

Дисциплина:
Оптические сети и квантовые
коммуникации

Тема занятия: Изучение технических
средств защиты информации в оптической
сети

Лабораторно-практическое занятие

Назначение этой работы – системные **знания** будущих специалистов

- Цель работы: изучить возможные способы физической и криптографической защиты оптических соединений (защита канала и защита сигнала) в транспортных сетях и сетях доступа на основе волоконно-оптической связи, попытаться понять назначение квантовых коммуникаций!
- Порядок выполнения: изучить возможности и оборудование для физической защиты волоконно-оптических линий связи и систем передачи, ответить на контрольные вопросы и решить задачу по варианту; изучить принципы криптографической защиты информации в оптических каналах связи, ответить на контрольные вопросы и решить задачу по варианту.
- Содержание работы: выполнение двух разделов с изучением представленных материалов, ответы на контрольные вопросы, решение двух задач.

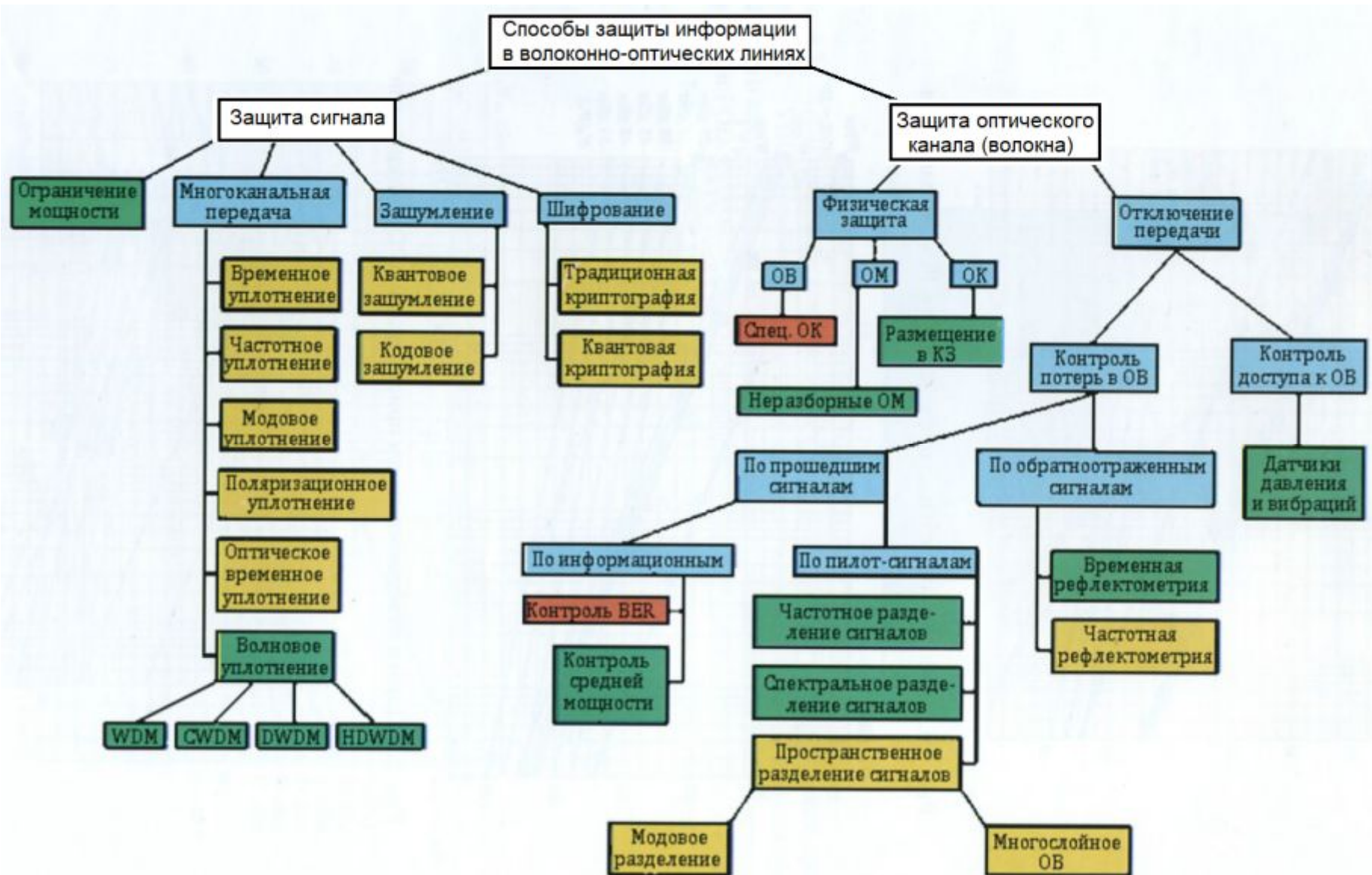
Содержание отчёта

- 1. Название работы. Ф.И.О. исполнителя с подписью. Руководитель занятия. Дата выполнения.
- 2. Цель занятия.
- 3. Содержание занятия с перечнем изучаемых разделов.
- 4. Краткие ответы на контрольные вопросы.
- 5. Решение задач и выводы по результатам выполнения работы.

Рекомендуемая литература для самостоятельного изучения

- 1. Шубин В.В. Информационная безопасность волоконно-оптических систем : монография / Шубин В.В.. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 257 с. — ISBN 978-5-9515-0242-1. — Текст : электронный // IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/89874.html> . — Режим доступа: для авторизованных пользователей
- 2. Ветров Ю.В. Криптографические методы защиты информации в телекоммуникационных системах: учеб. пособие / Ю.В. Ветров, С.Б. Макаров. — СПб.: Изд-во Политехн. ун-та, 2011. — 174 с. <https://elib.spbstu.ru/dl/2889.pdf/download/2889.pdf>
- 3. Козубов А.В., Гайдаш А.А., Кынев С.М., Егоров В.И., Иванова А.Е., Глейм, А.В., Мирошниченко Г.П. , Основы квантовой коммуникации: часть 1. — СПб: Университет ИТМО, 2019. — 85 с.
- 4. Румянцев К.Е. Квантовые технологии в телекоммуникационных системах: учебник/К.Е. Румянцев; Южный федеральный университет. Ростов-на Дону; Таганрог: Издательство Южного федерального университета, 2021.-346с. <https://elibrary.ru/qmwhwz> (доступ из библиотеки СибГУТИ)
- 5. ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ ПНСТ 799-2022 Информационные технологии КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Термины и определения. Information technology. Cryptographic data security. Terms and definitions ОКС 35.040 Срок действия с 2023-01-01 до 2026-01-01
- 6. ГОСТ Р 34.13 – 2015 Информационная технология. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. Режимы работы блочных шифров.- М.: Стандартинформ. 2016.- 30с.

Классификация способов защиты информации в волоконно-оптических линиях и системах передачи



О классификации способов технической защиты информации в оптических системах передачи

- Защита информации при передаче в оптической системе или сети может осуществляться различными способами, каждый из которых имеет свои преимущества и недостатки.
- Все способы защиты информации от утечки по оптическому каналу (волокну) делятся на две группы: **способы защиты сигналов** и **способы защиты каналов**. Способы защиты сигналов не защищают канал (волокну) от несанкционированных подключений, съёма и ввода-вывода сигналов или иных воздействий; они только затрудняют (в пределе делают невозможной) обработку перехваченных сигналов: структурирование и расшифровку.
- Способы защиты канала (волокна) также не в состоянии предотвратить подключение к каналу за пределами контролируемой зоны кабельной линии, но позволяют затруднить доступ, либо обнаружить попытку несанкционированного подключения и прервать или переключить передачу сигналов. Тем самым кроме защиты канала (волокна) защищается и передача сигнала.



Часть 1

ЗАЩИТА ОПТИЧЕСКОГО КАНАЛА (ВОЛОКНА). ФИЗИЧЕСКАЯ ЗАЩИТА

Технические средства физической защиты информации

- Построение Технических Средств Физической Защиты Информации (ТСФЗИ) от перехват в ВОСП основано на анализе возможностей нарушителя и физико-технических особенностях волоконно-оптических каналов связи:
- преимущества оптического волокна и кабеля как транспортной среды для информации связаны с возможностью построения транспортной среды из полностью диэлектрических материалов;
- высокой скоростью передачи информации при низком уровне шумов;
- ограниченностью дистанционных методов съема информации;
- возможностью конвергенции транспортных и измерительных сетей;
- высокая удаленность друг от друга активных сетевых элементов.

ТСФЗИ. Этап подхода к оптическому кабелю и волокну

- Оптический кабель может быть использован как среда для передачи информации оптическими сигналами и как среда для измерений воздействий и полей оптическим зондирующим излучением.
- - совмещение двух данных функций в одном кабеле позволяет реализовать функцию защиты от перехвата следующими способами:
- 1. Контроль намерений нарушителя по его действиям вблизи кабеля
- 2. Контроль состояния защитных покрытий/оболочек кабеля на предмет преднамеренного разрушения
- 3. Защита кабеля от разрушения защитных покрытий/оболочек кабеля
- 4. Защита волокна от несанкционированных измерений путем отвода оптических излучений.

Охрана периметра кабеля. Контроль намерений нарушителя по его действиям вблизи кабеля

- Действия нарушителя сопровождаются вибро-акустическими сигналами, воздействующими на волокно оптического кабеля и вызывающими в нем паразитные модуляции параметров оптического излучения;
 - на данных свойствах оптического кабеля функционируют распределенные волоконно-оптические системы охраны периметра объектов;
 - промышленно выпускается много подобных систем, в том числе в России:
 1. Волоконно-оптическая периметральная система охраны «ВОРОНтм» ООО «Прикладная радиофизика» www.neurophotonica.ru
 2. Волоконно-оптическая система охраны «СОВА» Инновационный центр «Оптика» www.centroptic.ru
 3. Оптоволоконная распределенная система вибромониторинга и охраны периметра ООО «Оптолекс» www.optolex.ru
 4. Когерентный рефлектометр «Дунай» ООО «Т8» www.t8.ru

Охрана периметра кабеля. Контроль намерений нарушителя по его действиям вблизи кабеля

- Принципы функционирования волоконно-оптических систем охраны периметра (ВОСОП) основаны на регистрации виброакустических колебаний окружающей среды методами:
 - 1. регистрации межмодовой интерференции
 - 2. регистрации спекл-структуры
 - 3. двух лучевой интерференции
 - 4. датчиками на брэгговских решетках
 - 5. когерентной рефлектометрии
- Что есть средство фиксации нарушения в системе защиты периметра:
- периметром является оптический кабель с чувствительным волокном или волокно телекоммуникационного кабеля (выделенное или используемое для передачи трафика)

Специальная защита кабеля

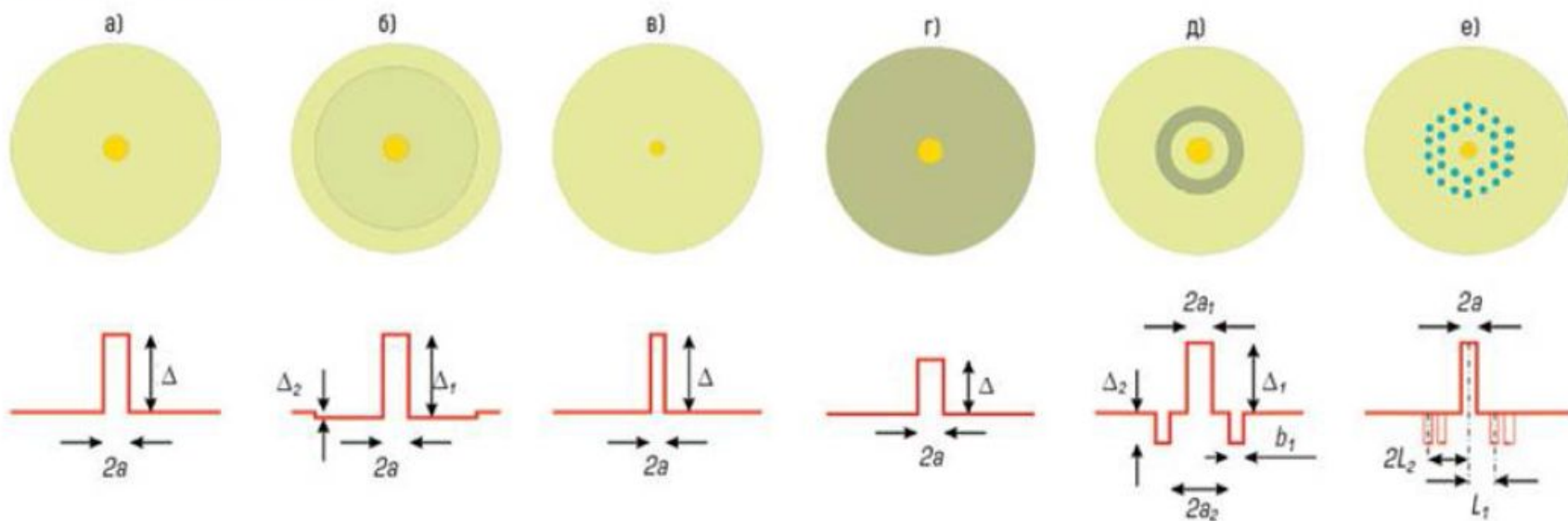
- В структуру оптического кабеля вводятся элементы, препятствующие разрушению и проникновению внутрь кабеля для последующего получения доступа к волокну:
- усиленное бронирование;
- защитное покрытие/оболочка с само разрушающимися при воздействии свойствами;
- воздействие на кабель регистрируется ТСЗИ не волоконно-оптическими методами, например, подводный кабель под высоким напряжением
- - защитные оболочки кабеля имеют прочную механическую защиту, содержащую металлическую оболочку;
- - в кабеле для подводного монтажа металлическая оболочка используется для электрического питания оптических усилителей, на которую подается высокое напряжение;
- - в зависимости от длины подводной части напряжение достигает нескольких 10 кВольт.

Специально защищённые волокна

Специальные волокна с защитой от несанкционированных измерений

применение оптоволокна со сложным распределением показателя преломления:

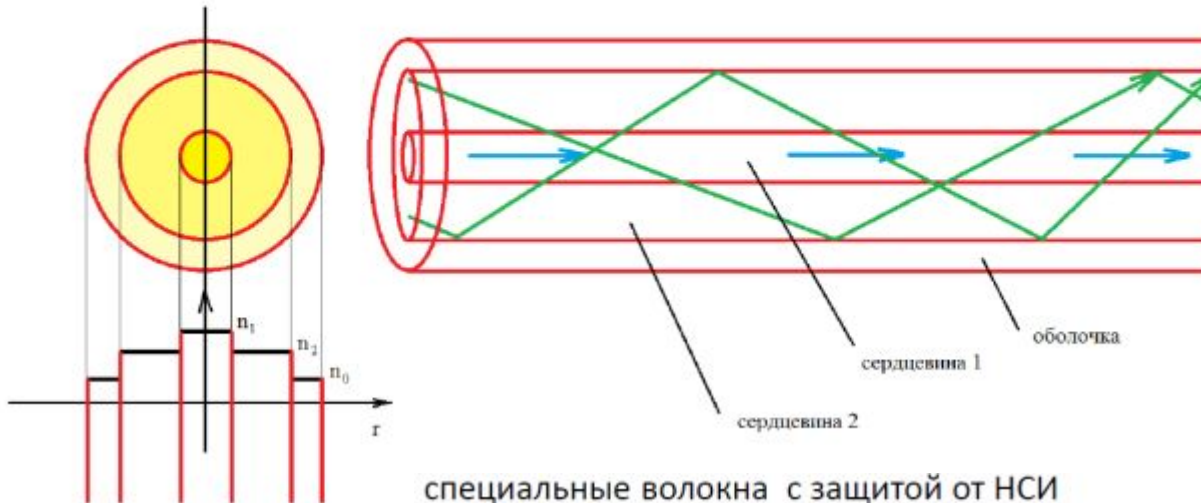
а — волокно с традиционным ступенчатым профилем показателя преломления; *б* — волокно с дипрессированной оболочкой; *в* — волокно с уменьшенной сердцевинной и, соответственно, уменьшенным диаметром модового поля; *г* — волокно с уменьшенным показателем преломления оболочки; *д* — волокно, с кольцевой «траншеей» в оболочке; *е* — микроструктурированное волокно HAF (Holed Assisted Fiber) с уменьшенными потерями на изгибах



Специально защищённое волокно

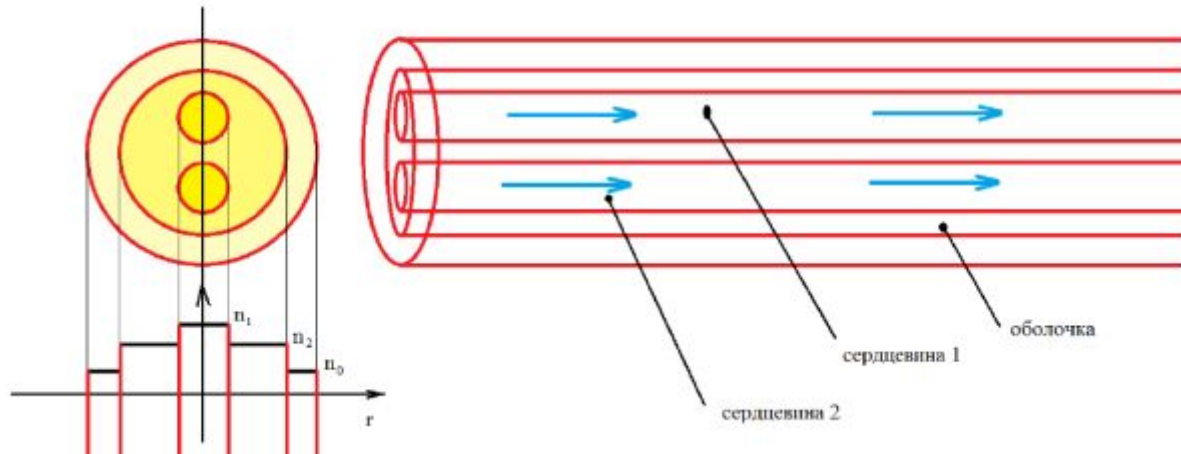
Специальное волокно с защитой от несанкционированного измерения

ступенчатое волокно со сдвоенными concentрическими сердцевинами для защищаемого трафика (1) и с защитным шумовым излучением (2)



специальные волокна с защитой от НСИ

ступенчатое волокно со сдвоенными разнесенными сердцевинами 1 и 2 для защищаемого трафика



Выводы по охране периметра кабеля

- 1. Охрана периметра оптической системы передачи или сети применима для защиты локальных сетей, так как охраняемый периметр ограничен дальностью действия системы;
- 2. Другие методы физической защиты применимы как в телекоммуникациях, так и локальной связи, но эффективность защиты связывается только со сложностью выполнения работ по нарушению защитных свойств;
- 3. Для защиты волокна от физического доступа могут быть использованы специальные оптические кабели с встроенными средствами защиты, когда возможны два направления защиты при вскрытии ОК:
 - воздействие на нарушителя с целью нанесения вреда его здоровью (электрическое, химическое);
 - воздействие на волокно с целью его обрыва для прекращения передачи сигналов.
- 4. Подобные системы защиты являются неотъемлемой частью монтируемой кабельной системы и первым рубежом защиты информационного трафика.

Мониторинг состояния оптического тракта. Этап работы с оптическим каналом для защиты методом мониторинга

Действия нарушителя по перехвату трафика направлены на получения доступа к оптическим информационным сигналам и сопровождающих их информативным сигналам.

В результате данных действий изменяются параметры сети, что может выявляться следующими методами:

- 1. Рефлектометрией оптических волокон на предмет возможных изменений в сети (на дистанции до 200 км);
- 2. Контроль временных параметров прохождения сигнала;
- 3. Контроль оптического бюджета в оптическом канале;
- 4. Контроль оптических параметров сигнала.

Мониторинг состояния оптического тракта. Рефлектометрия оптических волокон в составе комплексов защиты

Optical Time Domain Reflectometer, OTDR - оптический рефлектометр в системе мониторинга ВОЛС:

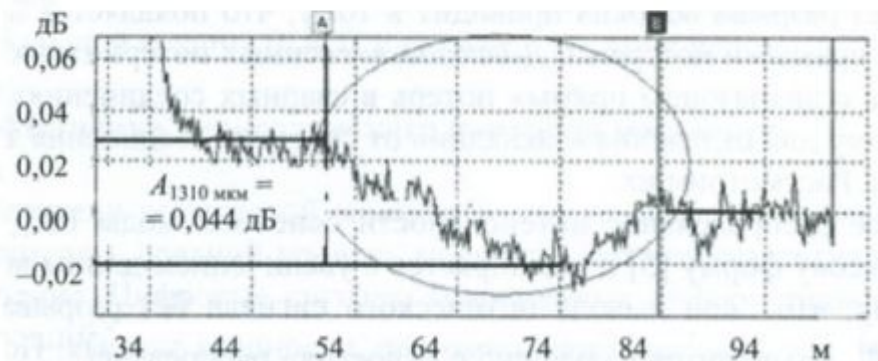
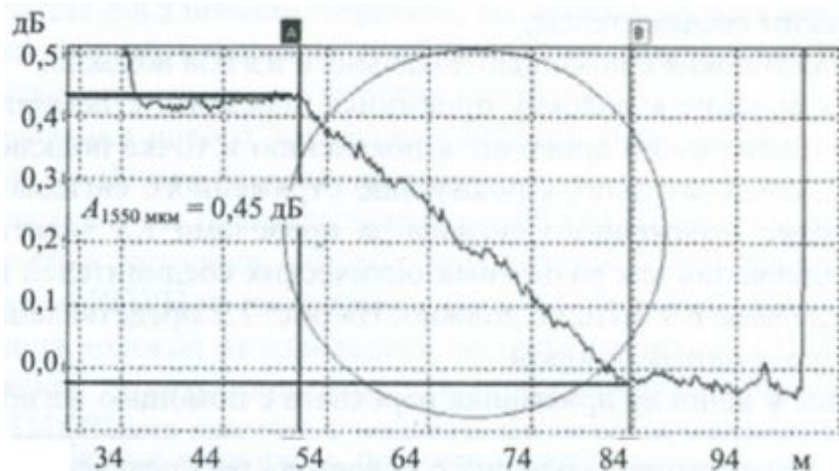
- 1. Программно-аппаратный комплекс "Сапфир" (НЕЛК, Москва).
- 2. Система мониторинга оптических волокон FIBERTEST (ИИТ, Беларусь).
- 3. Система мониторинга ВОЛС (КБПМ-ИБ, Москва).
- 4. Предложение по защите волоконно-оптических коммуникаций с помощью Remote Fiber Test System (RFTS), Optical Network Management System (ONMS) от Agilent Technologies – HP (AccessFiber); Wavetek Wandel&Goltermann (Atlas); GN Nettest (Orion); JDSU (ONMS); EXFO (FiberVisor) и другие

Мониторинг состояния оптического тракта. Обнаружение «закладок» в оптическом волокне методом рефлектометрии

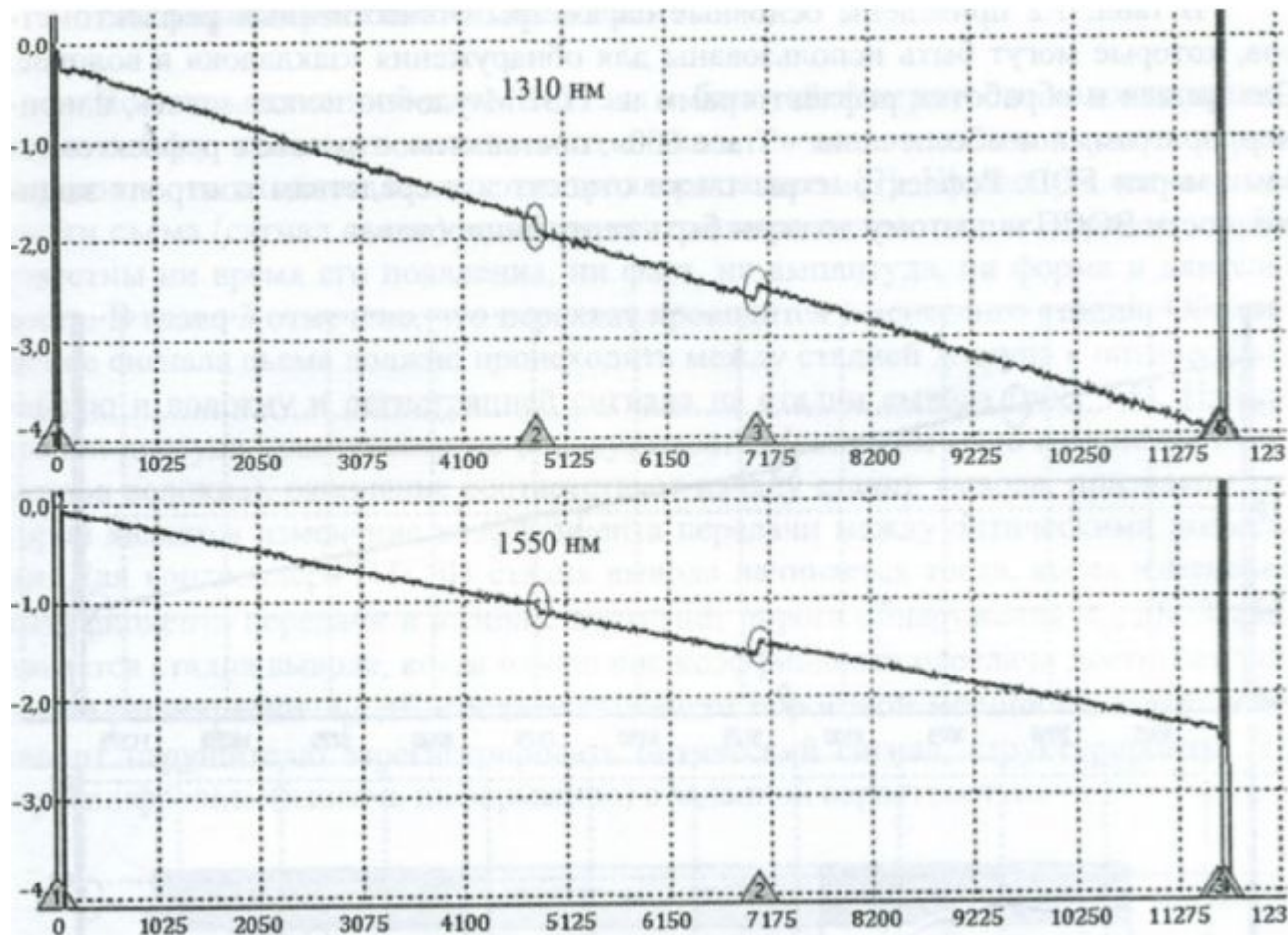
- Подключение технических средств для отвода и регистрации оптических сигналов («закладок») можно осуществить двумя способами: **с разрывом** волокна с помощью разъёмного оптического соединителя или отводов с оптическим соединителем; **без разрыва** волокна с помощью локального изгиба волокна или путём туннелирования на протяженном участке волокна.
- Любое подключение к волокну приёмника перехвата с помощью оптических соединителей неизбежно приводит к появлению в точке подключения воздушного зазора, т.е. на рефлектограмме к появлению отраженного сигнала. Если такой сигнал появляется за пределами зоны контроля линии, то это верный признак «закладки»!!!
- Подключение к волокну приёмника перехвата с помощью изгиба (или другого способа) без разрыва волокна приводит к тому, что появляется локальный дефект, но только с прямыми потерями без отражения. Диапазон внесённых потерь таких способов может совпадать с диапазоном прямых потерь в сварных соединениях (от 0,001 до 0,1дБ), поэтому для отделения «закладки» от сварных соединений требуются другие признаки, которые определяются из сравнения рефлектограмм с двух сторон измерения и на разных длинах волн (1310нм и 1550нм).

Мониторинг состояния оптического тракта. Обнаружение «закладок» в оптическом волокне методом рефлектометрии

Спектральная зависимость (зависимость от длины волны измерения) выводимого излучения через боковую поверхность без разрыва волокна может указывать на неоднородность (накладку), т.к. на рефлектограмме для двух волн потери на сварном соединении различны в прямом и обратном направлениях измерения и в расчёт принято брать среднее значение, но при этом на разных волнах потери в одном направлении сопоставимы, а потери от изгиба или накладки для двух волн в прямом и обратном направлении одинаковы на каждой из волн, но существенно (примерно в 10 раз) различны!!! Что позволяет идентифицировать неоднородность как «закладку». Примеры рефлектограмм на двух длинах волн для изгиба ОВ приведены далее.

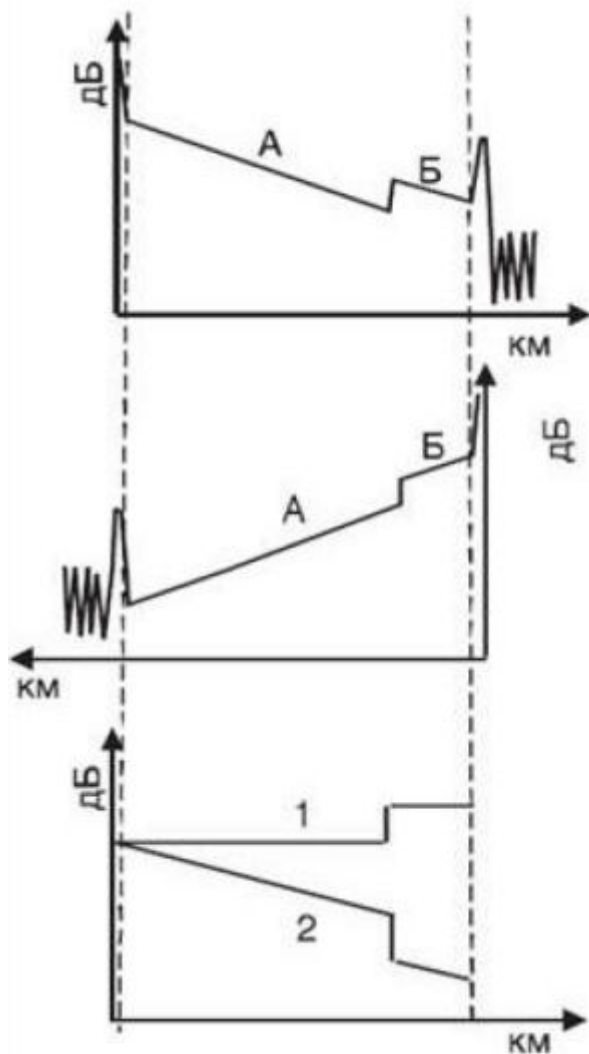


Рефлектограммы волокна на двух длинах волн. Прямое направление



Рефлектограммы волокна на двух длинах волн

Рефлектограммы волокна с противоположных направлений



Рефлектограмма измеренная со стороны волокна А.

Рефлектограмма измеренная со стороны волокна Б.

1. Полусумма рефлектограмм показывает изменение коэффициента рассеяния
2. Полуразность рефлектограмм показывает изменение величины потерь

Анализ попыток съёма сигнала

- Анализ попыток съёма с помощью различных способов позволяет разделить все сигналы на три категории: быстрый вывод, плавный вывод, ступенчатый вывод.
- Сигналы съёма различаются по амплитуде, длительности времени вывода и форме.
- При использовании устройств вывода и сбора излучения типа ответитель-прищепка осуществляется **быстрый вывод**, когда учитывается переходный процесс аппаратуры регистрации около 1с. Такой съём **преследует цель** зарегистрировать (или передать) сигнал с незащищённой ВОСП или с защищённой ВОСП, но только за время регистрации системы защиты.
- При **плавном выводе целью нарушителя** является сокрытие подключения, внесение минимальных потерь и регистрация перехваченного сигнала длительное время! Это способ представляет наибольшую опасность!
- **Ступенчатый вывод** преследует **цель** нейтрализации системы защиты, обнаруживающей плавный вывод путём многократного периодического вывода мощности сигнала на величину ниже порога обнаружения контроллера защиты.

Аппаратные средства защиты в ВОСП

Аппаратные средства защиты информации в волоконно-оптических коммуникациях

Коммутация линий

Режим динамического хаоса

Кодовое зашумление

Технология оптической CDMA

Применение разно-знаковых компенсаторов дисперсии

Мультиплексирование шума и сигнала на разных длинах волн

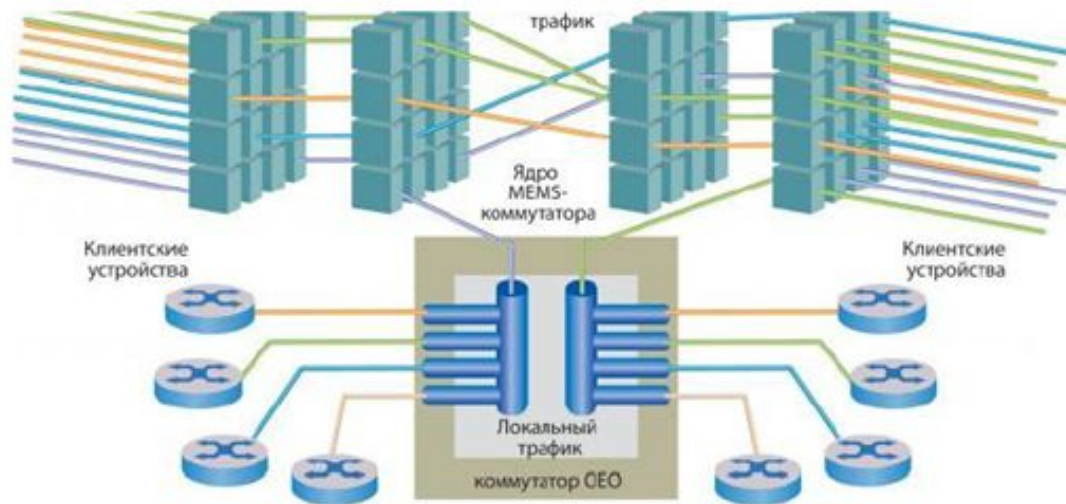
Контроль уровня битовых ошибок

Аппаратные средства защиты информационных систем — средства защиты информации и информационных систем, реализованных на аппаратном уровне.

Аппаратные средства защиты в ВОСП. Коммутация линий (волокон)

Аппаратные средства защиты информации в волоконно-оптических коммуникациях

Коммутация линий



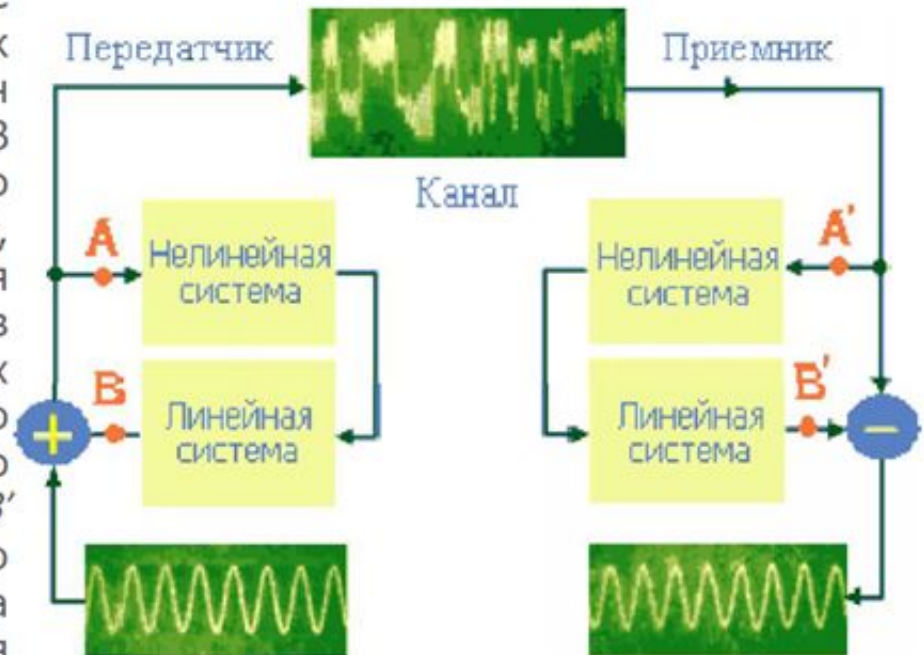
Коммутаторы на базе MEMS

Аппаратные средства защиты в ВОСП. Режим динамического хаоса

*Аппаратные средства защиты информации
в волоконно-оптических коммуникациях*

Режим динамического хаоса

Передатчик и приемник включают в себя такие же нелинейные и линейные системы, как источник. Дополнительно в передатчик включен сумматор, а в приемник - вычитатель. В сумматоре производится сложение хаотического сигнала источника и информационного сигнала, а вычитатель приемника предназначен для выделения информационного сигнала. Сигнал в канале хаотический и не содержит видимых признаков передаваемой информации, что позволяет передавать конфиденциальную информацию. Сигналы в точках A и A' , B и B' попарно равны. Поэтому при наличии входного информационного сигнала S на входе сумматора передатчика такой же сигнал будет выделяться на выходе вычитателя приемника.



Аппаратные средства защиты в ВОСП. Кодовое зашумление

*Аппаратные средства защиты информации в волоконно-оптических коммуникациях
Кодовое зашумление (метод случайного кодирования)*



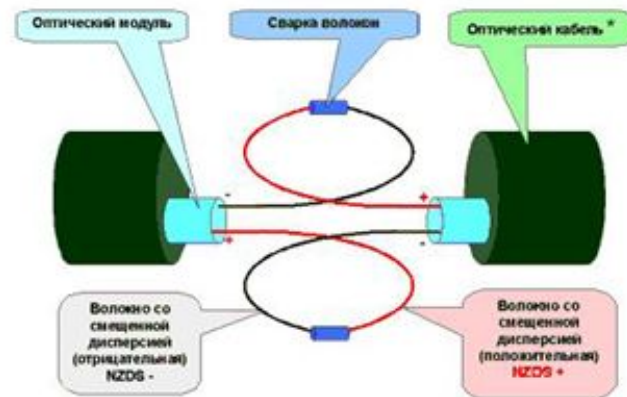
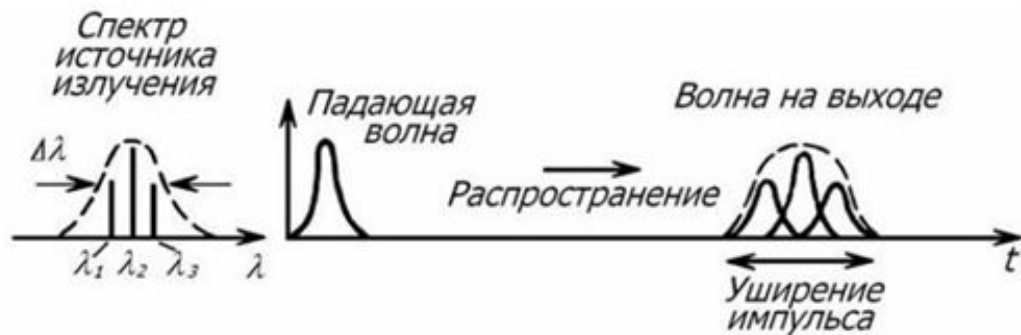
Один из алгоритмических методов, состоящий в применении специально подобранных преобразований передаваемой информации, которые гарантируют уменьшение вероятности правильного приема сообщений при оптимальном декодировании сигналов, получаемых из канала утечки информации.

Защита информации обеспечивается не за счет воздействия на параметры каналов утечки, а за счет вероятностного преобразования информации перед передачей по каналу связи. Невозможность восстановления информации злоумышленником основана на том свойстве, что канал утечки имеет меньшую пропускную способность, чем штатный канал пользователя. Способ кодирования выбирается так, чтобы в канале утечки количество возникающих ошибок сильно возрастало, обеспечивая эффект зашумления передаваемого сигнала, в то время как в основном канале обеспечивалась надежная связь.

Аппаратные средства защиты в ВОСП. Применение предискажения сигнала

Аппаратные средства защиты информации в волоконно-оптических коммуникациях

Применение разно-знаковых компенсаторов дисперсии



Аппаратные средства защиты в ВОСП. Применение OCDMA

Аппаратные средства защиты информации в волоконно-оптических коммуникациях

- *Защита трафика на основе технологии Optical Code Division Multiple Access (OCDMA)*

Технология связи множественного доступа с кодовым разделением, при которой каналы передачи имеют общую полосу частот, но разную кодовую модуляцию. В отличие от других методов доступа абонентов к сети, где энергия сигнала концентрируется на выбранных частотах (Frequency Division Multiple Access, FDMA) или временных интервалах (Time Division Multiple Access, TDMA), сигналы CDMA распределены в непрерывном частотно-временном пространстве. Фактически метод манипулирует и частотой, и временем, и энергией.

Преимущества

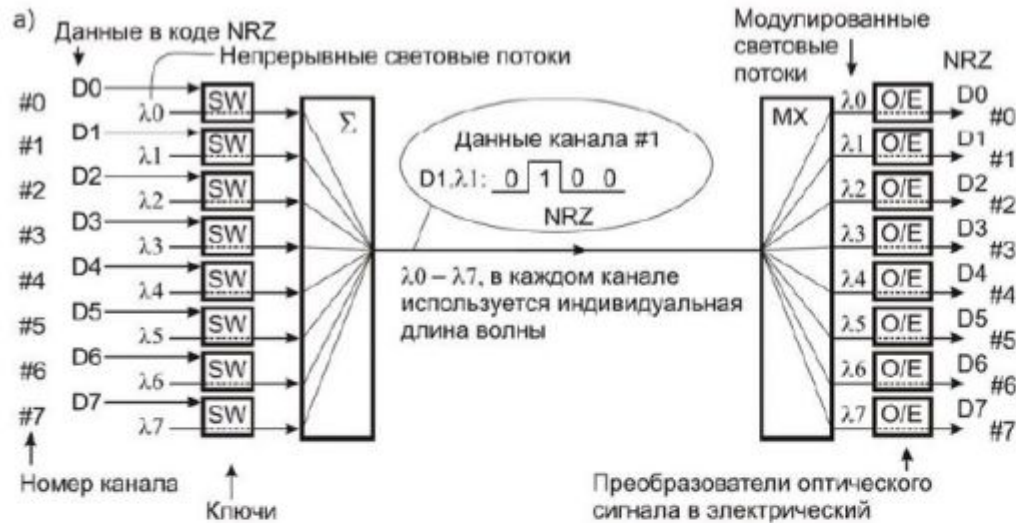
Высокая спектральная эффективность. Кодовое разделение позволяет обслуживать больше абонентов на той же полосе частот, чем другие виды разделения (TDMA, FDMA).

Гибкое распределение ресурсов. При кодовом разделении нет строгого ограничения на число каналов. С увеличением числа абонентов постепенно возрастает вероятность ошибок декодирования, что ведёт к снижению качества канала, но не к отказу обслуживания.

Более высокая защищённость каналов. Выделить нужный канал без знания его кода весьма трудно. Вся полоса частот равномерно заполнена шумоподобным сигналом.

Технология активно применяется в военной радиосвязи, в мобильных системах связи.

Аппаратные средства защиты в ВОСП. Применение OCDMA

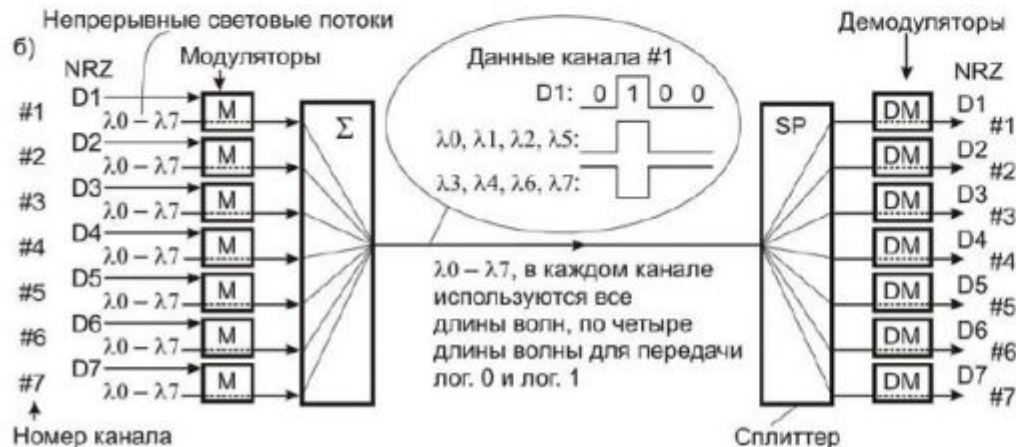


Защита трафика на основе технологии Optical Code Division Multiple Access (OCDMA)

Структурные схемы систем передачи данных с использованием технологий:

а) — WDM;

б) — CDMA



Основные положения по защите ВОСП

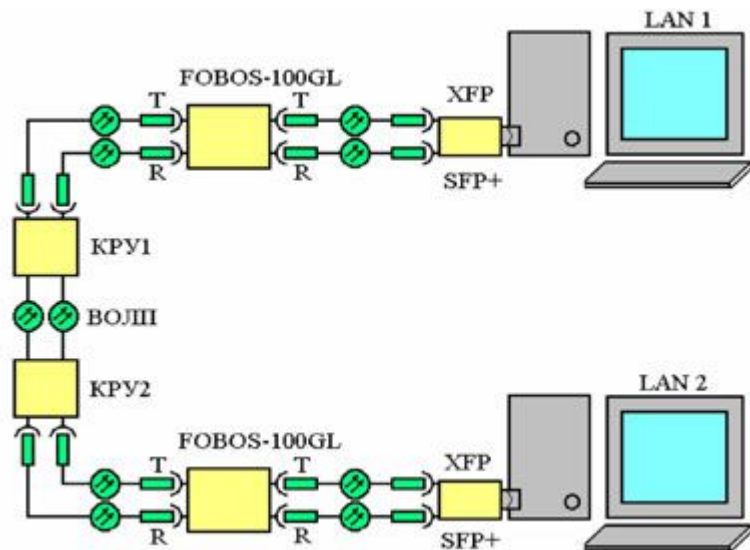
- Система защиты в ВОСП, которая обеспечивает безопасность информации ограниченного доступа при передаче за пределами контролируемой зоны, должна базироваться на следующих положениях:
- ВОСП должна иметь в своём составе следующие основные средства защиты: контроллер защиты, измеритель мощности, оптический рефлектометр, ПЭВМ со специализированным программным обеспечением. Контроллер может входить в состав ВОСП либо быть внешним. Оптический рефлектометр и ПЭВМ должны обеспечивать измерение, запись, обработку, хранение рефлектограмм. Также в составе средств защиты могут быть определены дополнительные устройства сигнализации (звуковые и световые устройства оповещения), управления уровнем мощности (аттенюаторы) и др.
- Контроллер защиты должен непрерывно осуществлять мониторинг уровней передачи в системе между передатчиком и приёмником оптических сигналов. При изменении уровня мощности или нарушении качества передачи по коэффициенту ошибок, контроллер должен переключить или отключить передачу сигнала по линии. При этом должна предусматриваться защита от ложных отклонений показателей контроля путём установления пороговых значений эксплуатации (временные интервалы, коэффициенты ошибок и др.).
- Контроллер блокирует включение системы передачи в работу, если нарушена или неработоспособна система защиты.
- Перед каждым включением защищённой ВОСП должны быть сняты и записаны в ПЭВМ рефлектограммы используемых волокон на рабочей длине волны. Полученные рефлектограммы с помощью спецпрограммного обеспечения сравниваются с измеренными ранее. В случае обнаружения локальных дефектов, которых не было на предыдущих рефлектограммах должны быть определены причины их появления и приняты меры по их устранению. И ТОЛЬКО ТОГДА ВКЛЮЧАЕТСЯ В РАБОТУ ЗАЩИЩЁННАЯ ВОСП.
- Перед первым включением ВОСП должны быть сняты и записаны все рефлектограммы с двух сторон системы и на разных длинах волн с целью обнаружения «закладок».

Программно-технические средства защиты информации (ПТСЗИ) высокоскоростных ВОСП (от 100 Мбит/с и до 100 Гбит/с) - FOBOS

- **Назначение:** Универсальные контроллеры защиты FOBOS-10GS, FOBOS-100GL, FOBOS-100GE (Fiber Optic Block Organizer Security) являются ПТСЗИ от утечки по оптическому каналу с участков волоконно-оптических линий передачи (ВОЛП), расположенных за пределами контролируемой зоны (КЗ) **без использования криптографии.**
Предназначены для создания защищенных ВОСП информации ограниченного доступа (до второй категории включительно). ВОСП объединяют локальные вычислительные системы в единую сеть по ВОЛП со скоростями передачи от 100 Мбит/с до 100 Гбит/с и более (технологии FE, GE, 10GE, 40GE, 100GE, STM 1 - STM 256, FC, WDM, CWDM, DWDM, HDWDM). Дальность передачи до 100 км.
- **Основные функции контроллеров защиты:**
 - Поддержка передачи цифровой информации по ВОЛП в реальном масштабе времени с пропускной способностью канала, заданной передатчиком ВОСП
 - Автоматическая настройка на любую длину оптических линий в установленных пределах
 - Активная защита от несанкционированной и непреднамеренной реконфигурации сети за пределами КЗ и попыткам доступа к средствам защиты
 - Постоянный контроль коэффициента передачи используемых оптических волокон с отключением передачи оптических сигналов при появлении дополнительных потерь 0,010 дБ и более. При этом вероятность отключения составит не менее 0,99999, а среднее время наработки на ложную тревогу - не менее 10000 часов. Время реакции контроллеров на нарушения – менее 0,2 с
 - Установка заданной мощности информационного оптического сигнала на входном полюсе ВОЛП
 - Световая и звуковая индикация состояния.



Типовая схема включения FOBOS и технические характеристики



Основные технические характеристики контроллеров защиты:

Тип контроллера защиты	Тип оптического волокна (рекомендация)	Рабочая длина волны, мкм	Коэффициент передачи ВОЛП, дБ	Максимальная дальность передачи (без усиления), км
FOBOS-10GS	MMF (G.651.1)	1,27 – 1,37	0 - 10	FE - 2 GE – 0,55 10GE -0,3 40GE, 100GE – 0,1
FOBOS-100GL	SMF (G.652)	1,47 – 1,57	0 - 25	FE – 100 GE – 100 10GE -70 40GE, 100GE – 10
FOBOS-100GE-S FOBOS-100GE-C FOBOS-100GE-L	SMF (G.653 – G.656)	1,507 - 1,513 1,547 - 1,553 1,607 – 1,613	0 - 30	FE - 100 GE – 100 10GE -70 40GE, 100GE – 10



Часть 2

ЗАЩИТА ОПТИЧЕСКОГО СИГНАЛА. КРИПТОГРАФИЧЕСКИЕ РЕШЕНИЯ

Что является предметом изучения этой части?

- Криптография в телекоммуникациях

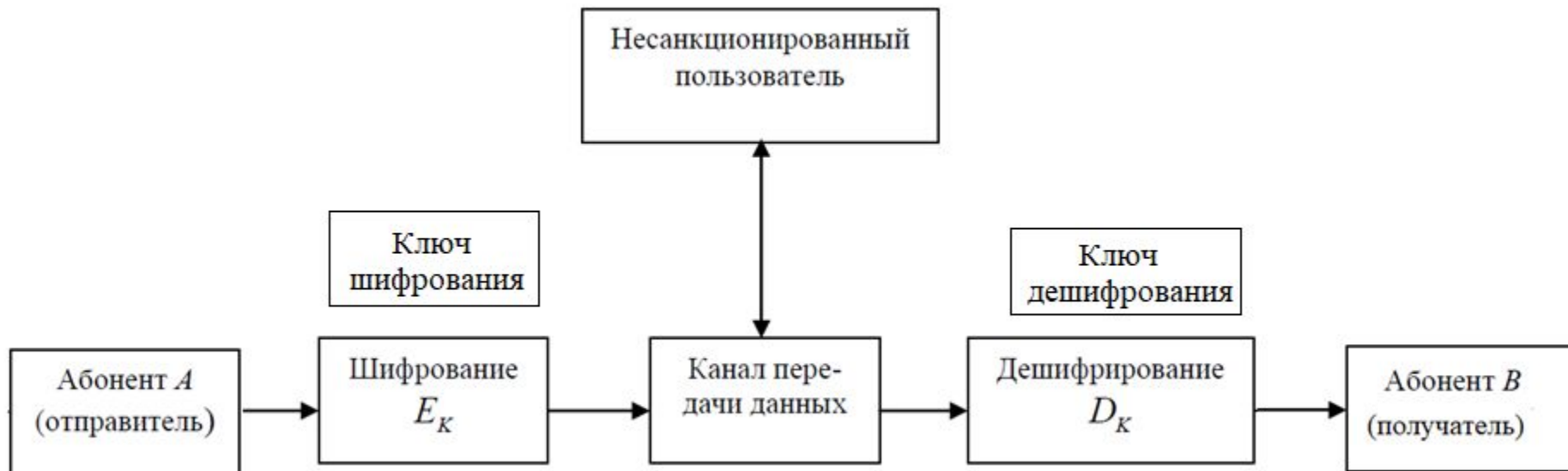
- Проблема тайной передачи сообщений существует столько времени, сколько существует письменность, более того, первоначально письменность сама по себе была методом тайной передачи информации, поскольку была доступна лишь избранным.
- Для реализации тайной передачи сообщения от одного адресата к другому существует два направления: во-первых, можно попытаться скрыть сам факт передачи сообщения, например, методами тайнописи, во-вторых, можно так преобразовать сообщение, чтобы постороннему лицу была недоступна информация, заключенная в сообщении.
- Первым направлением занимается *стеганография*, вторым — *криптография*.
- При изучении будут рассматриваться **криптографические методы защиты информации, передаваемой по телекоммуникационным системам**. Для защиты информации используется, прежде всего, шифрование. При шифровании происходит преобразование данных в вид, недоступный для чтения без соответствующей информации (ключа шифрования). Задача состоит в том, чтобы обеспечить конфиденциальность, скрыв информацию от лиц, которым она не предназначена, даже если они имеют доступ к зашифрованным данным. Кроме этого, используются криптографические методы контроля целостности переданной информации и криптографические методы аутентификации абонента, позволяющие убедиться, что информация передана именно данному абоненту.

Термины, необходимые для рассмотрения методов использования криптографии в телекоммуникационных системах

- **Система криптографическая (криптосистема)** — система обеспечения безопасности системы связи, использующая криптографические средства. В качестве подсистем может включать системы шифрования, аутентификации, имитационной защиты, цифровой подписи.
- **Система шифрования** — система обеспечения конфиденциальности, предназначенная для защиты информации от ознакомления с ее содержанием лиц, не имеющих права доступа к ней, путем шифрования информации. Математическая модель системы включает способ кодирования исходной и выходной информации, шифр и ключевую систему.
- **Система ключевая** — определяет порядок использования криптографической системы и включает системы установки и управления ключами.
- **Симметричные криптографические системы (симметричное шифрование, симметричные шифры, криптографические системы с секретным ключом)** — способ шифрования, в котором для шифрования и дешифрирования применяется один и тот же **секретный** криптографический ключ, который никогда не передается по от-крытому каналу связи.
- **Криптографическая система с открытым ключом (или асимметричное шифрование)** — система при которой используется пара ключей, причем **открытый ключ** передаётся по открытому (т. е. незащищённому, доступному для наблюдения) каналу, а криптографическая стойкость обеспечивается наличием **закрытого** ключа.
- **Система аутентификации** — криптографическая система, выполняющая функцию идентификации сторон в процессе информационного взаимодействия. Математическая модель системы включает протокол аутентификации.
- **Система имитационной защиты** (обеспечения целостности) информации — криптографическая система, выполняющая функцию аутентификации содержания сообщения или документа и предназначенная для защиты от несанкционированного изменения информации
- **Система цифровой подписи** — криптографическая система, выполняющая функцию аутентификации источника сообщения или документа.
- **Криптографический протокол** - коммуникационный протокол, реализованный с применением криптографических алгоритмов для решения задач защиты информации, в рамках которого стороны информационного взаимодействия последовательно выполняют определенные действия и обмениваются сообщениями

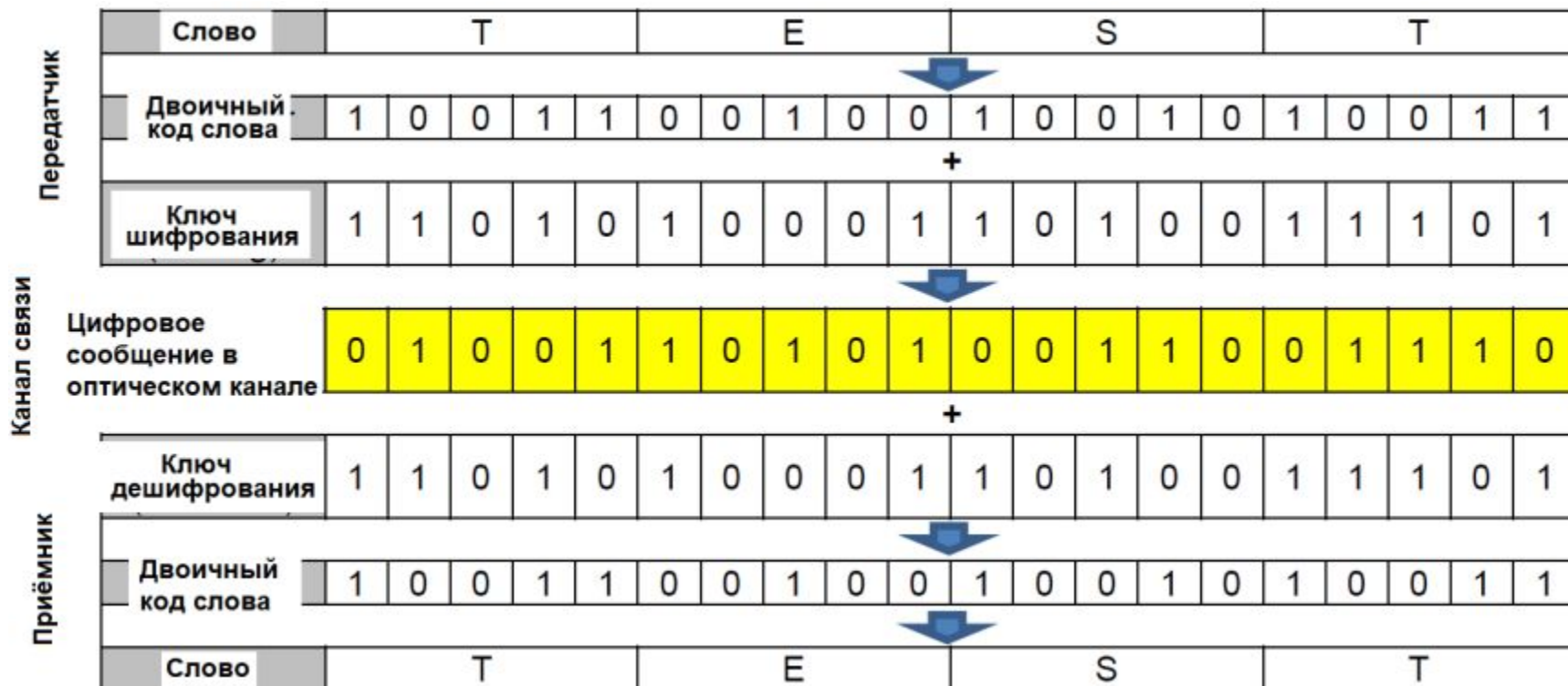
Шифрование и дешифрование в канале передачи

Шифрование и дешифрование сообщений происходит на входе и выходе канала передачи данных. Несанкционированный пользователь анализирует процесс передачи информации по каналу связи и имеет возможность формировать свои собственные сообщения и искажать передаваемую информацию.



Различают два типа алгоритмов шифрования: симметричные (с закрытым или секретным ключом) и асимметричные (с открытым ключом). В первом случае ключ шифрования совпадает с ключом дешифрования. В асимметричных алгоритмах для шифрования и дешифрования используются различные ключи, причем знание одного из них не дает практической возможности определить другой.

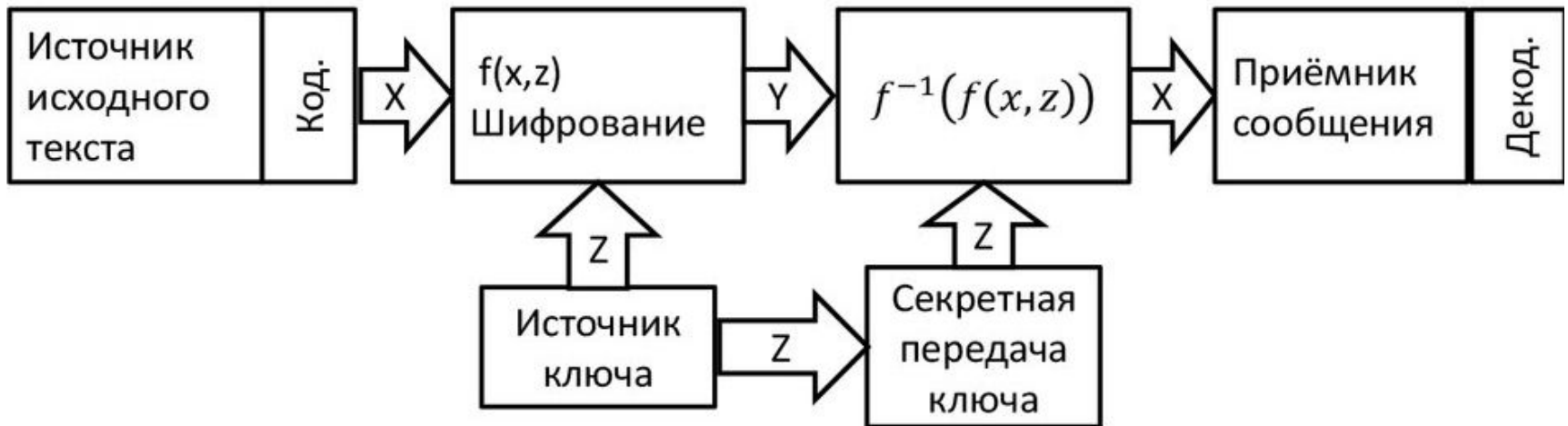
Пример схемы шифрования-дешифрования для канала связи с использованием симметричного ключа. Шифруемое слово представлено в двоичном формате букв. Шифрование и дешифрование производится симметрично с использованием двоичного ключа операцией сложения по модулю два



Основная идея криптографии – наличие ключа шифрования и его секретность

Классическая криптография

Криптографическая система с одним ключом (общим для шифрования и расшифрования)



Пояснение к принципу симметричного шифрования

Принцип работы симметричного шифрования:



Отправитель и получатель должны заранее договориться

1. о секретном ключе
2. об алгоритме
3. о векторе инициализации
4. о режиме вычислений
5. о заполнении пустых позиций

Существует 2 типа симметричных алгоритмов:

Блочные шифры (за 1 проход алгоритма обрабатывают блок байт размером 64 или 128 бит)

Потоковые шифры (за 1 проход алгоритма обрабатывают 1 байт или бит)

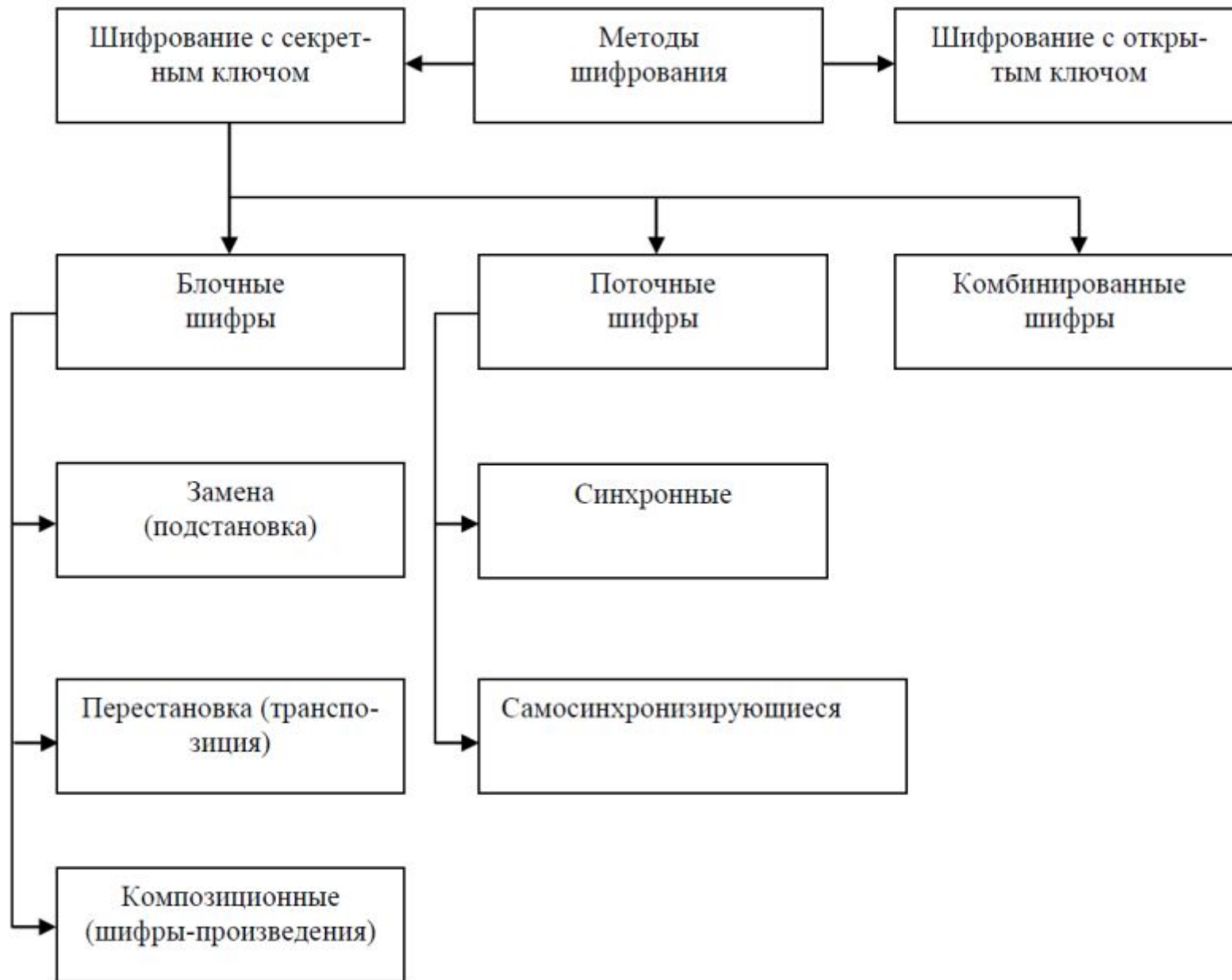
Асимметричное шифрование и его протокол RSA (по именам создателей: Rivest, Shamir, Adleman)

- Асимметричное шифрование основано на использовании того факта, что задача разложения большого числа на простые сомножители является трудной.
- Такая криптосистема базируется на следующих двух фактах из теории чисел:
 - 1. Задача проверки числа на простоту является сравнительно легкой;
 - 2. Задача разложения чисел вида $n = pq$ (p и q — простые числа) на множители является очень трудной, если мы знаем только n , а p и q — большие числа (это так называемая задача факторизации).
- Обмен сообщениями по протоколу RSA происходит следующим образом:
 - 1. Абонент-получатель шифрованных сообщений Б генерирует открытый и закрытый ключи.
 - 2. Открытый ключ получатель Б рассылает всем отправителям (в том числе А).
 - 3. Отправитель (А) шифрует сообщение открытым ключом получателя Б и отправляет его получателю.
 - 4. Получатель Б расшифровывает сообщение своим закрытым ключом.

Как обезопасить ключ шифрования?

- Роль инструкции для шифрования и дешифровки играет **шифровальный ключ**. Чем длиннее ключ, тем сложнее «взлом» шифра, а если длина ключа сопоставима с длиной зашифрованного текста, то его дешифровка без знания ключа может быть просто невозможной.
- Однако если ключ попадет в чужие руки, шифрование становится бессмысленным. Чтобы обеспечить безопасную передачу ключа, его можно отправить с доверенным курьером или по какому-то каналу, заведомо защищенному от прослушивания.
- Но когда шифруется едва ли не вся информация в сети, создавать специальные каналы для ключей нецелесообразно. Особенно учитывая, что ключи для шифрования нужно постоянно менять. Поэтому и шифровальные ключи, и сами зашифрованные сообщения передаются по одним и тем же каналам.

Методы шифрования. Классификация для телекоммуникаций



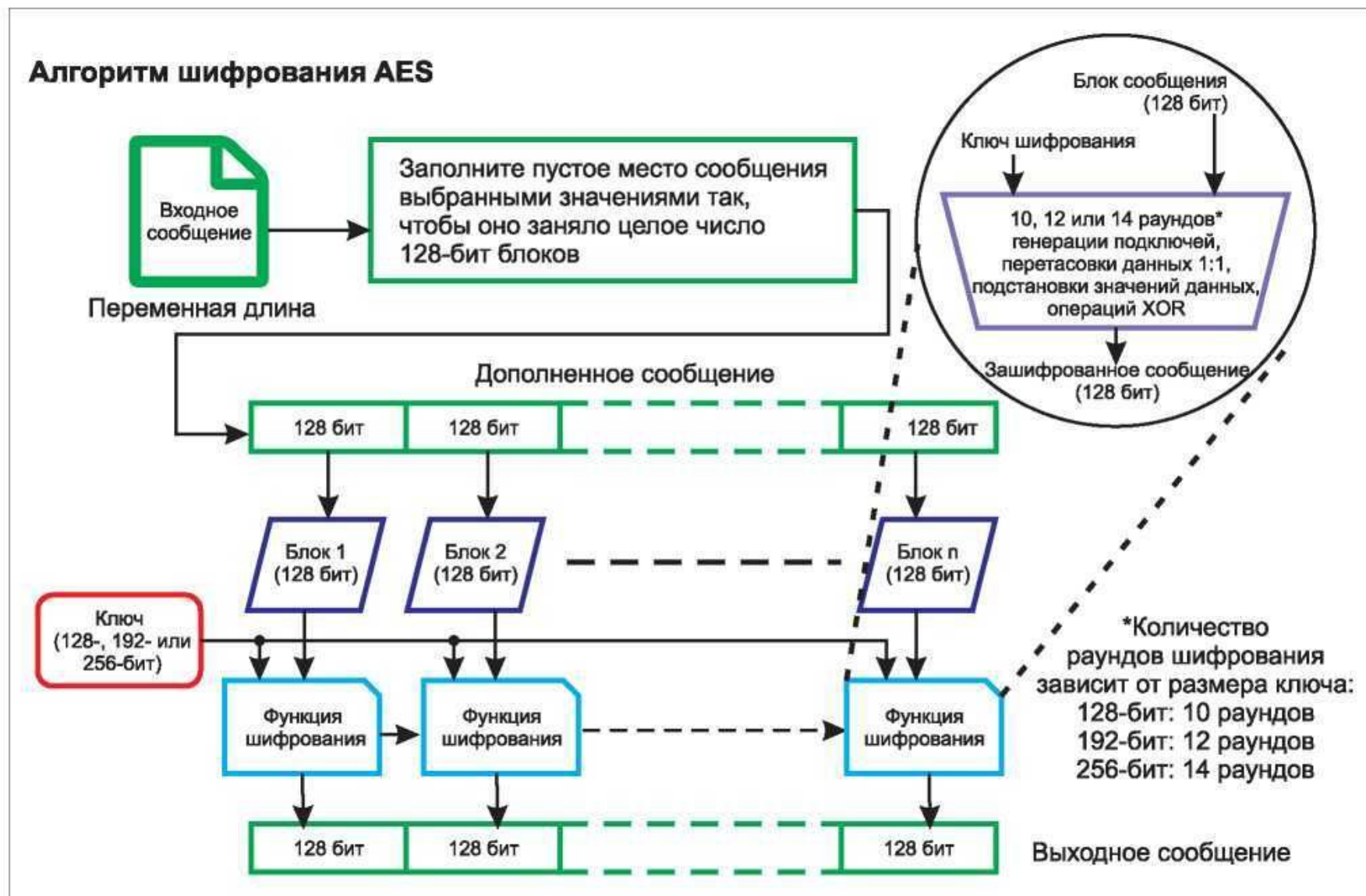
Блочные шифры и алгоритм шифрования AES

- Блочные шифры нашли широкое применение в телекоммуникационных системах (в транспортных каналах и в оптических сетях доступа). Они строятся на основе многократного применения относительно простых криптографических преобразований, к которым относятся подстановки и перестановки.
- Блочные шифры представляют собой семейство обратимых преобразований блоков (частей фиксированной длины) исходного текста. В процессе шифрования информация делится на порции величиной от одного до сотен бит. Блочные шифры наиболее распространены на практике. Примером такой структуры является конструкция Фейстеля, которая лежит в основе блочных шифров DES, ГОСТ 28147-89, AES и др. с использованием различного числа раундов шифрования. Двумя наиболее широко используемыми стандартами шифрования являются Advanced Encryption Standard (AES) и Data Encryption Standard (DES). Оба эти стандарта шифрования являются примерами блочных шифров, что означает, что они шифруют данные блоками фиксированного размера.
- БЛОЧНЫЙ ШИФР в телекоммуникациях различного уровня: AES, или Advanced Encryption Standard, - это алгоритм шифрования с симметричным ключом, который может быть сформирован по алгоритму Диффи-Хеллмана. Это одно из самых универсальных и наиболее любимых технических решений в сфере криптографии. AES реализует большое количество раундов шифрования.
- В основе AES лежит блочный шифр, который использует 128-битный размер блока и 128, 192 или 256-битные ключи для шифрования данных. AES 256 - это версия стандарта с 256-битными ключами (14 раундов шифрования). Этот стандарт широко считается самым безопасным стандартом цифровой криптографии, который обычно используется для наиболее надежной сквозной шифрованной связи, в том числе для оптических каналов на высоких скоростях (10/100 Гбит/с).

Принцип алгоритма AES

- Алгоритм AES был разработан двумя бельгийскими криптографами, Джоаном Деменом и Винсентом Риджменом, и был принят в качестве официального стандарта в 2001 году Национальным институтом стандартов и технологий США. Такое достижение свидетельствует о широком признании, которое получил стандарт. Уже более 20 лет AES 256 и шифрование AES в целом является одним из наиболее предпочтительных решений для разработчиков, желающих создать систему, в которой коммуникации хорошо защищены от постороннего или внешнего влияния и утечек. Вот упрощенная схема того, как это работает.
- Алгоритм шифрования AES основан на принципе **подстановок и перестановок** и имеет архитектуру для которой характерно:
 - представление шифруемого блока в виде двумерного байтового массива;
 - шифрование за один раунд всего блока данных;
 - выполнение криптографических преобразований, как над отдельными байтами массива, так и над его строками и столбцами. Это обеспечивает «диффузию» данных одновременно в двух направлениях — по строкам и по столбцам.
- **Реализация.**
- Алгоритм AES является довольно нетребовательным к ресурсам и может успешно применяться в микроконтроллерных системах, обладающих небольшой мощностью по обработке информации.
- AES хорошо работает даже на 8-битных контроллерах с минимальным объёмом памяти и позволяет шифровать и расшифровывать как данные в памяти самих микроконтроллеров, так при передаче этих данных по проводным и беспроводным сетям связи.

Общая схема алгоритма шифрования AES



Процесс шифрования AES (<https://skine.ru/articles/91790/>)

- Основная концепция шифрования заключается в том, что шифр заменяет каждую единицу информации другой, в зависимости от ключа безопасности. Например, *AES-256* завершает 14 раундов шифрования, что делает его невероятно безопасным.
- Шаги включают в себя разделение данных на блоки, замену разных байтов, смещение строк и смешивание столбцов, чтобы полностью *скремблировать* информацию. К концу процесса результатом является совершенно случайный набор символов, который не будет иметь смысла ни для кого, если у них нет ключа расшифровки.
- **Алгоритм шифрования AES состоит из пяти основных этапов:**
- **Расширение ключа** - производное секретного ключа, называемое ключами раунда, получается из ключа шифрования с использованием расписания ключей AES.
- **Добавить ключ раунда** - каждый байт матрицы комбинируется с байтом ключа раунда с помощью побитового XOR (исключающее «или»).
- **Замещающие байты** - шаг замещения, на котором каждый байт заменяется другим в соответствии с таблицей поиска.
- **Shift Rows** - шаг транспонирования, при котором последние три строки состояния циклически сдвигаются на определенное количество шагов.
- **Смешивание столбцов** - операция смешивания, которая работает со столбцами матрицы, объединяя четыре байта в каждом столбце.

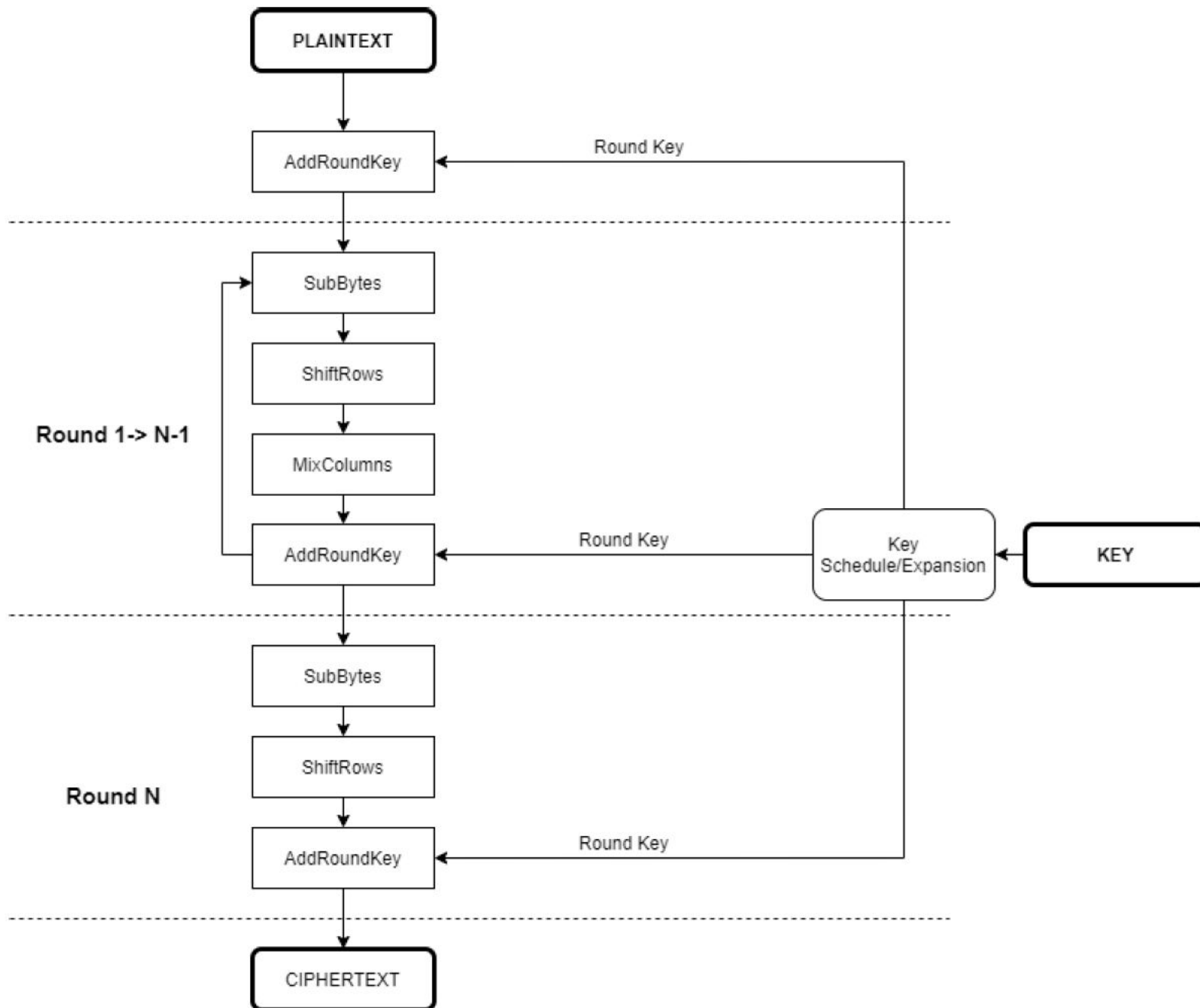
Процесс шифрования AES

- **Какой смысл каждого из этих шагов?**
- Многое происходит, когда наши данные зашифрованы, и важно понять, почему ключ **расширение является критическим** шаг, потому что он дает нам наши ключи для последующих раундов. В противном случае один и тот же ключ будет добавляться в каждом раунде, что облегчит взлом AES. В первом раунде добавляется начальный ключ, чтобы начать изменение простого текста.
- **шаг замещения байта**, где каждая из точек данных изменяется в соответствии с заранее определенной таблицей, **также выполняет важную роль**. Это изменяет данные нелинейным способом, чтобы ввести в заблуждение информацию. Путаница – это процесс, который помогает скрыть связь между зашифрованными данными и исходным сообщением.
- **Сдвиг строк также имеет решающее значение**, выполняя то, что известно как диффузия. В криптографии диффузия по существу означает транспонирование данных для добавления усложнения. При смещении строк данные перемещаются из исходного положения, что еще больше помогает скрыть их. **Смешайте столбцы** действует аналогичным образом, изменяя данные по вертикали, а не по горизонтали.
- В конце раунда добавляется новый ключ раунда, полученный из начального ключа. Это добавляет большую путаницу к данным.

Процесс шифрования AES

- **Почему так много раундов?**
- Процессы **добавление круглых ключей, подстановка байтов, смещение строк и смесительные колонны** изменяет данные, но все еще может быть взломан криптоанализом, который является способом изучения криптографического алгоритма, чтобы сломать его.
- **Ускоренные атаки** являются одним из **ключевые угрозы**. Это атаки, которые могут взломать шифрование с меньшими усилиями, чем перебор. Когда разрабатывался AES, были обнаружены быстрые атаки на срок до шести раундов процесса. Из-за этого были добавлены дополнительные четыре раунда для минимума **128-битный AES как запас прочности**. Получающиеся 10 раундов дают методу шифрования достаточно места для предотвращения коротких атак в соответствии с современными технологиями и технологиями..
- **Почему бы нам не добавить больше раундов, чтобы повысить безопасность?**
- С большинством вещей в безопасности, должно быть **компромисс между чистой защитной силой, удобством использования и производительностью**. Если вы установите десять стальных дверей с засовами в каждой точке входа в ваш дом, это, несомненно, сделает его более безопасным. Также потребуется неоправданно много времени, чтобы войти и выйти, поэтому мы никогда не видим, чтобы кто-то делал это.
- То же самое относится и к шифрованию. Мы могли бы сделать его более безопасным, добавив больше раундов, но это также было бы медленнее и намного менее эффективно. **10, 12 и 14 раундов AES были установлены, потому что они обеспечивают хороший компромисс** между этими конкурирующими аспектами, по крайней мере, в нынешнем технологическом ландшафте.

Процесс шифрования AES



Размер ключа шифрования и его возможные комбинации

Размер ключа	Возможные комбинации
1 бит	2
2 биты	4
4 биты	16
8 биты	256
16 биты	65536
32 биты	4.2×10^9
56 бит (DES)	7.2×10^{16}
64 биты	1.8×10^{19}
128 бит (AES)	3.4×10^{38}
192 бит (AES)	6.2×10^{57}
256 бит (AES)	1.1×10^{77}

AES-256, имеющий **длину ключа 256 бит**, поддерживает самый большой размер битов и практически не может быть взломан грубой силой в соответствии с текущими стандартами вычислительной мощности, что делает его на сегодняшний день самым надежным стандартом шифрования.

Алгоритм Диффи-Хеллмана (Diffie-Hellman, DH) формирования и распределении секретного ключа с использованием незащищенного канала

- Алгоритм Диффи-Хеллмана не применяется для шифрования сообщений или формирования электронной подписи. Его назначение – в распределении ключей.
- Он позволяет двум или более пользователям обменяться без посредников ключом, который может быть использован затем для симметричного шифрования. Это была первая криптосистема, которая позволяла защищать информацию без использования секретных ключей, передаваемых по защищенным каналам.
- Алгоритм построен на простой формуле: $A = G^a \bmod P$
- В приведенном далее расчете, **модификация** означает операцию по модулю. По сути, это расчеты, чтобы **выяснить остаток** после деления левой части на правую.
- В качестве примера: $15 \bmod 4 = 3$
- Остаток от деления по модулю означает следующее: мы делим одно число на другое с остатком. Целую часть выкидываем, а остаток — это то, что нам нужно. Обозначается такое деление словом **mod**.
- Например, $12 \bmod 5 = 2$, потому что $12 = 2 \times 5 + 2$
- $13 \bmod 4 = 1$, потому что $13 = 3 \times 4 + 1$
- $10 \bmod 2 = 0$, потому что $10 = 5 \times 2 + 0$
- В криптографии деление по модулю применяется часто, потому что зная два исходных числа найти остаток очень легко, а вычислить первое число, зная второе и остаток — невозможно.
- Если $X \bmod 5 = 1$, то X может быть равен 6, 11, 16, 21 и так далее — остаток от деления каждого из этих чисел по модулю 5 равен одному. Поэтому пересылать остаток от деления по модулю можно, а первое число — нет.

Алгоритм Диффи-Хеллмана передачи секретного ключа по незащищенному каналу (обмен между А и Б)

Итак, пусть Алиса и Боб решили обмениваться шифрованными сообщениями, но в их распоряжении имеется только незащищенный открытый канал связи, при этом никаких возможностей встретиться или передать секретный ключ через кого-нибудь другого у них нет. В соответствии с алгоритмом Диффи—Хеллмана для успешного решения задачи Алиса и Боб должны выполнить следующие действия.

Прежде всего они открыто договариваются о том, что будут использовать одностороннюю функцию $Y = D^x \bmod P$. Затем они договариваются о значениях параметров D и P . Пусть, например, они договорились, что $D = 7$ и $P = 13$, то есть функция имеет вид $Y = 7^x \bmod 13$. Еще раз подчеркнем, что в соответствии с алгоритмом Диффи—Хеллмана вся эта информация не является секретной, и даже если переговоры будут подслушаны Евой, это не даст ей возможности прочитать сообщения Алисы и Боба.

Пример использования алгоритма Диффи-Хеллмана для формирования ключа шифрования без использования закрытого канала связи

1	Алиса секретным образом выбирает произвольное число А (закрытый ключ Алисы)	Пусть, например, $A = 2$	Боб также секретно выбирает произвольное число В (закрытый ключ Боба)	Пусть, например, $B = 4$
2	Алиса вычисляет значение а односторонней функции Y, используя в качестве аргумента свое секретное число А: то есть $a = D^A \bmod P$ (открытый ключ Алисы)	$a = 7^2 \bmod 13 = 10$	Боб также вычисляет значение b односторонней функции Y, используя в качестве аргумента свое секретное число В: $b = D^B \bmod P$ (открытый ключ Боба)	$b = 7^4 \bmod 13 = 2401 \bmod 13 = 9$
3	Алиса посылает Бобу свой открытый ключ а	10	Боб посылает Алисе свой открытый ключ b	9
4	Алиса, получив от Боба число b, вычисляет по формуле $K = b^A \bmod P$ (разделяемый секретный ключ)	$K = 9^2 \bmod 13 = 81 \bmod 13 = 3$	Боб, получив от Алисы число a, вычисляет по формуле $K = a^B \bmod P$ (разделяемый секретный ключ)	$K = 10^4 \bmod 13 = 10000 \bmod 13 = 3$

Что такое алгоритм шифрования AES 256 GCM?

- AES 256 GCM — это алгоритм шифрования, который использует блочный шифр Advanced Encryption Standard (AES) с длиной ключа в 256 бит и режимом гаммирования с обратной связью по шифротексту Galois/Counter Mode (GCM).
- GCM — это аутентифицированное шифрование, которое обеспечивает конфиденциальность данных (шифрование) и целостность данных (аутентификация) с использованием одного и того же ключа. Он также обеспечивает аутентификацию источника данных, что означает, что получатель может убедиться в том, что данные были созданы тем, кем они должны быть и никто другой не мог их изменить или подделать.

Контрольные вопросы 1

- 1. Какие способы защиты информации предусмотрены в ВОЛС и системах передачи и что при этом классифицируется?
- 2. Какими способами можно защитить оптические каналы и волокна?
- 3. Какими способами можно защитить сигналы, передаваемые в оптических волокнах оптического кабеля?
- 4. Какими способами можно защитить от перехвата информацию в оптическом кабеле?
- 5. Как можно проконтролировать намерения нарушителя возле оптического кабеля?
- 6. Чем фиксируется нарушение защитного периметра оптического кабеля?
- 7. Что может помешать нарушителю в оптическом кабеле для доступа к волокнам?
- 8. Как можно выявить действия нарушителя по перехвату трафика в оптической системе передачи?
- 9. Что такое оптическая рефлектометрия?
- 10. Что позволяет выявить рефлектометрия?
- 11. Как можно обнаружить «закладки» методами рефлектометрии?
- 12. Чем характеризуются «закладки» на рефлектограмме?
- 13. Чем отличаются быстрый вывод, плавный вывод и ступенчатый вывод?
- 14. Что показывают рефлектограммы с одного и двух направлений измерений и на разных длинах волн?
- 15. Перечислите аппаратные средства защиты в ВОСП?
- 16. Что даёт с точки зрения защиты информации применение разнознаковых компенсаторов дисперсии?
- 17. Что такое OCDMA и какое отношение это имеет к защите информации?
- 18. Для чего предназначены и какие функции защиты выполняют контроллеры FOBOS?

Контрольные вопросы 2

- 19. Что такое криптосистема?
- 20. Для чего нужно шифрование информационного трафика?
- 21. Что представляет собой симметричное и асимметричное шифрование?
- 22. Что такое аутентификация?
- 23. Что есть криптографический протокол?
- 24. Что такое «сложение по модулю два»?
- 25. В чём смысл шифрования по протоколу RSA?
- 26. Что такое ключ шифрования?
- 27. Как обезопасить ключ шифрования?
- 28. Какие методы шифрования информации применяются в телекоммуникационных системах?
- 29. Что представляет собой блочный шифр?
- 30. Что такое AES?
- 31. В чём состоит принцип действия AES?
- 32. Что представляет собой раунд шифрования?
- 33. Сколько возможных комбинаций у ключа AES256?
- 34. Для чего применяется алгоритм Диффи-Хеллмана?
- 35. Что обозначает AES256 GCM?

Задача

Используя алгоритм Диффи-Хеллмана вычислите разделяемый секретный ключ шифрования по варианту и представьте его в двоичном подходящим по разряду коде. Для решения задачи используйте примеры, приведённые выше.

Подробно представьте все этапы вычисления!

Вариант, последняя цифра студ. билета или номера пароля		0	1	2	3	4	5	6	7	8	9
Секретное число стороны А	Х	2	3	4	5	6	7	6	5	4	3
	Д	4	5	4	6	7	3	2	3	5	8
	Р	6	6	7	8	5	6	12	2	4	7
Секретное число стороны Б	Х	3	4	5	6	7	6	5	4	3	2
	Д	4	5	4	6	7	3	2	3	5	8
	Р	6	6	7	8	5	6	12	2	4	7