Оригинальная статья / Original article

https://doi.org/10.21869/2223-1536-2025-15-4-107-122

УДК 623.746, 004.056

Оценка возможности применения квантовой криптографии и протокола LoRaWAN 2 для установления связи с беспилотным летательным аппаратом

М. Ю. Алемпьев[1], Д. С. Коптев[1] ✉, В. Г. Довбня[1], М. О. Ревякина[2]

[1] Юго-Западный государственный университет
ул. 50 лет Октября, д. 94, г. Курск 305040, Российская Федерация

[2] Орловский государственный университет имени И. С. Тургенева
ул. Комсомольская, д. 95, г. Орёл 302026, Российская Федерация

✉ e-mail: d.s.koptev@mail.ru

Резюме

Цель исследования. *Современные беспилотные летательные аппараты сталкиваются с проблемами устойчивой связи в условиях радиопомех, сложного рельефа (горы, леса) или активного радиоэлектронного подавления. Одним из возможных решений данной проблемы является применение принципов квантовой криптографии в сочетании с новейшими протоколами связи, такими как LoRaWAN2, способствующими обеспечению защищённой и стабильной передачи данных в сложных условиях.*
Целью исследования является оценка возможности применения квантовой криптографии и протокола LoRaWAN 2 для установления и поддержании постоянной устойчивой связи с беспилотным летательным аппаратом.
Методы *исследования основаны на понятиях теории статистической радиотехники, теории распространения радиоволн ультравысокочастотного диапазона. Использованы методы многокритериального анализа, параметрического и структурного синтеза. Проанализированы принципы передачи информации с беспилотных летательных аппаратов. Проведена критическая оценка характеристик БПЛА с применением квантовой криптографии и протокола LoRaWAN 2.*
Результаты. *Приведены аналитические выражения и сравнительные характеристики для оценки перспектив применения квантовой криптографии и протокола LoRaWAN 2 с беспилотными летательными аппаратами. Показано, что при использовании квантовой криптографии вероятность перехвата данных в канале связи с БПЛА составит примерно 1%, что существенно увеличивает его защищенность в отличие от RSA-2048. Квантовая криптография улучшает безопасность БПЛА и получение ключа при незначительном увеличении массы, энергопотребления и скорости. В ближайшие годы с развитием компактных систем её перспективное внедрение станет стандартом для коммерческих дронов.*
Заключение. *В качестве перспективных направлений исследований и применения в области использования беспилотных летательных аппаратов следует рассматривать применение технологии квантовой криптографии и протокола LoRaWAN 2, способствующие повышению характеристик БПЛА: большую дальность, энергоэффективность, безопасность и масштабируемость.*

Ключевые слова: *квантовая криптография; воздушная среда передачи данных; беспилотный летательный аппарат; канал передачи данных; воздействие радиопомех; стандарт связи; пропускная способность канала.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Оценка возможности применения квантовой криптографии и протокола LoRaWAN2 для установления связи с беспилотным летательным аппаратом / М. Ю. Алемпьев, Д. С. Коптев, В. Г. Довбня, М. О. Ревякина // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2025. Т. 15, № 4. С. 107–122 https://doi.org/ 10.21869/2223-1536-2025-15-4-107-122

Поступила в редакцию 07.10.2025 *Подписана в печать 04.11.2025* *Опубликована 26.12.2025*

Evaluation of the possibility of using quantum cryptography and the LoRaWAN 2 protocol to establish communication with an unmanned aerial vehicle

Mikhail Y. Alempiev[1], Dmitry S. Koptev[1] ✉, Vitaly G. Dovbnya[1], Maria O. Revyakina[1]

[1] Southwest State University
50 Let Oktyabrya Str. 94, Kursk 305040, Russian Federation

[2] Orel State University named after I. S. Turgenev
95 Komsomol'skaya Str., Orel 302026, Russian Federation

✉ e-mail: d.s.koptev@mail.ru

Abstract

Purpose of research. *Modern unmanned aerial vehicles face challenges in maintaining reliable communications in the face of radio interference, difficult terrain (mountains, forests), or active electronic countermeasures. One possible solution to this problem is the application of quantum cryptography principles in combination with the latest communication protocols, such as LoRaWAN 2, which help ensure secure and stable data transmission in challenging environments. The Purpose of the esearch is to evaluate the feasibility of using quantum cryptography and the LoRaWAN 2 protocol to establish and maintain continuous, stable communication with an unmanned aerial vehicle.*

Methods. *The research methods are based on concepts from statistical radio engineering theory and ultra-high-frequency radio wave propagation theory. Multicriteria analysis, parametric synthesis, and structural synthesis methods are used. The principles of information transmission from unmanned aerial vehicles are analyzed. A critical assessment of the performance of a UAV using quantum cryptography and the LoRaWAN 2 protocol is conducted.*

Results. *Analytical expressions and comparative characteristics are presented to assess the potential for using quantum cryptography and the LoRaWAN 2 protocol with unmanned aerial vehicles. It is shown that using quantum cryptography, the probability of data interception in a UAV communication channel is approximately 1%, significantly increasing its security compared to RSA-2048. Quantum cryptography improves UAV security and key retrieval with a slight increase in weight, power consumption, and speed. In the coming years, with the development of compact systems, its promising implementation will become the standard for commercial drones.*

Conclusion. *As promising areas of research and application in the field of using unmanned aerial vehicles, the use of quantum cryptography technology and the LoRaWAN 2 protocol should be considered, which contributes to improving the characteristics of UAVs: high range, energy efficiency, security and scalability.*

Keywords: *quantum cryptography; air data transmission medium; unmanned aerial vehicle; data transmission channel; exposure to radio interference; communication standard; channel capacity.*

Conflict of interest: *The Authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Alempiev M.Y., Koptev D.S., Dovbnya V.G., Revyakina M.O. Evaluation of the possibility of using quantum cryptography and the LoRaWAN 2 protocol to establish communication with an unmanned aerial vehicle. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Serija: Upravlenie, vychislitel'naja tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering.* 2025;15(4):107–122. (In Russ.) https://doi.org/10.21869/2223-1536-2025-15-4-107-122

Received 07.10.2025 *Accepted 04.11.2025* *Published 26.12.2025*

***

Введение

Современные беспилотные летательные аппараты (БПЛА) обладают возможностью адаптации к выполнению различных задач по обслуживанию гражданской инфраструктуры. Однако их эффективность зависит от условий использования и технических характеристик самого БПЛА. В условиях ограниченности заряда батареи, сложности управления, наличия помех и непредсказуемости среды их применение может быть неэффективным.

Рассмотрим типовые характеристики БПЛА DJI Phantom 4 Pro, часто используемого для выполнения задач сотрудниками спасательных служб и сотрудниками полиции. Рассматриваемый дрон обладает дальностью полета в 4,5 км при условии хорошей видимости и скорости полета 72 км/ч, временем полета – 30–40 мин при стандартной массе в 1,2 кг и высотой полета до 500 м. Также DJI Phantom 4 Pro способен выполнять поставленные задачи в условиях дождя, снега, тумана и скорости ветра до 15 м/с. Емкость аккумуляторной батареи дрона составляет 4400 мАч. Для мониторинга на дроне используется камера с высоким разрешением 4K (4096×2160) при битрейте в 100 Мбит/с и видеокодеком H.264, способная снимать в режиме 4K/60 кадров в секунду с поддержкой угла обзора в 360 градусов, однако, данные характеристики актуальны только при использовании режима автономного управления дроном.

В режиме дистанционного управления БПЛА поддерживает видео в максимальном разрешении 1080p (1920×1080) с частотой кадров 60 кадров в секунду и битрейтом в 10 Мбит/с, но дальность полета ограничена 5 км. При использовании разрешения 720p (1280×720) максимальная дальность может быть увеличена до 10 км. Передача данных с БПЛА в обоих случаях на пульт дистанционного управления (ПДУ) происходит на частоте 2,4 ГГц с использованием частотно-импульсной модуляции, что существенно ограничивает дальность полета в режиме дистанционного управления.

Вероятность битовой ошибки при использовании БПЛА в идеальных условиях при дистанционном управлении может достигать 5%, в автономном режиме – до 20%. Основной причиной роста вероятности ошибки является использования записи и передачи видеоданных различного разрешения с БПЛА: чем выше качество передаваемой информации, тем выше вероятность ошибки [1].

Обеспечение безопасности передачи данных между БПЛА и ПДУ – это ключевой фактор, обеспечивающий выполнение поставленных задач дроном, особенно при выполнении операций сотрудниками государственных служб. Рассмотрим несколько методов увеличения безопасности канала связи.

Шифрование данных – это метод защиты информации, основанный на использовании ключей шифрования информации, который позволяет повысить защищенность доступа к информации. Однако к минусам можно отнести то, что требуются высокие вычислительные мощности и скорости передачи данных, а также существует зависимость от ключей, которые могут быть взломаны.

Использование протоколов безопасности – это метод защиты информации, основанный на использовании протоколов, которые реализуют шифрование, аутентификацию и защиту от атак. К минусам можно отнести зависимость от стабильного канала передачи данных, снижение скорости передачи данных, сложности настройки работы с протоколами.

Использование методов проверки целостности – это метод защиты информации, основанный на использовании контроля за неизменностью данных при передаче. К минусам можно отнести снижение скорости передачи данных из-за обращения к сторонним серверам для проверки, наличие поддержки сторонних серверов, возможность взлома ключей проверки целостности [2].

Использование методов синхронизации – этот метод защиты информации позволяется обеспечить точную синхронизацию между БПЛА и ПДУ, а также минимизировать задержки. К минусам относятся наличие зависимости от GPS, которая отвечает за синхронизацию, снижение скорости передачи данных из-за обращения к сторонним серверам для проверки, наличие поддержки сторонних серверов.

Использование методов защиты от ошибок – этот метод защиты информации использует коды коррекции ошибок для исправления ошибок при передачи данных. К минусам относятся увеличение объема передаваемых данных из-за наличия кодов коррекции, а также увеличение времени передачи данных из-за процессов по исправлению передаваемой информации.

Квантовая криптография – это метод защиты информации, основанный на принципах квантовой механики. В отличие от классической криптографии, которая опирается на сложность математических задач (например, факторизацию больших чисел), квантовая криптография использует фундаментальные свойства квантовых частиц (например, фотонов) для создания абсолютно защищённых каналов связи [3].

Рассмотрим основные принципы квантовой криптографии и следствия из них:

1. Принцип квантовой неопределённость (принцип Гейзенберга) позволяет говорить о невозможности измерить квантовое состояние частицы (например, поляризацию фотона), не изменив его, а, следовательно, любая попытка перехвата информации о квантовом ключе будет обнаружена.

2. Принцип квантовой запутанности позволяет говорить о том, что две частицы могут быть связаны так, что изменение состояния одной мгновенно влияет на другую, независимо от расстояния (используется в протоколах распределения квантовых ключей (например, E91)) [4].

3. Принцип невозможности клонирования (теорема о запрете клонирования), суть его заключается в том, что невозможно создать точную копию неизвестного квантового состояния. Данное обстоятельство позволяет предотвратить атаки типа «человек посередине» (MITM) [5].

Преимущества квантовой криптографии:

– абсолютная безопасность – защита основана на законах физики, а не на вычислительной сложности;

– обнаружение подслушивания – любые попытки перехвата ключа оставляют следы;

– устойчивость к квантовым компьютерам – в отличие от RSA и ECC, которые могут быть взломаны алгоритмом Шора и др. [6].

Ограничения и проблемы квантовой криптографии:

– ограниченная дальность (около 100–500 км по оптоволокну, до 120 км через свободное пространство);

– высокая стоимость оборудования (однофотонные детекторы, квантовые повторители);

– уязвимость к атакам на реализацию (например, лазерное ослепление детекторов) [7].

Материалы и методы

БПЛА DJI Phantom 4 Pro способен достигнуть дальности полета в 4,5 км, так как работает на частоте 2,4 ГГц (стандарт Wi-Fi). В качестве альтернативного канала связи возможно использование сетей 5G и стандартов LoRaWAN.

5G/LTE-M позволяет обеспечить широкий радиус действий и высокую скорость передачи данных с БПЛА на ПДУ, однако требуется постоянное подключение к мобильной сети, что, например, в условиях проведения спасательных операций в удаленных районах невозможно.

Использование системы передачи данных по стандарту LoRaWAN 2 позволяет расширить радиус зоны управлениям дроном до 100 км, но имеет ограничение в пропускной способности канала, что ограничивает возможность получения видеоданных путем передачи через радиоканал связи.

Перспективным является использование стандарта LoRaWAN 2 в качестве дополнительного источника передачи данных между БПЛА и ПДУ, который позволяет расширить радиус полета максимально в теории до 100 км без использования мобильных сетей связи. Рассмотрим более подробно характеристики и возможности стандарта LoRaWAN 2.

LoRaWAN 2 – это эволюция оригинального протокола LoRaWAN 1, разработанного LoRa Alliance. Основная цель обновления – улучшение безопасности, энергоэффективности, масштабируемости

и поддержки новых сценариев использования (например, промышленного IoT (Internet of Things), умных городов).

LoRaWAN 2 поддерживает две версии протокола (1.x и 2.x) и использует LR-FHSS (Long Range Frequency Hopping Spread Spectrum):

– альтернатива LoRa для восходящего канала (UL);

– устойчивость к помехам за счет частотного скачкообразного расширения спектра;

– поддержка высокой плотности устройств (до 1 млн на гейт);

– скорость передачи до 100 кбит/с.

LoRaWAN 2 позволяет уменьшить затраты на энергопотребление устройством:

– адаптивное управление мощностью передачи (ADR+);

– оптимизация циклов сна (меньше служебных сообщений).

Также стандарт поддерживает IPv6 – возможность прямой интеграции с Интернетом (без шлюзовых преобразований) [8].

Устройства по стандарту LoRaWAN 2 возможно применять в сложных условиях:

– сложно-рельефная местность (горы, леса) – сигнал LoRaWAN проходит через препятствия лучше, чем Wi-Fi или Bluetooth;

– демонстрирует высокую устойчивость к атмосферным помехам;

– обладает высокой спектральной и энергетической скрытностью, что обеспечивает высокую защищенность от преднамеренных помех.

LoRaWAN 2 использует двухключевую схему аутентификации (Network Session Key + Application Session Key) и улучшенное шифрование. На рисунке 1 представлено шифрование AES в LoRaWAN.

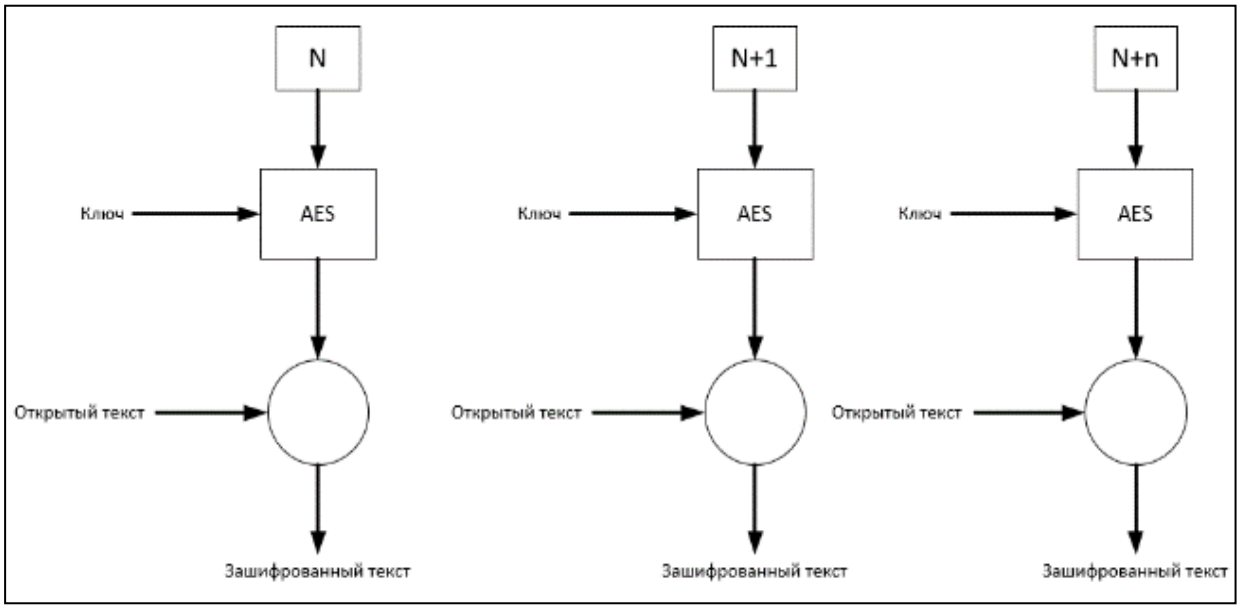

Рис. 1. Шифрование AES-256 в LoRaWAN 2

Fig. 1. AES-256 encryption in LoRaWAN 2

Взлом LoRaWAN требует перебора 2^{128} комбинаций (AES-128) → 2^{256} (AES-256), однако, в отличие от использования квантовой криптографии, возможен.

По сравнению с Wi-Fi (WPA2/WPA3), LoRaWAN 2 не требует постоянного обмена ключами. БПЛА с LoRaWAN 2 защищён от атак типа «человек посередине» и перехвата данных.

Масштабируемость LoRaWAN 2 позволяет поддерживать тысячи устройств на одну базовую станцию благодаря использованию ALOHA-протокол с частотным и временным разделением каналов.

Одна базовая станция поддерживает десятки тысяч устройств (в теории). На рисунке 2 отображено взаимодействие БПЛА при использовании дронов ретрансляторов с протоколом LoRaWAN.

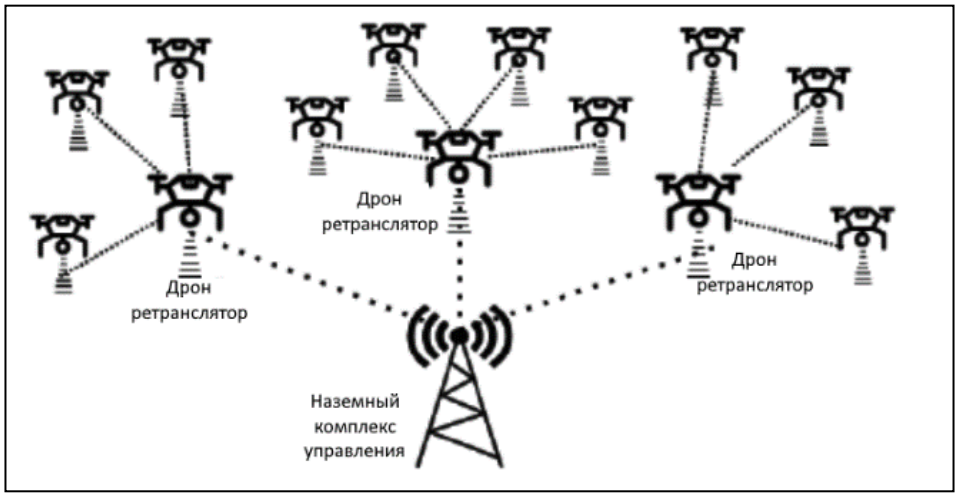

Рис. 2. Масштабируемость связи при использовании протокола LoRaWAN

Fig. 2. Communication scalability when using the LoRaWAN protocol

Для сравнения: Wi-Fi (даже в mesh-сетях) – до 200–300 устройств. LoRaWAN 2 позволяет управлять роем БПЛА без перегрузки сети [9].

LoRaWAN используется LoRa модуляцию (чрезвычайно низкочастотная модуляция) и работает на субгигагерцовых частотах (868 МГц в Европе, 915 МГц в США), что обеспечивает большую дальность и имеет следующие характеристики:

– дальность LoRaWAN 2 в городских условиях – 5–10 км;

– дальность в открытой местности – до 100 км;

– Wi-Fi (2,4/5 ГГц) – до 300 м (в идеальных условиях);

– Bluetooth Low Energy (BLE) – до 100 м.

LoRaWAN 2 позволяет БПЛА работать на больших расстояниях без потери связи, что критично для мониторинга сельхозугодий, ЛЭП и других протяжённых объектов [10].

LoRaWAN 2 поддерживает Adaptive Data Rate (ADR), автоматически подстра-

ивая скорость передачи под условия связи:

– чувствительность приёмника LoRa – до –148 дБм (для SF12);

– устойчивость к замираниям (благодаря технологии Chirp Spread Spectrum CSS).

БПЛА с LoRaWAN 2 менее подвержен помехам от других радиоустройств, чем Wi-Fi/BLE.

Примерами успешного использования БПЛА с сенсорами и датчиками LoRaWAN являются: организация автономной видеосъемки удаленной местности; передачи данных с датчиком, установленных на БПЛА, при мониторинге местности; обеспечение логистики в удалённых районах (доставка медикаментов, оборудования, небольших грузов); организация непрерывного мониторинга критической инфраструктуры (линий электропередач, трубопроводов, объектов инфраструктуры жизнеобеспечения).

Квантовая криптография (например, протоколы QKD – Quantum Key Distribution) обеспечивает абсолютную защиту от перехвата ключей шифрования, что критически важно для БПЛА, работающих в условиях киберугроз.

Совместное применение квантовой криптографии и LoRaWAN 2 позволяет создавать и использовать БПЛА с защищённым каналом связи (невозможностью перехвата данных) и устойчивой работой в условиях радиоэлектронной борьбы. Подобное совместное использование позволит увеличить дальность действия БПЛА на защищенном канале связи до 100 км и сотен километров с применением mesh-ретрансляции [11].

Результаты и их обсуждение

Оценим возможность интеграции дополнительного передатчика связи по стандарту LoRaWAN 2 с использованием квантовой криптографии. В качестве примера базового БПЛА рассматриваем DJI Phantom 4 Pro.

Квантовая криптография (например, протоколы QKD – Quantum Key Distribution) обеспечивает абсолютную защиту от перехвата ключей шифрования, что критически важно для БПЛА, работающих в условиях киберугроз. Рассмотрим влияние внедрения квантовой криптографии в канал связи на ключевые параметры БПЛА с целью улучшения безопасности без значительного увеличения массы и энергопотребления [12].

Исходные данные для расчета влияния применения квантовой криптографии на БПЛА:

1. Традиционная криптография (алгоритм AES-256): вычислительная нагрузка составляет примерно 100 мВт, типичный чип имеет массу до 10 г и теоретически взламывается квантовыми компьютерами (алгоритм Шора) [13].

2. Квантовая криптография (QKD, например, BB84): вычислительная нагрузка составляет от 200 до 500 мВт, чип имеет массу от 50 до 100 г (миниатюрные системы для БПЛА), безопасность обеспечивается законами квантовой физики (невозможность клонирования состояния).

Оценка влияния на массу, энергопотребление, скорость работы БПЛА:

1. Прирост массы:

$$\Delta m = 1200 + 100 = 1300 \text{ г.}$$

Для БПЛА массой 1,2 кг это увеличение массы на 8%, что некритично.

2. Прирост энергопотребления:

$$\Delta P = \frac{4400}{0,5} + 500 = 9300 \text{ мВт} \cdot \text{ч},$$

где 4400 мАч – емкость аккумуляторной батареи; 0,5 ч – время работы БПЛА.

Для БПЛА с энергопотребление 8800 мВт·ч минимальное время работы сократится на 7% (примерно 28 мин), что приемлемо.

3. Изменение скорости:

$$v = 72 \cdot \frac{1200}{1300} = 66,46 \text{ км} \cdot \text{ч}.$$

Для БПЛА с изначальной скоростью 72 км/ч сократится максимальная скорость на 8%, что приемлемо.

На основании расчета можно сделать вывод, что такие параметры, как масса, энергопотребление и скорость, изменятся в пределах до 10%.

Оценка риска перехвата данных проводится на основании следующих исходных данных: вероятность перехвата классического RSA-2048: ~10^{-3} (при атаке методом brute force + side-channel); вероятность перехвата QKD: ~10^{-20} (невозможно без изменения квантового состояния).

Таким образом, для БПЛА, передающего данные каждые 10 с, за 1 ч (360 передач) вероятность перехвата данных составит:

– при использовании классической криптографии:

$$P_{\text{ош}} = 1 - (1 - 10^{-3})^{360} \approx 30\%,$$

где 10^{-3} – вероятность перехвата данных при использовании RSA-2048; 360 – количество передач сигналов за 1 ч;

– при использовании алгоритма квантовой криптографии QKD:

$$P_{\text{ош}} = 1 - (1 - 10^{-20})^{360} \approx 1\%,$$

где 10^{-20} – вероятность перехвата данных при использовании QKD; 360 – количество передач сигналов за 1 ч;

На основании расчета можно сделать вывод, что при использовании квантовой криптографии вероятность перехвата данных в канале связи составляет примерно 1%, что существенно увеличивает защищенность канала в отличие от RSA-2048 с вероятность примерно 30%.

Рассмотрим влияние на настройку канала передачи данных при использовании квантовой криптографии.

Исходные данные для расчета влияния применения квантовой криптографии на БПЛА:

– время установки ключа RSA-2048: ~100 мс;

– время установки ключа QKD: ~1 мс (для современных систем) [13].

При использовании квантовых сетей ключи распределяются мгновенно (прирост 100% по сравнению с классическими методами обмена ключами по открытому каналу).

Рассмотрим влияние использования протокола LoRaWAN 2 на параметры БПЛА. Оценку возможно произвести по нескольким ключевым аспектам: масса,

энергопотребление, дальность связи, помехоустойчивость.

Оценка влияния на массу, энергопотребление, скорость работы БПЛА:

1. SMD чип LoRaWAN 2 имеет массу 10 г. Прирост массы с учетом чипа квантовой криптографии составит

$$\Delta m = 1300 + 10 = 1310 \text{ г.}$$

Для БПЛА массой 1,3 кг это увеличение составит менее 1%, что некритично. Общее увеличение массы от исходной DJI Phantom 4 Pro составит менее 9%.

2. LoRaWAN 2 оптимизирован для работы с низким энергопотреблением (LPWAN), что является главной особенностью протокола.

Типичное энергопотребление LoRa-модуля, встраиваемого в БПЛА:

– ~10 мВт·ч при передаче (на мощности +14 дБм);

– потребление в режиме ожидания ~0,1 мВт·ч.

Сравнение с Wi-Fi/Bluetooth модулями БПЛА:

– Wi-Fi (в режиме передачи) – ~50–100 мВт·ч;

– Bluetooth Low Energy (BLE) – ~10–30 мВт·ч (но меньшая дальность) [14].

Прирост энергопотребления с учетом наличия чипа квантовой криптографии:

$$\Delta P = 9300 + 10 = 9310 \text{ мВт} \cdot \text{ч}.$$

Для БПЛА с энергопотребление 9310 мВт·ч минимальное время работы сократится на 7–8% (примерно 27 мин) от изначальных 30 мин, что приемлемо.

3. С учетом применения протокола LoRaWAN 2 для управления БПЛА, который теоретически способен организовать передачу данных на 100 км, проведем расчет дальности полета БПЛА от ПДУ:

$$S = 66,46 \cdot 0,45 = 29,91 \text{ км} \cdot \text{ч}.$$

Для БПЛА с изначальной дальностью полета 4,5 км прирост максимального расстояния составит на 664,7%, что является существенным показателем.

4. LoRaWAN 2 работает на частотах 868 МГц (Европа), 915 МГц (США), 928 МГц (Азия), которые имеют хорошую помехозащищенность, так как имеют низкую проницаемость для помех.

5. Для модуляции LoRa с использованием квантового кодирования и исправлением ошибок вероятность битовой ошибки может быть оценена по формуле

$$P_b \approx 0,5 \cdot Q(\sqrt{SNR \cdot 2^{SF+1}} - \\ - \sqrt{1,386 \cdot SF + 1,154},$$

где SNR – отношение сигнал/шум; SF – коэффициент расширения спектра; Q – квадратурная составляющая [15].

SNR имеет диапазон от 1,5 дБ до 3 дБ, в зависимости от уменьшения коэффициента расширения спектра от 12 до 7.

При требуемом отношении SNR на 3 дБ вероятность битовой ошибки BER примерно равна 10^{-3}, или 0,1% [16].

Рассмотрим результаты влияния квантовой криптографии (QKD) и протокола LoRaWAN 2 на характеристики БПЛА (табл. 1 и 2).

Таблица 1. Влияния QKD на БПЛА

Table 1. Effects of QKD on UAVs

Параметр	Классическая криптография	Квантовая криптография	Изменение
Безопасность	Уязвима к квантовым атакам	Абсолютная защита	+100%
Масса БПЛА	1200 г	1300 г	+100 г
Энергопотребление	8800 мВт	9300 мВт	+500 мВт
Скорость	72 км/ч	66,46 км/ч	–5,54 км/ч
Задержка ключа	100 мс	1 мс	100 раз быстрее

Таблица 2. Влияния LoRaWAN 2 и QKD на БПЛА в сравнении с Wi-Fi/BLE

Table 2. Impact of LoRaWAN 2 and QKD on UAVs compared to Wi-Fi/BLE

Параметр	LoRaWAN 2	Wi-Fi / BLE	Изменение
Масса ЛА	1310 г	1200 г	На 110 г увеличена
Энергопотребление	9310 мВт	8800 мВт	Увеличено на 6%
Дальность	29,91 км	4,5 км	Увеличено на 664,7%
Помехоустойчивость	CSS + ADR	Чувствителен к помехам	Сложнее взломать
Вероятность ошибки	0,1%	5%	Уменьшено на 4,9%

Квантовая криптография (QKD) улучшает безопасность БПЛА и получение ключа при незначительном увеличении массы, энергопотребления и скорости. В ближайшие годы с развитием компактных QKD-систем её перспективное внедрение станет стандартом для коммерческих дронов.

LoRaWAN 2 обеспечивает большую дальность, меньшую вероятность ошибки, помехоустойчивость при незначительном увеличении энергопотребления по сравнению с Wi-Fi и BLE, что делает его идеальным выбором для БПЛА в качестве способа связи на расстояния до 30 км [17].

Выводы

Таким образом, обобщая вышеизложенное, можно сделать следующие выводы:

– LoRaWAN 2 оптимизирован для низкого энергопотребления и в сочетании с квантовой криптографией энергопотребление БПЛА некритично увеличивается, что является важным фактором для БПЛА с ограниченным запасом батареи;

– дальность связи LoRaWAN (до 100 км в открытой местности) позволяет БПЛА увеличить радиус действия и работать на больших расстояниях без потери сигнала;

– LoRaWAN поддерживает тысячи устройств в одной сети, что полезно для роевых систем БПЛА;

– использование БПЛА с LoRaWAN 2 снижает вероятность ошибки в 5 раз;

– квантовая криптография устраняет расходы (такие как дополнительное энергопотребление, увеличение передаваемых данных, скорость передачи, скорость настройки ключей) на сложные системы шифрования, так как защита встроена на физическом уровне;

– квантовая криптография обеспечивает абсолютную защиту от перехвата благодаря принципам квантовой механики;

– даже при попытке взлома злоумышленник оставит следы, и полученный сигнал моментально сообщит о вмешательстве, что делает систему устойчивой к атакам;

– в сочетании с LoRaWAN 2 обеспечивается двойная защита данных от перехвата информации и пагубного влияния помех.

Внедрение квантовой криптографии и LoRaWAN 2 делает БПЛА более живучими в сложных условиях на дальних расстояниях от ПДУ, открывая новые возможности для спасательных, поисковых и коммерческих операций.

Использование протокола LoRa WAN 2 для передачи видеоданных при мониторинге на БПЛА является нецелесообразно из-за ограничений в пропускной способности канала связи в 100 кбит/с, однако, данного канала связи достаточно для управления и передачи команд для выполнения автономных задач дроном.

Результаты указывают на перспективу применения комбинации квантовой криптографии (максимальная защищенность канала связи) и LoRaWAN 2 (дальность + энергоэффективность), которая делает БПЛА идеальной платформой для защищённой, автономной и масштабируемой связи с возможностью выполнять различные задачи.

Список литературы

1. Кузнецова И. А., Гильязов М. Р. Влияние высоты полета беспилотного летального аппарата при обработке данных в автоматизированных программных обеспечениях // Научно-образовательный журнал для студентов и преподавателей «StudNet». 2021. № 5. URL: https://cyberleninka.ru/article/n/vliyanie-vysoty-poleta-bespilotnogo-letalnogo-apparata-pri-obrabotke-dannyh-v-avtomatizirovannyh-programmnyh-obespecheniyah (дата обращения: 10.09.2025).

2. Скрыпников А. В., Денисенко В. В., Евтеева К. С. Защита данных при передаче по беспроводным каналам связи // Международный журнал гуманитарных и естественных наук. 2019. № 8-2. С. 35–38.

3. Паринов М. В., Ветохин В. В., Фёдоров С. М. Анализ возможностей и методика модернизации систем управления, навигации и связи беспилотных летательных аппаратов промышленного назначения на примере изделий фирмы DJI // Вестник Воронежского государственного технического университета. 2023. № 6. С. 147–155.

4. Булатова А. Р. Квантовая криптография и квантовые вычисления // Вестник Пензенского государственного университета. 2025. № 1 (49). С. 11–14.

5. Букашкин С. А., Черепнев М. А. Квантовые устройства в криптографии // International Journal of Open Information Technologies. 2023. Vol. 11, N 1. P. 104–108.

6. Выдрин Д. Ф., Ситдиков Д. Р. Основные параметры беспроводной технологии LoRaWAN // Academy. 2019. № 2 (41). С. 22–24.

7. Муртазин М. М. Безопасность данных энергоффективной сети LORAWAN // Электронная наука. 2022. № 2. С. 2–8.

8. Олейникова А. В., Сурудин Д. С., Шафеев Д. Е. Квантовые компьютеры: надежды и реальность // Перспективы развития информационных технологий. 2016. № 30. С. 145–153.

9. Довгаль В. А. Интеграция сетей и вычислений для построения системы управления роем дронов как сетевой системы управления // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2022. № 1 (296). С. 62–76.

10. Довгаль В. А., Османи К. А. Разработка системы расширения дальности беспилотного летательного аппарата с помощью технологии беспроводной связи LORA // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2022. № 3 (306). С. 69–76.

11. Муртазин М. М. Безопасность данных энергоффективной сети LORAWAN // Электронная наука. 2022. № 2. С. 2–8.

12. Серикова Ю. И., Малыгина Е. А. Уязвимости криптографических систем с различными протоколами квантового распределения ключа и ключевая роль биометрии в квантовой криптографии // Universum: технические науки. 2017. № 11 (44). С. 13–15.

13. Олейникова А. В., Сурудин Д. С., Шафеев Д. Е. Квантовые компьютеры: надежды и реальность // Перспективы развития информационных технологий. 2016. № 30. С. 145–153.

14. Оценка возможности применения канала радиосвязи для передачи видеоинформации между беспилотным подводным аппаратом и пультом дистанционного управления / М. Ю. Алемпьев, А. Е. Семенова, Д. С. Коптев, В. Г. Довбня // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2025. Т. 15, № 1. С. 64–78. https://doi.org/10.21869/2223-1536-2025-15-1-64-78

15. Оценка дальности полёта и передачи видеоинформации при мониторинге чрезвычайных ситуаций с беспилотного летательного аппарата в сложных метеорологических условиях / М. Ю. Алемпьев, А. Е. Семенова, Д. С. Коптев, В. Г. Довбня // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2024. Т. 14, № 2. С. 21–39. https://doi.org/10.21869/2223-1536-2024-14-2-21-39

16. Леушин А. В. LoRa как новый вид модуляции. Принцип работы, основные параметры, помехоустойчивость // Техника радиосвязи. 2022. № 2 (53). С. 28–42.

17. Использование пеленгатора радиомаяков на беспилотном летательном аппарате в поисково-спасательных операциях / М. Ю. Алемпьев, А. Е. Семенова, Д. С. Коптев [и др.] // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2024. Т. 14, № 4. С. 129–145. https://doi.org/10.21869/2223-1536-2024-14-4-129-145

References

1. Kuznetsova I.A., Gilyazov M.R. The influence of the flight altitude of an unmanned aerial vehicle in data processing in automated software. *Scientific and Educational Journal for Students and Teachers «StudNet»*. 2021;(5). (In Russ.) Available at: https://cyberleninka.ru/article/n/vliyanie-vysoty-poleta-bespilotnogo-letalnogo-apparata-pri-obrabotke-dannyh-v-avtomatizirovannyh-programmnyh-obespecheniyah (accessed 10.09.2025).

2. Skrypnikov A.V., Denisenko V. V., Evteeva K.S. Data protection during transmission over wireless communication channels. *Mezhdunarodnyi zhurnal gumanitarnykh i estestvennykh nauk = International Journal of Humanities and Natural Sciences*. 2019;(8-2):35–38. (In Russ.)

3. Parinov M.V., Vetokhin V.V., Fedorov S.M. Analysis of the possibilities and methods of modernization of control, navigation and communication systems of unmanned aerial vehicles for industrial purposes using the example of DJI products. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta = Bulletin of Voronezh State Technical University*. 2023;(6):147–155. (In Russ.)

4. Bulatova A.R. Quantum cryptography and quantum computing. *Vestnik Penzenskogo gosudarstvennogo universiteta = Bulletin of Penza State University*. 2025;(1):11–14. (In Russ.)

5. Bukashkin S.A., Cherepnev M.A. Quantum d0evices in cryptography. *International Journal of Open Information Technologies*. 2023;11(1):104–108. (In Russ.)

6. Vydrin D.F., Sitdikov D.R. Basic parameters of the LoRaWAN wireless technology. *Academy*. 2019;(2):22–24. (In Russ.)

7. Murtazin M. M. Data security of the LORAWAN energy efficient network. *Elektronnaya nauka = Electronic Science*. 2022;(2):2–8. (In Russ.)

8. Oleinikova A.V., Surudin D.S., Shafeev D.E. Quantum computers: hopes and reality. *Perspektivy razvitiya informatsionnykh tekhnologii = Prospects for the Development of Information Technology*. 2016;(30):145–153. (In Russ.)

9. Dovgal V.A. Integration of networks and computing for building a drone swarm control system as a network management system. *Vestnik Adygeiskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki = Bulletin of the Adygea State University. Series 4: Natural, Mathematical and Technical Sciences*. 2022;(1):62–76. (In Russ.)

10. Dovgal V.A., Osmani K.A. Development of a system for extending the range of an unmanned aerial vehicle using LORA wireless communication technology. *Vestnik Adygeiskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskie nauki = Bulletin of the Adygea State University. Series 4: Natural, mathematical and technical sciences*. 2022;3:69–76. (In Russ.)

11. Murtazin M.M. Data security of the LORAWAN energy efficient network. *Electronic Science*. 2022;(2):2–8. (In Russ.)

12. Serikova Yu.I., Malygina E.A. Vulnerabilities of cryptographic systems with various protocols of quantum key distribution and the key role of biometrics in quantum cryptography. *Universum: Technical Sciences*. 2017;(11):13–15. (In Russ.)

13. Oleinikova A.V., Surudin D.S., Shafeev D.E. Quantum computers: hopes and reality. *Prospects for the development of information technology*. 2016;(30):145–153. (In Russ.)

14. Alempyev M.Yu., Semenova A.E., Koptev D.S., Dovbnya V.G. Assessing the feasibility of using a radio communication channel to transmit video information between an unmanned underwater vehicle and a remote control. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*. 2025;15(1):64–78. (In Russ.) https://doi.org/10.21869/2223-1536-2025-15-1-64-78

15. Alempyev M.Yu., Semenova A.E., Koptev D.S., Dovbnja V.G. Estimating the flight range and video transmission performance of an unmanned aerial vehicle (UAV) for emergencies monitored in complex meteorological conditions. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*. 2024;14(2):21–39. (In Russ.) https://doi.org/10.21869/2223-1536-2024-14-2-21-39

16. Leushin A.V. LoRa as a new type of modulation. Operating principle, basic parameters, noise immunity. *Tekhnika radiosvyazi = Radio communication technology*. 2022;(2):28–42. (In Russ.)

17. Alempyev M.Yu., Semenova A.E., Koptev D.S., et al. Using a radio beacon direction finder on an unmanned aerial vehicle in search and rescue operations. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika, informatika. Meditsinskoe priborostroenie = Proceedings of the Southwest State University. Series: Control, Computer Engineering, Information Science. Medical Instruments Engineering*.. 2024;4(4):129–145. (In Russ.) https://doi.org/10.21869/2223-1536-2024-14-4-129-145

Информация об авторах / Information about the Authors

Алемпьев Михаил Юрьевич, аспирант кафедры космического приборостроения и систем связи, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: mihail.alempiev@mail.ru, ORCID: 0009-0009-6412-7899

Mikhail Y. Alempiev, Postgraduate at the Department of Space Instrumentation and Communication Systems, Southwest State University, Kursk, Russian Federation, e-mail: mihail.alempiev@mail.ru, ORCID: 0009-0009-6412-7899

Коптев Дмитрий Сергеевич, старший преподаватель кафедры космического приборостроения и систем связи, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: d.s.koptev@mail.ru, ORCID: 0000-0002-7759-579X

Dmitry S. Koptev, Senior Lecturer of the Department of Space Instrumentation and Communication Systems, Southwest State University, Kursk, Russian Federation, e-mail: d.s.koptev@mail.ru, ORCID: 0000-0002-7759-579X

Довбня Виталий Георгиевич, доктор технических наук, доцент, профессор кафедры космического приборостроения и систем связи, Юго-Западный государственный университет, г. Курск, Российская Федерация, e-mail: vit_georg@mail.ru

Vitaly G. Dovbnya, Doctor of Sciences (Engineering), Associate Professor, Professor of the Department of Space Instrumentation and Communication Systems, Southwest State University, Kursk, Russian Federation, e-mail: vit_georg@mail.ru

Ревякина Мария Олеговна, кандидат технических наук, ведущий научный сотрудник лаборатории молекулярной, трансляционной и цифровой кардиоиммунологии, Орловский государственный университет имени И. С. Тургенева, г. Орёл, Российская Федерация, e-mail: revyakina_masha@mail.ru, ORCID: 0000-0003-1593-5290

Maria O. Revyakina, Candidate of Sciences (Engineering), Leading Researcher at the Laboratory of Molecular, Translational and Digital Cardioimmunology, Orel State University named after I. S. Turgenev, Orel, Russian Federation, e-mail: revyakina_masha@mail.ru, ORCID: 0000-0003-1593-5290