Государственное бюджетное общеобразовательное учреждение города Москвы "Школа № 2072"

**Система передачи ключей шифрования с помощью лазера**

Участники:

Голиков Михаил, класс 11 И

Сердюков Алексей, класс 11 И

Руководитель:

Ануфриев Вадим Юльевич, тренер-преподаватель

Москва, 2024

**Оглавление**

[Реферат 3](#_Toc159151291)

[Определения 3](#_Toc159151292)

[Введение 4](#_Toc159151293)

[Цель и задачи работы 5](#_Toc159151294)

[Обоснование выбора цели проекта и способа реализации 5](#_Toc159151295)

[Структурная схема работы устройств 8](#_Toc159151296)

[Пример использования 9](#_Toc159151297)

[Блок-схема работы программ 11](#_Toc159151298)

[Планы по развитию 15](#_Toc159151299)

[Выводы 15](#_Toc159151300)

[Список литературы 16](#_Toc159151301)

# Реферат

В данном документе описан принцип работы лазерной передачи ключей шифрования для побитового засекречивания данных, а именно:

* Способ передачи самих ключей шифрации
* Цели передачи ключей и пояснение к общему принципу работы шифрования
* Принцип работы на физическом носителе

Данное способ передачи информации помогает пользователям безопасно передавать засекреченные данные, не беспокоясь о возможности их дешифровки.

# Определения

Побитовое шифрование – это метод шифрования данных, при котором каждый бит исходного сообщения преобразуется с использованием специального ключа.

Квантовый компьютер – это устройство, которое использует принципы квантовой механики для обработки информации. В отличие от классических компьютеров, которые работают на основе битов, квантовые компьютеры используют кубиты для представления и обработки данных, что позволяет им выполнять определенные задачи значительно быстрее, чем традиционные компьютеры.

РЛС – радиолокационные системы.

Arduino – это платформа для создания прототипов электронных устройств, основанная на простой микроконтроллерной плате. Arduino позволяет людям без специальных знаний в области электроники и программирования создавать интерактивные устройства, управляемые программным обеспечением.

Хэш-функция – это математическая функция, которая преобразует входные данные произвольной длины в фиксированный набор битов (хеш-значение). Хэш-функции широко используются в криптографии и информационной безопасности для проверки целостности данных, создания цифровых подписей и других целей.

# Введение

Проблема взлома ключей шифрования с помощью квантовых компьютеров актуальна в сфере криптографии и информационной безопасности. С ростом мощности квантовых компьютеров возникает реальная угроза для существующих алгоритмов шифрования, таких как RSA и ECC, которые используются в настоящее время для защиты конфиденциальной информации.

Профессиональное сообщество выражает явный запрос на решение этой проблемы, так как безопасность информации является ключевым аспектом в различных областях, включая финансы, здравоохранение, правительственные коммуникации и технологические инновации. Кроме того, потенциальные пользователи информационных систем также требуют надежных средств шифрования для защиты своих данных от возможных атак, включая атаки с использованием квантовых компьютеров.

Предложенное средство решения, такое как передача ключей шифрования через лазер со спутника с последующим кодированием каждого бита отдельным ключом, представляет собой попытку борьбы с угрозой квантового взлома. Это позволяет свести зависимость битов в зашифрованном сообщении к нулю, что делает его более устойчивым к атакам с использованием квантовых компьютеров.

На сегодняшний день существуют прототипы и аналоги систем передачи на основе фотонов (например: оптоволокно, спутниковая связь). Однако, потребность в модификации и развитии таких систем остается высокой, особенно с учетом их массового использования.

Лазерная технология для передачи ключей шифрования через спутник имеет преимущества перед интернетом в контексте квантовой криптографии. Во-первых, лазерная передача ключей обеспечивает физическую безопасность, так как попытки перехвата данных могут быть обнаружены через мониторинг изменений в световом потоке, а также использованием РЛС на физическое присутствие перехватчика между отправителем и получателем. Это делает ее более надежной в сравнении с интернет-передачей, которая подвержена угрозам атак посредством вмешательства в сеть.

# Цель и задачи работы

Способы лазерной передачи информации различны и не являются предметом исследования данной работы. Мы попытались создать систему для обучения новых специалистов, которая может быть воссоздана в самых различных условиях.

Учитывая, что в настоящее время очень хорошо распространена технология Arduino, логично использовать её для решения поставленной задачи.

Таким образом целью моей работы является разработка учебного оборудования для студентов и школьников, способного передавать данные на расстояние путем испускания лазерных импульсов.

Задачами проекта являются:

1. Создание физических устройств для передачи информации по лазерному каналу.

2. Разработка программного кода для надлежащей работы оборудования.

3. Разработка и реализация 4-х систем определения целостности отправляемых данных:

a. использование бита чётности при отправке каждого байта.

b. разделение каждого байта дополнительными битами начала и конца.

c. проверка пакета байтов используя хэш-функцию.

d. сравнение итоговой хэш-функции на наличие как отдельных ошибок в коде, так и на возможность подмены данных между спутником и пользователем.

# Обоснование выбора цели проекта и способа реализации

В наши дни уже существуют и продолжают активно развиваться технологии, связанные с квантовым миром. Одной из таких технологий является квантовых компьютер. Его особенностью является возможность одновременно обрабатывать огромное количество данных. Учитывая, что и по сей день большинство алгоритмов шифрования опираются на принцип сложности подбора простых чисел, чьё произведение будет равно ключу передачи, нам следует заранее подготовиться к угрозе нарушения информационной безопасности с помощью квантовых компьютеров. Одним из основных квантовых компьютеров массового потребления уже сегодня можно считать Gemini (и его более простая версия – Gemini mini). Их мощностей пока недостаточно для взлома ключей безопасности, но сам факт того, что их можно приобрести должен настораживать (Рисунок 1).

В ближайшем будущем квантовые компьютеры смогут находить даже мельчайшие закономерности в отправляемых сообщениях. Значит, необходимо шифровать сообщение так, чтобы закономерностей не существовало вовсе. На данный момент известен лишь алгоритм шифрования сообщения, не имеющего закономерностей в принципе. Его суть заключается в использовании ключа шифрования, длина которого равна или больше отправляемого сообщения. При этом данный ключ никак не должен быть связан с чем-либо. Однако если использовать современные способы передачи информации, то передача такого ключа будет либо бессмысленной, либо невозможной. И тут как раз таки может пригодиться передача данных с помощью лазера.



Рисунок 1. Квантовый компьютер Gemini

Для реализации моего проекта используется технология Arduino, так как она не является какой-то узко направленной технологией, её можно приобрести почти в любой точке Земного шара, а также она не является дефицитной или дорогой. Эти преимущества позволят людям изучать технологию лазерной передачи на всей территории Российской Федерации (или даже по всему миру).

На данный момент пользователю необходимо собрать 2 устройства (передатчик и приёмник), после чего при помощи Arduino IDE загрузить в платы соответствующие коды. В одном из них пользователь прописывает отправляемое сообщение, во втором пороговое значение для сенсора. После этого необходимо лишь направить лазер на сенсор, и в мониторе порта мы увидим сообщение, которое передаёт лазер.

Последнюю версию кодов, а также 3D модели спутника и приёмника (которые реализованы в виде кубсаток) можно скачать из репозитория GitHub по ссылке: <https://github.com/Prototype721/Laser_Infobez>.

# Структурная схема работы устройств

В схему входят 2 физических устройства: приёмник и передатчик. Оба сделаны по технологии “Кубсат”, которую применяют для настоящих спутников. Подразумевается изучение передачи данных между спутниками, однако при установке солнечной панели на телефон возможна передача и с наземными устройствами. На приёмнике установлена солнечная панель, на передатчике - лазерный модуль, который по команде Arduino передаёт сигнал (луч) с определённой частотой. Программа передающего спутника кодирует ключ в двоичный сигнал, добавляет бит четности, начальный нулевой и конечный ненулевой биты, после чего отправляет последовательность путём лазерного излучения на солнечную панель приёмника. Когда лазерный луч попадает на панель, та начинает давать большее напряжение. Мы можем считать значения с солнечной панели, определить пики напряжения, произвести обратную функцию дешифрации (с проверкой на точность принятых сигналов через бит чётности), после чего вывести их в монитор порта Arduino. На данный момент была также реализована функция передачи некоторых данных на сайт при помощи технологии Bluetooth. Однако нам известно, что таким образом данные можно перехватить. Поэтому в будущем данная технология будет заменена на более безопасную. В качестве данных передаются возможные данные о передающем спутнике, так как алгоритм создания хэш-функций определенной длины ещё не реализован. С другой стороны, мы можем наглядно увидеть, что данные передаются без помех. С примером работы устройств можно ознакомиться по ссылке: <https://www.youtube.com/watch?v=xR01-1oiD9Y>.

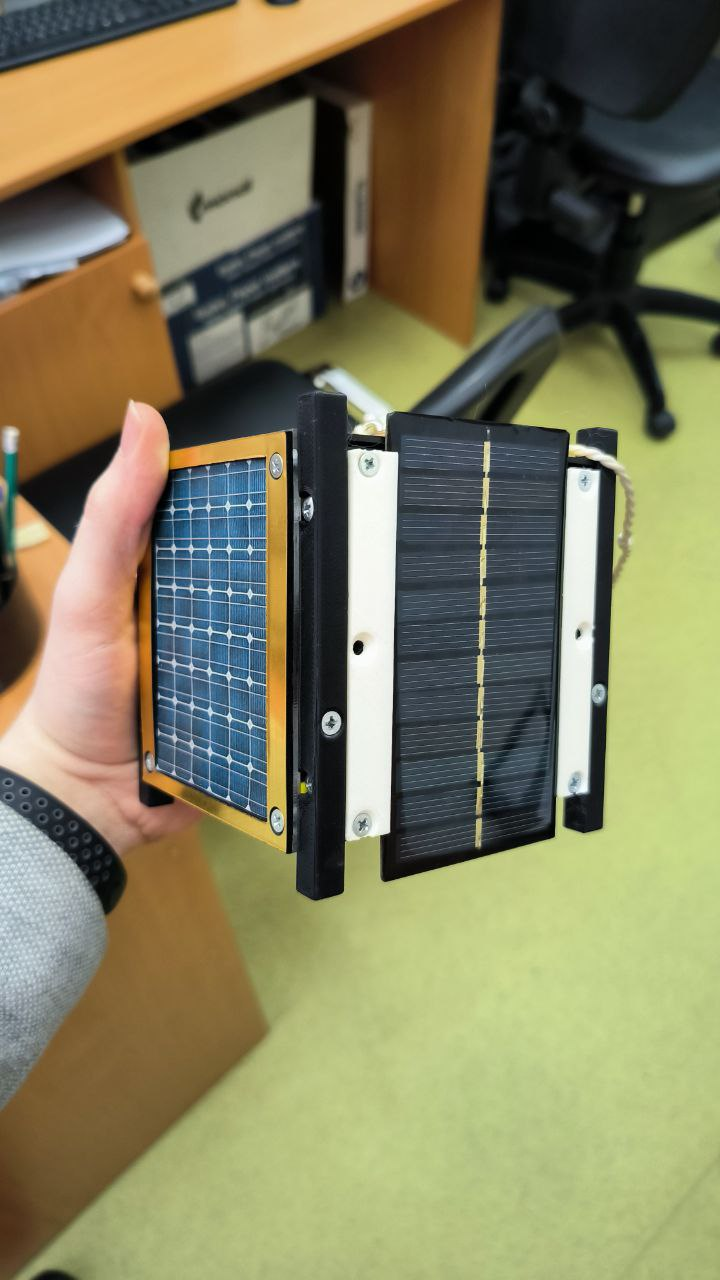


Рисунок 2. Принимающий спутник с солнечной панелью

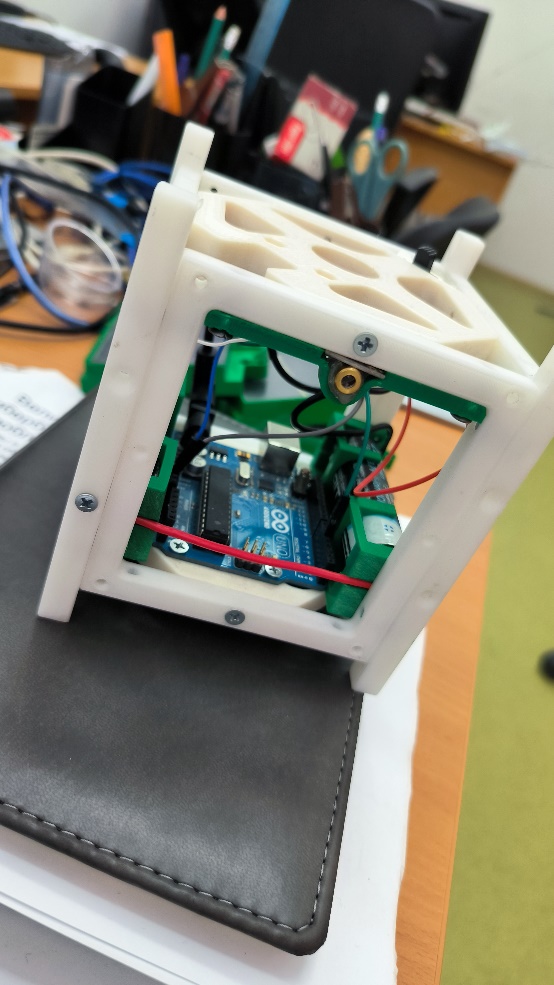


Рисунок 3. Передающий спутник с лазером

# Пример использования

В качестве основного примера использования данной технологии является передача ключей со спутника на устройство. Для этого на самом спутнике устанавливается мощный лазер, способный доставлять данные через атмосферу Земли. У пользователя необходимо наличие особого датчика (например: солнечной панели) на лицевой или тыльной стороне смартфона. При необходимости передачи секретной информации смартфон передаёт спутнику по открытому каналу связи следующие данные: id отправителя, id получателя, длина требуемого ключа (может быть больше отправляемого сообщения). Спутник создаёт ключ шифрования необходимой длины и отправляет его отправителю и получателю через лазерный канал передачи данных. Пользователи направляют свои датчики в небо, после чего при помощи систем ориентации в пространстве (например: GPS) спутник направляет лазер и начинает передачу ключа шифрования (Рисунок 4). Если в момент передачи произошли некоторые сбои, то приёмник информирует об этом, после чего части ключа отправляются повторно. Далее отправитель шифрует свое сообщение и отправляет уже через стандартный канал передачи данных своё сообщение. Получатель принимает зашифрованное сообщение и расшифровывает его. В руках злоумышленников (в теории) будут лишь id получателя и отправителя, их координаты, длина ключа шифрования и само зашифрованное сообщение без единой закономерности. Из недостатков такого способа можно отметить следующие:

1. Зависимость от погодных условий
2. Необходимость получателя и отправителя пребывать вне всяких помещений, укрытий
3. Возможность перехвата данных ключа, вызванных отражением фотонов лазера от атомов атмосферы
4. Возможность зашумления канала с помощью постороннего источника излучения и т.п.



Рисунок 4. Человек направляет смартфон в сторону спутника (Муляж, данная картинка нужна лишь для понимания принципа, оригинал картинки [здесь](https://www.oarsandalps.com/blogs/oarsmans-guide/international-dark-sky-week-astro-101))

Однако мы считаем, что данные недостатки являются терпимыми по сравнению с возможностями, создаваемыми данным способом. Данная технология может быть использована как среди общественности, так и среди специальных государственных служб. Для работы такой системы пользователю необходимо иметь лишь маленькую солнечную панель, что является весьма компактным решением.

# Блок-схема работы программ

Блок-схема работы алгоритма изображена на рисунках 5-7.

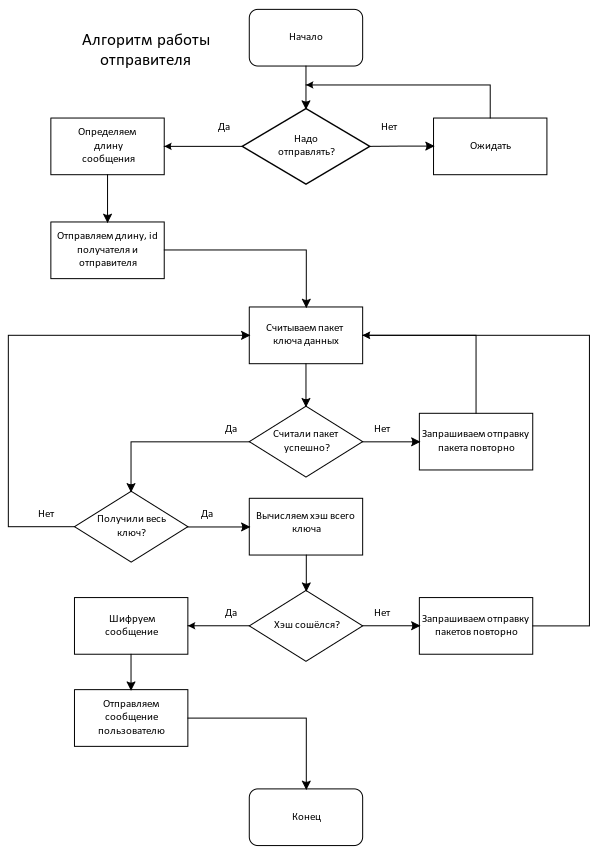


Рисунок 5. Блок-схема работы алгоритма отправителя

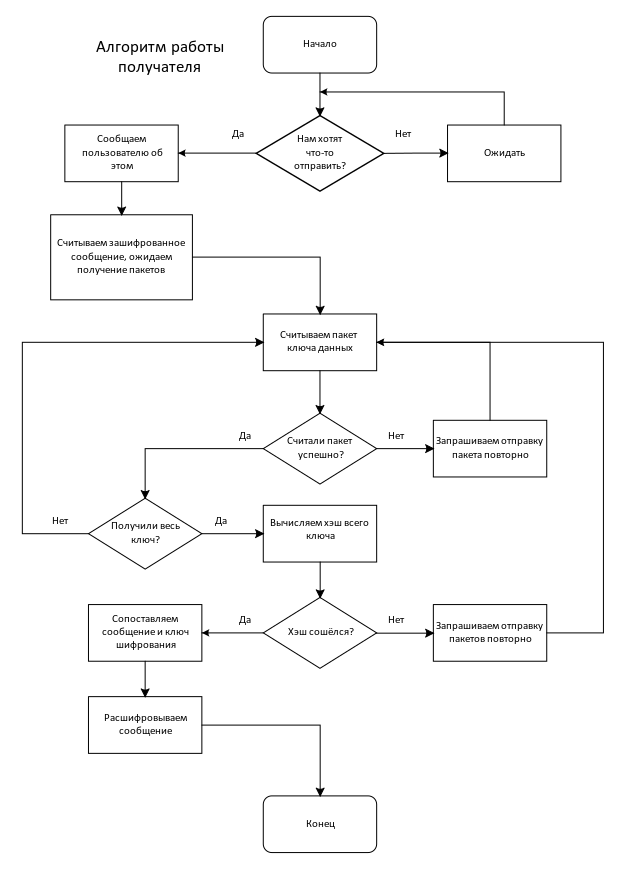


Рисунок 6. Блок-схема работы алгоритма получателя

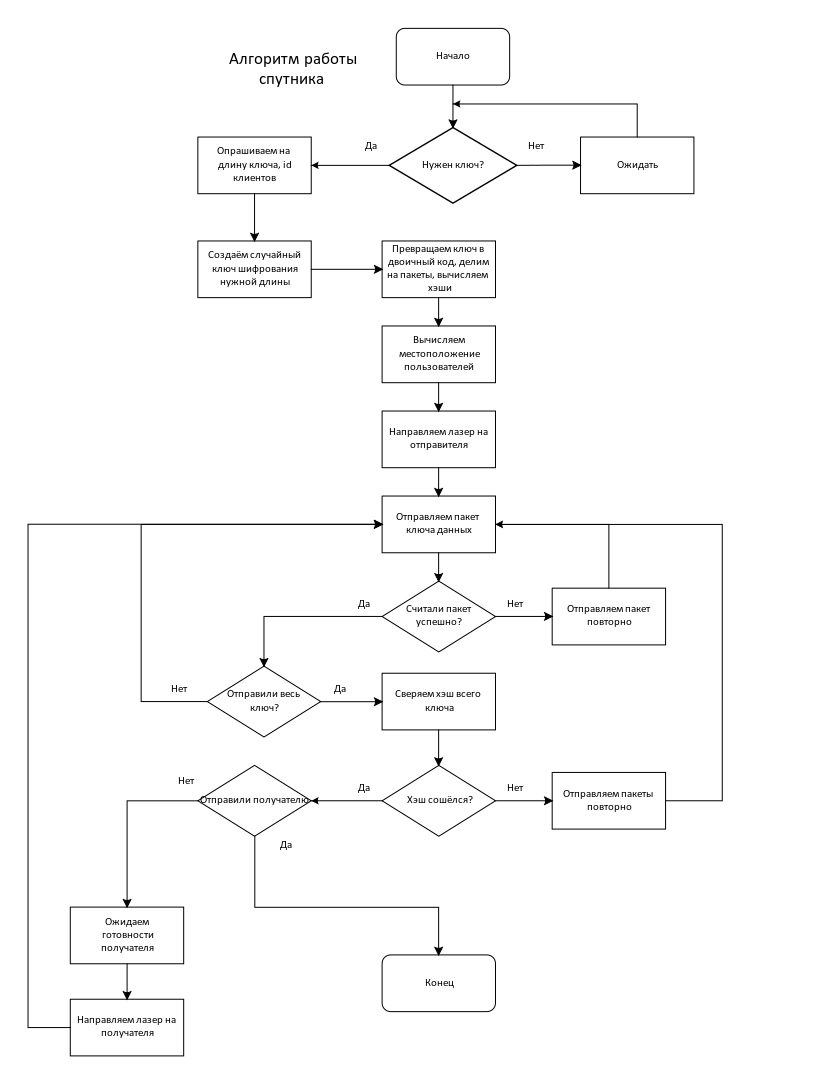


Рисунок 7. Блок-схема работы алгоритма спутника

# Планы по развитию

1. ***Доработать систему определения повреждений.***

Для того, чтобы снизить трафик и увеличить скорость работы устройств мы планируем ввести механизм вычисления хэш-функций для пакетов сообщения. При создании общего ключа шифрования будут создаваться хэш-функции отдельных его частей, которые будут отправляться в конце каждого пакета данных. Если данные различаются, то происходит повторная отправка части ключа. Также будет отдельная хэш-функция для всего ключа. Если хеши будут различаться, то придется искать искажения с последующим восстановлением.

1. ***Сделать механизм защиты от перехвата.***

На спутнике будет установлена РЛС для обнаружения шпионских устройств между передатчиком и приёмником. Также будет создан механизм защиты от подмены ключа шифрование путем направления иного излучателя на панель приёмника.

1. ***Защита для глаз.***

Было бы непредусмотрительно выпускать продукт на рынок, не имея этой функции. Во-первых, можно заставлять пользователя смотреть в другую сторону от спутника. Во-вторых, можно подавать сигнал в таких диапазонах передачи, чтобы вред глазам от излучения был минимизирован.

# Выводы

В результате работы над проектом пришлось освоить много нового:

1. Язык программирования Arduino (С-подобный язык).
2. Работа в команде.
3. Создание 3D моделей устройств.
4. Воплощение моделей в реальности.
5. Исправление огромного числа ошибок.
6. Алгоритм работы устройств и тп.

Наши устройства позволять снизить порок в разработку систем безопасности, что будет способствовать увеличению количества представитель информационной безопасности, которые так необходимы в сегодняшние дни!

# Список литературы

1. Gemini - 2-кубитный настольный квантовый компьютер: <https://www.switch-science.com/products/8679?_pos=2&_sid=5e461a55c&_ss=r>
2. Наш GitHub: <https://github.com/Prototype721/Laser_Infobez>.
3. Видео на Youtube: <https://www.youtube.com/watch?v=xR01-1oiD9Y>.