Енин Николай Николаевич
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко

Синицын Юрий Юрьевич
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко

Грибанов Евгений Владимирович
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко

Гуйдалаев Мамми Гамзатович
Краснодарское высшее военное училище
имени генерала армии С. М. Штеменко

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ ПРИ ОБМЕНЕ ДАННЫМИ ПО ВОЛОКОННО-ОПТИЧЕСКИМ ЛИНИЯМ СВЯЗИ
ANALYSIS OF EXISTING METHODS FOR ENSURING INFORMATION CONFIDENTIALITY IN DATA TRANSMISSION OVER FIBER-OPTIC COMMUNICATION LINES

Аннотация. В статье анализируются современные методы обеспечения конфиденциальности данных в ВОЛС, физические и логические угрозы, включая скрытые способы перехвата и уязвимости оборудования. Рассмотрены криптографические методы, мониторинг состояния линий, оптическое шифрование и перспективы квантового распределения ключей. На основе анализа источников [1, 2, 4] сделан вывод о необходимости многоуровневого подхода, объединяющего физические, криптографические и организационные меры.

Abstract. The article analyzes modern methods for ensuring data confidentiality in fiber-optic communication lines. It examines physical and logical threats, including hidden interception techniques and equipment vulnerabilities. Special attention is given to cryptographic methods, line condition monitoring, optical encryption, and the prospects of quantum key distribution. Based on the analysis of sources [1, 2, 4], it is concluded that a multi-layered approach, combining physical, cryptographic, and organizational measures, is necessary.

Ключевые слова: Волоконно-оптические линии связи; конфиденциальность информации; защита данных; криптографические методы; перехват сигнала; мониторинг ВОЛС; оптическое шифрование; квантовое распределение ключей; безопасность каналов связи.

Keywords: Fiber-optic communication lines; information confidentiality; data protection; cryptographic methods; signal interception; FOCS monitoring; optical encryption; quantum key distribution; communication channel security.

Волоконно-оптические линии связи являются основным средством передачи больших объёмов данных на большие расстояния. Они отличаются высокой пропускной способностью, низким уровнем потерь и устойчивостью к электромагнитным помехам. Однако вопреки распространённому мнению, система оптоволоконной связи не является абсолютно защищённой от несанкционированного доступа. Исследования показывают, что существуют физические и логические методы перехвата оптического сигнала, требующие комплексного подхода к защите информации. Необходимость в такой защите обусловлена тем, что утечка информации может

происходить незаметно, при этом злоумышленник получает доступ к конфиденциальным данным без активного вмешательства в работу сети. Кроме того, последствия подобных атак могут быть критическими для корпоративных и государственных сетей, где передаются стратегически важные данные, что делает вопрос безопасности ВОЛС приоритетным в современных телекоммуникационных системах.

Физические угрозы конфиденциальности связаны с особенностями распространения света в оптическом волокне. Физический перехват является одной из наиболее опасных угроз, так как осуществляется на уровне среды передачи и может быть практически незаметен. При изгибе или микродеформации волокна часть света выходит из сердцевины, что позволяет злоумышленнику установить фотодетектор и извлечь полезный сигнал без заметного ухудшения качества линии. Данная уязвимость подробно описана в современных исследованиях и подтверждена лабораторными экспериментами [1]. При создании микробендов или макробендов часть сигнала выходит за пределы сердцевины и может быть зафиксирована специальными датчиками. Схема утечки сигнала при изгибе волокна представлена на рисунке 1. Подобные воздействия не вызывают заметного ухудшения качества канала, что делает перехват скрытым и труднодоступным для обнаружения без специализированных средств мониторинга. При этом современные методы физического контроля и мониторинга линии, такие как измерение параметров поляризации и распределённое отслеживание рассеяния света, позволяют выявлять подобные аномалии, но их внедрение требует значительных технических ресурсов и высокой квалификации персонала. В совокупности это подчёркивает необходимость сочетания физических и криптографических методов защиты для обеспечения полной конфиденциальности передаваемой информации.

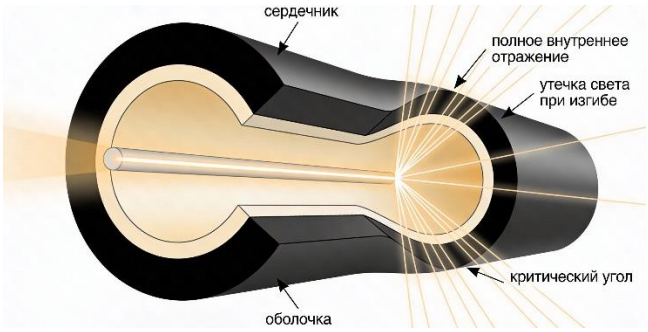

Рисунок 1 – Механизм утечки света при изгибе оптического волокна

Механизм утечки света при изгибе волокна наглядно демонстрирует, что даже небольшая деформация линии может привести к излучению части оптического сигнала в оболочку, где его возможно перехватить с помощью чувствительных приёмников. Такой тип воздействия особенно опасен тем, что он практически не отражается на качестве передаваемого сигнала, что затрудняет его обнаружение стандартными средствами мониторинга. Кроме того, современные технологии позволяют злоумышленникам фиксировать утечки на больших расстояниях, что делает физическую защиту линии крайне важной. Принципы анализа и классификации угроз информационной безопасности, включая физические угрозы ВОЛС, систематизированы в исследованиях по автоматизированным системам [10]. Понимание физических механизмов перехвата позволяет перейти к рассмотрению способов защиты, среди которых особую роль играют криптографические методы. Их сравнительные характеристики представлены в таблице 1, позволяющей оценить различия между классическими и квантовыми подходами к защите конфиденциальных данных. Использование криптографических алгоритмов в сочетании с контролем физического состояния линии обеспечивает многоуровневую защиту, значительно снижая риск несанкционированного доступа к передаваемой информации.

Таблица 1

Сравнительные характеристики криптографических алгоритмов

Алгоритм	Тип	Основное назначение	Устойчивость
AES-256	Симметричный	Шифрование трафика	Высокая
ГОСТ «Кузнечик»	Симметричный	Государственные информационные системы	Высокая
RSA-2048	Асимметричный	Обмен ключами	Средняя
ГОСТ Р 34.10–2012	Асимметричный	Цифровая подпись	Высокая

Помимо физических воздействий, на безопасность влияют логические угрозы. Они включают компрометацию активного оборудования, внедрение вредоносных программ, атаки на канальном и сетевом уровнях, а также перехват трафика при отсутствии или неправильной настройке средств шифрования. Анализ уязвимостей показывает, что логические атаки становятся всё более распространёнными благодаря удалённому доступу к узлам сети. Современные взгляды на доктрины информационного воздействия в киберпространстве, включая методы противодействия логическим угрозам, рассмотрены в работах по анализу подходов ведущих стран к кибербезопасности [12].

Криптографические методы защиты являются основой обеспечения конфиденциальности данных на всех уровнях сетевой модели. Классические алгоритмы симметричного шифрования, такие как AES-256 и ГОСТ «Кузнечик», обеспечивают высокую производительность и устойчивость к взлому, что особенно важно для высоконагруженных магистральных линий связи [3]. Для обмена ключами и установления защищённых сессий применяются асимметричные алгоритмы и гибридные протоколы типа TLS и IPsec, объединяющие преимущества симметричной и асимметричной криптографии. Современные исследования подчёркивают важность интегрированных решений, использующих мониторинг состояния канала для динамической адаптации ключей и параметров шифрования. Новые подходы к защите информации включают оптическое шифрование на физическом уровне, при котором преобразования происходят непосредственно в оптическом диапазоне. В исследовании Khalili и соавторов (2025) описана система шифрования, встроенная в оптические интерферометры Маха–Цендера, позволяющая защищать данные на скорости 100 Гбит/с без значимых задержек [1]. Такой подход минимизирует зависимость от электронных криптографических процессоров и повышает устойчивость сети к атакам, связанным с традиционными методами перехвата. Современные исследования также рассматривают применение гомоморфного шифрования, позволяющего обрабатывать данные в зашифрованном виде без необходимости их расшифровки, что особенно актуально для распределённых вычислений и IoT-сетей, использующих оптоволоконные линии связи [4].

Методы пассивного и активного мониторинга ВОЛС направлены на своевременное выявление несанкционированного доступа и вмешательства. Среди них анализ изменения распределения амплитуды и фазы сигнала, сопоставление состояний поляризации на разных участках линии, использование распределённых оптических датчиков на основе обратного рассеяния и выявление изменений частотного спектра. Исследования последних лет показали высокую эффективность методов многоканального анализа состояния поляризации (SOP) для раннего обнаружения вмешательства, особенно в протяжённых магистральных линиях [3]. Отдельного внимания заслуживают методы точного определения местоположения внешних воздействий на линию связи, которые могут быть адаптированы из смежных областей, таких как системы определения координат места падения боеприпасов на основе волоконно-оптических датчиков [9]. Наиболее перспективным направлением обеспечения конфиденциальности является квантовое распределение ключей, ключевое преимущество которого заключается в

невозможности незаметного перехвата. Любое измерение квантового состояния фотона искажает его, что фиксируется системой [2]. В 2025 году Toshiba Europe продемонстрировала успешную передачу зашифрованных сообщений по коммерческой сети протяжённостью 250 км без охлаждаемых детекторов, что существенно упростило внедрение квантовой криптографии и сделало её доступной для операторов связи и критически важных объектов [6].

Эффективность защиты информации в ВОЛС повышается при сочетании технических методов с организационными мерами, включающими контроль доступа к кабельным каналам, регулярный аудит конфигураций оборудования, регламентированные действия персонала, резервирование маршрутов передачи и периодическое тестирование каналов на наличие аномалий. Комплексное применение физической защиты, криптографии и организационных мер создаёт многоуровневую систему защиты, способную противостоять широкому спектру угроз. Современные достижения в области оптического шифрования и квантового распределения ключей демонстрируют высокую эффективность в предотвращении атак и открывают перспективы для построения защищённых сетей связи следующего поколения. Только такой комплексный подход позволяет гарантировать высокий уровень конфиденциальности и устойчивость коммуникаций к современным и перспективным угрозам [1-6, 9-12].

Список литературы:

1. Khalili A., Abedi K. Design and analysis of optical encryption for optical transport networks with a rate of 100Gbps based on Mach–Zehnder interferometers // Scientific Reports. – 2025. – Vol. 15, No. 4. – P. 1-12.

2. Sellami A. Enhancing the Secure Transmission of Data Over Optical Networks: Quantum Key Distribution Methods // Optics & Laser Technology. – 2024. – Vol. 158. – P. 107-119.

3. Li Y., Zhang H., Wang L. Fiber eavesdropping detection and location in optical communication systems using multi-channel SOP estimation // Photonics. – 2025. – Vol. 12, No. 7. – P. 215-229.

4. Alqahtani A.S., Trabelsi Y., Ezhilarasi P. Homomorphic encryption algorithm providing security and privacy for IoT with optical fiber communication // Optical and Quantum Electronics. – 2024. – Vol. 56, No. 8. – P. 1-18.

5. Yuan Zhiyong, Zhong Zhangshen, Xiong Feilong. Research on security protection of fiber optic network encryption for privacy information disclosure // Laser Journal. – 2025. – Vol. 38, No. 3. – P. 45-60.

6. Toshiba Europe researchers send secure quantum messages over commercial fiber network // Financial Times. – 2025. – Apr 23.

7. Курбонов С.С. Безопасность передовых оптических коммуникационных сетей связи // Cyberleninka. – 2021. – URL: https://cyberleninka.ru/article/n/bezopasnost-peredovyh-opticheskih-kommunikatsionnyh-setey (дата обращения: 12.12.2025).

8. Патент № 2730420 C1 Российская Федерация, МПК F41J 5/00, G01V 1/24, G01V 1/30. Способ определения координат места падения боеприпаса: № 2020106341: заявл. 10.02.2020: опубл. 21.08.2020 / А. В. Акишин, А. Е. Смелов, С. А. Иванов [и др.]. – EDN KLLLMM.

9. Анализ и классификация угроз информационной безопасности на автоматизированных системах / Д. А. Охотин, А. В. Акишин, Н. В. Хечиев [и др.] // Вектор научной мысли. – 2025. – № 1 (18). – С. 389-392. – EDN OCDJJU.

10. Алашеев, В. В. Взгляды США на разработку доктрины информационного воздействия в киберпространстве / В. В. Алашеев, А. В. Акишин, М. Н. Чеснаков // Проблемы технического обеспечения войск в современных условиях: Труды III Межвузовской научно-практической конференции, Санкт-Петербург, 16 февраля 2018 года. Том 1. – Санкт-Петербург: ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ВОЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ВОЕННАЯ АКАДЕМИЯ СВЯЗИ ИМЕНИ МАРШАЛА СОВЕТСКОГО СОЮЗА С. М. БУДЕННОГО» МИНИСТЕРСТВА ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, 2018. – С. 67-71. – EDN XMGZPF.