УДК 004.056.5: 621.382
DOI 10.33764/2618-981X-2025-6-106-113

А. А. Медведев[1]✉, Д. Н. Титов[1]

Методика передачи зашифрованной информации посредством световых импульсов

[1]Сибирский государственный университет геосистем и технологий,
г. Новосибирск, Российская Федерация
e-mail: andrey_medvedev.01@mail.ru

Аннотация. Статья посвящена исследованию возможности реализации защищенного оптического канала связи на базе бюджетных компонентов. Предложена экспериментальная модель, включающая лазерные указки в качестве источника света, фотоприемники, два микроконтроллера и персональные компьютеры, с расстоянием между передатчиком и приемником в 20 см. Основная цель работы — доказать работоспособность алгоритма шифрования Twofish в условиях отсутствия аппаратного усиления сигнала и формирования импульсов. Даже при исключении усилителей мощности с передающей стороны и дополнительной обработки сигнала с приемной система обеспечивает передачу данных со скоростью 1,66 байт/с, что подтверждает принципиальную возможность использования минимальной элементной базы для задач с требованиями к безопасности. Экспериментально выявлено, что увеличение дистанции передачи требует модификации схемы: внедрения формирователей сигнала, усилителей тока и входного каскада. Результаты демонстрируют потенциал подхода, сочетающего программное шифрование и физическую передачу через оптический канал, для локальных систем, функционирующих в условиях радиомолчания или ограниченного бюджета.

Ключевые слова: оптическая связь, оптическая передача данных, безопасность данных, беспроводная связь

A. A. Medvedev[1]✉, D. N. Titov[1]

Technique of transmitting encrypted Information by means of light pulses

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
e-mail: andrey_medvedev.01@mail.ru

Abstract. The article is devoted to the study of the possibility of realizing a secure optical communication channel based on low-cost components. An experimental model including laser pointers as a light source, photodetectors, two microcontrollers and personal computers with a distance between the transmitter and receiver of 20 cm is proposed. The main objective of the work is to prove the performance of the Twofish encryption algorithm in the absence of hardware signal amplification and pulse shaping. Even with the exclusion of power amplifiers on the transmitting side and additional signal processing on the receiving side, the system provides data transmission at a rate of 1.66 bytes per second, which confirms the fundamental possibility of using the minimum element base for tasks with high security requirements. It is experimentally revealed that increasing the transmission distance requires modification of the circuit: introduction of signal conditioners, current amplifiers and input stage. The results demonstrate the potential of an approach combining software encryption and physical transmission through an optical channel for local systems operating under conditions of radio silence or limited budget. Translated with DeepL.com (free version)

Keywords: optical communication, optical data transmission, data security, wireless communication

Введение

Разработка альтернативных систем защищенной передачи данных приобретает особую значимость в контексте уязвимости традиционных беспроводных каналов к перехвату и экономической нецелесообразности оптоволоконных решений для локальных приложений. В условиях ограниченного бюджет актуальным становится создание систем, использующих минимальную аппаратную базу без компромисса в уровне безопасности. Цель работы — экспериментальное обоснование возможности построения защищенного оптического канала связи на базе бюджетных компонентов с отказом от усилителей мощности, формирователей сигнала и специализированного оборудования. Ключевой задачей является доказательство гипотезы о том, что даже при использовании дешевых компонентов система способна обеспечить криптостойкую передачу данных в условиях дневного освещения (400 лк) с воздушной средой в качестве канала.

Анализ уязвимостей беспроводных технологий Wi-Fi и Bluetooth

Беспроводные сети Wi-Fi и Bluetooth, несмотря на широкое применение, сохраняют критические уязвимости, связанные с особенностями их протоколов и реализацией механизмов безопасности. В случае Wi-Fi основным риском остается передача данных в открытых сетях без шифрования, что позволяет злоумышленникам перехватывать трафик через анализ пакетов. Даже в защищенных сетях использование устаревших стандартов, таких как WEP, создает угрозу за счет статических ключей и слабой криптостойкости. Протокол WEP может быть взломан за минуты через атаки на векторы инициализации, что делает его непригодным для современных применений.

Более современные протоколы WPA и WPA2, хотя и обеспечивают повышенную безопасность, также имеют ограничения. WPA, использующий протокол TKIP, уязвим к атакам на целостность пакетов, таким как атака Michael, которая позволяет блокировать сеть через отправку ложных фреймов. WPA2, несмотря на применение AES-шифрования в рамках протокола CCMP, остается подверженным офлайн-брутфорсу паролей, особенно в публичных сетях, где отсутствует встроенное шифрование. Уязвимость KRACK (Key Reinstallation Attack) в WPA2 дополнительно усугубляет риски, позволяя злоумышленникам перехватывать и модифицировать трафик. Даже WPA3, внедряющий 256-битное шифрование и протокол SAE (Simultaneous Authentication of Equals), требует физического присутствия пользователя для аутентификации, что ограничивает его применимость в масштабных системах [1, 2].

Технология Bluetooth демонстрирует уязвимости на этапе сопряжения устройств. Обмен ключами инициализации в незашифрованном канале создает риск перехвата через атаки Eavesdropping или Man-in-the-Middle (MITM). Режимы защиты, такие как минимальный уровень безопасности в Bluetooth Low Energy (BLE), упрощают несанкционированный доступ. Уязвимости в стеке протоколов, например, эксплойт BlueBorne, позволяют удаленное выполнение кода

без необходимости сопряжения, что критично для медицинского оборудования и промышленных систем. Использование коротких ключей шифрования (менее 128 бит) в ранних версиях Bluetooth дополнительно снижает криптостойкость [1, 2].

Общей проблемой для обеих технологий является слабая аутентификация в публичных сетях и зависимость от корректной настройки устройств. В Wi-Fi фишинг через поддельные точки доступа (Evil Twin) и атаки на роуминг остается актуальным. В Bluetooth недостаточная проверка устройств в процессе сопряжения и упрощенные процедуры аутентификации в BLE повышают риск компрометации.

Методы и методики

В основе разработанной системы лежит гибридный подход, сочетающий программное шифрование данных с использованием алгоритма Twofish и их физическую передачу через оптический канал [3] на базе бюджетных компонентов. Экспериментальные испытания системы проводились в условиях дневного комнатного освещения (400 лк) с воздушной средой в качестве канала передачи между лазерным модулем и фотоприемным устройством, при этом никаких дополнительных оптических элементов или экранирующих материалов не применялось. Адаптированный алгоритм Twofish, реализованный на стороне микроконтроллера, обеспечивает криптостойкость за счет 128-битных ключей и использует для работы блоки данных размером 128 бит. На микроконтроллер передается массив байт исходного файла, выбранного на стороне персонального компьютера, через UART-интерфейс со скоростью 9600 бод, где этот массив преобразуются с помощью алгоритма шифрования сначала в измененный массив байт, а потом в оптические сигналы с помощью лазерного модуля RKP-LD-I650A03 с длиной волны 650 нм и мощностью излучения от 2 до 5 мВт. Приемная часть системы включает фотодиод BPW20RF с спектральным диапазоном чувствительности от 400 до 1100 нм, темновым током 2 нА и обратным напряжением в 10 В. К обеим частям подключены микроконтроллеры Arduino Mega 2560, обеспечивающий обработку сигнала без усилителей и формирователей. Микроконтроллер выполняет функцию физического уровня, преобразуя цифровые данные в оптические сигналы и обратно [4]. Расстояние между передатчиком и приемником составило 20 см, что подтвердило возможность работы системы в условиях отсутствия дополнительной аппаратной обработки. Модель всей системы приведена на рис. 1. Алгоритм работы, показанный на рис. 2, разделен на три ключевых этапа: инициализация системы, обработка входящих данных и формирование ответа.

Инициализация системы. При запуске микроконтроллер настраивает аппаратные ресурсы: последовательный порт, четыре цифровых выхода (пины 7, 6, 5, 4) конфигурируются как выходы для управления лазерными модулями. Для исключения ложных срабатываний все лазеры принудительно устанавливаются в состояние LOW.

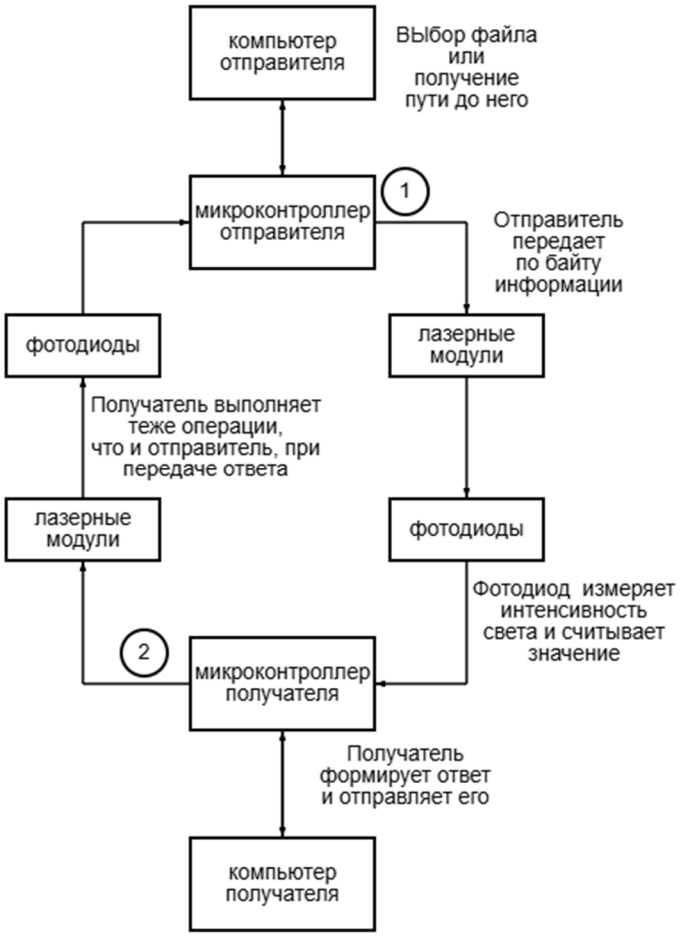

Рис. 1. Модель системы

Цикл обработки данных (рис. 3). Основной алгоритм функционирует в бесконечном цикле, ожидая входящие данные. При получении байта активируется специальная процедура обработки, которая реализует обработку в две стадии: декодирование младших и старших бит по 4 за раз. Каждый из четырех лазерных модулей последовательно активируется на 75 мс в соответствии с состоянием половины битов от входного байта. Например, если третий бит (маска 1 <<2) установлен в 1, лазер на пине 6 включается. Одновременно считываются показания фотодиодов (аналоговые входы A0–A3), которые сравниваются с пороговыми значениями. Пороги были определены экспериментально для каждого канала отдельно. Декодирование старших 4 бит. Аналогичная процедура выполняется для битов 4–7, но с использованием тех же четырех фотодиодов.

Формирование ответа. Результирующий байт, полученный путем объединения показаний всех фотодиодов, отправляется на микроконтроллер получателя и его компьютер через UART. Функция Serial.flush() обеспечивает принудительную очистку буфера передачи, минимизируя задержки между операциями. Для исключения наложения импульсов после каждой итерации цикла светодиоды возвращаются в состояние LOW.

Оптимизация временных параметров. Ключевым параметром системы является длительность импульса (onDuration = 75 мс), подобранная экспериментально. Это значение компромиссно учитывает: время реакции фотодиода, стабилизацию аналоговых показаний аналогово-цифровых преобразователей (АЦП), ограничения скорости передачи данных. Тестирование показало, что уменьшение длительности до 50 мс приводит к критичному росту уровня ошибок, а увеличение свыше 100 мс — к снижению пропускной способности. Корректность передачи подтверждается сравнением исходных и принятых данных с использованием механизма расшифрования на уровне персонального компьютера.

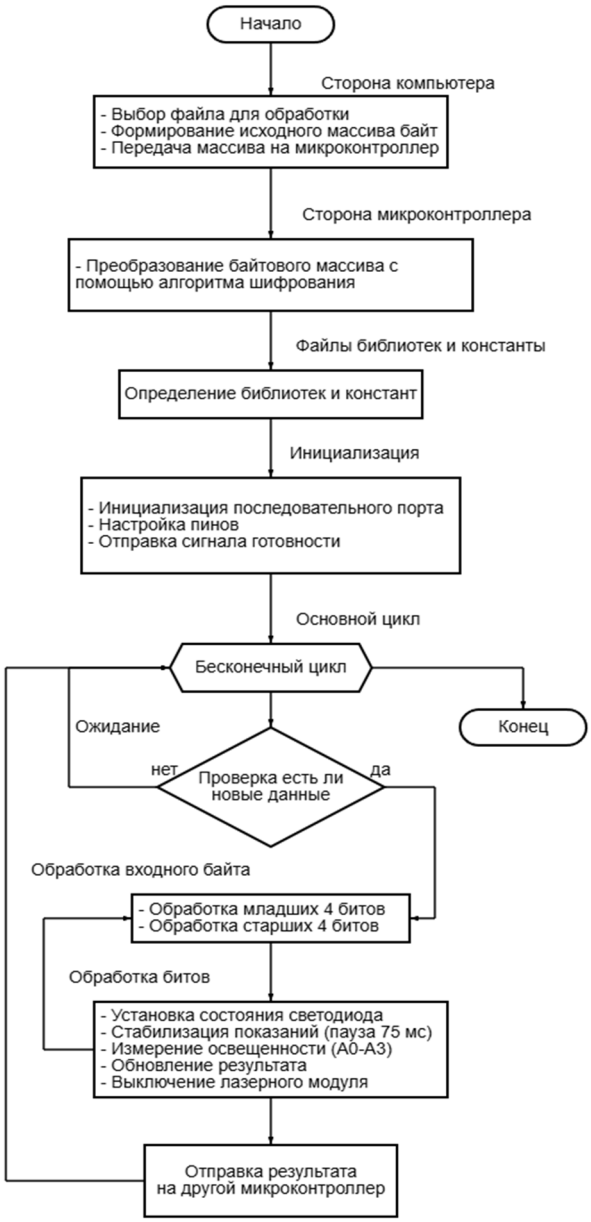

Рис. 2. Блок-схема алгоритма передачи данных

```
void processByte(byte inputByte) {
  resultByte = 0;

  // Обработка младших 4 бит
  for (int i = 0; i < 4; i++) {
    digitalWrite(ledPins[i], (inputByte & (1 << i)) ? HIGH : LOW);
    delay(onDuration);
    int reading = analogRead(ldrPins[i]);
    if (reading > thresholds[i]) resultByte |= (1 << i);
    digitalWrite(ledPins[i], LOW);
  }

  // Обработка старших 4 бит
  for (int i = 0; i < 4; i++) {
    digitalWrite(ledPins[i], (inputByte & (1 << (i + 4))) ? HIGH : LOW);
    delay(onDuration);
    int reading = analogRead(ldrPins[i]);
    if (reading > thresholds[i]) resultByte |= (1 << (i + 4));
    digitalWrite(ledPins[i], LOW);
  }

  Serial.write(resultByte); // Отправка результата
}
```

Рис. 3. Цикл обработки входящих байт

Результаты

Экспериментальные исследования показали, что длительность светового импульса критически влияет на надежность передачи данных. При фиксированном расстоянии между светодиодом и фоторезистором (20 см) оптимальное время импульса составило 75 мс, обеспечивая уровень ошибок менее 1 % (рис. 4). Уменьшение длительности до 50 мс приводило к резкому росту ошибок, тогда как увеличение свыше 75 мс не давало значимых преимуществ. Это связано с необходимостью компромисса между временем стабилизации фоторезистора и скоростью передачи. По временным характеристикам выявлено, что передача одного байта занимает 600 мс (75 мс × 8 бит), что соответствует скорости 1,66 байт/с (рис. 5), что очень медленно по сравнению с другими технологиями беспроводной передачи данных [5, 6].

Основным преимуществом предложенного решения является отсутствие необходимости в усилителях мощности для передающей стороны и обработки сигнала для приемной. Использование лазерного модуля RKP-LD-I650A03 и фотодиода BPW20RF подтвердило возможность построения системы на базе бюджетных компонентов. Однако для увеличения дальности передачи требуется модернизация схемы: внедрение усилителя тока для лазера и операционного усилителя для фотодиода, что теоретически позволит увеличить расстояние в несколько раз.

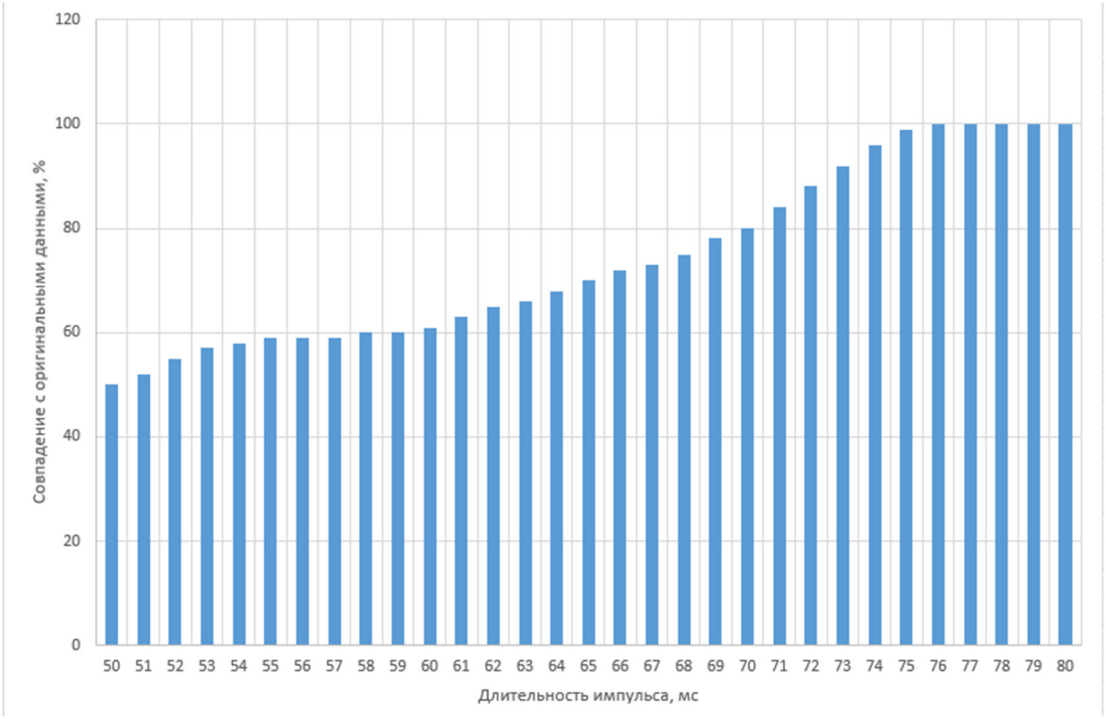

Рис. 4. Процент полученных ошибок в зависимости от длины светового импульса

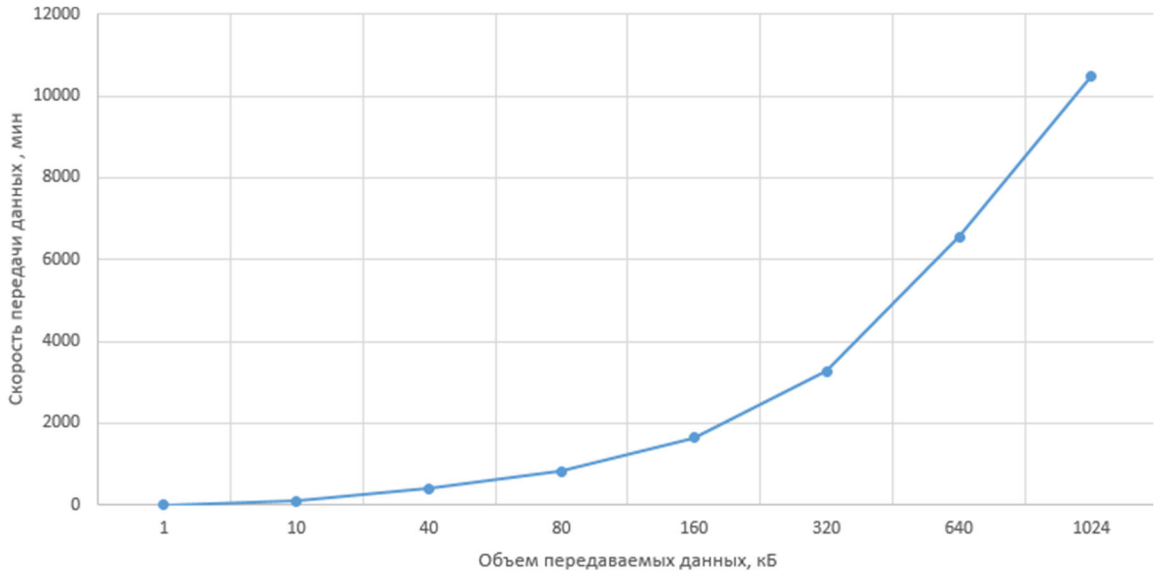

Рис. 5. Скорость передачи данных в минуту в зависимости от объема входных данных

Заключение

Разработан прототип системы защищенной оптической связи, использующий алгоритм Twofish и бюджетные компоненты (лазерный модуль RKP-LD-I650A03, фотодиод BPW20RF, микроконтроллеры Arduino Mega 2560). Экспериментально доказана возможность передачи данных на расстоянии 20 см без при-

менения усилителей и формирователей сигнала. Установлено, что скорость передачи (1,66 байт/с) и уровень ошибок (1-2 %) ограничены аппаратными характеристиками компонентов, но соответствуют требованиям задач с критически важной безопасностью и малыми объемами данных.

Перспективы развития системы связаны с интеграцией пакетной передачи и аппаратной оптимизацией, включая использование квантово-криптографических методов [7]. Предложенный подход может быть применен в изолированных средах, где исключено использование традиционных беспроводных технологий [5, 6].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Саенко М. А., Мельников Д. А., Данилов М. А. Анализ уязвимостей беспроводных каналов передачи информации // Образовательные ресурсы и технологии. – 2023. – № 1(42). – С. 82-90.

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

3. Пислар И. В., Браиловский В.В., Рождественская М.Г., Иванчук М.М. Возможности использования световых лучей видимого диапазона в системах скрытой передачи информации // Системный анализ и прикладная информатика. – 2018. – № 1. – С. 27-36.

4. Гришин И. В. Перспективы развития беспроводных систем передачи данных на базе светодиодов видимого излучения / И.В. Гришин, В. А. Хричков, Т. Р. Ялунина // Труды учебных заведений связи. – 2017 – №3(2). – С. 68–76.

5. Оразова М. Скорость технологии Li-fi / М. Оразова, М. Якубов. // European science. – 2022 – №63 – С. 5–9.

6. Валитова А. Р. Li-Fi – новейшая технология передачи данных через светодиоды // Вестник науки. – 2019 – №5(14) – Том №4. – С. 466–468.

7. Дрон К. К. О перспективах совместного использования методов квантовой и классической криптографии / К.К. Дрон, О.В. Артюшкин // Вестник Хакасского государственного университета им. Н.Ф. Катанова. – 2018. – № 24. – С. 8-11.