# Методы защиты информации в системах связи и передачи данных

- Проверил(а):
- Сделал: Рахимжанов Арман Серикбекович с гр.ФПР-207

- Среди всего многообразия способов несанкционированного перехвата информации особое место занимает анализ трафика в сети доступа, поскольку сеть доступа - самый первый и самый удобный источник связи между абонентами в реальном масштабе времени, и при этом самый незащищенный.
- Сеть доступа имеет еще один недостаток с точки зрения безопасности - возможность перехвата речевой информации из помещений, по которым проходит телефонная линия, и где подключен телефонный аппарат (далее оконечное оборудование (ОО)), даже тогда, когда не ведутся телефонные переговоры. Для такого перехвата существует специальное оборудование, которое подключается к телефонной линии внутри контролируемого помещения или даже за его пределами. Требования к оборудованию противодействия данных угрозам описывают НД ТЗІ 2.3-002-2011, НД ТЗІ 2.3-003-2011, НД ТЗІ 4.7-001-2011 и некоторые другие нормативные документы.
- В общем случае от ОО к АТС и обратно передаются:
- сигналы управления и сигнализации стандартного оборудования (ТА, модем и т.д.);
- сигналы передачи данных, речь;
- сигналы сигнализации и управления нестандартного оборудования (охранная, пожарная сигнализация и др.).

# Методы защиты информации в канале связи

- Методы защиты информации в канале связи можно разделить на две группы: основанные на ограничении физического доступа к линии и аппаратуре связи;
- основанные на преобразовании сигналов в линии к форме, исключающей (затрудняющей) для злоумышленника восприятие или искажение содержания передачи.

- Методы первой группы в основном находят применение в системах правительственной связи, где осуществляется контроль доступа к среде передачи данных.

- Методы второй группы направлены на обратимое изменение формы представления передаваемой информации. Преобразование должно придавать информации вид, исключающий ее восприятие при использовании аппаратуры, стандартной для данного канала связи. При использовании же специальной аппаратуры восстановление исходного вида информации должно требовать затрат времени и средств, которые по оценке владельца защищаемой информации делают бессмысленным для злоумышленника вмешательство в информационный процесс.
- При защите обмена данными решающее значение имеет форма представления сигнала в канале связи.

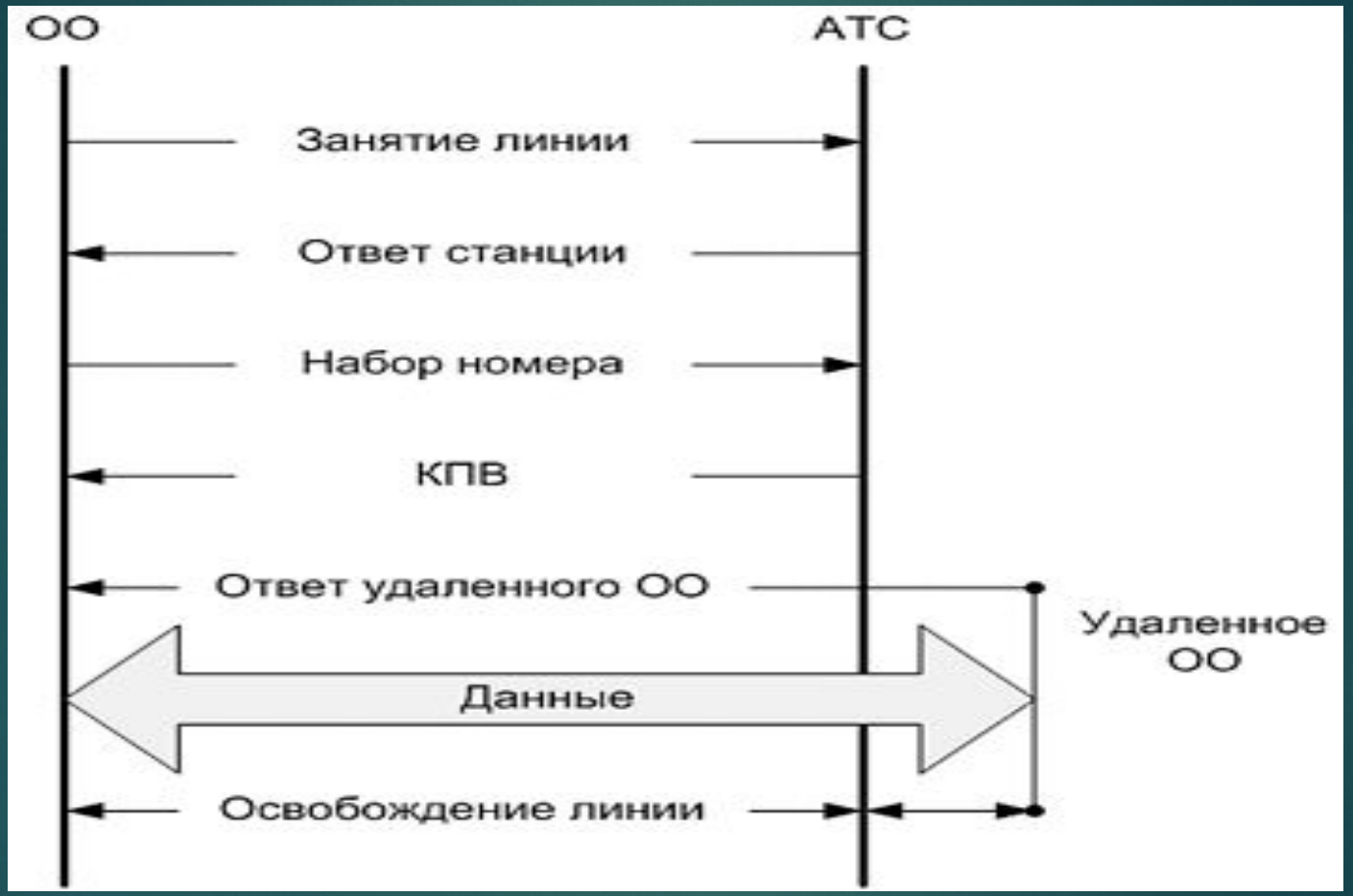
Следует учесть, что деление на "аналоговый" или "цифровой" сигнал условно. Для некоторых вариантов механизмов защиты информации требуется взаимная синхронизация и обмен служебными посылками между взаимодействующей аппаратурой защиты, т.е. присутствует цифровой режим, однако, поскольку этот режим не связан непосредственно с речевым обменом, требования к его скоростным характеристикам достаточно свободны.

- С другой стороны, символьный (цифровой) обмен в протяженных каналах всегда осуществляется через модемное преобразование в виде аналогового сигнала.
- Попробуем провести краткий анализ вариантов угроз информации в канале связи. Для удобства анализа проведем классификацию канала связи по степени защищенности (защиты) передаваемой информации.
- Полученные результаты сведем в таблицу 1. На рисунках 1, 2 изобразим структурные схемы передачи данных для соответствующих каналов на примере взаимодействия ОО (КСЗИ) с АТС и удаленным ОО (КСЗИ).

**Таблица 1.** *Анализ вариантов угроз информации в канале связи.*

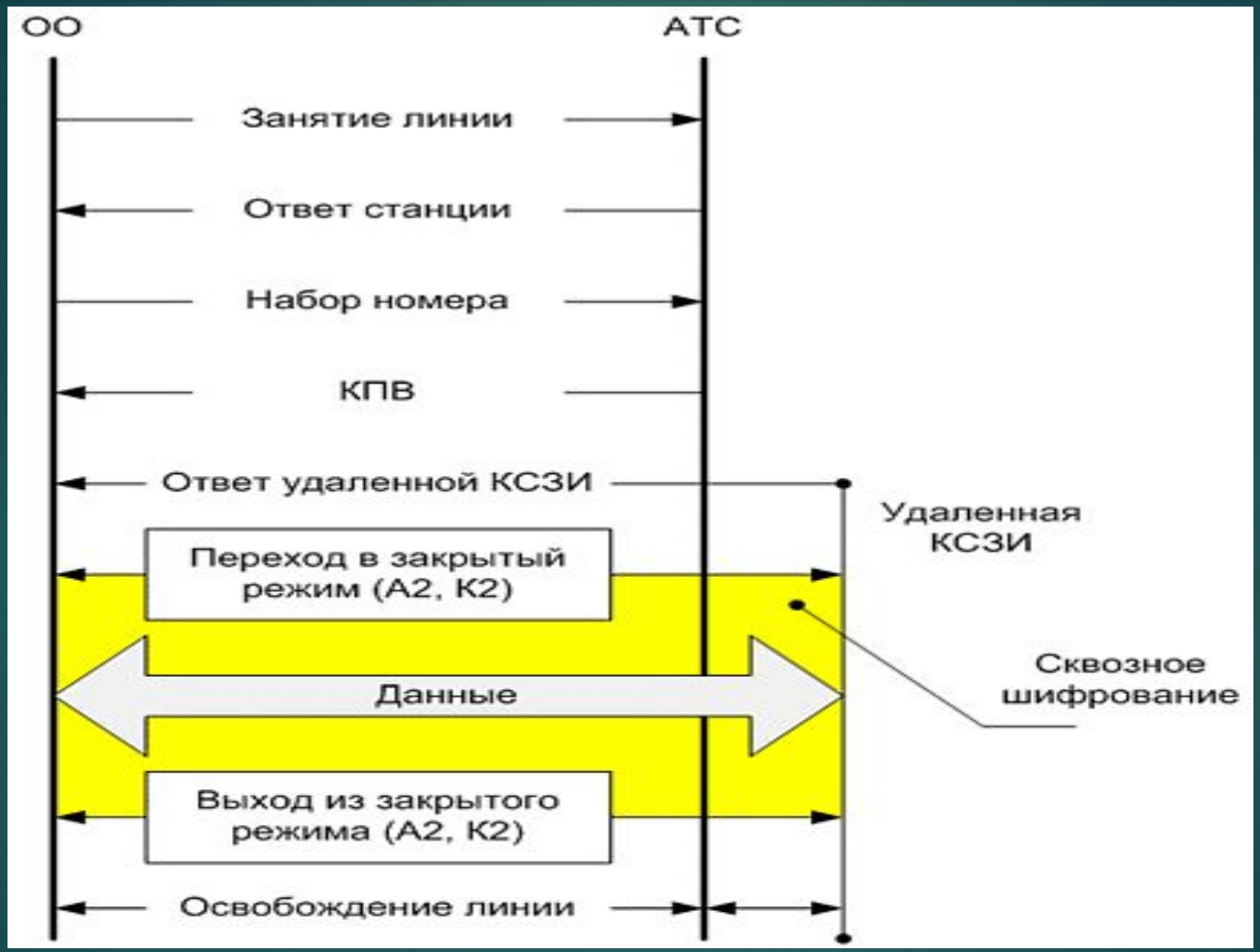
| Класс защиты канала связи | Варианты угроз информации |
| --- | --- |
| Открытый канал | Защита информации основана на ограничении доступа к линии. Возможно несанкционированное подключение к линии. Возможен перехват: При использовании услуги "Междугородная связь по паролю" возможно перехватить этот пароль, так как он передается с помощью DTMF; Управляющей информации для/от АТС; Всех данных, передаваемых по каналу связи, вне зависимости от используемой технологии передачи; Управляющей информации ОО (удаленное управление ОО, сигнализацией и т.д. Особенно небезопасен перехват команд отключения для некоторых видов охранной сигнализации). Возможен перехват/модификация трафика и его полный анализ. |
| Полузакрытый канал (закрывается только информация, управляющая информация передается в открытом виде). | Защита информации основана как на ограничении доступа к линии, так и на КЗИ. Данные закрываются с использованием КСЗИ (по ГОСТ 28147-89 в любом режиме). Возможно несанкционированное подключение к линии. Возможем перехват: при использовании услуги "Междугородная связь по паролю" также возможно перехватить этот пароль (если он набирался в открытом режиме); управляющей информации для/от АТС; момента установления защищенного соединения (возможен перехват ключей); открытых данных/разговора. Возможен перехват трафика но анализ только управляющей информации и открытых данных (опять проблема перехвата команд отключения систем охранной сигнализации). |

Структурная схема передачи данных в открытом канале показана на рисунке 1.




Структурная схема передачи данных в открытом канале показана на рисунке 1.

# **Рисунок 2.** *Передача данных в полузакрытом канале данных.*




Примечание:
А2 - алгоритм 2, К2 - ключ алгоритма А2.

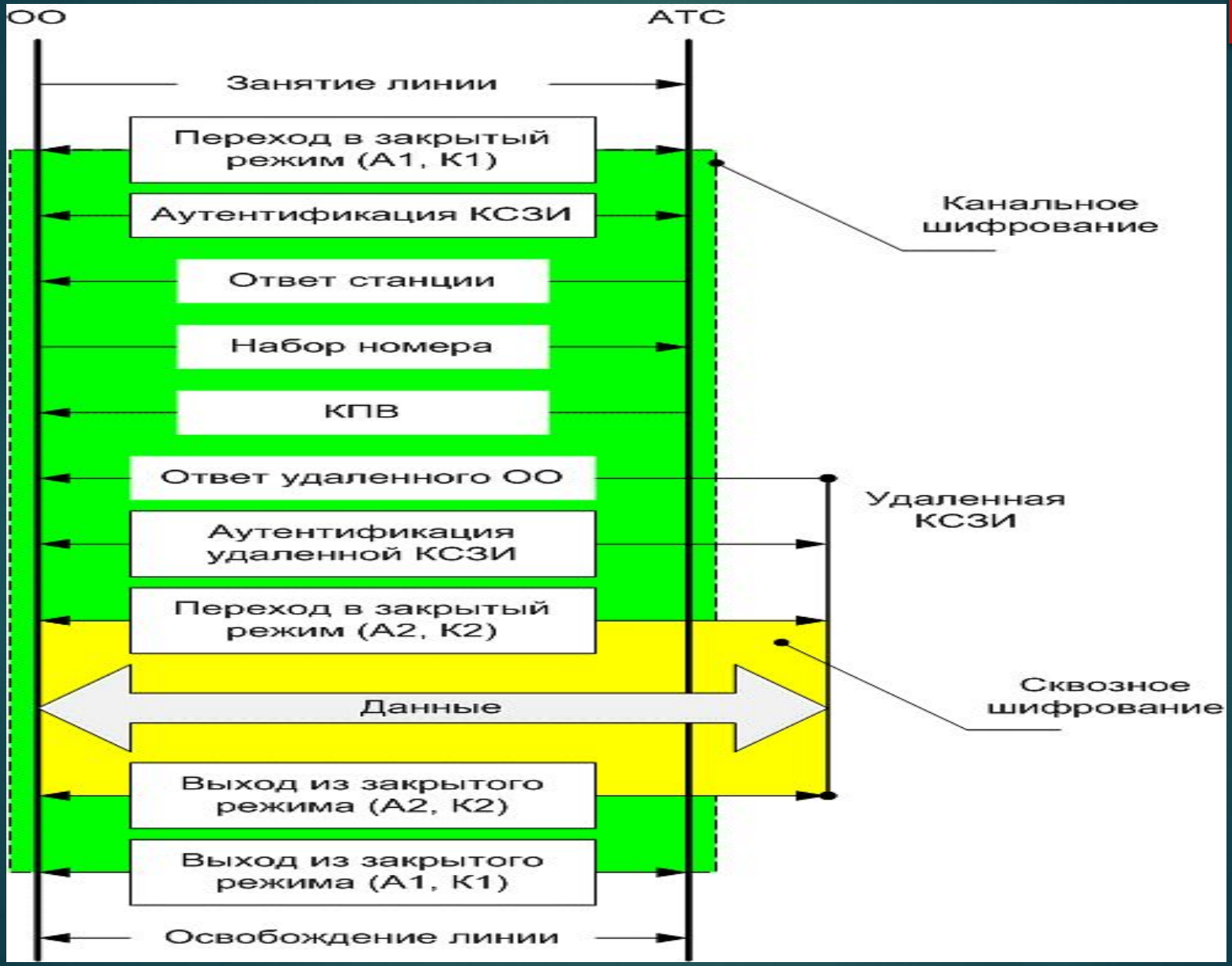
- Основная проблема, с которой сталкиваются пользователи сетей, где применяется сквозное шифрование, связана с тем, что служебная информация. используемая для учстановления соединения, передается по сети в незашифрованном виде. Опытный криптоаналитик может извлечь для себя массу полезной информации, зная кто с кем, как долго и в какие часы общается через сеть доступа. Для этого ему даже не потребуется быть в курсе предмета общения.
- По сравнению с канальным, сквозное шифрование характеризуется более сложной работой с ключами, поскольку каждая пара пользователей должна быть снабжена одинаковыми ключами, прежде чем они смогут связаться друг с другом. А поскольку криптографический алгоритм реализуется на верхних уровнях модели OSI, приходится также сталкиваться со многими существенными различиями в коммуникационных протоколах и интерфейсах сети доступа (для примера: отправитель - канал ТЧ, получатель - 2B+D). Все это затрудняет практическое применение сквозного шифрования

- Приведенные выше методы защиты информации уже не удолетворяют современных требованиям. При использовании этих методов злоумышленник может перехватывать адресную информацию, вести мониторинг передаваемых данных, несанкционированно подключаться к линии, искажать передаваемую информацию.
- Единственным возможным методом, удовлетворяющим всем современны требованиям, является использования комбинации канального и сквозного шифрования. При этом может закрывается вся передаваемая по каналу связи информация.
- Комбинация канального и сквозного шифрования данных в сети доступа обходится значительно дороже, чем каждое из них по отдельности. Однако именно такой подход позволяет наилучшим образом защитить данные, передаваемые по сети. Шифрование в каждом канале связи не позволяет злоумышленнику анализировать служебную информацию, используемую для маршрутизации. А сквозное шифрование уменьшает вероятность доступа к незашифрованным данным в узлах сети.

- При этом злоумышленник может проводить анализ только открыто передаваемых данных, но не может нелегально использовать линию связи.
- Структурная схема передачи данных в закрытом канале показана на рисунке 3.
- Кратко опишем механизм взаимодействия КСЗИ и АТС (удаленной КСЗИ) в предложенном методе.
- При занятии линии (получении сигнала вызова от АТС) происходит автоматический переход в закрытый режим связи (А1, К1). После перехода в закрытый режим, абонентский комплект (АК) или криптографический модуль перед АК АТС аутентифицирует КСЗИ. Данный шаг необходим для устранения возможности несанкционированного использования линии. После проведения аутентификации возможен выход из закрытого режима.

- При вызове со стороны вызывающего абонента, АТС принимает адресную информацию, устанавливает соединение.
- При ответе удаленной КСЗИ возможны два варианта: аутентификации удаленной КСЗИ и переход в закрытый режим (А2, К2) либо переход в закрытый режим (А2, К2) и аутентификация удаленной КСЗИ.
- Аутентификация удаленной КСЗИ необходима для противодействия атаке, при которой удаленная КСЗИ злоумышленника при помощи перекоммутации выдает себя за КСЗИ легального пользователя

**Рисунок 3.** *Передача данных в закрытом канале данных (закрываются все данные).*



Примечание:
A1 - алгоритм 1, K1 - ключ алгоритма A1;
A2 - алгоритм 2, K2 - ключ алгоритма A2.

- После удачной аутентификации удаленной КСЗИ также возможен выход из защищенного режима (отказ от вхождение в защищенный режим).
- Также при передаче данных необходимо проводить т.н. проверку обратного кода. Проверка обратного кода - представляет собой процедуру защиты, осуществляемую в процессе передачи данных. Заключается в том, что у удаленной КСЗИ периодически запрашивается идентифицирующая информация, которая и называется обратным кодом. Эта информация сравнивается с эталонной, сохраненной при аутентификации в начале сеанса связи. При несовпадении кодов передача блокируется. Проверкой обратного кода можно обнаружить факт изменения (перекоммутации) направлений выдачи данных или злоумышленного использования приемного устройства зарегистрированного (законного) корреспондента

.

Предъявляемые требования к взаимодействию криптоалгоритмов можно описать с помощью логического выражения:

**[(A1=A2) U (A1 A2)])∩ (K1≠K2)=True**