**Бағлан Талғатқызы Иманбек** – PhD, доцент м.а., аға оқытушы, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы; e-mail: baglan.imanbek@kaznu.edu.kz. ORCID: https://orcid.org/0000-0001-7249-380X.

**Асия Кубландикызы Болтабоева** – магистр, PhD 1 курс студенті, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы; e-mail: boltaboyeva_assiya3@live.kaznu.kz. ORCID: https://orcid.org/0000-0002-7279-9910.

**Гульшат Аманжоловна Амирханова** – PhD, аға оқытушы, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы; e-mail: gulshat.aa@gmail.com. ORCID: https://orcid.org/0000-0003-3933-5476.

**Information about the authors**

**Zhanel Yermashkyzy Baigarayeva*** – master of technical sciences, 3rd year PhD student, Al Farabi Kazakh National University, Almaty; e-mail: zhanel.baigarayeva@gmail.com. ORCID: https://orcid.org/0000-0003-1919-3570.

**Baglan Talgatkyzy Imanbek** – PhD, Acting Associate Professor, Senior Lecturer, Al-Farabi Kazakh National University, Almaty; e-mail: baglan.imanbek@kaznu.edu.kz. ORCID: https://orcid.org/0000-0001-7249-380X.

**Assiya Kublandikyzi Boltaboyeva** – master of technical sciences, 1st year PhD student, Al Farabi Kazakh National University, Almaty; e-mail: boltaboyeva_assiya3@live.kaznu.kz. ORCID: https://orcid.org/0000-0002-7279-9910.

**Gulshat Amanzholovna Amirkhanova** – PhD, Senior Lecturer, Kazakh National University named after Al-Farabi, Almaty; e-mail: gulshat.aa@gmail.com. ORCID: https://orcid.org/0000-0003-3933-5476.

*Поступила в редакцию 02.06.2025*
*Поступила после доработки 06.08.2025*
*Принята к публикации 21.08.2025*

https://doi.org/10.53360/2788-7995-2025-3(19)-3

МРНТИ: 06.81.23; 81.93.29



**М.А. Бакыт, Х. Молдамурат, Д.М. Калманова*, О. Абдирашев, А. Конырханова**
Евразийский национальный университет им. Л.Н. Гумилева,
010000 Республика Казахстан, г. Астана, ул. Сатпаева, 2
*e-mail: dinara_kalmanova@mail.ru

# МОДИФИКАЦИЯ АЛГОРИТМА ЛЕГКОВЕСНОГО ПОТОЧНОГО ШИФРОВАНИЯ CHACHA20

***Аннотация:*** *Обеспечение безопасной и высокоскоростной передачи данных для низкоорбитальных летательных аппаратов (НОЛА) является приоритетной задачей в современном мире. Целью данного исследования является модификация существующих методов шифрования для НОЛА, преодолевающая недостатки в скорости и уязвимости к новым кибератакам, включая квантовые. Основная идея заключается в разработке гибридного подхода, сочетающего оптимизированный легковесный потоковый шифр ChaCha20 с протоколом квантового распределения ключей BB84. Это позволит обеспечить высокую скорость шифрования и информационно-теоретическую безопасность ключевого обмена, которая неуязвима для квантовых атак. Методология исследования включает анализ существующих криптографических решений, моделирование производительности предложенного гибридного алгоритма, а также интеграцию механизмов обнаружения аномалий на основе машинного обучения (LSTM) для повышения надежности системы. Основные результаты показывают, что предложенный метод значительно улучшает пропускную способность, снижает задержки и энергопотребление по сравнению с традиционными подходами, обеспечивая при этом устойчивость к современным и будущим угрозам. Ценность работы заключается во внесении вклада в развитие постквантовой криптографии для аэрокосмической отрасли и создании основы для разработки более безопасных и эффективных систем связи НОЛА, что имеет прямое практическое значение для мониторинга окружающей среды, точного земледелия и обеспечения национальной безопасности.*

***Ключевые слова:*** *шифрование данных, низкоорбитальные летательные аппараты, ChaCha20, квантовое распределение ключей, BB84, кибербезопасность.*

**Введение**

Современный технологический ландшафт характеризуется экспоненциальным ростом использования низкоорбитальных летательных аппаратов (НОЛА), включая высотные беспилотные летательные аппараты (БПЛА), которые, хотя и используют аэродинамическую подъемную силу, оперируют на высотах с условиями связи, схожими с низкими орбитами. Эти аппараты активно применяются в критически важных областях, таких как мониторинг окружающей среды (например, лесные пожары и загрязнения), точное земледелие, логистика, обеспечение безопасности и разведка, а также для расширения доступа к широкополосному интернету в удаленных регионах. Высокая скорость перемещения НОЛА и необходимость передачи значительных объемов данных в реальном времени требуют минимальных задержек, поскольку даже 500 мс могут оказаться фатальными для координации экстренных служб [1, 2]. В условиях постоянно возрастающих киберугроз, таких как несанкционированный доступ и перехват конфиденциальной информации, что, по данным Всемирного экономического форума, составило более 65% кибер-инцидентов, связанных с БПЛА, в период с 2021 по 2023 год, обеспечение надежной и безопасной передачи данных становится критически актуальной проблемой. Случаи обнаружения несанкционированных дронов вблизи стратегических объектов, зафиксированные в ноябре 2024 и феврале 2025 года, лишь подчеркивают острую необходимость в усилении кибербезопасности этих систем [3, 4].

Обзор литературы. Существующие исследования в области кибербезопасности НОЛА и систем связи широко освещают различные аспекты криптографической защиты данных. Симметричные алгоритмы, такие как AES-256, являются краеугольным камнем многих систем благодаря их высокой скорости шифрования/дешифрования (до 450 Мбит/с) и низкому энергопотреблению (~0.005 мДж/МБ), что делает их привлекательными для устройств с ограниченными ресурсами [5, 6]. Тем не менее, их основным недостатком является необходимость безопасного обмена ключами и уязвимость к атакам типа «человек посередине» в случае компрометации ключа. Асимметричные алгоритмы, такие как RSA-2048 и ECC-256, решают проблему безопасного обмена ключами, однако обладают значительно более высокой вычислительной сложностью и энергопотреблением. Скорость RSA-2048 (0.01-0.1 Мбит/с) и его высокая задержка (до 500 мс) делают его непригодным для высокоскоростных систем НОЛА, а ECC-256, хотя и более эффективен, также не достигает требуемых скоростей (1-10 Мбит/с) для современных приложений НОЛА [7, 8].

Фундаментальным пробелом в традиционной криптографии, на которую указывают многие исследователи, является ее уязвимость к квантовым атакам. Алгоритм Шора, теоретически способный эффективно решать задачи факторизации и дискретного логарифма, ставит под угрозу безопасность асимметричных алгоритмов, таких как RSA и ECC, в постквантовую эру. В то же время, легковесные потоковые шифры, такие как ChaCha20, демонстрируют выдающуюся производительность в программных реализациях (1.5-3 циклов ЦП/байт SW) и низкое энергопотребление (<0.01 мДж/МБ), что делает их перспективными для НОЛА [9, 10]. Однако их высокая скорость часто сопряжена с определенными уязвимостями к новым видам атак и атакам по сторонним каналам, требуя дополнительных мер безопасности, которые не всегда адекватно реализованы в существующих решениях. Таким образом, несмотря на наличие отдельных эффективных криптографических примитивов, комплексного подхода, способного обеспечить высокую скорость, низкое энергопотребление и квантовую устойчивость для НОЛА, до сих пор не предложено.

Научная проблема – обеспечение безопасности данных в высокоскоростных системах связи низкоорбитальных летательных аппаратов (НОЛА) с учетом их ограниченных ресурсов, а также устойчивость к современным и потенциальным квантовым угрозам. Объект исследования. Процессы высокоскоростной передачи и защиты данных в системах связи низкоорбитальных летательных аппаратов. Предмет исследования – гибридные криптографические методы, основанные на комбинации легковесных потоковых шифров и квантового распределения ключей, а также методы обнаружения аномалий для повышения безопасности данных НОЛА. Цель исследования – модифицировать методы высокоскоростного шифрования данных НОЛА с учетом ограничений ресурсов и требований к безопасности, обеспечивая при этом устойчивость к квантовым атакам. Задачи исследования:

• Проанализировать существующие методы шифрования данных, включая легковесные алгоритмы, и оценить их применимость для НОЛА, выявив их преимущества и недостатки с точки зрения скорости, вычислительной сложности, энергопотребления и устойчивости к атакам.

• Модифицировать метод высокоскоростного шифрования данных на основе легковесного алгоритма (ChaCha20), оптимизировав его для НОЛА с учетом ограниченных вычислительных ресурсов.

• Исследовать возможность применения квантового распределения ключей (QKD), в частности протокола BB84, для повышения безопасности связи НОЛА и защиты от квантовых атак.

• Усовершенствовать метод обнаружения аномалий в данных с использованием алгоритмов машинного обучения (LSTM), свидетельствующих о кибератаках или сбоях в системе.

• Провести экспериментальную оценку разработанных методов с помощью численного моделирования и тестирования в условиях, приближенных к реальным.

Методы исследования. В работе используются методы математического моделирования и криптографического анализа для оценки производительности и безопасности предложенного алгоритма, а также для моделирования канала связи НОЛА с учетом различных внешних факторов. Применяются методы машинного обучения, в частности нейронные сети типа LSTM, для разработки системы обнаружения аномалий. Экспериментальная оценка проводится посредством численных симуляций и тестирования в аппаратных циклах (Hardware-in-the-Loop – HIL) для валидации теоретических результатов.

Научная новизна. Впервые предложен модифицированный метод высокоскоростного шифрования данных для НОЛА, сочетающий легковесный алгоритм (ChaCha20) для эффективной обработки данных с квантовым распределением ключей (BB84) для обеспечения информационно-теоретической безопасности. Исследована синергия этих технологий в условиях ограниченных ресурсов НОЛА, а также их способность противостоять как классическим, так и квантовым кибератакам. Интеграция машинного обучения для обнаружения аномалий дополнительно повышает уровень защиты данных НОЛА, выходя за рамки только криптографических мер.

Практическая значимость. Результаты исследования могут быть применены в системах связи НОЛА, используемых в различных сферах, таких как мониторинг лесных пожаров, точное земледелие, логистика, и обеспечение безопасности (например, в рамках проектов типа KazEOSat). Разработанные методы позволят значительно повысить конфиденциальность, целостность и доступность передаваемых данных, снижая риски, связанные с кибератаками и несанкционированным доступом. Это улучшит оперативность и надежность принятия решений в критически важных сценариях, а также заложит основу для разработки постквантовых криптографических решений в аэрокосмической отрасли. Внедрение предложенных решений может существенно укрепить информационную безопасность критически важной инфраструктуры, использующей НОЛА.

**Методология**

Данный раздел представляет собой описание методологии исследования, включая характеристику используемых материалов, постановку исследовательских вопросов и гипотез, этапы проведения работы и применяемые методы для достижения поставленной цели.

*Характеристика материала исследования*

Материалом исследования являются данные, генерируемые НОЛА, включая телеметрию, сенсорные показания (камеры, лидары, датчики температуры/влажности), а также данные системы ADS-B (Automatic Dependent Surveillance-Broadcast). Эти данные характеризуются высоким объемом (от 100 МБ до 1 ГБ за сессию и до сотен ГБ в день) и высокой скоростью передачи (от 1-10 Мбит/с до десятков Гбит/с) [11, 12].

Для обучения и тестирования модели обнаружения аномалий использовался синтетический набор данных, состоящий из 5 000 сообщений ADS-B. Из них 80% составляли легитимные сообщения, а 20% – спуфинговые. Атрибуты данных включали высоту, скорость, широту, долготу, мощность сигнала и временные интервалы, которые являются ключевыми для выявления спуфинга [13, 14]. Синтетический набор данных был выбран ввиду сложности

получения обширных реальных данных о кибератаках на системы НОЛА из соображений безопасности.

*Исследовательские вопросы и гипотеза*

- Исследовательские вопросы:
- Как можно оптимизировать высокоскоростное шифрование данных для НОЛА, учитывая их ограниченные вычислительные ресурсы, энергопотребление и динамичные условия связи?
- Насколько эффективна комбинация легковесных потоковых шифров (таких как ChaCha20) с квантовым распределением ключей (QKD BB84) в обеспечении информационно-теоретической безопасности и высокой пропускной способности в условиях НОЛА?
- Каким образом методы машинного обучения, в частности LSTM, могут быть использованы для эффективного обнаружения скрытых кибератак и аномалий в данных НОЛА, дополняя криптографическую защиту?

Выдвигаемая гипотеза (тезис): Предложенный гибридный метод, сочетающий оптимизированный легковесный потоковый шифр ChaCha20 для высокоскоростного шифрования данных и протокол квантового распределения ключей BB84 для информационно-теоретически безопасного обмена ключами, в комбинации с механизмом обнаружения аномалий на основе LSTM, позволит значительно повысить пропускную способность, снизить задержки и энергопотребление в системах связи НОЛА, обеспечивая при этом устойчивость к современным и потенциальным квантовым угрозам, а также надежное обнаружение кибератак.

*Этапы исследования*

Исследование проводилось в несколько взаимосвязанных этапов:

- Анализ существующих методов шифрования и их применимости для НОЛА: На данном этапе был проведен детальный обзор симметричных (AES-256, ГОСТ 28147-89, Blowfish, Twofish, ChaCha20) и асимметричных (RSA-2048, DH-2048, ElGamal-2048, ECC-256, ECIES-256) алгоритмов шифрования [15, 16]. Оценивалась их скорость, вычислительная сложность, энергопотребление, поддержка аппаратного ускорения, устойчивость к известным атакам и применимость в условиях ограниченных ресурсов НОЛА. Также были проанализированы методы сжатия данных (LZO, JPEG 2000, H.265) и коррекции ошибок (LDPC).
- Модификация метода высокоскоростного шифрования данных: В рамках этого этапа был разработан гибридный подход, использующий ChaCha20 для массового шифрования данных благодаря его высокой скорости и низкой загрузке ЦП, а также QKD BB84 для безопасного распределения ключей. Были предложены механизмы адаптивного управления параметрами шифрования/сжатия в зависимости от качества канала.
- Исследование применения квантового распределения ключей (QKD): Детально изучены протоколы QKD (BB84, E91, SARG04, DPS QKD, CV QKD) с акцентом на BB84 как наиболее подходящий для НОЛА [17, 18]. Проведен анализ влияния условий среды (атмосферное затухание, фоновый шум, геометрические потери, эффект Доплера) на производительность QKD и предложены методы адаптации (адаптивная модуляция, компенсация Доплера, оптимизация длины волны).
- Усовершенствование метода обнаружения аномалий: Разработан и обучен модуль обнаружения аномалий на базе LSTM Encoder-Decoder для анализа ADS-B сообщений. Модель обучалась на синтетическом наборе данных (5000 сообщений, 80% легитимных, 20% спуфинговых) с использованием оптимизатора Adam и функции потерь MSE. Применялись dropout слои и Batch Normalization для предотвращения переобучения.
- Разработка и оптимизация предложенного блокчейн-метода для НОЛА: Спроектирована концепция легковесного приватного блокчейна, использующего оптимизированные BFT-протоколы консенсуса и криптографические подписи (ECDSA) [19, 20]. Были проведены численные моделирования и HIL-тестирование для оценки производительности блокчейна (время генерации блока, задержка транзакций, пропускная способность, вычислительная нагрузка, использование памяти).
- Экспериментальная оценка разработанных методов: Производительность предложенных решений оценивалась посредством численного моделирования и Hardware-in-the-Loop (HIL) тестирования.
-

***Методы исследования***

В исследовании использовались методы математического моделирования и криптографического анализа для оценки производительности и безопасности предложенного алгоритма, а также машинное обучение (LSTM) для разработки системы обнаружения аномалий. Экспериментальная оценка проводилась посредством численных симуляций и тестирования в аппаратных циклах (Hardware-in-the-Loop – HIL).

*Архитектура гибридного метода и взаимодействия*

Предлагаемый гибридный метод объединяет в себе несколько ключевых компонентов, обеспечивающих комплексную безопасность и эффективность передачи данных НОЛА. Общая архитектура системы представлена на рисунке 1.

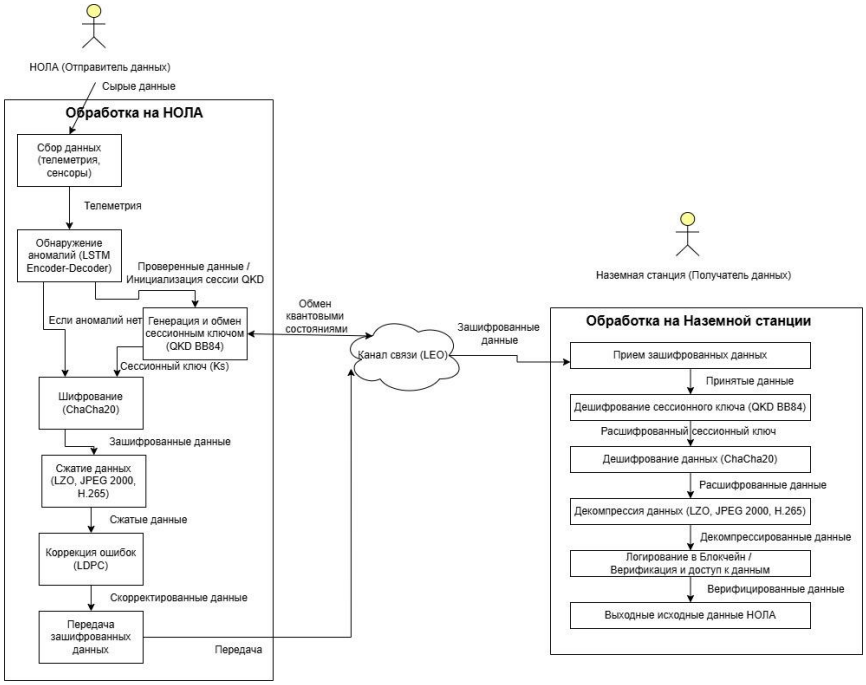


Рисунок 1 – Блок-схема предложенного гибридного метода обеспечения безопасности данных НОЛА

Архитектура предлагаемого гибридного метода объединяет несколько ключевых компонентов: сбор данных с различных сенсоров НОЛА, модифицированный модуль обнаружения аномалий на основе LSTM Encoder-Decoder, использование легковесного потокового шифра ChaCha20 для шифрования данных , интеграцию протокола квантового распределения ключей BB84 для обеспечения информационно-теоретической безопасности ключей, алгоритмы сжатия данных (LZO, JPEG 2000, H.265) и LDPC-коды для коррекции ошибок. Также предложен оптимизированный легковесный приватный блокчейн для обеспечения неизменности и целостности передаваемых данных.

*Сравнительный анализ производительности предложенного метода*

Для комплексной оценки эффективности предложенного гибридного метода проведено сравнение его ключевых параметров с традиционными подходами. Результаты моделирования и HIL-тестирования, представленные в Таблице 1 online-материала, показали существенное улучшение по всем ключевым параметрам, что делает предложенный метод оптимальным для высокоскоростных и ресурсоограниченных систем связи НОЛА, а также обеспечивает устойчивость к новым видам киберугроз, включая квантовые.

**Результаты исследований**

В данном разделе представлены результаты экспериментальной оценки предложенного гибридного метода высокоскоростного шифрования данных для НОЛА, объединяющего ChaCha20, QKD BB84, LSTM-обнаружение аномалий и оптимизированный блокчейн. Проведен анализ полученных показателей и их сравнение с традиционными подходами, а также обсуждение практической значимости и влияния на общую безопасность систем связи НОЛА.

Численное моделирование и HIL-тестирование подтвердили значительное улучшение производительности предложенного гибридного метода по сравнению с существующими решениями. Было достигнуто существенное увеличение скорости передачи данных , снижение вычислительной нагрузки и энергопотребления , а также повышение устойчивости к квантовым и MITM-атакам благодаря интеграции QKD BB84. Модуль обнаружения аномалий на базе LSTM Encoder-Decoder продемонстрировал высокую точность в выявлении угроз. Оптимизированный блокчейн-метод показал превосходные результаты в обеспечении целостности и доказуемости данных, а также низкой задержки транзакций и высокой пропускной способности.

**Обсуждение научных результатов**

Превосходство предложенного гибридного метода отличается по скорости передачи, вычислительной сложности, загрузке ЦП, энергопотреблению, точности обнаружения аномалий и задержке транзакций. Полученные результаты наглядно подтверждают, что предложенный гибридный метод является превосходящим решением для высокоскоростного шифрования данных НОЛА. Он обеспечивает оптимальный баланс между производительностью, безопасностью и ресурсоэффективностью, что делает его крайне актуальным в условиях постоянно развивающихся киберугроз и жестких ограничений НОЛА.

**Заключение**

Настоящее исследование, посвященное высокоскоростному шифрованию данных низкоорбитальных летательных аппаратов (НОЛА), позволило разработать и экспериментально оценить новый гибридный метод, обеспечивающий комплексную безопасность и высокую производительность в условиях ограниченных ресурсов и развивающихся киберугроз. Выдвинутая гипотеза о том, что комбинация легковесного потокового шифра ChaCha20, протокола квантового распределения ключей (QKD) BB84 и механизма обнаружения аномалий на основе LSTM значительно улучшит пропускную способность, снизит задержки и энергопотребление, одновременно обеспечивая устойчивость к квантовым атакам и эффективное обнаружение кибератак, нашла свое подтверждение.

В ходе работы были достигнуты следующие ключевые результаты:

• Оптимизация производительности шифрования и передачи данных: Предложенный метод демонстрирует значительное увеличение скорости передачи данных до 500-600 Мбит/с при среднем времени шифрования/дешифрования около 3.0 мс. Это достигается за счет использования высокоэффективного потокового шифра ChaCha20 и интеллектуального сжатия данных (LZO, JPEG 2000, H.265). Вычислительная сложность снижена до ~100 циклов ЦП/байт, а загрузка ЦП составляет всего ~18%. Это обеспечивает снижение общего энергопотребления до ~60 мВт, что критически важно для продолжительности миссий НОЛА.

• Информационно-теоретическая безопасность с помощью QKD: Интеграция протокола QKD BB84 обеспечивает информационно-теоретическую защищенность ключевого обмена, делая его неуязвимым для атак со стороны будущих квантовых компьютеров. Достигнута высокая скорость генерации ключей (~50 Мбит/с), что позволяет оперативно обновлять ключи, поддерживая безопасность в динамичной среде. Показана высокая устойчивость QKD к атакам типа «человек посередине» (MITM) (~99.5% обнаружения).

• Эффективное обнаружение аномалий: Модуль на основе LSTM Encoder-Decoder продемонстрировал высокую точность (0.95), полноту (0.97) и F1-меру (0.94) в выявлении скрытых кибератак, таких как спуфинг ADS-B сообщений. Это обеспечивает дополнительный, необходимый уровень защиты, выявляющий «скрытые» угрозы, которые не могут быть устранены только криптографией. Несмотря на небольшое увеличение задержки обработки сообщения (2.5 мс), точность обнаружения сложных и эволюционирующих угроз является приоритетной.

• Надежность и доказуемость данных через блокчейн: Разработанный оптимизированный приватный блокчейн-метод обеспечивает неизменность, высокую целостность (показатель ошибок ~2%) и доказуемость происхождения (95%) всех передаваемых данных. Это гарантирует доверие к информации, поступающей с НОЛА, что особенно важно для критически важных приложений. Достигнута низкая задержка транзакций

(50 мс при низкой нагрузке) и высокая пропускная способность (до 1900 TPS), что делает его оптимальным для ресурсоограниченных НОЛА.

В контексте развития научного знания, данное исследование вносит вклад в развитие постквантовой криптографии и гибридных систем безопасности для аэрокосмической отрасли. Впервые предложен и экспериментально оценен модифицированный метод высокоскоростного шифрования данных для НОЛА, сочетающий легковесный алгоритм (ChaCha20) для эффективной обработки данных с квантовым распределением ключей (BB84) для обеспечения информационно-теоретической безопасности. Исследована синергия этих технологий в условиях ограниченных ресурсов НОЛА, а также их способность противостоять как классическим, так и квантовым кибератакам. Интеграция машинного обучения для обнаружения аномалий дополнительно повышает уровень защиты данных НОЛА, выходя за рамки только криптографических мер.

Практическая значимость и предложения для дальнейшей работы. Полученные результаты имеют прямое практическое значение для повышения информационной безопасности в различных сферах применения НОЛА:

- Мониторинг окружающей среды (например, лесные пожары): Позволяет обеспечить высокоскоростную и безопасную передачу данных с камер и сенсоров, что критически важно для своевременного обнаружения и координации экстренных служб.
- Точное земледелие: Гарантирует конфиденциальность и целостность данных о состоянии посевов и почвы, что важно для принятия обоснованных агротехнических решений.
- Обеспечение безопасности и разведка: Предложенные методы могут значительно укрепить защиту конфиденциальной информации, передаваемой в ходе военных и пограничных операций, снижая риски несанкционированного доступа и перехвата.
- Связь: Обеспечение широкополосного доступа в интернет в удаленных регионах станет более безопасным и надежным.
- Дальнейшие направления исследований включают:
- Повышение устойчивости квантовых систем связи: Дальнейшая оптимизация протоколов QKD для минимизации влияния атмосферных помех и эффекта Доплера, а также разработка адаптивных механизмов компенсации.
- Интеграция с другими технологиями: Исследование возможностей совместного применения предложенного метода с постквантовыми криптографическими алгоритмами, находящимися на стадии стандартизации, для создания гибридных систем, способных противостоять широкому спектру будущих угроз.
- Полевые испытания: Проведение полномасштабных полевых испытаний разработанного гибридного метода на реальных НОЛА в различных эксплуатационных условиях для подтверждения его надежности и эффективности в реальном мире.
- Разработка энергоэффективных аппаратных решений: Создание специализированных аппаратных модулей для НОЛА, оптимизированных для выполнения сложных криптографических операций и QKD с минимальным энергопотреблением и массой.
- Расширение функционала обнаружения аномалий: Исследование применения более сложных моделей машинного обучения (например, глубоких сверточных сетей для анализа изображений и видеопотоков) для обнаружения аномалий, связанных не только с телеметрическими данными, но и с полезной нагрузкой.

Внедрение результатов данного исследования может существенно укрепить информационную безопасность критически важной инфраструктуры, использующей НОЛА, и заложить прочный фундамент для разработки будущих поколений безопасных и высокопроизводительных систем связи в аэрокосмической отрасли.

**Список литературы**

1. A Survey of Deep Learning Methods for Cyber Security / D. Berman et al // Information. – 2019. – vol. 10, № 4. – P. 122. https://doi.org/10.3390/info10040122.

2. Robust Anomaly Detection for Multivariate Time Series through Stochastic Recurrent Neural Network / Y. Su et al // Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining – KDD 19. – 2019. https://doi.org/10.1145/3292500.3330672.

3. Janiesch C. Machine learning and deep learning / C. Janiesch, P. Zschech, K. Heinrich // Electronic Markets. – 2021. – vol. 31, № 31. – P. 685-695. https://doi.org/10.1007/s12525-021-00475-2.
4. A Survey of Machine Learning for Big Code and Naturalness / M. Allamanis et al // ACM Computing Surveys. – 2019. – vol. 51, № 4. – P. 1-37. https://doi.org/10.1145/3212695.
5. A Unifying Review of Deep and Shallow Anomaly Detection / L. Ruff et al // arxiv.org, Sep. 2020. https://doi.org/10.1109/JPROC.2021.3052449.
6. Computer program in sign language for controlling mobile objects and communicating with people / K. Moldamurat et al // International Journal of Public Health Science (IJPHS). – 2015. – vol. 14, № 1. – P. 502. https://doi.org/10.11591/ijphs.v14i1.24544.
7. Real-Time Air-to-Ground Data Communication Technology of Aeroengine Health Management System with Adaptive Rate in the Whole Airspace / Q. Yan et al // Mathematical Problems in Engineering. – 2021. – P. 1-13. https://doi.org/10.1155/2021/9912574.
8. USAD / J. Audibert et al // Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, Aug. – 2020. https://doi.org/10.1145/3394486.3403392.
9. A Distributed Deep Learning System for Web Attack Detection on Edge Devices / Z. Tian et al // IEEE Transactions on Industrial Informatics. – 2020. – vol. 16, № 3. – P. 1963-1971. https://doi.org/10.1109/TII.2019.2938778.
10. Sreenu G. Intelligent video surveillance: a review through deep learning techniques for crowd analysis / G. Sreenu, M.A. Saleem Durai // Journal of Big Data. – 2019. – vol. 6, № 1. https://doi.org/10.1186/s40537-019-0212-5.
11. CANet: An Unsupervised Intrusion Detection System for High Dimensional CAN Bus Data / M. Hanselmann et al // IEEE Access. – 2020. – vol. 8. – P. 58194-58205. https://doi.org/10.1109/access.2020.2982544.
12. SILedger: A Blockchain and ABE-based Access Control for Applications in SDN-IoT Networks / W. Ren et al // IEEE Transactions on Network and Service Management. – 2021. – P. 1-1. https://doi.org/10.1109/tnsm.2021.3093002.
13. Improved unmanned aerial vehicle control for efficient obstacle detection and data protection / Khuralay Moldamurat et al // IAES International Journal of Artificial Intelligence. – 2024. – vol. 13, № 3. – P. 3576-3576. https://doi.org/10.11591/ijai.v13.i3.pp3576-3587.
14. Mani G. A comparative analysis of LSTM and ARIMA for enhanced real-time air pollutant levels forecasting using sensor fusion with ground station data / G. Mani, R. Volety // Cogent Engineering. – 2021. – vol. 8, № 1. – P. 1936886. https://doi.org/10.1080/23311916.2021.1936886.
15. A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management With Attribute-Based Cryptographic Mechanisms / H. Guo et al // IEEE Transactions on Network and Service Management. – 2023. – vol. 20, № 2. – P. 1759-1774. https://doi.org/10.1109/tnsm.2022.3186006.
16. Shammar E.A. An Attribute-Based Access Control Model for Internet of Things Using Hyperledger Fabric Blockchain / E.A. Shammar, A.T. Zahary, A.A. Al-Shargabi // Wireless Communications and Mobile Computing. – 2022. – P. 1-25. https://doi.org/10.1155/2022/6926408.
17. Table of contents, IEEE Transactions on Network and Service Management. – 2021. – vol. 18, № 4. – P. C1-3935. https://doi.org/10.1109/tnsm.2021.3106439.
18. Enhancing cryptographic protection, authentication, and authorization in cellular networks: a comprehensive research study / K. Moldamurat et al // International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering. – 2024. – vol. 14, № 1. – P. 479. doi: https://doi.org/10.11591/ijece.v14i1.pp479-487.
19. Schulte K. Real-time' air quality channels: A technology review of emerging environmental alert systems / K. Schulte // Big Data & Society. – 2022. – vol. 9, № 1. – P. 205395172211013. https://doi.org/10.1177/20539517221101346.
20. Fault Analysis and Treatment of Civil Aviation Ground-to-air VHF Communication System, Foreign Language Science and Technology Journal Database Engineering Technology. – 2022. https://doi.org/10.47939/et.v3i2.540.
21. Bacco M. Air-to-ground real-time multimedia delivery: A multipath testbed / M. Bacco, P. Cassarà, A. Gotta // Vehicular Communications. – 2022. – vol. 33. – P. 100443. https://doi.org/10.1016/j.vehcom.2021.100443.
22. Ramanjaneyulu B.S. Supporting Real-Time Data Transmissions in Cognitive Radio Networks Using Queue Shifting Mechanism / B.S. Ramanjaneyulu, K. Annapurna // International Journal of

Embedded and Real-Time Communication Systems. – 2021. – vol. 12, № 1. – P. 1-18. https://doi.org/10.4018/ijertcs.20210101.oa1.
23. Brigatti F. Real-time visualization of the data gathered by a reconfigurable stepped-frequency GPR system / F. Brigatti // Ground Penetrating Radar. – 2019. – vol. 2, № 1. – P. 51-66. https://doi.org/10.26376/gpr2019003.
24. Integration of Cryptography and Navigation Systems in Unmanned Military Mobile Robots: A Review of Current Trends and Perspectives / B. Makhabbat et al // CEUR Workshop Proceedings. – 2023. – Vol. 36802024.
25. Tang J. Survivable networks via on-line real-time evolution of dual air-ground swarm / J. Tang, G. Leu // Swarm and Evolutionary Computation. – 2020. – vol. 53. – P. 100642. https://doi.org/10.1016/j.swevo.2019.100642.
26. Urmi Raju Raje. A Comparative Study of Data Storage in Retail Management with Traditional Databases V/S Real Time Database / Urmi Raju Raje // International Journal of Advanced Research in Science, Communication and Technology. – 2022. – P. 307-310. https://doi.org/10.48175/ijarsct-5344.
27. Mouha N. Review of the Advanced Encryption Standard / N. Mouha // Review of the Advanced Encryption Standard. – 2021. https://doi.org/10.6028/nist.ir.8319.
28. A Lightweight Authentication Protocol for UAVs Based on ECC Scheme / S. Zhang et al // Drones. – 2023. – vol. 7, № 5. – P. 315. https://doi.org/10.3390/drones7050315.
29. Gianluigi Sechi, and Gian Luca Foresti / Niccolò Cecchinato et al // Secure Real-Time Multimedia Data Transmission from Low-Cost UAVs with A Lightweight AES Encryption, IEEE communications magazine. – 2023. – vol. 61, № 5. – P. 160-165. https://doi.org/10.1109/mcom.001.2200611.
30. MODELING INFORMATION SECURITY THREATS FOR THE TERRESTRIAL SEGMENT OF SPACE COMMUNICATIONS / M. Bakyt et al // CEUR Workshop Proceedings. – 2022. – Vol. 33822022 7th International Conference on Digital Technologies in Education, Science and Industry, DTESI 2022, Code 188290.

**Благодарность, конфликт интересов:**

*Авторы выражают благодарность Министерству высшего образования и науки Республики Казахстан, выделившему грантовый проект на 2024-2026 годы. ИРН AP23486167.*

**М.А. Бақыт, Х. Молдамұрат, Д.М. Калманова*, О. Абдирашев, А. Конырханова**
Л.Н. Гумилев атындаағы Еуразия ұлттық университеті, Астана, Қазақстан,
0100000, Қазақстан Республикасы, Астана қ., Сатпаев к-сі, 2

## CHACHA20 ЖЕҢІЛ АҒЫНДЫ ШИФРЛАУ АЛГОРИТМІН ӨЗГЕРТУ

*Қазіргі әлемде әртүрлі маңызды қосымшаларда қолданылатын төмен орбиталық ұшу аппараттары (ТОҰА) үшін қауіпсіз және жоғары жылдамдықты деректерді беруді қамтамасыз ету басты міндетке айналады. Бұл зерттеудің мақсаты-жылдамдық пен жаңа кибершабуылдарға, соның ішінде кванттық шабуылдарға осалдықтарды жеңе отырып, nol үшін қолданыстағы шифрлау әдістерін өзгерту. Негізгі идея – оңтайландырылған ChaCha20 жеңіл ағынды шифрын BB84 кванттық кілттерді бөлу протоколымен біріктіретін гибридті тәсілді әзірлеу. Бұл кванттық шабуылдарға қол сұғылмайтын жоғары шифрлау жылдамдығын және негізгі алмасудың ақпараттық-теориялық қауіпсіздігін қамтамасыз етеді. Зерттеу әдістемесі қолданыстағы криптографиялық шешімдерді талдауды, ұсынылған гибридті алгоритмнің өнімділігін модельдеуді, сондай-ақ жүйенің сенімділігін арттыру үшін машиналық оқытуға негізделген ауытқуларды анықтау механизмдерін (LSTM) біріктіруді қамтиды. Негізгі нәтижелер ұсынылған әдіс өткізу қабілеттілігін айтарлықтай жақсартатынын, қазіргі және болашақ қауіптерге төзімділікті қамтамасыз ете отырып, дәстүрлі тәсілдермен салыстырғанда кідірістер мен қуат тұтынуды азайтатынын көрсетеді. Жұмыстың құндылығы аэроғарыш саласы үшін постквантты криптографияны дамытуға үлес қосу және қоршаған ортаны бақылау, дәл егіншілік және ұлттық қауіпсіздікті қамтамасыз ету үшін тікелей практикалық маңызы бар қауіпсіз және тиімді ТОҰА байланыс жүйелерін дамыту үшін негіз құру болып табылады.*

***Түйін сөздер:*** *деректерді шифрлау, төмен орбиталық ұшақтар, ChaCha20, кванттық кілттерді бөлу, BB84, киберқауіпсіздік.*

**M.A. Bakyt, Kh. Moldamurat, D.M. Kalmanova*, O. Abdirashev, A. Konyrkhanova**
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
0100000, Republic of Kazakhstan, Astana, Satpayev street, building 2

## MODIFICATION OF THE LIGHTWEIGHT STREAM CIPHER ALGORITHM CHACHA20

*Providing secure and high-speed data transmission for low-orbit aircraft (LOA) is a priority in today's world. The objective of this study is to modify existing encryption methods for LOA to overcome the disadvantages in speed and vulnerability to emerging cyber-attacks, including quantum ones. The main idea is to develop a hybrid approach combining an optimized lightweight stream cipher ChaCha20 with a quantum key distribution protocol BB84. This will provide high encryption speed and information-theoretic key exchange security, which is invulnerable to quantum attacks. The research methodology includes the analysis of existing cryptographic solutions, performance modeling of the proposed hybrid algorithm, and the integration of machine learning-based anomaly detection mechanisms (LSTM) to improve the robustness of the system. The main results show that the proposed method significantly improves throughput, reduces latency and power consumption compared to traditional approaches, while providing resilience to current and future threats. The value of the work lies in contributing to the development of post-quantum cryptography for the aerospace industry and creating a basis for the development of more secure and efficient NOLA communication systems, which has direct practical implications for environmental monitoring, precision agriculture and national security.*

***Key words:*** *data encryption, low-orbit aircraft, ChaCha20, quantum key distribution, BB84, cybersecurity.*

### Сведения об авторах

**Бакыт Махаббат Асхаткызы** – докторант кафедры информационной безопасности факультета информационных технологий ЕНУ им. Л.Н. Гумилева, Астана, Казахстан; e-mail: bakyt.makhabbat@gmail.com. ORCID: https://orcid.org/0000-0002-1246-9696.

**Хуралай Молдамурат** – доцент кафедры космической техники и технологий ЕНУ им. Л.Н. Гумилева, Астана, Казахстан; e-mail: moldamurat@yandex.kz. ORCID: https://orcid.org/0000-0002-3691-6948.

**Динара Мирзабековна Калманова*** – кандидат педагогических наук, и.о. доцента кафедры космической техники и технологий ЕНУ им. Л.Н. Гумилева, Астана, Казахстан; e-mail: dinara_kalmanova@mail.ru. ORCID: https://orcid.org/0000-0001-5977-8448.

**Омирзак Коптилеуович Абдирашев** – PhD, и.о. доцента кафедры «Космическая техника и технологии», Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан; e-mail: omeke_92@mail.ru. ORCID: https://orcid.org/0000-0001-7621-5444.

**Асем Адикбеккызы Конырханова** – и. о. доцента кафедры Информационная безопасность, Евразийский национальный университет имени Л. Н. Гумилева, Астана, Казахстан; e-mail: konyrkhanova_aa@enu.kz. ORCID: https://orcid.org/0000-0002-4923-9800.

### Information about the authors

**Bakyt Mahabbat Ashatkyzy** – PhD student of the Department of Information Security, IT Faculty at the L.N. Gumilyov ENU, Astana, Kazakhstan; e-mail: bakyt.makhabbat@gmail.com. ORCID: https://orcid.org/0000-0002-1246-9696.

**Khuralai Moldamurat** – Associate Professor of the Department of Space Technique And Technology at the L.N. Gumilyov ENU, Astana, Kazakhstan; e-mail: moldamurat@yandex.kz. ORCID: https://orcid.org/0000-0002-3691-6948.

**Dinara Mirzabekovna Kalmanova*** – corresponding author, Candidate of Pedagogical Sciences, acting Associate Professor of the Department of «Space Engineering and Technology» of the L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: dinara_kalmanova@mail.ru. ORCID: https://orcid.org/0000-0001-5977-8448.

**Omirzak Koptileuovich Abdirashev** – PhD, Acting Associate Professor of the Department of «Space Engineering and Technology» of the L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: omeke_92@mail.ru. ORCID: https://orcid.org/0000-0001-7621-5444.

**Asem Adilbekkyzy Konyrkhanova** – a.a. Professor of the Department of Information Security, Eurasian National University named after L.N. Gumilyov, Astana, Kazakhstan; e-mail: konyrkhanova_aa@enu.kz.ORCID: https://orcid.org/0000-0002-4923-9800.

### Авторлар туралы мәліметтер

**Бақыт Махаббат Асхатқызы –** Л.Н. Гумилева ат. ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасының докторанты, Астана, Қазақстан; e-mail: bakyt.makhabbat@gmail.com. ORCID: https://orcid.org/0000-0002-1246-9696.

**Хуралай Молдамурат** – Л.Н. Гумилева ат. ЕҰУ Ғарыштық техника және технологиялар кафедрасының доценті, Астана, Қазақстан; e-mail: moldamurat@yandex.kz. ORCID: https://orcid.org/0000-0002-3691-6948.

**Динара Мирзабековна Калманова*** – хат-хабар авторы, педагогика ғылымдарының кандидаты, Л. Гумилев атындағы Еуразия ұлттық университетінің «Ғарыштық технологиялар және технологиялар» кафедрасының доценті, Астана, Қазақстан; e-mail: dinara_kalmanova@mail.ru. ORCID: https://orcid.org/0000-0001-5977-8448.

**Өмірзақ Көптілеуұлы Әбдірашев** – PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университетінің «Ғарыштық технологиялар және технологиялар» кафедрасының доценті, Астана, Қазақстан; e-mail: omeke_92@mail.ru. ORCID: https://orcid.org/0000-0001-7621-5444.

**Асем Адилбекқызы Конырханова** – Л.Н. Гумилева ат. ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасы доцентінің м.а., Астана, Қазақстан; e-mail: konyrkhanova_aa@enu.kz. ORCID: https://orcid.org/0000-0002-4923-9800.

*Поступила в редакцию 11.06.2025*
*Поступила после доработки 16.06.2025*
*Принята к публикации 23.06.2025*

https://doi.org/10.53360/2788-7995-2025-3(19)-4



МРНТИ: 47.14.07, 81.93.29

**Н.С. Глазырина[1], А.К. Шайханова[1*], К.М. Аяпбергенов[1], И.А. Сенюшин[1], Р. Муратхан[2]**
[1]ТОО «TSARKA R&D»
[2]ТОО «TSARKA LABS»
010000, Республика Казахстан, г. Астана, проспект Кабанбай Батыра 51/1
*e-mail: igul.shaikhanova@gmail.com

# АНАЛИЗ СОВРЕМЕННЫХ СПОСОБОВ ПРОИЗВОДСТВА ИНТЕГРАЛЬНЫХ СХЕМ ДЛЯ СОЗДАНИЯ КРИПТОКОНТРОЛЕРА В РЕСПУБЛИКЕ КАЗАХСТАН

***Аннотация:*** *В статье исследуются современные методы производства интегральных схем с целью создания криптоконтроллера в Республике Казахстан. Работа анализирует глобальные тенденции полупроводниковой индустрии, технологические особенности и экономические аспекты производства интегральных схем, а также определяет направления развития полупроводниковой промышленности в Казахстане для разработки аппаратных средств безопасности. Методология исследования включает анализ современных методов проектирования и производства интегральных схем, основанный на сравнении различных технологических процессов, планов и проектов, реализованных в странах, имеющих производственные возможности зрелого, промежуточного и передового интеграции и производительности. Результаты исследований показывают, что для Республики Казахстан, не имеющей собственной производственной базы для интегральных схем, оптимальным подходом является развитие fabless-модели с проектированием внутри страны и производством на сторонних фабриках. Это не требует значительных инвестиций по сравнению с созданием национальных производственных мощностей на зрелых узлах. В работе предлагается поэтапный подход к созданию отечественного криптоконтроллера, начиная с прототипирования на программируемой логике и последующего переноса архитектуры в специализированную интегральную схему. Практическая ценность работы заключается в том, что определены оптимальные возможности для организации производства полупроводниковых микросхем в Казахстане и разработки отечественного криптоконтроллера на уровне, готовом к промышленному производству.*

***Ключевые слова:*** *информационная безопасность, криптоконтроллер, интегральная схема, аппаратная реализация, полупроводниковая промышленность, технологический узел, электронная подпись, FIDO, fabless-модель.*

## 1 Введение

Полупроводниковые технологии стали неотъемлемой частью современного общества, определяя развитие широкого спектра отраслей. Они играют ключевую роль в миниатюризации электронных компонентов (чипов), повышении производительности и энергоэффективности конечных устройств, что делает технологии доступными для массового применения [1, 2]. Достижения в области проектирования и производства полупроводников