Информационные процессы, Том 25, № 2, 2025, стр. 142–150.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Программно-аппаратный комплекс защищенной передачи данных с применением технологий квантового распределения ключей[1]

П. Ю. Вацков[*], Ю. К. Кожемятько[**], О. В. Колесников[**], Е. М. Маврин[*], В. Г. Потапов[***], П. В. Че[*]

[*] *Сколковский институт науки и технологий, Москва*
[**] *Московский технический университет связи и информатики, Москва, Россия*
[***] *Институт проблем передачи информации им. А.А. Харкевича Российской академии наук, Москва*
Поступила в редколлегию 7.07.2025 г. Принята 25.07.2025 г.

Аннотация—В статье представлены результаты разработки экспериментального образца программно-аппаратного комплекса защищенной передачи данных в мобильных сетях стандартов 4G/5G с применением технологий квантового распределения ключей. Показаны структура, изложены основные принципы работы, представлены сведения как об аппаратной, так и о программной части комплекса. Разработанный образец представляет законченное изделие, позволяющее осуществлять защищённый обмен текстовыми, аудио- и видео сообщениями. Герметичный кейс, в котором размещено изделие, позволяет использовать его как в помещении, так и на открытой площадке.

КЛЮЧЕВЫЕ СЛОВА: квантовое распределение ключей (КРК), мобильные сети 4G/5G, квантовая криптография, защищённые каналы связи.

DOI: 10.53921/18195822_2025_25_2_142

1. ВВЕДЕНИЕ

Объем данных, создаваемых и потребляемых человечеством, стремительно увеличивается. По прогнозам экспертов, к 2025 году этот показатель достигнет 181 зеттабайта [1], что почти вдвое превышает объем данных, зафиксированный три года назад. На фоне этого роста всё более актуальным становится вопрос защиты информации как на персональном уровне, так и в контексте обеспечения безопасности критической инфраструктуры. В настоящее время ключевым механизмом сохранения конфиденциальности данных считаются технологии шифрования [2]. Однако появление высокопроизводительных квантовых компьютеров, способных эффективно решать задачи криптоанализа благодаря своей исключительной вычислительной мощности, а также развитие алгоритмов подбора ставят под сомнение надёжность современных методов защиты. Увеличение длины ключей шифрования может временно компенсировать угрозы, однако это решение сопряжено с существенным ростом требований к вычислительным ресурсам [3].

В этой связи возникает настоятельная необходимость защиты информации от квантовых атак, которые представляют собой воздействие программных или программно-аппаратных средств, использующих вычислительные возможности квантовых компьютеров для получения несанкционированного доступа к данным, защищённым традиционными методами шифрования. Для противодействия таким угрозам предлагаются более надёжные методы обеспечения

[1] Работа выполнена при поддержке ОАО "Российские железные дороги"

криптографической защиты, среди которых особое место занимает постквантовая криптография, основанная на программном подходе. Однако безопасность данных методов пока не может быть окончательно подтверждена. На данный момент отсутствует возможность достоверно оценить эффективность применения известных вариантов квантовых атак к алгоритмам постквантовой криптографии. Ситуация может измениться в будущем с появлением новых алгоритмов “подбора” ключей, которые на сегодняшний день остаются неизвестными.

Одновременно с этим, существующий аппаратный метод квантового распределения ключей способен обеспечить безопасность на базе фундаментальных законов физики и свойств фотона, квантовое состояние которого невозможно измерить не разрушив его. Безопасность данного подхода останется нерушимой даже в случае будущих достижений в области вычислительных мощностей или компьютеров.

В рамках данного подхода был разработан экспериментальный образец программно-аппаратного комплекса защищенной передачи данных в мобильных сетях стандартов 4G/5G с применением технологий квантового распределения ключей (ПАК ЗПД КРК). Структура разработанного комплекса представлена на Рис. 1.

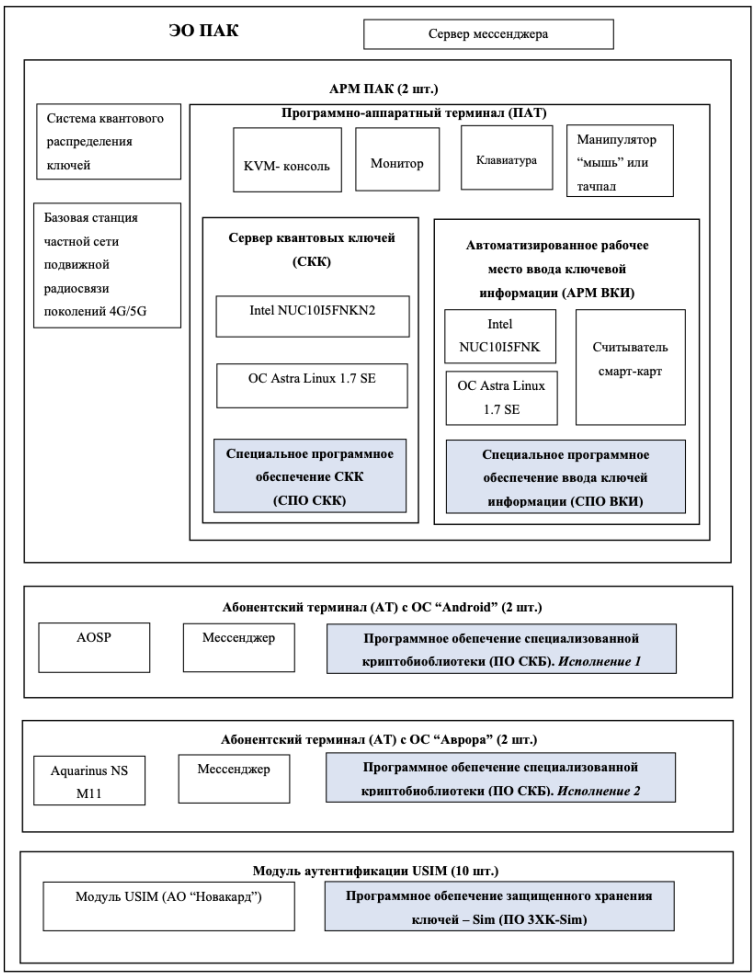

Рис. 1. Составные части ПАК ЗПД КРК

2. РАЗРАБОТКА АППАРАТНОЙ ЧАСТИ

При проектировании ПАК ЗПД КРК оптимальным было признано решение, при котором один и тот же программно-аппаратный комплекс обеспечивает защищённую связь между абонентскими терминалами, работающими под управлением разных операционных систем. Таковыми были выбраны ОС Android как одна из самых популярных операционных систем для мобильных устройств, а также Аврора – российская мобильная операционная система, которая развивается как продукт, предназначенный для корпоративных пользователей и государственных учреждений. В соответствии с этим ПАК ЗПД КРК составляют два одинаковых набора устройств: абонентские терминалы под управлением каждой из выбранных операционных систем, а также автоматизированное рабочее место (АРМ) ПАК. АРМ ПАК включает в себя базовую станцию, а также программно-аппаратный терминал (ПАТ). В состав ПАТ входит сервер квантовых ключей (СКК), и автоматизированное рабочее место ввода ключевой информации (АРМ ВКИ). АРМ ВКИ состоит из мини-ПК, KVM-консоли, монитора, клавиатуры и манипулятора «мышь».

Для обеспечения работы мессенджера в составе ПАК ЗПД КРК имеется сервер мессенджера. Работа серверной платформы в составе комплекса обеспечивается путём инсталляции в его вычислительный комплекс специального программного обеспечения сервера мессенджера, работающего в среде ОС Ubuntu Server 20.04.01 LTS.

Компоновка оборудования, входящего в состав ПАК ЗПД КРК, требует решения нескольких задач. Аппаратура должна быть размещена так, чтобы ей было удобно пользоваться, перемещать и развёртывать. При этом, так как использование ПАК ЗПД КРК предполагается не только в помещении, но и на открытых площадках, оборудование должно быть защищено от внешних воздействующих факторов, в первую очередь от дождя и ударов.

Подбор устройств под требуемые задачи показал, что необходимые габариты пространства для размещения аппаратуры должны составлять не менее $410 \times 340 \times 170$ мм. Далее, после фиксации габаритных размеров компонентой базы, с учетом тепловых выделений основных блоков ПК, трассировки и крепежных нюансов, скомпонована схема для выявления минимально-требуемых внутренних габаритов кейса для установки основных блоков.

В качестве наружной оболочки было предложено применить пыле-влагозащищенный кейс, обеспечивающий в транспортном положении уровень защиты IP67. Такие кейсы изготавливаются литьем под давлением из стеклонаполненного полипропилена. Корпус кейса обладает достаточной ударной прочностью и широким диапазоном рабочих температур.

Среди нескольких моделей кейсов, подходящих под требования к размещению аппаратуры, наиболее оптимальной была признана модель «Калибр 5040» производителя ООО «НПО ПРОФПОЛИМЕРКЕЙС». Кейс имеет следующие преимущества:

- сбалансированное соотношение гибкости и прочности;
- повышенная вязкость разрушения, что исключает растрескивание даже при точечных нагрузках;
- устойчивость к воздействию агрессивных химических веществ;
- высокая термостойкость (не теряет свойств до температуры -40 °C);
- эффективная защита содержимого от ударных нагрузок;
- низкая электропроводность материала.

Габаритные размеры кейса «Калибр 5040» $660 \times 507 \times 356$ мм, а конечная масса кейса после его сборки составила 43 кг. Для удобства работы кейс устанавливается на стойку-штатив. Конструкция подставки АРМ ПАК позволяет регулировать высоту рабочего положения в диапазоне от 800 до 1400 мм, что обеспечивает комфортное использование для оператора. Общий вид АРМ ПАК показан на Рис. 2.

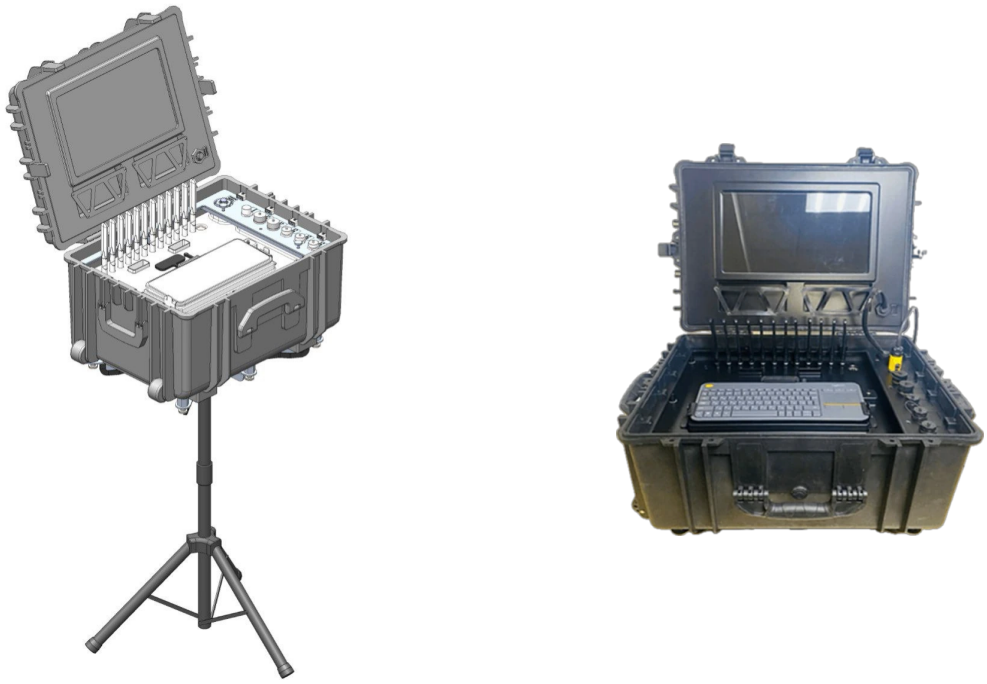

Рис. 2. Общий вид АРМ ПАК: проект и физическая реализация

Структура, состав и массогабаритные характеристики компонентов АРМ ПАК спроектированы таким образом, чтобы процесс развертывания до выхода на рабочий режим мог быть выполнен двумя операторами, минимизируя время развертывания. Для подключения к СКРК при подготовке к работе на объекте размещения АРМ ПАК оснащен специальным интерфейсом взаимодействия с внешней криптографической аппаратурой выработки и распределения ключей. Панель управления и интерфейсные разъемы расположены таким образом, чтобы закрытие крышки с установленным в нее информационным монитором осуществлялось без препятствий. Интерфейсы подключения внешних устройств имеют установочные ключи и маркировочные знаки, обеспечивающие правильное подключение разъемов при монтаже. Внешний вид изделия соответствует образцам внешнего вида, отобранным и утвержденным в процессе разработки дизайна. Изделие в собранном виде не имеет выступающих, вращающихся и подвижных элементов внутренних конструкций.

Для обеспечения удобства обслуживания и ремонта предусмотрена возможность разборки и сборки АРМ ПАК с использованием общедоступных инструментов, взаимозаменяемых монтажных креплений и элементов. При выполнении монтажных и демонтажных операций минимизировано использование клея при фиксации элементов между собой. Унификация технического обеспечения аппаратной платформы обеспечивается применением серийно выпускаемых технических средств и конструктивных частей.

3. РАЗРАБОТКА ПРОГРАММНОЙ ЧАСТИ

ПАК ЗПД КРК представляет собой уникальное решение, сочетающее передовые технологии квантовой криптографии и защищенные каналы связи. Использование квантовых ключей (КК) и специализированного программного обеспечения обеспечивает высокий уровень конфиденциальности и безопасности данных, что делает систему подходящей для применения в корпоративных и государственных структурах. В основу программной части ПАК ЗПД КРК вошли 5 единиц ПО, относящихся к СКЗИ, и 2 единицы, необходимые для настройки и управления аппаратной частью.

3.1. Разработка защищенного мессенджера с использованием квантовых технологий

Был разработан специализированный мессенджер, обеспечивающий безопасную передачу текстовых, голосовых и видеоданных. Уникальность решения заключается в интеграции технологии квантового распределения ключей, что делает его практически неуязвимым для современных кибератак.

Мессенджер поддерживает следующие типы данных:

– текстовые сообщения с количеством символов до 1000 в кодировке UTF-8;
– голосовые звонки и сообщения между двумя пользователями;
– видеозвонки с разрешением не менее 1080p (FullHD).

Интерфейс мессенджера представлен на Рис. 3. На каждой из пар изображений слева представлены снимки экрана мобильного телефона под управлением ОС Аврора, справа – ОС Android. На рисунке последовательно показаны экран авторизации ПО мессенджера, список контактов, окно чата и экраны звонков.

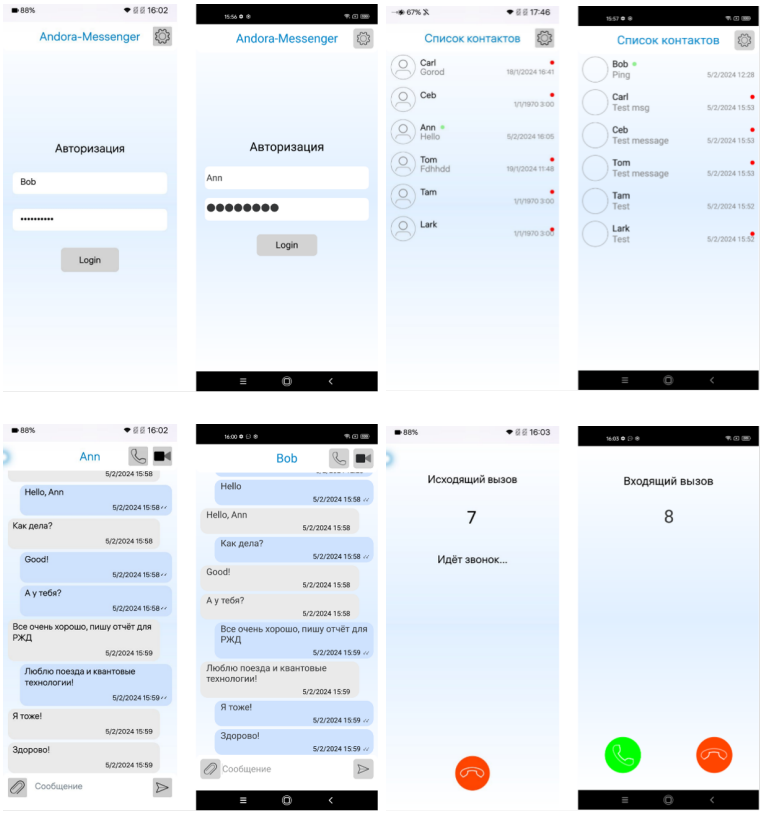

Рис. 3. Пользовательский интерфейс мессенджера

3.2. Инфраструктура менеджера

Для связи абонентских терминалов внутри сети применяется сервер мессенджера с установленным ПО сервера мессенджера. База данных ПО сервера мессенджера содержит информацию о пользователях мессенджера, их правах доступа, парольную информацию, а также хранит в виде буфера передаваемые данные в зашифрованном виде до момента подтверждения о получении сообщения у получателя. При эксплуатации сервер мессенджера не взаимодействует со средствами криптографической защиты информации и системой квантового

распределения ключей, что обеспечивает отсутствие конфликтов и поддерживает целостность функциональности каждого компонента ПАК ЗПД КРК.

4. БЕЗОПАСНОСТЬ ДАННЫХ

Шифрование и имитозащиту пакетов данных обеспечивает разработанное программное обеспечение специализированной криптобиблиотеки (ПО СКБ). Так как ОС Android имеет принципиальные отличия в архитектуре от ОС Аврора, ПО СКБ имеет исполнение для каждой из операционных систем. Для работы с ключевой информацией используется программное обеспечение сервера квантовых ключей (ПО СКК), которое получает квантовые ключи от системы квантового распределения ключей и распределяет их между абонентскими терминалами.

Для ввода ключей связи разработано специальное программное обеспечение ввода ключевой информации (СПО ВКИ), которое формирует код в шестнадцатеричном формате и его QR-код. Пользователь может ввести код вручную или отсканировать QR-код при входе в учетную запись мессенджера, что упрощает процесс настройки безопасного соединения.

4.1. Защищенное хранение ключей

Для подключения абонентских терминалов к локальной сети, формируемой базовой станцией 4G/5G, работающей в пределах 15 метров, используются аутенфицированные сим-карты, на которые установлено разработанное программное обеспечение защищенного хранилища ключей в модуле аутентификации типа USIM [4] (ПО ЗХК-SIM). Сим-карта используется исключительно для аутентификации абонентских терминалов в сети, формируемой базовой станцией.

Основной функционал ПО ЗХК-SIM заключается в работе с ключевой информацией и включает следующие действия:

- создание защищенного хранилища ключевой информации;
- запись, чтение и хранение параметров и ключей связи с системой квантовых ключей в энергонезависимой памяти;
- возможность удаления ключевой информации.

Доступ к хранилищу ключей предоставляется только после успешной аутентификации, что обеспечивает дополнительный уровень защиты данных [5].

4.2. Технологии квантового распределения ключей

Уникальность разработки ПАК ЗПД КРК во многом определена технологией квантового распределения ключей. Квантовые ключи вырабатываются системой КРК, связывающей два абонентских терминала посредством протокола ProtoQA, в основе которого лежит протокол CRISP [6]. Распределение ключей включает две фазы:

1. Получение КК от СКРК;
2. Распределение КК между СКБ абонентских терминалов.

Для своевременного и синхронного обеспечения квантовыми ключами все абонентские терминалы распределены между двумя АРМ ПАК. Все АРМ ПАК оснащены компонентами СКРК, при этом не все связаны друг с другом квантовыми каналами. Компоновка предусматривает одновременное использование большого числа абонентских терминалов. Система распределения ключевой информацией обеспечивает КК любые два АТ, независимо от того, к

какому АРМ ПАК они приписаны. АРМ ПАК фактически является узлом связи, включая в себя базовую станцию и сервер квантовых ключей. СКК отвечает за сопряжение с СКРК, за первичную генерацию ключей доставки и отправку шифрограмм абонентских ключей по запросу абонента. Один СКК может обслуживать одну или несколько СКРК. Мобильное устройство всегда привязывается только к одному СКК. СКК взаимодействуют между собой через транспортную сеть ПАК [7].

В качестве управляющей операционной системы мини-ПК, на которых установлено ПО СКК и СПО ВКИ, обеспечивающие работу серверов, используется отечественная операционная система Astra Linux. Это решение соответствует требованиям по использованию локализованного программного обеспечения и обеспечивает высокий уровень защищенности на уровне операционной системы.

5. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

В предлагаемом АПК реализована гибридная архитектура защиты, сочетающая КРК, классические алгоритмы и элементы постквантовой криптографии. Это позволяет обеспечить устойчивость как к современным, так и перспективным угрозам, включая квантовые атаки.

Ключи, сгенерированные с помощью КРК-сервера, обладают полной случайностью и не поддаются перехвату без нарушения квантового состояния. Для защиты трафика (текста, аудио, видео) применяется симметричное шифрование с одноразовыми ключами, что исключает их повторное использование.

Ключи хранятся в защищённых модулях — USIM-картах с ПО SKSS, обеспечивающим автоматическое удаление ключевого материала по завершении сессии. На стороне сервера используется аппаратная изоляция с криптографическим шифрованием памяти и контролем доступа.

Система включает внутреннюю инфраструктуру мониторинга и логирования: все действия с ключами (создание, передача, удаление) фиксируются в защищённом журнале и анализируются в реальном времени для обнаружения подозрительной активности.

В случае недоступности КРК-канала предусмотрен переход на проверенные классические или постквантовые алгоритмы без прерывания работы комплекса. Обновление криптографического стека осуществляется модульно, без остановки основных функций.

6. ОЦЕНКА УСТОЙЧИВОСТИ

Разработана математическая модель гибридной криптосистемы, включающая КРК, устойчивое симметричное шифрование и постквантовую криптографию. Предложено единое выражение для описания сеанса защищённой связи с учётом параметров канала, времени, объёма данных и уровня стойкости:

$$C = \begin{cases} E_{K_Q}(M), & \text{если } f_k \cdot T \cdot |K_Q| \geq V \text{ и } \gamma(K_Q) \geq \gamma_{\min} \\ E_{K_{PQ}}(M), & \text{если } f_k \cdot T \cdot |K_Q| < V \text{ или } \gamma(K_Q) < \gamma_{\min} \end{cases}$$

– C — зашифрованное сообщение;
– M — исходный текст;
– EK_K — шифрование с использованием квантового ключа;
– EK_{PQ} — шифрование с использованием постквантового ключа;
– f_k — скорость генерации ключей;
– T — длительность сессии;
– $\gamma(K_K)$ — стойкость ключа;

– δ — вероятность компрометации (не более 2^{-n}).

Модель позволяет оценивать устойчивость системы и использовать её как инструмент проектирования защищённой связи. Также впервые предложено расширить безопасность до абонентского уровня с помощью USIM-карт с контролем жизненного цикла ключей и логированием всех операций.

7. ЗАКЛЮЧЕНИЕ

Разработан экспериментальный образец программно-аппаратного комплекса защищенной передачи данных в мобильных сетях стандартов 4G/5G с использованием технологий КРК. Решение основано на гибридной архитектуре, сочетающей аппаратные и программные модули: генерация и распределение ключей, квантозащищённый мессенджер, системы шифрования и логирования. Система позволяет осуществлять защищённый обмен текстовыми, аудио- и видео сообщениями внутри локальной сети, формируемой базовой станцией из состава АРМ ПАК. Аппаратура ПАК ЗПД КРК размещена в герметичном кейсе, обеспечивающем защиту от дождя и ударов, что позволяет оперативно развернуть рабочее место не только в помещении, но и на открытой площадке. Реализована поддержка ОС Android и AOSP.

Особое внимание уделено защите ключей на стороне пользователя (USIM + SKSS), внутреннему мониторингу и совместимости с существующей телеком-инфраструктурой. Модульная архитектура и использование открытых решений обеспечивают масштабируемость и технологическую независимость.

Предложенный подход может стать основой для построения телекоммуникационных систем, устойчивых к квантовым угрозам.

СПИСОК ЛИТЕРАТУРЫ

1. Statista. Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2020, with Forecasts from 2021 to 2025. [Электронный ресурс]: www.statista.com/statistics/871513/worldwide-data-created/.

2. I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, and C. C.-W. Lim, “Security of device-independent quantum key distribution protocols: A review,” Phys. Rev. A, vol. 105, no. 6, pp. 062409, Jun. 2022.

3. R. Bavdekar, E. J. Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, “Post-quantum cryptography: A review of techniques, challenges and standardizations,” in Proc. 2023 Int. Conf. Inf. Netw. (ICOIN), Bangkok, Thailand, Jan. 2023, pp. 251–256.

4. GlobalPlatform Technology Card Specification Version 2.3.1 Public Release March 2018 Document Reference: GPC_SPE_034. [Электронный ресурс]: `https://globalplatform.org/wp-content/uploads/2018/05/GPC_CardSpecification_v2.3.1_PublicRelease_CC.pdf`

5. Р 1323565.1.003-2017. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи. – М.: Стандартинформ, 2017. – 16 с.;

6. Р 1323565.1.029–2019 «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем». – М.: Стандартинформ, 2020. – 10 с.;

7. ТК 26 МР 26.4.004-2021 «Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации». – М.: Технический комитет по стандартизации «Криптографическая защита информации», 2021. – 61 с.

Software and Hardware Complex for Secure Data Transmission Using Quantum Key Distribution Technologies

P. Y. Vatskov, Y. K. Kozhemyako, O. V. Kolesnikov, E. M. Mavrin, V. G. Potapov P. V. Che

This article presents the results of developing an experimental prototype of a software and hardware complex for secure data transmission in 4G/5G mobile networks using quantum key distribution (QKD) technologies. The structure and fundamental operational principles are outlined, along with details of both the hardware and software components. The developed prototype is a fully functional system capable of secure text, audio, and video messaging. Encased in a hermetically sealed, ruggedized case, the system can be deployed both indoors and outdoors.

KEYWORDS: quantum key distribution (QKD), mobile networks 4G/5G, quantum cryptography, secure communication channels.