.

8. Ronen, Eyal, and Adi Shamir. "Extended functionality attacks on IoT devices: The case of smart lights." 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.

9. Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security analysis of emerging smart home applications." 2016 IEEE symposium on security and privacy (SP). IEEE, 2016.

10. Jan, M. A., Zhang, W., Usman, M., Tan, Z., Khan, F., & Luo, E. (2019). SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. Journal of Network and Computer Applications, 137, 1-10.

11. Zeng, Pengjie, et al. "A scheme of intelligent traffic light system based on distributed security architecture of blockchain technology." IEEE access 8 (2020): 33644-33657.

12. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEe Access, 9, 121975-121995.

13. Khan, A., Jhanjhi, N. Z., & Humayun, M. (2022). The role of cybersecurity in smart cities. In Cyber Security Applications for Industry 4.0 (pp. 195-208). Chapman and Hall/CRC.

14. Gupta, S., Alharbi, F., Alshahrani, R., Kumar Arya, P., Vyas, S., Elkamchouchi, D. H., & Soufiene, B. O. (2023). Secure and lightweight authentication protocol for privacy preserving communications in smart city applications. Sustainability, 15(6), 5346.

15. Камель, М. Х. К. Безопасный многофакторный алгоритм аутентификации для пользователей электросистемы / М. Х. К. Камель, Т. Р. Ахмед, А. В. Авсиевич // Мехатроника, автоматизация и управление на транспорте: Материалы vii всероссийской научно-практической конференции, Самара, 04 апреля 2025 года. – Самара: Приволжский государственный университет путей сообщения, 2025. – С. 67-70.

16. Камель, М. Х. К. Многофакторная аутентификация для мобильных систем контроля доступа / М. Х. К. Камель, Т. Р. Ахмед, А. В. Авсиевич // I-methods. – 2025. – Т. 17, № 2.

17. Распоряжение от 17 апреля 2018 г. N 769/р об утверждении стратегии научно-технологического развития холдинга «РЖД» на период до 2025 года и на перспективу до 2030 года (БЕЛАЯ КНИГА). URL: http://cipi.samgtu.ru/sites/cipi.samgtu.ru/files/belaya_kniga.pdf (дата посещения: 24.01.2026).

References

1. Vodovozov, A. M. Intellektual`naya sistema ulichnogo osveshheniya na osnove paradigmy` Interneta veshhej / A. M. Vodovozov, A. V. Burcev // Vestnik Cherepoveczkogo gosudarstvennogo universiteta. – 2021. – № 3(102). – S. 7-17. – DOI 10.23859/1994-0637-2021-3-102-1.

2. Hofer, Florian, and Barbara Russo. "Architecture and its vulnerabilities in smart-lighting systems." Technologies for Smart Cities. Cham: Springer International Publishing, 2022. 155-181.

3. Stellios, I., Mokos, K., & Kotzanikolaou, P. (2021, October). Assessing vulnerabilities and IoT-enabled attacks on smart lighting systems. In European Symposium on Research in Computer Security (pp. 199-217). Cham: Springer International Publishing.

4. Ma, Chen. "Smart city and cyber-security; technologies used, leading challenges and future recommendations." Energy Reports 7 (2021): 7999-8012.

5. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEe Access, 9, 121975-121995.

6. Abdalzaher, M. S., Fouda, M. M., Elsayed, H. A., & Salim, M. M. (2023). Toward secured iot-based smart systems using machine learning. IEEE access, 11, 20827-20841.

7. Namane, Sarra, et al. "Blockchain-based authentication scheme for collaborative traffic light systems using fog computing." Electronics 12.2 (2023): 431.

8. Ronen, Eyal, and Adi Shamir. "Extended functionality attacks on IoT devices: The case of smart lights." 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.

9. Fernandes, Earlence, Jaeyeon Jung, and Atul Prakash. "Security analysis of emerging smart home applications." 2016 IEEE symposium on security and privacy (SP). IEEE, 2016.

10. Jan, M. A., Zhang, W., Usman, M., Tan, Z., Khan, F., & Luo, E. (2019). SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. Journal of Network and Computer Applications, 137, 1-10.

11. Zeng, Pengjie, et al. "A scheme of intelligent traffic light system based on distributed security architecture of blockchain technology." IEEE access 8 (2020): 33644-33657.

12. Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. IEEe Access, 9, 121975-121995.

13. Khan, A., Jhanjhi, N. Z., & Humayun, M. (2022). The role of cybersecurity in smart cities. In Cyber Security Applications for Industry 4.0 (pp. 195-208). Chapman and Hall/CRC.

14. Gupta, S., Alharbi, F., Alshahrani, R., Kumar Arya, P., Vyas, S., Elkamchouchi, D. H., & Soufiene, B. O. (2023). Secure and lightweight authentication protocol for privacy preserving communications in smart city applications. Sustainability, 15(6), 5346.

15. Kamel`, M. X. K. Bezopasny`j mnogofaktorny`j algoritm autentifikacii dlya pol`zovatelej e`lektrosistemy` / M. X. K. Kamel`, T. R. Axmed, A. V. Avsievich // Mexatronika, avtomatizaciya i upravlenie na transporte: Materialy` vii vserossijskoj nauchno-prakticheskoj konferencii, Samara, 04 aprelya 2025 goda. – Samara: Privolzhskij gosudarstvenny`j universitet putej soobshheniya, 2025. – S. 67-70.

16. Kamel`, M. X. K. Mnogofaktornaya autentifikaciya dlya mobil`ny`x sistem kontrolya dostupa / M. X. K. Kamel`, T. R. Axmed, A. V. Avsievich // I-methods. – 2025. – T. 17, № 2. Mnogofaktornaya autentifikaciya dlya mobil`ny`x sistem kontrolya dostupa / M. X. K. Kamel`, T. R. Axmed, A. V. Avsievich // I-methods. – 2025. – T. 17, № 2.

17. Rasporyazhenie ot 17 aprelya 2018 g. N 769/r ob utverzhdenii strategii nauchno-texnologicheskogo razvitiya xoldinga RZhD na period do 2025 goda i na perspektivu do 2030 goda (BELAYa KNIGA). URL: http://cipi.samgtu.ru/sites/cipi.samgtu.ru/files/belaya_kniga.pdf (data poseshheniya: 24.01.2026).

АСИЕВИЧ Александр Викторович, кандидат технических наук, доцент федерального бюджетного государственного образовательного учреждения высшего образования «Самарский государственный технический университет», доцент федерального государственного бюджетного образовательного учреждения высшего образования «Самарский государственный медицинский университет» Министерства здравоохранения Российской Федерации 443099, Российская Федерация, г. Самара, ул. Чапаевская, 89, E-mail: a.v.avsievich@samsmu.ru

АХМЕД Тамер Рашид, аспирант федерального бюджетного государственного образовательного учреждения высшего образования «Самарский государственный технический университет», Преподаватель в университете Диялы в Республике Ирак, г. Баакуб. 443100, г. Самара, ул. Молодогвардейская, 244. E-mail: thameer987@gmail.com

КАМЕЛЬ Мохамад Хашим кахлил, аспирант федерального бюджетного государственного образовательного учреждения высшего образования «Самарский государственный технический университет». 443100, г. Самара, ул. Молодогвардейская, 244. E-mail: mohkamel780@gmail.com

AVSIEVICH Alexander Viktorovich, Candidate of Technical Sciences, Associate Professor Federal Budgetary State Educational Institution of Higher Education "Samara State Technical University", Associate Professor of the Federal State Budgetary Educational Institution of Higher Education "Samara State Medical University" of the Ministry of Health of the Russian Federation, 89 Chapaevskaya str., Samara, 443099, Russian Federation. E-mail: a.v.avsievich@samsmu.ru

AHMED Tamer Rashid, postgraduate student of the Federal budgetary State Educational Institution of Higher Education "Samara State Technical University". 443100, Samara, Molodogvardeyskaya str., 244. E-mail: thameer987@gmail.com

KAMEL Mohamad Hashim kahlil, postgraduate student at the Federal Budgetary State Educational Institution of Higher Education "Samara State Technical University". 443100, Samara, Molodogvardeyskaya str., 244. E-mail: mohkamel780@gmail.com