Безопасность GSM

Архитектура сетей GSM, атаки на соединения и защита от них.

[Архитектура сетей GSM](#_feprdy6pi8ni)

[Терминология сетей GSM](#_ae7i4f9gii3)

[Аспекты безопасности](#_2ci2tgfx15d)

[Методы перехвата GSM](#_xrdaezoylv4)

[Фальшивая BTS](#_ide48bm4b7bq)

[Пассивное прослушивание эфира](#_5lieun1jr4ef)

[Клонирование модуля SIM](#_v0rnrcli3pxk)

Практическое [задание](#_3tfrjxxltv85)

[Дополнительные материалы](#_1pj11aaentb8)

[Используемая литература](#_uvp6qax5r1ok)

#

#

# Архитектура сетей GSM

Сеть GSM состоит из мобильной и стационарной частей. Мобильная представляет собой множество клиентских мобильных станций, а стационарная — инфраструктуру серверной части сети: базовые станции, аппаратуру уплотнения, проводные каналы, шифровальное и коммутационное оборудование, регистры абонентов, технические средства защиты информации.



*Рис. 1. Архитектура сети GSM*

## Терминология сетей GSM

**Мобильная станция** (**MS** — mobile station) включает приемник и передатчик, необходимые для соединения с сетью GSM. В MS входит модуль идентификации абонента **SIM** (Subscriber Identity Module), в котором хранятся все индивидуальные данные. Они могут потребоваться для оплаты аутентификации пользователя. В SIM-карте, выполненной в виде смарт-карты, содержится множество идентификаторов и таблиц: список абонентских услуг, PIN-код, международный идентификатор мобильного абонента **IMSI**, данные о местоположении мобильного абонента: **TMSI** и **LAI**.

**Базовая станция** (**BTS** — **base transceiver station**) — приемопередатчик, закрепленный на основе. Формирует поле соты GSM.

**Система базовых станций** (**BSS** — base station system) — множество BTS, формирующее зону покрытия сотовой сети.

**Контроллер базовых станций** (**BSC** — base station controller) — управляет базовыми станциями. Резервирует частоты, переключает с одной станции на другую, ищет мобильные станции. Контроллер уплотняет радиоканалы для соединений с проводными каналами.

**Подсистема радиосвязи** (**RSS** — radio subsystem = **MS+BSS+BCS**) — состоит из множества базовых и мобильных станций и формируемых ими электромагнитных полей.

**Центр коммутации мобильной связи** (**MSC** — mobile switching center) — является коммутатором **ISDN**, цифровой сети обмена данными. MSC устанавливает соединение с контроллерами BSC, другими центрами MSC, образуя стационарную магистральную сеть системы GSM. В большинстве случаев MSC управляет несколькими контроллерами BSC.

**Шлюз MSC** (**GMSC** — **gateway MSC**) соединен с сетью общего пользования ТфОП/ISDN.

**Домашний регистр** (**HLR** — home location register) и **гостевой регистр** (**VLR** — visitor location register) — представляют собой базу данных мобильных станций, постоянно зарегистрированных в системе конкретного оператора и расположенных в области обслуживания местного центра коммутации MSC. В HLR хранятся все сведения о пользователях. Статическая информация включает номер ISDN мобильного абонента (MSISDN), оплаченные услуги и ключ аутентификации. В HLR содержится динамическая информация — например, данные о текущей зоне местоположения мобильной станции LAI, которые обновляются при переходе MS из текущей зоны. Эти данные нужны, чтобы взимать оплату или осуществлять роуминг.

**Подсистема сетей и коммутации** (**NSS** — **network subsystem** = **MSC + HLR + VLR**) — ядро системы GSM. Соединяет беспроводную сеть со стандартными сетями общего пользования ТфОП/ISDN, переключает подсистемы базовых станций BSS. NSS определяет местоположение пользователей в любой точке земного шара, обеспечивает оплату, роуминг пользователей между поставщиками услуг связи в разных странах.

**Центр эксплуатации и обслуживания** (**OMC** — **operation and maintenance center**) обеспечивает работу отдельных элементов GSM (MSC, BSC, GMSC и других), выполняет функции администрирования: тарификацию и мониторинг трафика. Принимает меры в случае отказа отдельных элементов сети.

**Центр аутентификации** (**AUC** — authentication centre) представляет базу данных, позволяющую определить, разрешен ли допуск к услугам системы абоненту, имеющему данный модуль идентификации (SIM-карту). Центр AUC, как и SIM-карта, содержит секретный ключ абонента, который используется для его аутентификации и шифрования на радиоучастке. АUC содержит значения, необходимые для аутентификации, алгоритмы аутентификации и шифрования.

**Регистр идентификации оборудования** (**EIR** — equipment identity register) представляет базу данных, содержащую список разрешенного в сети оборудования. Каждая мобильная станция может быть идентифицирована ее кодом **IMEI**, который помечает запрет, если устройство украдено, не поддерживается сетью и в ряде других случаев.

**с** составляют **операционную подсистему** (**OSS** — operating subsystem).

## Аспекты безопасности

На радиоучастке GSM реализованы механизмы информационной безопасности. Это шифрование/дешифрование речи между мобильной и базовой станциями, а также аутентификация мобильной станции. Предусмотрена защита местоположения мобильной станции, которое является конфиденциальной информацией.

Тонкости работы с GSM:

1. При шифровании используется стандартизированный ETSI-алгоритм поточного шифрования, который реализуется в MS и в центре аутентификации AUC. В SIM-карте на основании индивидуального секретного ключа и случайного числа, полученного из сети, формируется ключ шифрования. Он вычисляется по алгоритму, который хранится в SIM-карте.
2. В системе GSM применяется сложная схема уплотнения, объединяющая несколько иерархий кадров. В каналах трафика и ассоциированных с ними каналах управления 26 кадров образуют *мультикадр*. 51 мультикадр составляет *суперкадр*. 2048 суперкадров образуют высший уровень временной иерархии системы GSM — *гиперкадр*. Он продолжается почти 3,5 часа и включает 2715648 временных слотов. Такая логическая структура нужна для процедуры шифрования на радиоучастке: номера кадра помогают обеспечить конфиденциальность разговора.
3. Если при аутентификации пользователя используется его международный идентификатор, IMSI требует его скрывать — чтобы защитить приватные данные, к которым относится местоположение мобильной станции. Перехватив IMSI на радиоучастке, нарушитель может обнаружить личность пользователя, передающего сообщение. Чтобы защититься от этой угрозы, ИБ-значение IMSI передается только один раз — при первом соединении мобильной станции с сетью и по запросу от сети, к которой приписана мобильная станция. В этот момент сеть не знает IMSI.
4. Аутентификация пользователя выполняется после регистрации с помощью анализа TMSI. После завершения аутентификации пользователя устанавливаются новые параметры мобильной станции TMSI и LAI. Эта информация обновляется в VLR и HLR. Строго говоря, HLR инициирует удаление информации о пользователе из предыдущего VLR и ее перенос в новый VLR. Новые параметры TMSI и LAI передаются мобильной станции из VLR, причем TMSI должен передаваться по радиоканалу в зашифрованном виде.

# Методы перехвата GSM

## Фальшивая BTS

Имея на руках оборудование базовой станции (пикосоты), можно ставить помехи оригинальным базовым станциям и получать конфиденциальную информацию с мобильных станций. Это могут быть TMSI и LAI при включении телефона, текст отправляемого сообщения или номер вызываемого абонента, пеленг на мобильную станцию.

Владея двумя фальшивыми BTS, можно установить местоположение абонента методом триангуляции. Используя аутентификационную информацию, посланную MS, при обращении к реальной BTS можно получить доступ к услугам от имени другого абонента. Получив ключи от соединения и сбросив MS на реальную BTS, которая будет думать, что MS прошла аутентификацию, можно снимать эфир, слушать речь и читать смс.

Универсальной защиты от этого вида атаки на соединение не существует. Есть несколько советов:

1. Если видите на мобильной станции полный сигнал сети, но не можете совершить вызов или отправить смс — вас зацепила фальшивая BTS.
2. Обнаружив признаки соединения с фальшивой BTS, выключите мобильную станцию, отойдите на 500–800 шагов и включите ее снова. Это почти на 100 % гарантирует, что вы успешно перерегистрируетесь в сети GSM и получите нескомпрометированные ключи соединения.
3. Если во время разговора вы услышали «цифровые» помехи, прервите соединение и перезагрузите телефон. Произошла ошибка декодера речи, которую может вызвать попытка несанкционированного доступа к соединению.

## Пассивное прослушивание эфира

При этом методе данные снимают с антенны, расшифровывают с помощью радужных таблиц. В качестве антенны можно использовать любой телефон с модифицированной прошивкой или обычную ТВ-антенну в паре с тюнером на базе E4000.

От пассивного прослушивания эфира никто не застрахован — скорее всего, о нем вы даже не узнаете. Расшифровывать дампы соединений после свертывания, блочно-диагонального перемежения и поточного шифрования непросто, но это вопрос времени.

## Клонирование модуля SIM

Атака на сеть GSM, основанная на методе социальной инженерии, наиболее популярна и имеет наивысшую вероятность успеха. Злоумышленники вводят в заблуждение должностных лиц оператора и получают дубликаты SIM-карт.

Еще есть способ изготовить дубликат SIM-карты самостоятельно —потребуется считыватель и программатор. Но у SIM-карты нет интерфейса, чтобы извлекать ключ аутентификации. Его подбор может переполнить счетчик активации алгоритма аутентификации, что испортит SIM-карту.

От клонирования SIM-карты никто не застрахован. Контролируйте свой баланс. Заказывайте у оператора распечатку операций и проверяйте. Если обнаружите лишние — пишите заявление на блокировку клона, разбирательство и возмещение денежных средств, потраченных не вами.

# Домашнее задание

Ответьте письменно на вопросы:

1. Как можно использовать сигнал, который создает помехи на колонке при входящем вызове на близлежащий мобильный телефон?
2. Почему в самолетах просят выключить мобильные устройства?
3. Можно ли носить мобильный телефон рядом с кардиостимулятором?
4. Как быстро развернуть GSM-сеть?
5. Как быстро вывести из строя GSM-сеть?

Аргументируйте свои ответы.

# Дополнительные материалы

1. [Статья про прослушивание GSM-эфира](https://habr.com/post/200914/).
2. [Статья про GSM-сети](https://ru.bmstu.wiki/%D0%A1%D0%B5%D1%82%D0%B8_%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B0_GSM).

# Используемая литература

Для подготовки данного методического пособия были использованы следующие ресурсы:

1. [Статья про прослушивание GSM-эфира](https://habr.com/post/200914/).
2. [Статья про GSM-сети](https://ru.bmstu.wiki/%D0%A1%D0%B5%D1%82%D0%B8_%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B0_GSM).