



# ИССЛЕДОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ И АТАК В СЕТЯХ SS7

2018

## СОДЕРЖАНИЕ

Введение.....	3
Термины и обозначения.....	3
Резюме.....	4
Уязвимости сетей SS7 .....	5
Методика исследования .....	5
Портрет участников .....	5
Статистика по основным видам угроз.....	6
Утечка информации об абоненте .....	10
Утечка информации об операторе.....	12
Перехват трафика абонента .....	12
Мошенничество .....	13
Отказ в обслуживании .....	16
Меры защиты и их эффективность.....	17
Атаки на сети SS7 .....	22
Методика .....	22
Статистика по выявленным атакам.....	23
Утечка информации .....	25
Мошенничество .....	26
Перехват трафика.....	26
Отказ в обслуживании .....	27
Пример атаки.....	28
Заключение.....	31

## ВВЕДЕНИЕ

Современный мир уже невозможно представить без мобильной связи. Так, в жизнь каждого, кто пользуется интернет-услугами (ДБО, платежными системами, мобильными банками, интернет-магазинами, порталами государственных услуг), прочно вошли SMS с одноразовыми кодами для подтверждения различных операций. Безопасность этого способа аутентификации основана лишь на ограничении доступа злоумышленников к телекоммуникационным сетям.

Нельзя забывать и про стремительно развивающийся интернет вещей, который распространяется повсеместно, проникая и в управление промышленными процессами, и в инфраструктуру городов. Сбои в работе мобильной сети могут полностью парализовать эти системы, приводя как к единичным случаям остановки устройств умного дома или автомобиля, вызывая недовольство клиентов оператора, так и к более опасным последствиям, например транспортным коллапсам или перебоям в электроснабжении.

В данном отчете представлены результаты исследования защищенности сетей SS7. Стандарт Signaling System 7 используется для обмена служебной информацией между сетевыми устройствами в телекоммуникационных сетях. В то время, когда разрабатывался этот стандарт, доступ к сети SS7 имели лишь операторы фиксированной связи, поэтому безопасность не была приоритетной задачей. Сегодня сигнальная сеть уже не является в той же степени изолированной, поэтому злоумышленник, тем или иным путем получивший к ней доступ, имеет возможность эксплуатировать недостатки безопасности для того, чтобы прослушивать голосовые вызовы абонентов, читать SMS, похищать деньги со счетов, обходить системы тарификации или влиять на функционирование мобильной сети.

Несмотря на появление сетей нового поколения 4G, использующих иную систему сигнализации — Diameter, проблемы безопасности SS7 будут оставаться актуальными еще долгое время, так как операторы связи все еще должны обеспечивать поддержку стандартов 2G/3G и взаимодействие между сетями разных поколений. Более того, исследования доказывают, что протокол Diameter подвержен тем же угрозам, что и SS7. Уязвимости этого протокола, а также описание возможных кросс-протокольных атак, во время которых эксплуатируются недостатки как Diameter, так и SS7, будут опубликованы в одном из следующих аналитических отчетов.

Мы решили показать не только уязвимости, которые мы выявляем в ходе работ по анализу защищенности сетей SS7, но и факты реальной эксплуатации этих уязвимостей, чтобы продемонстрировать масштабы проблем безопасности современных сетей связи. Мы проследили, как менялась ситуация с защищенностью сетей SS7 в течение последних трех лет; узнали, какие средства защиты используются операторами связи и насколько существующие решения эффективны в реальных условиях.

## ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

HLR (Home Location Register) — база данных, которая содержит информацию об абоненте.

MSC (Mobile Switching Center) — мобильный телефонный коммутатор.

SS7 (Signaling System 7) — общеканальная система сигнализации, используемая в международных и местных телефонных сетях.

STP (Signaling Transfer Point) — пограничный узел для маршрутизации сигнальных сообщений.

VLR (Visitor Location Register) — база данных, которая содержит информацию о нахождении и перемещении абонента.



## РЕЗЮМЕ

**Защищенность сетей SS7 все еще на низком уровне.** Все исследованные сети содержат опасные уязвимости, которые позволяют нарушить доступность сервисов для абонентов. Практически в каждой сети можно прослушать разговор абонента или прочитать входящие SMS, а мошеннические операции можно успешно проводить в 78% сетей.

**Злоумышленники осведомлены об уязвимостях и эксплуатируют их.** Система обнаружения и предотвращения атак PT Telecom Attack Discovery фиксирует реальные атаки, которые злоумышленники проводят на сети операторов связи. Преимущественно они направлены на сбор информации об абонентах и конфигурации сети. Однако мы наблюдаем и такие атаки, которые, по всей вероятности, осуществляются с целью мошенничества, перехвата трафика абонента и нарушения доступности.

**Операторы осознают существующие риски.** Принимаются меры, направленные на снижение вероятности реализации угроз. На сегодняшний день удалось сократить риск утечки информации о сети и абонентах. В 2017 году во всех исследованных сетях функционировала система SMS Home Routing, а в каждой третьей сети была установлена система фильтрации и блокировки сигнального трафика.

**Используемые решения недостаточно эффективны.** Несмотря на активное внедрение дополнительных систем защиты, все сети оказались подвержены уязвимостям, связанным как с частными случаями некорректной настройки оборудования, так и с архитектурными проблемами сигнальных сетей SS7, которые невозможно устранить имеющимися средствами. Только комплексный подход к решению проблем безопасности, включающий регулярный анализ защищенности, поддержание параметров сети в актуальном состоянии, постоянный мониторинг сигнального трафика и своевременное выявление нелегитимной активности, может обеспечить высокий уровень защиты от преступников.

Если у вас возникнут вопросы, пожалуйста, свяжитесь с нами:  
[info@ptsecurity.com](mailto:info@ptsecurity.com)



## УЯЗВИМОСТИ СЕТЕЙ SS7

### Методика исследования

Каждый год эксперты Positive Technologies проводят десятки работ по анализу защищенности сигнальных сетей SS7. В ходе проверок моделируются действия потенциального нарушителя, который, как предполагается, осуществляет атаки из международной или национальной сети, внешней по отношению к оператору. Злоумышленник имеет возможность отправлять в тестируемую сеть запросы протоколов уровня приложений, которые могут привести к реализации различных угроз как в отношении самого оператора, так и его абонентов, если оператор не принимает достаточных мер защиты. Для эмуляции вредоносного узла используется специальное оборудование — PT Telecom Vulnerability Scanner.

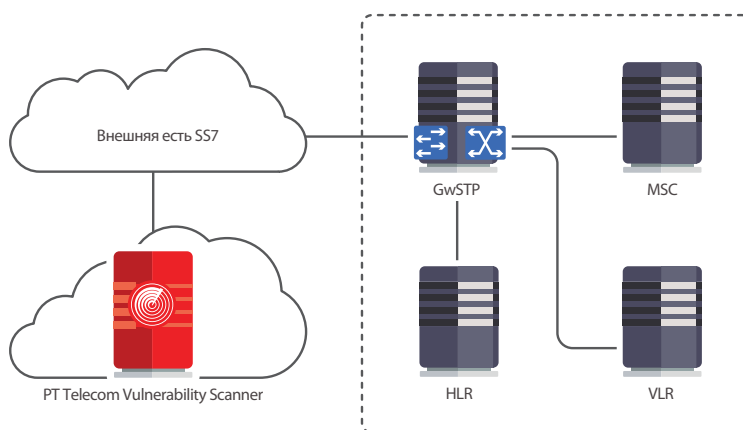


Рисунок 1. Схема работ по анализу защищенности сетей SS7

Для исследования мы выбрали 24 наиболее информативных проекта по анализу защищенности сетей SS7 в 2016–2017 годах, в ходе которых проводился максимально полный перечень проверок. В рамках сравнительного анализа мы также использовали данные, представленные в нашем аналитическом [отчете](#) за 2015 год.

### Портрет участников

В 2016–2017 годах в исследовании принимали участие операторы стран Европы (в том числе России) и Ближнего Востока.

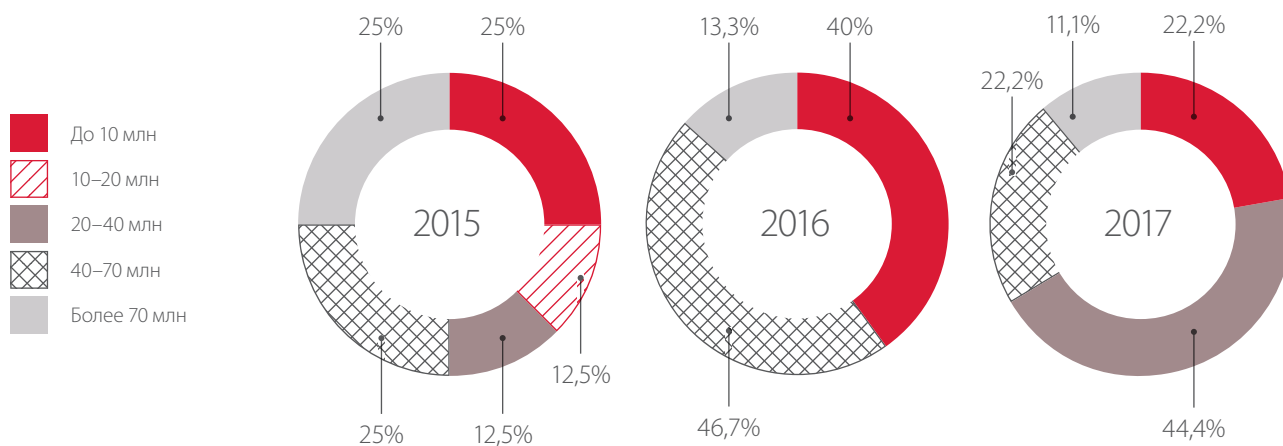


Рисунок 2. Распределение операторов связи по объему абонентской базы

Половину участников составили операторы связи с объемом абонентской базы более 40 миллионов человек. Небольшие компании, число абонентов которых не превышало 10 миллионов, преимущественно являлись виртуальными мобильными операторами на базе более крупных телекоммуникационных компаний.

### Статистика по основным видам угроз

Мы выделяем следующие угрозы, которые может реализовать злоумышленник, эксплуатируя недостатки защищенности сетей операторов мобильной связи:

- + раскрытие информации об абоненте;
- + раскрытие информации о сети оператора;
- + перехват абонентского трафика;
- + мошенничество;
- + отказ в обслуживании.

Каждая из перечисленных угроз несет как репутационные, так и финансовые риски для оператора. Непосредственную опасность для абонента представляют угрозы мошенничества, перехвата трафика, отказа в обслуживании и раскрытия местоположения, которые могут привести к значительным денежным потерям, нарушению приватности и доступности абонентов сети.

Под раскрытием информации об абоненте понимается утечка идентификаторов IMSI, раскрытие местоположения абонента, а также иной информации, например текущего баланса или деталей профиля. Раскрытие информации о сети оператора чревато утечкой данных о конфигурации сети SS7.

В настоящий момент известны такие техники перехвата абонентского трафика в сетях SS7, которые позволяют прослушивать или перенаправлять на сторонние номера входящие и исходящие голосовые вызовы, а также перехватывать SMS пользователей.

Атаки с целью мошенничества могут осуществляться как в отношении оператора, так и в отношении абонентов. Например, изменение платежной категории для вызовов в роуминге или обход системы тарификации могут принести ущерб оператору связи, а перевод средств со счета, перенаправление вызовов на платные номера или подписка на платные сервисы — пользователям сети.

В данном исследовании мы рассматриваем отказ в обслуживании только в отношении отдельных абонентов, поскольку в рамках аудита защищенности лишь малое число операторов осуществляют тестирование сетевых элементов, которое может быть чревато сбоями в работе мобильной сети. Необходимо учесть, что нарушение функционирования может быть массовым в случае, если злоумышленники располагают базой абонентов оператора или обладают ресурсами, достаточными для подбора идентификаторов абонентов.

Уровень осведомленности операторов о проблемах защищенности сетей SS7 постепенно растет, в связи с чем операторы начинают внедрять средства защиты от атак. Если в 2015 году каждая исследованная сеть была подвержена всем видам угроз, то за последние два года обозначились позитивные изменения в общем уровне защищенности сетей.

Таблица 1. Доли уязвимых сетей по типам угроз

	2015	2016	2017
Раскрытие информации об абоненте	100%	100%	100%
Раскрытие информации о сети оператора	100%	92%	63%
Перехват абонентского трафика	100%	100%	89%
Мошенничество	100%	85%	78%
Отказ в обслуживании абонентов	100%	100%	100%

Операторы связи начинают более серьезно относиться к проблемам безопасности сетей SS7 и внедряют средства защиты

Заметно снизились риски утечки информации о сети оператора, мошенничества и перехвата абонентского трафика. Тем не менее каждая исследованная сеть, как и прежде, подвержена уязвимостям, которые позволяют получить информацию об абонентах или вызвать отказ в обслуживании.

Рассмотрим доли успешных попыток атак, которые эксперты смогли реализовать в рамках работ по анализу защищенности.

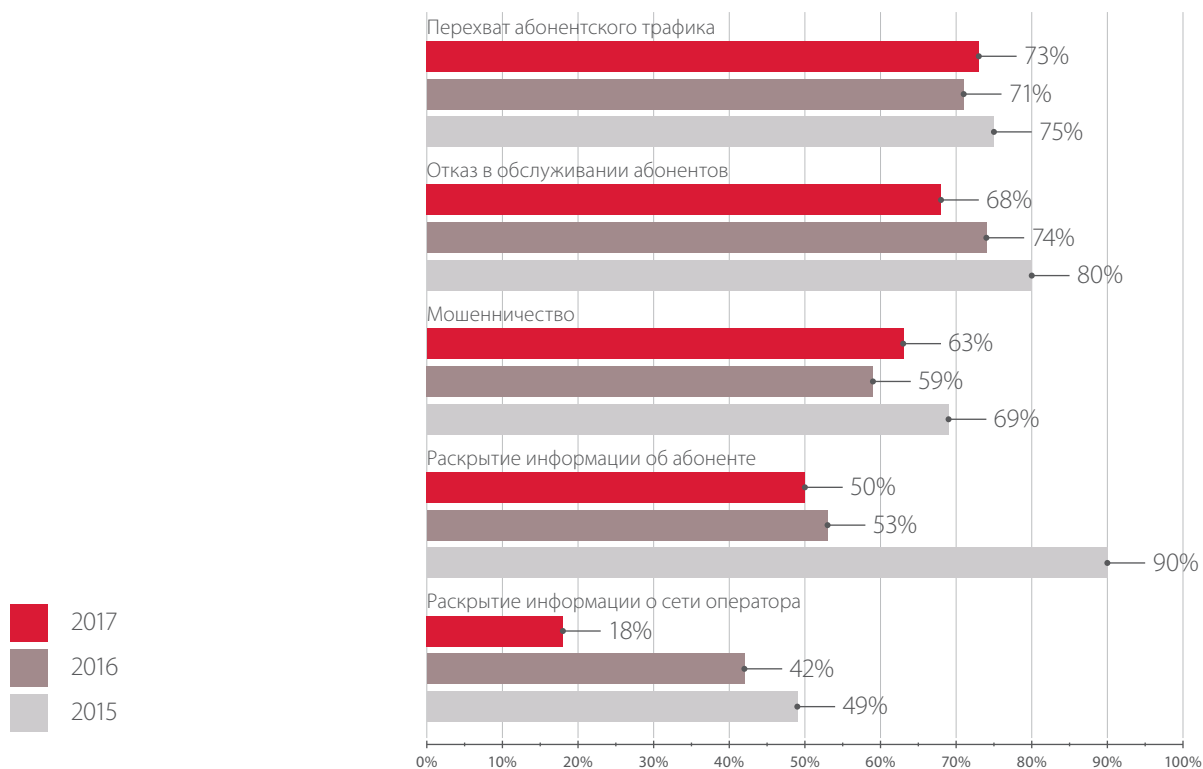


Рисунок 3. Доли успешных атак по типам угроз

Как видно, в первую очередь операторы принимают меры, направленные на снижение риска раскрытия информации о сети и абонентах, поскольку эти сведения служат исходными данными для реализации множества других атак. По сравнению с 2015 годом доля успешных атак, направленных на раскрытие информации о сети оператора, снизилась почти втрое, и в два раза реже удавалось получить данные об абонентах сети. Способы защиты от такого рода атак достаточно просты, а на рынке ИБ существуют готовые решения, но при этом уязвимы для раскрытия информации об абонентах по-прежнему 100% сетей, что говорит о недостаточной эффективности существующих решений.

Для остальных видов угроз процент успешно осуществленных атак изменился незначительно. Как мы покажем далее, причина состоит в том, что внедрение систем фильтрации и блокировки трафика не может компенсировать архитектурные проблемы SS7, для минимизации этих рисков необходим иной подход.

Можно выделить следующие причины, по которым возможна реализация тех или иных угроз:

- + отсутствие проверки реального местоположения абонента;
- + невозможность проверки принадлежности абонента сети;
- + недостатки конфигурации SMS Home Routing;
- + отсутствие фильтрации сообщений.

Как показывают результаты, нарушитель может проводить большинство атак, эксплуатируя уязвимости, которые связаны с отсутствием проверки реального местоположения абонента и его принадлежности сети оператора.

Архитектурные проблемы сетей SS7 не решаются существующими средствами фильтрации трафика

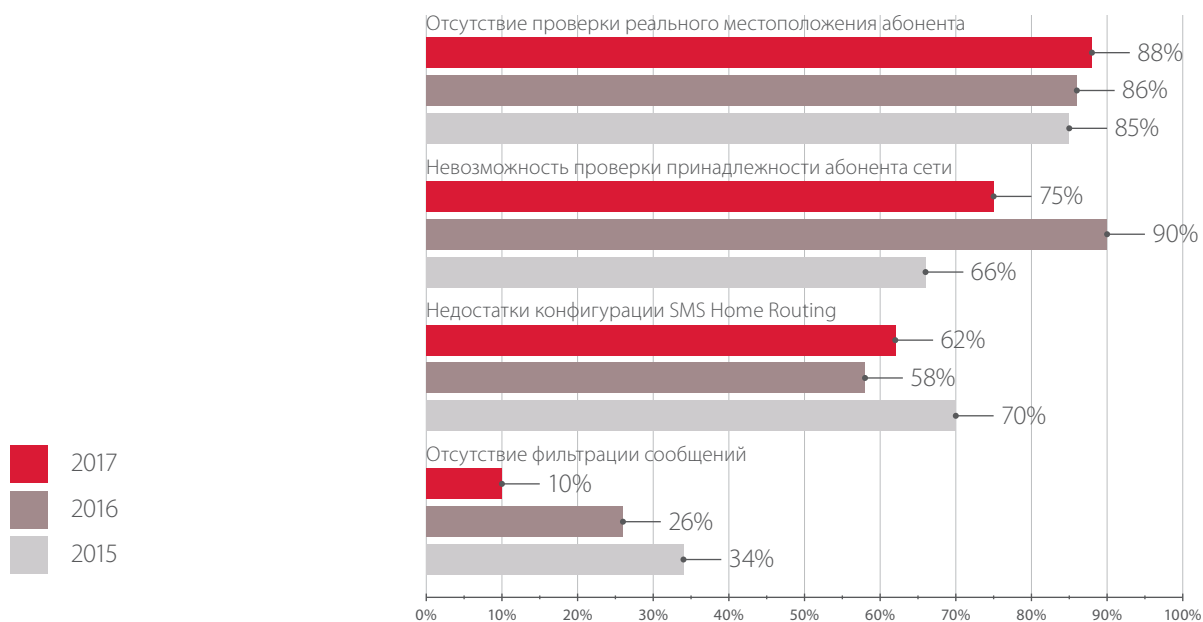


Рисунок 4. Уязвимости (доли успешных атак)

В частности, возможны атаки, направленные на раскрытие местоположения абонента, перенаправление или перехват вызова, перехват SMS, изменение платежной категории или профиля абонента. Отсутствие проверки местоположения относится к сигнальным сообщениям, приходящим в домашнюю сеть абонента из сети, в зоне действия которой пребывает абонент в роуминге. Если сигнальное сообщение составлено корректно, нет возможности проверить его подлинность только по полученным параметрам. Нужна дополнительная проверка, на самом ли деле абонент находится в той сети, откуда пришел сигнальный трафик.

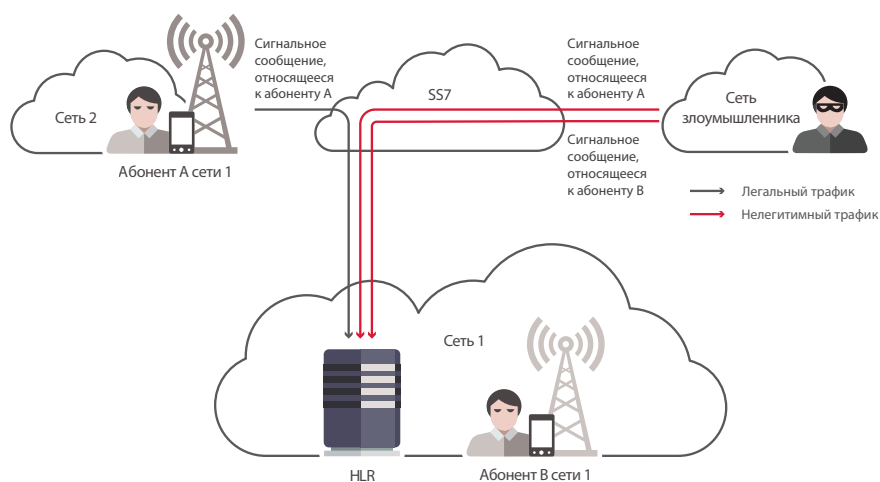


Рисунок 5. Отсутствие проверки реального местоположения абонента

Сложность проверки принадлежности абонента сети связана с сигнальными сообщениями, направляемыми оператором связи в адрес своих абонентов, находящихся в роуминге, к другой сети, в которой эти абоненты на данный момент зарегистрированы. Для определения нелегитимного трафика нужно проверять соответствие источника сообщения и идентификатора абонента. Если адрес источника и идентификатор абонента соответствуют одному оператору, то сообщение легитимное. Но если соответствие не найдено, это еще не означает фальсификацию сообщения, так как адрес источника может быть изменен, например, транзитным оператором. С полной уверенностью можно говорить о нелегитимности данного вида сигнального трафика, если он поступает из внешних сетей и направлен в адрес абонентов домашней сети.



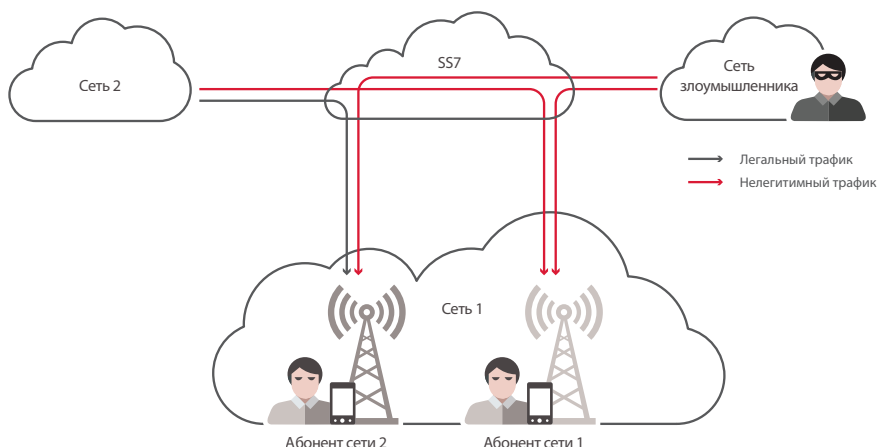


Рисунок 6. Отсутствие проверки принадлежности абонента сети

SMS Home Routing — аппаратно-программный комплекс, предназначенный для сокрытия реальных идентификаторов абонентов и адресов сетевого оборудования, — используется в 85% исследованных сетей, однако некорректная настройка позволяет осуществлять атаки в обход механизма защиты. В сетях, где система SMS Home Routing отсутствовала, были успешны абсолютно все попытки получить идентификаторы абонентов и информацию о сети.

Операторы активно внедряют системы фильтрации и блокировки сигнального трафика: в 2017 году они функционировали уже в трети исследованных сетей. Как результат, атаки, эксплуатирующие уязвимости, связанные с отсутствием фильтрации сообщений, на сегодняшний день успешны лишь в 10% случаев, что в три раза лучше показателей предыдущих лет.

Для проведения атак используются стандартные сообщения, предназначенные для выполнения служебных операций. Эти сообщения должны проходить проверку на границе или внутри сети оператора, чтобы пресечь нелегитимные запросы. Одна и та же атака может быть осуществлена несколькими сообщениями (методами), при этом успешность различных методов неодинакова. Далее мы подробно разберем, с помощью каких методов и с какой долей вероятности злоумышленники могут реализовать все перечисленные угрозы.



## Утечка информации об абоненте

Как уже упоминалось выше, первоочередной мерой по снижению вероятности проведения большинства атак является снижение риска раскрытия IMSI — уникальных идентификаторов абонентов. По сравнению с 2015 годом узнать IMSI по телефонному номеру абонента в прошедшем году удавалось приблизительно в 4 раза реже.

Определить местоположение абонента сегодня удается в 75% сетей, при этом доля успешных атак с использованием различных методов составляет 33%, что также значительно лучше предшествующих показателей.

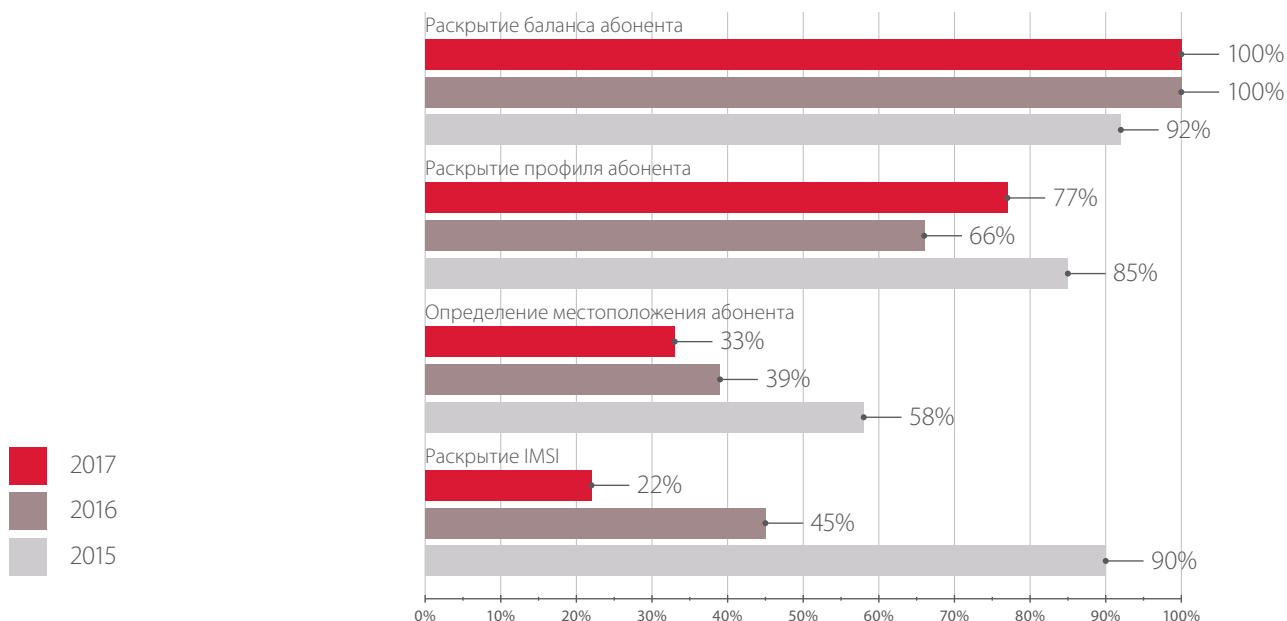


Рисунок 7. Доли успешных атак по типам угроз, связанных с получением информации об абоненте

Раскрытие информации об абоненте может быть реализовано четырьмя методами, успешность которых показана на рис. 8.

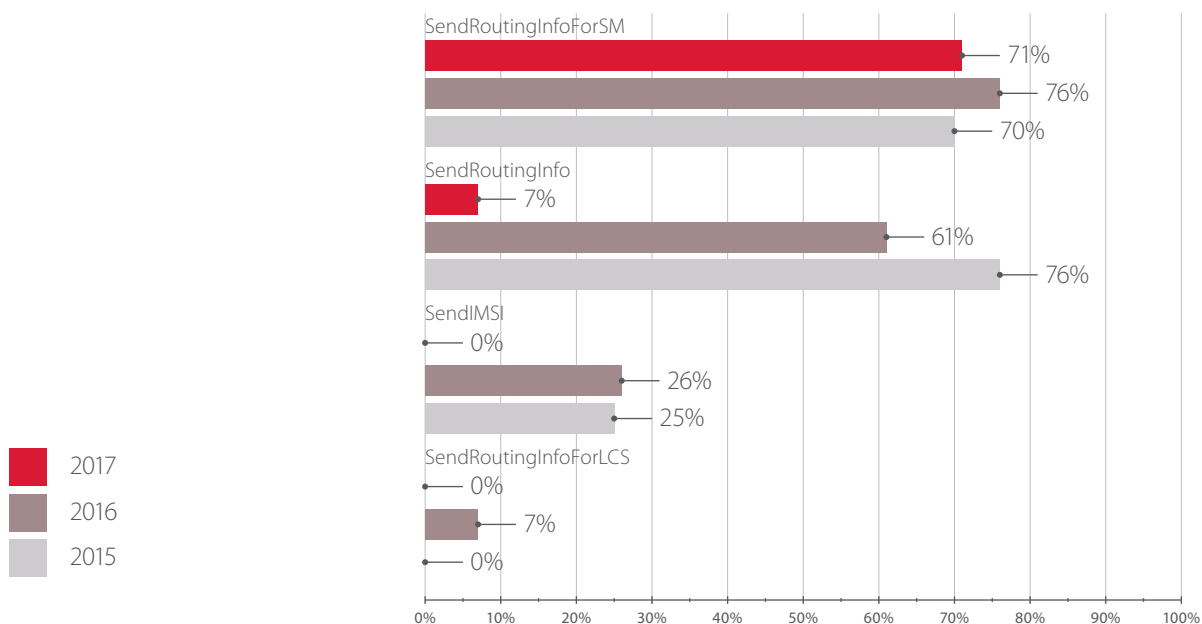


Рисунок 8. Методы, используемые для получения IMSI абонента (доли успешных атак)

Снижение доли успешных атак методами SendRoutingInfo и SendIMSI связано с внедрением средств фильтрации в сетях операторов. Сообщение SendRoutingInfo используется для получения маршрутной информации об абоненте при входящем голосовом вызове и должно передаваться только в пределах домашней сети оператора. Сообщение SendIMSI для запроса IMSI абонента по его телефонному номеру в настоящее время практически не используется операторами, однако обрабатывается в сетях мобильной связи для того, чтобы полностью обеспечить соответствие стандартам.

Метод SendRoutingInfoForLCS был успешно проэксплуатирован лишь в двух исследованных сетях, что также связано с эффективной фильтрацией сообщений. Метод служит для запроса информации сервисами, для работы которых необходимы данные о местоположении пользователя.

Сообщение SendRoutingInfoForSM отправляется для получения маршрутной информации, которая требуется для доставки входящего SMS. Чтобы не раскрывать реальные идентификаторы абонентов и адреса сетевых элементов, сообщение, поступившее из внешней сети, должно перенаправляться системе SMS Home Routing и возвращать виртуальные данные. Несмотря на то, что в большинстве сетей используется SMS Home Routing, мы зачастую сталкиваемся с некорректной конфигурацией граничного сетевого оборудования (STP/FW), в результате которой запрос отправляется к HLR в обход устройства SMS Router и возвращает настоящий IMSI абонента и данные о конфигурации сети оператора.

Определить местоположение абонента в основном удавалось при помощи метода ProvideSubscriberInfo. Это связано с архитектурными недостатками сетей SS7. Сообщение ProvideSubscriberInfo должно обрабатываться только в том случае, если источник сообщения и идентификатор абонента соответствуют одному и тому же оператору. Проблема заключается в том, что в связи с архитектурными особенностями сетей SS7 невозможно определить принадлежность абонента сети оператора. Для защиты от таких атак необходимо использовать системы фильтрации трафика.

В 2015 году мы предполагали, что операторы хорошо осведомлены об атаках методом AnyTimeInterrogation, который раскрывает местоположение пользователя по его телефонному номеру, и о соответствующих методах защиты, — поскольку ни одна из наших попыток не была успешна. Однако в последующие два года мы столкнулись с сетями, в которых отсутствовала фильтрация этого сообщения.

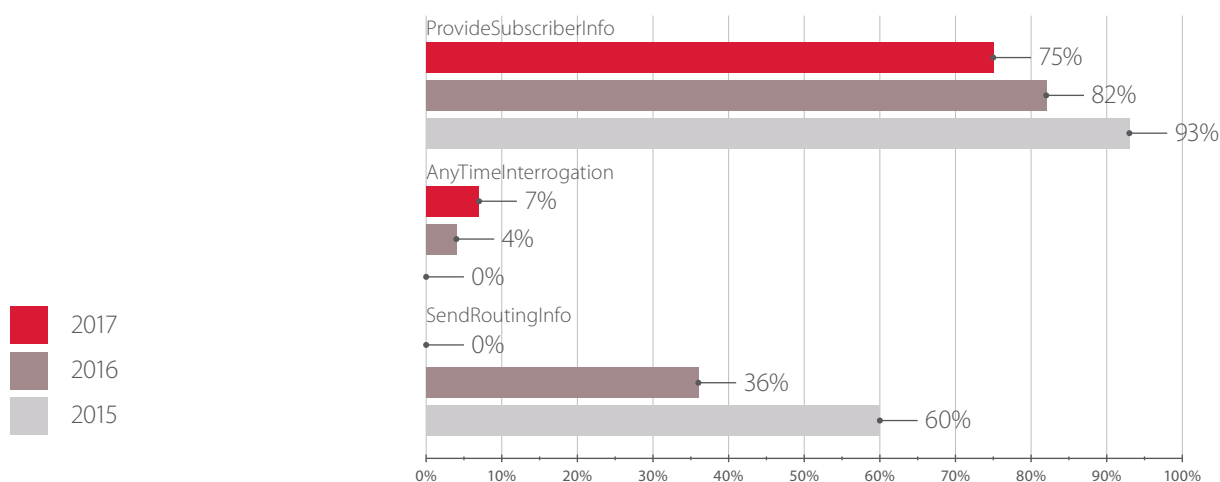


Рисунок 9. Методы, использующиеся для определения местоположения абонента (доли успешных атак)

Раскрытие баланса или деталей профиля пользователя не несет непосредственной серьезной опасности, поэтому защита от этих угроз, по всей видимости, находится в меньшем приоритете. Кроме того, обеспечить защиту от большинства используемых методов возможно только при постоянном мониторинге и фильтрации сигнального трафика. Реализовать соответствующие атаки можно в каждой исследованной сети, для этого используются следующие сообщения:

- + RestoreData;
- + InterrogateSS;
- + ProcessUnstructuredSS;
- + UpdateLocation;
- + AnyTimeSubscriptionInterrogation

В 2017 году в ходе работ по анализу защищенности удавалось осуществить атаки всеми методами кроме AnyTimeSubscriptionInterrogation.

### Утечка информации об операторе

В ходе проверок удалось осуществить более половины атак, связанных с проблемами настройки SMS Home Routing, которые позволяют получить данные о конфигурации сети. Тем не менее в целом операторы добились значительного снижения вероятности раскрытия такой информации.

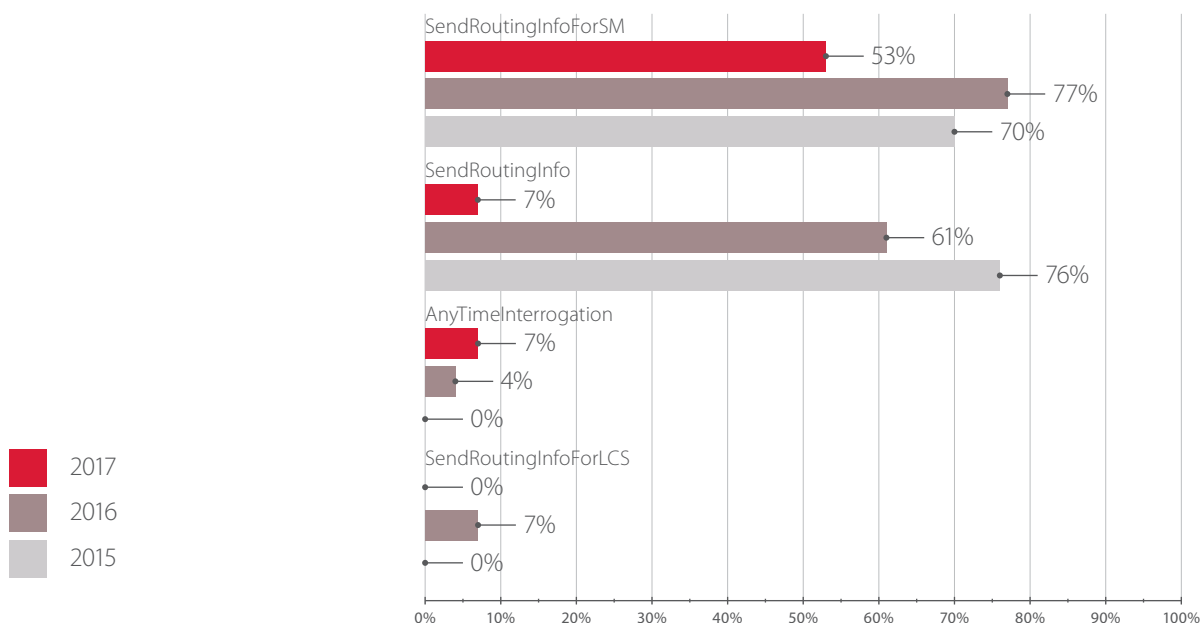


Рисунок 10. Методы, используемые для получения информации о конфигурации сети SS7 (доли успешных атак)

Рост числа успешных атак методом SendRoutingInfoForSM в 2016 году вызван тем, что мы исследовали несколько сетей, в которых система SMS Home Routing отсутствовала.

### Перехват трафика абонента

Риск перехвата пользовательского трафика по-прежнему остается достаточно высоким. Подавляющее большинство попыток перехватить SMS абонентов оказались успешными. На сегодняшний день посредством SMS передается крайне важная информация — пароли для двухфакторной аутентификации, которые отправляют сервисы, предоставляющие услуги ДБО, интернет-платежей и пр. Утечка таких данных может сильно повлиять на репутацию оператора связи и послужить для клиентов, в том числе для компаний с большим объемом трафика, поводом к расторжению договора.

**9 из 10 SMS**  
могут быть перехвачены  
мошенниками



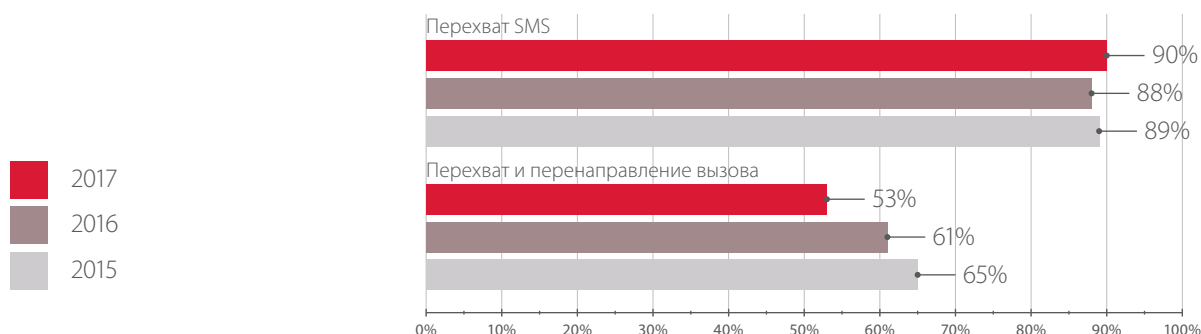


Рисунок 11. Методы, используемые для перехвата и переадресации трафика абонента (доли успешных атак)

Прослушать или перенаправить на сторонние номера входящие и исходящие вызовы абонентов удавалось более чем в половине случаев.

Под перенаправлением понимается только передача вызова на сторонний номер. Развитие этой атаки позволяет установить соединение таким образом, чтобы злоумышленник смог прослушать разговор абонента.

Сообщение UpdateLocation служит для оповещения HLR о смене абонентом обслуживающего коммутатора. Путем отправки поддельного запроса на регистрацию абонента в сети злоумышленника осуществляется перехват входящих SMS или вызовов. При поступлении входящего вызова сеть оператора отправляет запрос в фальшивую сеть для получения роумингового номера абонента. Злоумышленник может отправить в ответ номер собственной АТС и в этом случае входящий трафик поступит на его оборудование. Затем, после отправки повторного запроса на регистрацию абонента в настоящей сети, злоумышленник может перенаправить вызов на номер абонента. В результате разговор будет проходить через подконтрольное злоумышленнику оборудование. Такой же принцип лежит в основе перехвата входящих вызовов методом RegisterSS, но в этом случае устанавливается безусловная переадресация входящих вызовов на номер АТС злоумышленника.

Высокий процент успешных атак связан с отсутствием проверки реального местоположения абонента. Чтобы снизить вероятность атак с использованием этих методов, необходимо обеспечить постоянный мониторинг сигнального трафика и анализ нелегитимной активности для выявления подозрительных узлов, построения списков запрещенных и доверенных сетей, немедленной блокировки запросов из запрещенных источников.

Исходящие вызовы прослушиваются по схожей схеме: специально сформированное сообщение InsertSubscriberData заменяет в профиле абонента, хранящемся в базе данных VLR, адрес платформы для тарификации вызовов. При поступлении запроса по новому адресу злоумышленник сначала перенаправляет исходящий вызов на подконтрольное ему оборудование и лишь затем — на вызываемого абонента.

Таким образом злоумышленник получает возможность прослушивать любой разговор абонента.

### Мошенничество

Известен широкий спектр методов, которые могут быть использованы преступниками в целях получения финансовой выгоды за счет оператора или абонентов сети. Эти методы можно разделить на четыре категории:

- + нелегитимная переадресация входящих или исходящих вызовов;
- + эксплуатация USSD-запросов;
- + манипулирование SMS;
- + изменение профиля абонента.

### 78% сетей

подвержены угрозе мошенничества

Мошенник может узнать данные паспорта и кодовую фразу, выдав себя за сотрудника банка

### Нелегитимная переадресация входящих или исходящих вызовов

Злоумышленник может перенаправлять голосовые вызовы абонентов на платные номера или на сторонний номер с целью уклонения от тарификации. Соединение будет оплачиваться за счет абонента в случае установки безусловной переадресации на номер злоумышленника или за счет оператора связи — в случае регистрации абонента в ложной сети и подмены его роумингового номера.

Перенаправление вызовов позволяет осуществлять и иные мошеннические схемы. Так, например, если абонент совершает исходящий звонок в банк, то перенаправив его на собственный номер и представившись сотрудником банка, преступник может узнать конфиденциальную информацию, необходимую для подтверждения личности, в частности данные паспорта и кодовое слово. Возможна и обратная ситуация: путем переадресации входящих вызовов злоумышленник может выдать себя за абонента, например для подтверждения банковских операций.

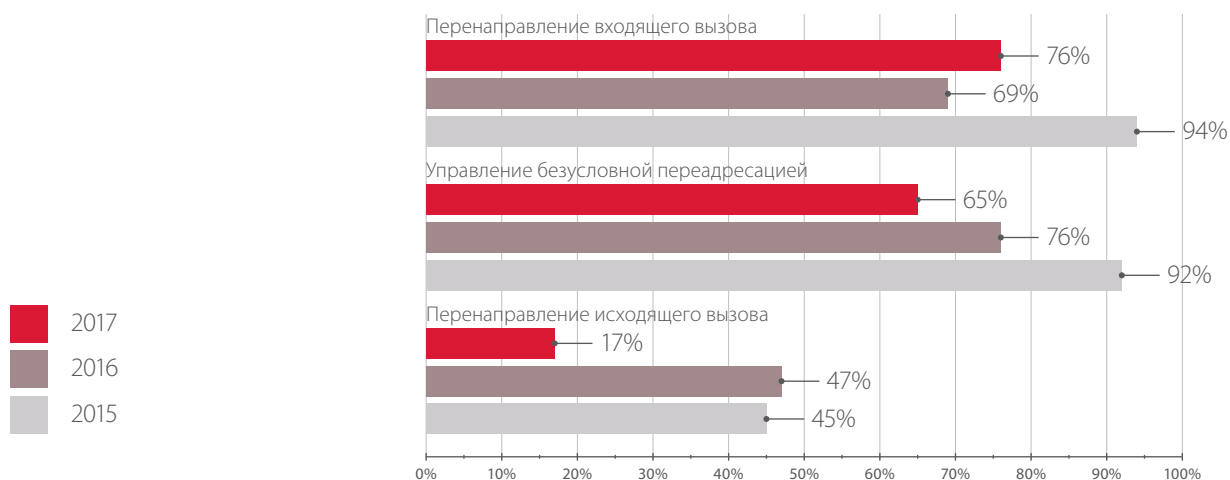


Рисунок 12. Доли успешных атак, направленных на переадресацию голосовых вызовов абонента

Перенаправление вызовов осуществляется с использованием уже упомянутых методов UpdateLocation, RegisterSS, InsertSubscriberData, а также метода AnyTimeModification, с помощью которого можно внести изменения в профиль абонента (заметим, что ни одна атака методом AnyTimeModification не привела к нужному результату).

### Эксплуатация USSD-запросов

Злоумышленник может перевести деньги со счета абонента или партнеров оператора, эксплуатируя возможность отправки поддельных USSD-запросов методом ProcessUnstructuredSSRequest. Другой метод — UnstructuredSSNotify — используется для отправки оповещений абонентам от имени различных сервисов, в том числе и от самого оператора. Злоумышленник может отправить поддельное уведомление от лица доверенного сервиса, содержащее инструкции, которые требуется выполнить абоненту: отправить SMS на платный номер для

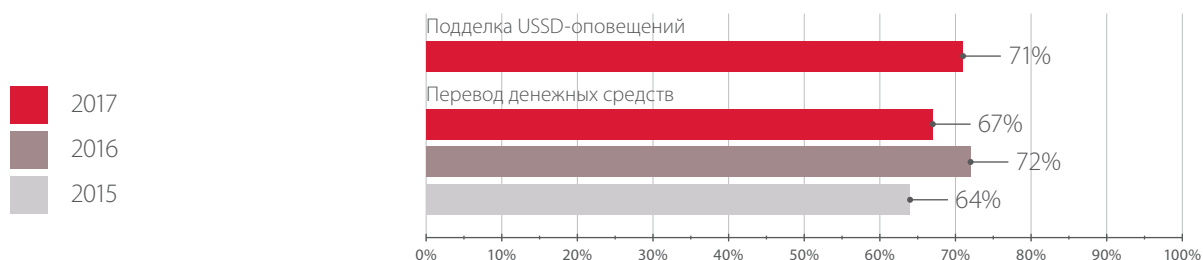
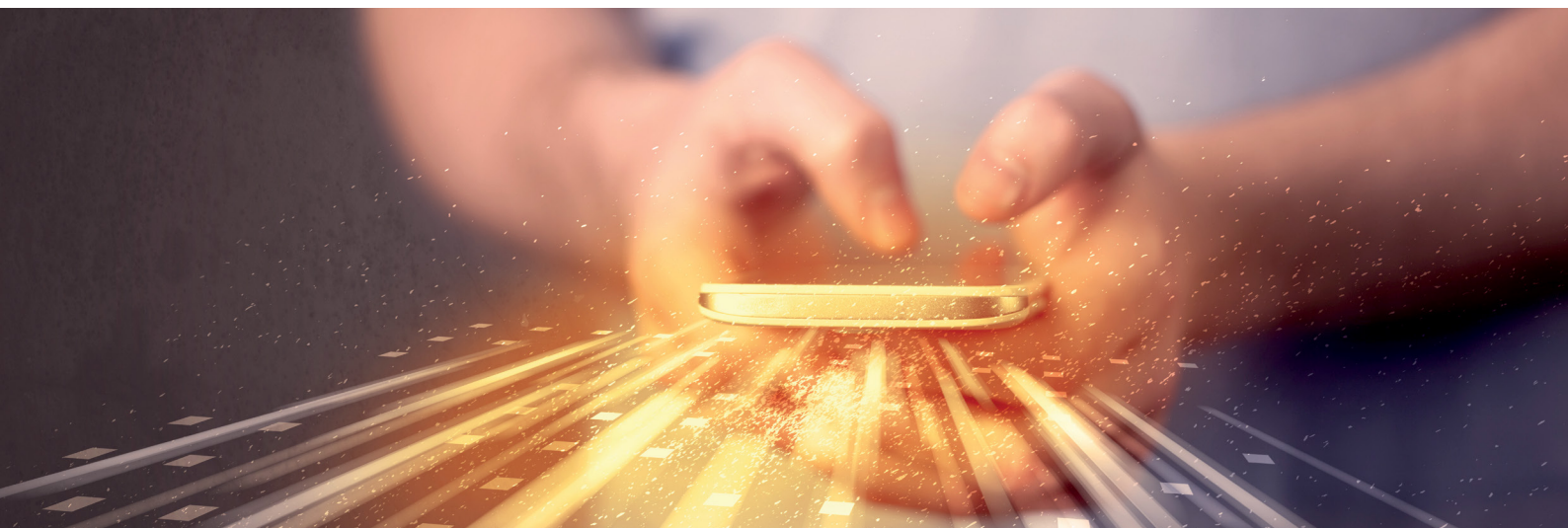


Рисунок 13. Угрозы, связанные с подделкой USSD-запросов (доли успешных атак)



Все сети позволяют отправлять поддельные SMS от имени абонентов или доверенных сервисов

подключения услуги, позвонить по фальшивому номеру банка в связи с подозрительными операциями по карте или перейти по ссылке для обновления приложения.

### Манипулирование SMS

Фишинговую или рекламную рассылку сообщений можно организовать, отправляя поддельные SMS от имени произвольных абонентов или сервисов с помощью методов MT-ForwardSM и MO-ForwardSM. Метод MT-ForwardSM предназначен для доставки входящих сообщений и может применяться злоумышленниками для формирования подложных входящих SMS. Несанкционированное использование метода MO-ForwardSM позволяет отправлять исходящие сообщения от имени и за счет абонентов сети. В 2017 году все сети, где проводились соответствующие проверки в ходе анализа защищенности, оказались подвержены уязвимостям, связанным с недостаточным анализом сигнального трафика, которые позволяют отправить подложные сообщения.

### Изменение профиля абонента

Информация о платформе тарификации и подписках на услуги хранится в профиле абонента. Для обхода системы тарификации в реальном времени необходимо удалить O-CSI-подписку абонента, которая используется для совершения абонентом исходящих вызовов, или подменить адрес платформы тарификации на фиктивный. В целях предотвращения нетарифицируемых вызовов в параметрах O-CSI указывается, что при недоступности платформы необходимо завершить вызов. Тем не менее этот параметр можно подменить таким образом, чтобы вызов продолжался без обращения к платформе. В результате легитимная платформа не будет получать информацию о вызовах и, соответственно, не будет производить тарификацию.

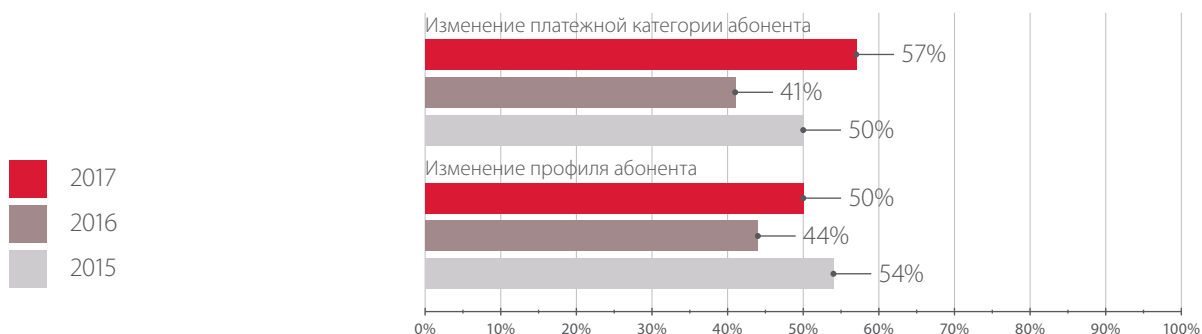


Рисунок 14. Доли успешных атак, направленных на внесение изменений в профиль абонента

Отказ в обслуживании  
абонентов возможен  
в 100% сетей

Атаки методами InsertSubscriberData и DeleteSubscriberData были успешно осуществлены более чем в 80% случаев, а попытки атак методом AnyTimeModification не приводили к результату.

### Отказ в обслуживании

На сегодняшний день атаки, нацеленные на отказ в обслуживании отдельных абонентов, возможны в каждой исследованной сети. Выявленные недостатки связаны с архитектурными проблемами протоколов (невозможность проверки принадлежности абонента сети и отсутствие проверки реального местоположения абонента) и позволяют успешно проводить атаки следующими методами:

- + UpdateLocation;
- + RegisterSS;
- + InsertSubscriberData;
- + PurgeMS.

Все попытки атак приводили к отказу в обслуживании абонентов, за исключением метода InsertSubscriberData (83% успешных атак). С этой же целью может быть использован и метод AnyTimeModification, однако параметры безопасности всех исследованных сетей препятствовали прохождению этих запросов.

Помимо возможности совершать голосовые вызовы и обмениваться SMS, абонент может лишиться доступа в интернет при проведении атаки методом InsertSubscriberData.

Несмотря на то, что рассматриваемые нарушения функционирования сети целенаправленны и затрагивают в каждом случае только одного абонента, не исключен и массовый сбой в обслуживании, если злоумышленник располагает базой идентификаторов абонентов либо может подобрать идентификаторы перебором.

Такие сбои в обслуживании могут быть критическими для устройств, относящихся к интернету вещей. Это стремительно развивающийся рынок, насчитывающий миллиарды устройств, для работы которых требуется доступ к телекоммуникационным сетям. Периодический выход из строя систем умного дома, систем видеонаблюдения, устройств, отслеживающих местоположение автомобиля, или остановка промышленных процессов предприятия может привести к значительному оттоку клиентов.

При проведении исследований мы установили, что среднее время недоступности абонента после такой атаки составляет более трех часов, а в некоторых случаях при выполнении запроса на нарушение доступности изменяется текущий профиль абонента в базе данных, и оборудование не способно произвести восстановление профиля, даже когда абонент перезагружает устройство. Это случалось при атаках на нарушение доступности методами PurgeMS и InsertSubscriberData.

При удалении из HLR адреса VLR, в котором в текущий момент зарегистрирован абонент, посредством процедуры PurgeMS, инициированной неким третьим узлом, происходит следующее. Входящие вызовы не могут маршрутизироваться на обслуживающий абонента VLR/MSC, поскольку в HLR адрес регистрации отсутствует. При этом исходящие вызовы абоненту доступны, поскольку регистрационная запись в VLR не изменялась.

Восстановление регистрации в HLR обычным способом — перезагрузкой телефона (или иного устройства) — не работает, так как VLR не инициирует процедуру UpdateLocation в отношении HLR, полагая, что в регистрационных данных абонента нет изменений.

В результате восстановить регистрацию, а соответственно, и доступность абонента для входящих вызовов, можно только при регистрации в зоне действия другого обслуживающего MSC, например если сначала вручную выбрать сеть

**3 часа** — среднее время  
недоступности абонента



Сбои в работе умных устройств могут привести к оттоку клиентов

другого оператора, а затем снова выбрать домашнюю сеть. Другой вариант — переместиться в зону действия другого MSC домашней сети.

### Меры защиты и их эффективность

Выявленные уязвимости связаны как с некорректной настройкой сетевого оборудования или средств защиты, так и с фундаментальными недостатками сетей SS7. Если в первом случае для устранения уязвимостей достаточно внести изменения в конфигурацию устройств, то архитектурные проблемы сетей могут быть решены только путем корректной фильтрации и мониторинга сигнального трафика. Чтобы обеспечить анализ и блокировку поступающих сообщений без нарушения функционирования сети требуется специальное дополнительное оборудование. Рассмотрим, какие средства защиты применялись в исследуемых сетях и в какой степени они способствуют снижению рисков реализации угроз.

Почти во всех сетях был установлен комплекс SMS Home Routing. С 2016 года операторы начали внедрять системы фильтрации и блокировки сигнального трафика, а в 2017 году такие системы функционировали уже в каждой третьей исследованной сети.

Таблица 2. Установленные средства защиты (доля сетей)

	2015	2016	2017
Система SMS Home Routing	100%	67%	100%
Система фильтрации и блокировки сигнального трафика	0%	7%	33%

Система SMS Home Routing направлена на противодействие раскрытию IMSI абонента и конфигурации сети методом SendRoutingInfoForSM, и действительно, процент успешных атак в случае ее установки снижается на треть. Однако в связи с неправильной настройкой оборудования в 67% случаев можно получить реальные данные.

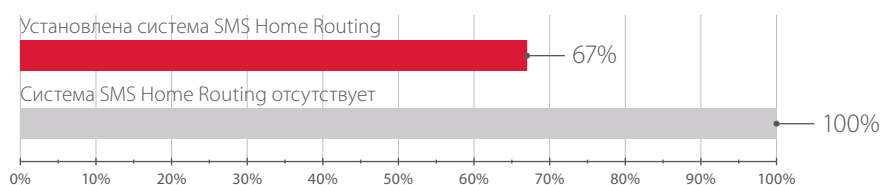


Рисунок 15. Получение IMSI методом SendRoutingInfoForSM в зависимости от наличия системы SMS Home Routing (доли успешных атак)

Следует помнить, что система SMS Home Routing не может использоваться для защиты от остальных видов атак. Более того, эта система не предназначена для защиты сети, а устанавливается для правильной маршрутизации входящих SMS. Как показывают результаты исследований, сети, где используется SMS Home Routing, не являются более защищенными по сравнению с остальными, возможно по той причине, что операторы зачастую полагаются исключительно на SMS Home Routing, пренебрегая дополнительными средствами защиты.

Сравним результаты попыток проведения атак различными методами, для противодействия которым на сегодняшний день рекомендуется использовать системы фильтрации и блокировки сигнального трафика.

■ Установлена система  
фильтрации и блокировки  
сигнального трафика

■ Система фильтрации  
и блокировки сигнального  
трафика отсутствует

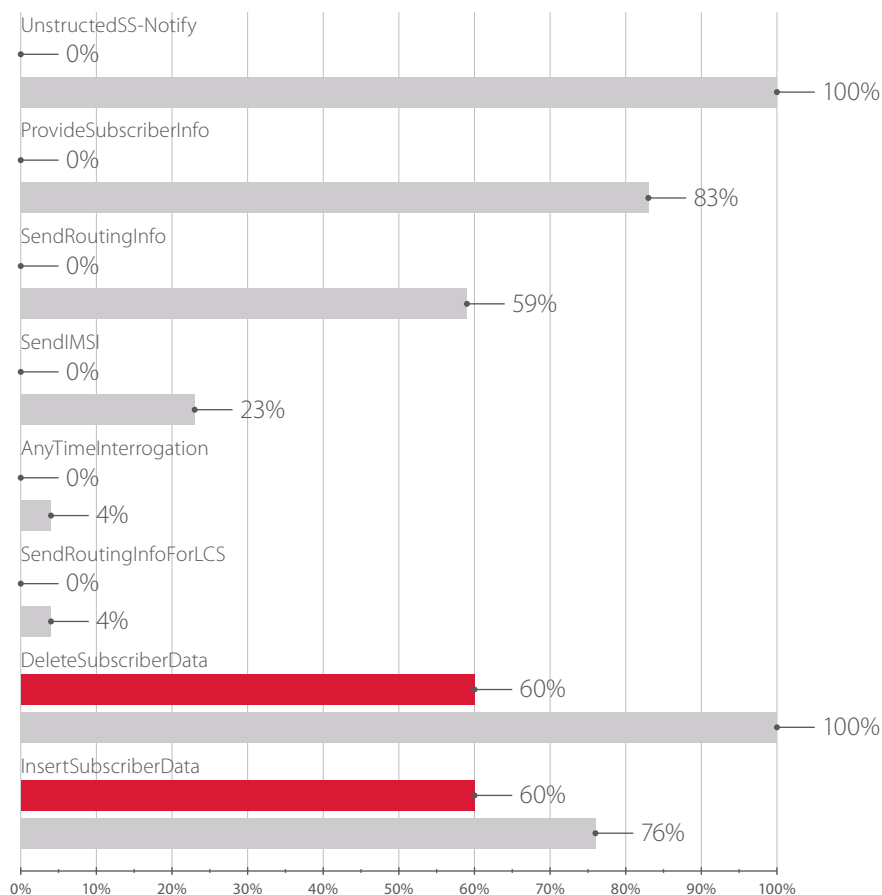


Рисунок 16. Доли успешных атак в зависимости от наличия системы фильтрации и блокировки сигнального трафика

**Использование системы  
фильтрации не способно  
обеспечить абсолютную  
безопасность сети**

Как мы видим, корректная фильтрация сигнального трафика позволяет снизить риски прохождения несанкционированных запросов. Это отчасти подтверждает и следующая диаграмма, на которой сравнивается возможность реализации каждой угрозы. Стоит выделить тот факт, что в сетях, где была внедрена система фильтрации и блокировки трафика, не удалась ни одна попытка отследить местоположение абонента. В остальных сетях попытки определить местоположение были успешны в 40% случаев.

■ Установлена система  
фильтрации и блокировки  
сигнального трафика

■ Система фильтрации  
и блокировки сигнального  
трафика отсутствует

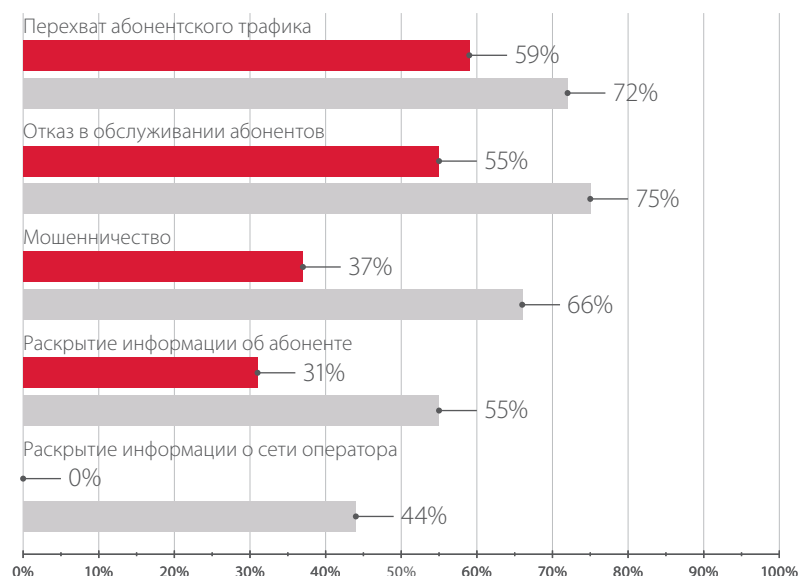


Рисунок 17. Доли успешных атак в зависимости от наличия системы фильтрации и блокировки сигнального трафика

В то же время очевидно, что даже использование системы фильтрации не способно обеспечить абсолютную безопасность сети. Разберемся, почему так происходит.

Все описываемые в данном отчете сообщения подразделяются на три категории, определенные в GSMA IR.82:

- 1) сообщения, передаваемые исключительно между устройствами домашней сети оператора;
- 2) сообщения, которые передаются из домашней сети оператора в гостевую сеть абонента;
- 3) которые передаются из гостевой сети в домашнюю сеть оператора.

Проще всего обеспечить защиту от атак с использованием сообщений первой и второй категорий. Для этого требуется правильно настроить сетевое оборудование и фильтрацию сигнального трафика для корректного анализа поступающих сообщений. Риски прохождения атак, эксплуатирующих сообщения первой категории, к 2017 году уже были сведены к минимуму.

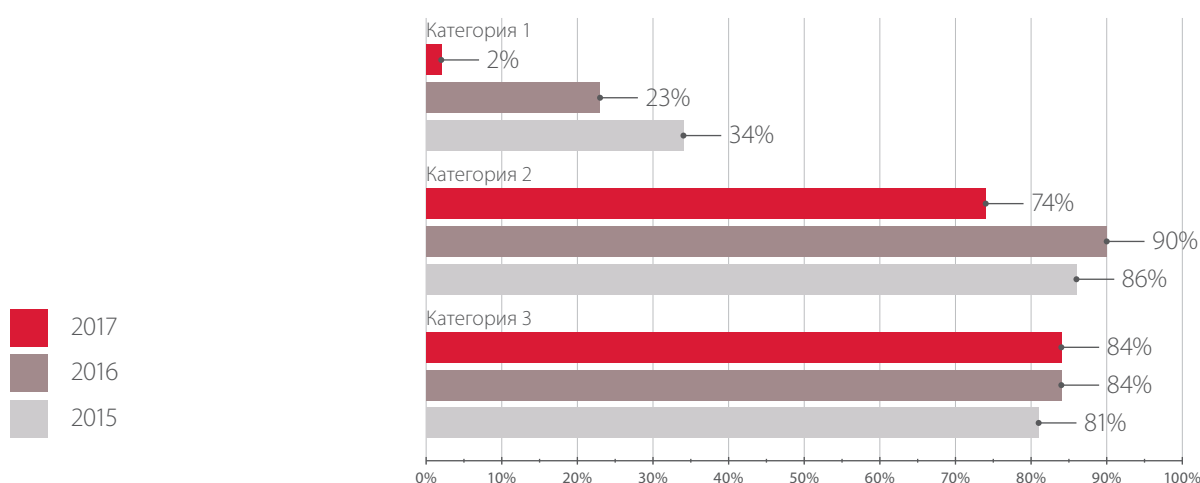


Рисунок 18. Доли успешных атак по категориям сообщений

Системы фильтрации трафика позволяют полностью защититься от атак, в которых задействованы сообщения первой категории, а в случае использования сообщений второй категории доля успешных атак снижается в два раза.

Иначе обстоит ситуация с третьей категорией. Необоснованная блокировка таких сообщений может повлиять на обслуживание абонента, действительно находящегося в роуминге. Например, ошибочная блокировка легитимной

#### Категория 1

SendRoutingInfo  
SendRoutingInfoForLCS  
SendIMSI  
AnyTimeInterrogation  
AnyTimeSubscriptionInterrogation  
AnyTimeModification

#### Категория 2

ProvideSubscriberInfo  
InsertSubscriberData  
DeleteSubscriberData  
UnstructuredSS-Notify

#### Категория 3

SendRoutingInfoForSM  
UpdateLocation  
RestoreData  
ProcessUnstructuredSS-Request  
InterrogateSS  
RegisterSS  
EraseSS  
PurgeMS  
Mt-ForwardSM  
Mo-ForwardSM

Сигнальные сообщения, рассматриваемые в данном отчете

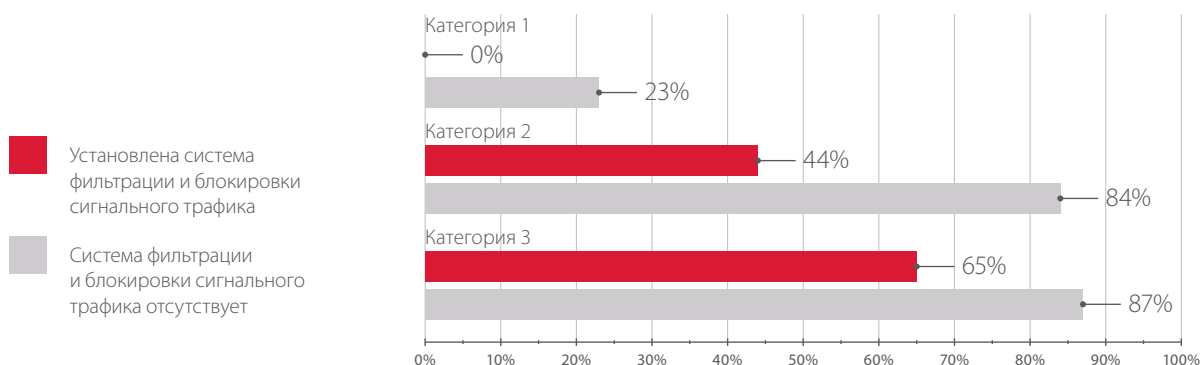


Рисунок 19. Доли успешных атак по категориям сообщений в зависимости от наличия системы фильтрации и блокировки сигнального трафика

регистрации абонента во внешней сети может привести к тому, что абонент останется без связи в роуминге, а для оператора это означает явное недополучение прибыли и возможную потерю клиента. Выявление нелегитимных запросов представляет собой сложную техническую задачу. Рекомендуется фильтровать сообщения на основе списков доверенных и запрещенных источников, предоставляемых роуминг-партнерами, однако объемы таких списков и потребность в их постоянном обновлении значительно усложняют реализацию решения на практике. Из опасений нарушить функционирование сети операторы очень осторожно подходят к вопросу блокировки подобных сообщений. Однако сообщения этой категории позволяют злоумышленнику реализовать все виды угроз, от раскрытия информации о сети и абоненте до перехвата пользовательского трафика, мошенничества и нарушения доступности абонентов.

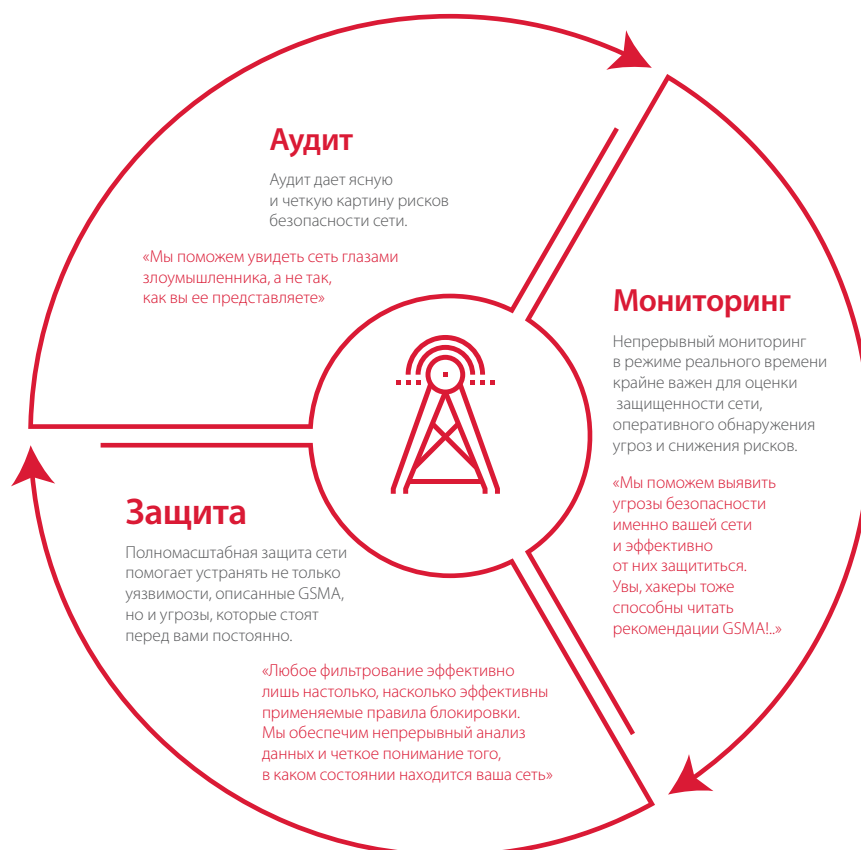
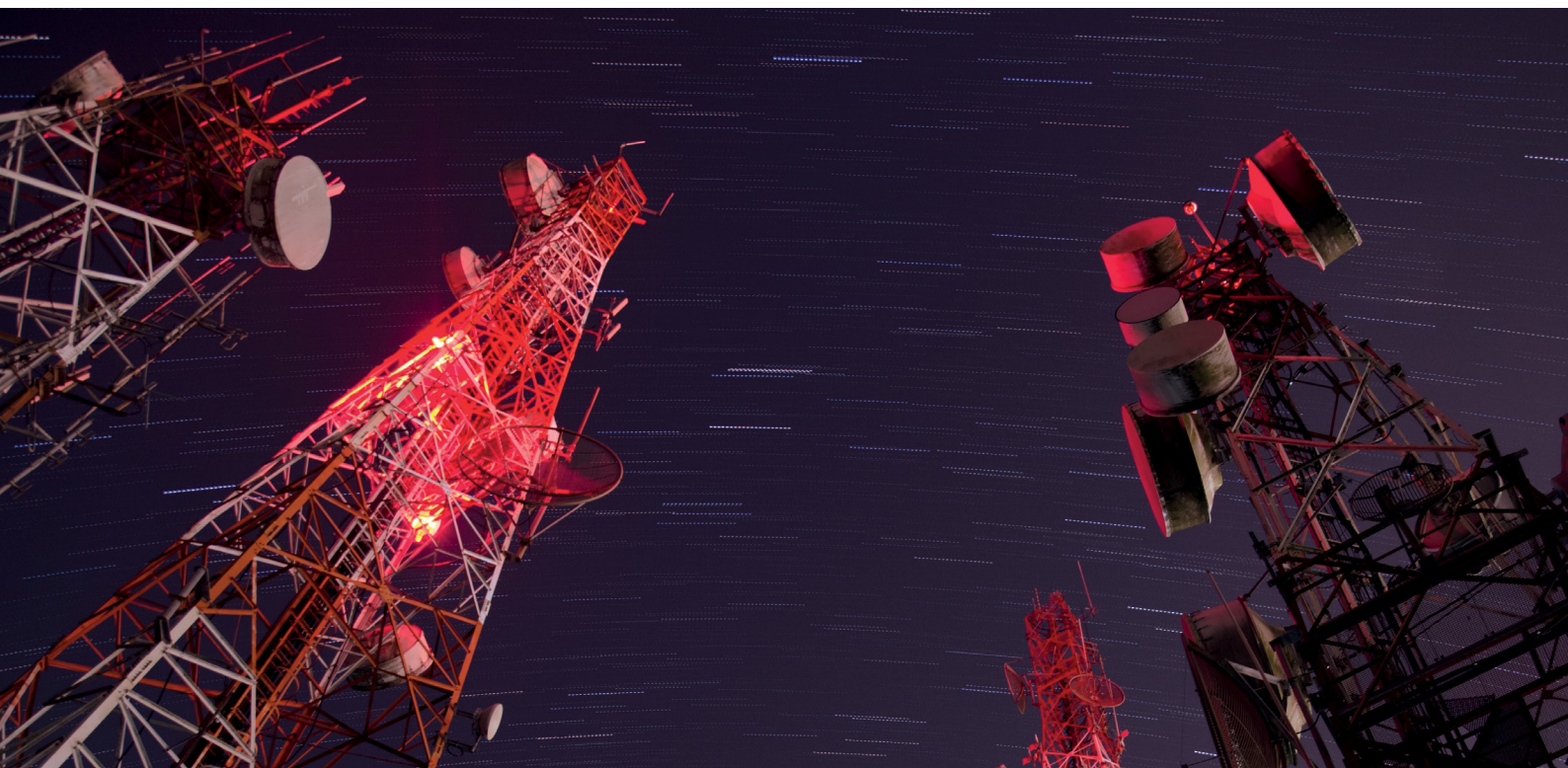


Рисунок 20. Рекомендуемый подход к обеспечению безопасности сигнальной сети





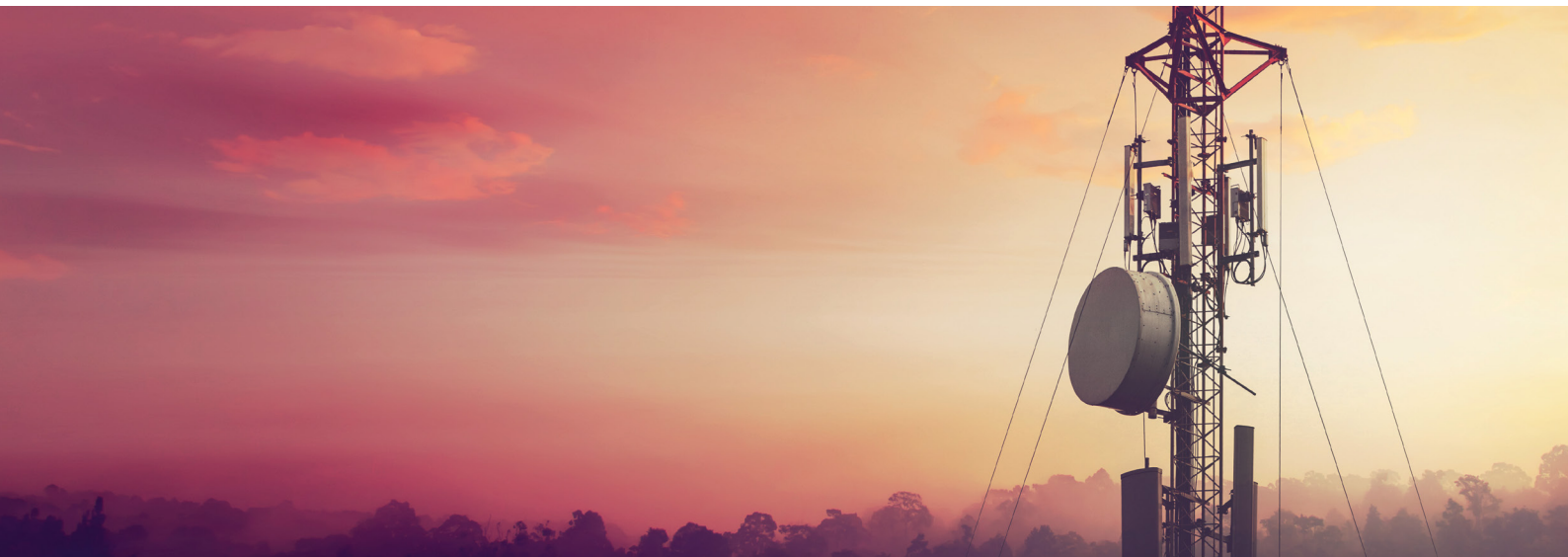
Для достижения высокого уровня защиты от всех видов рассматриваемых угроз необходим комплексный подход к информационной безопасности. В первую очередь важно проводить регулярный анализ защищенности сигнальной сети, так как это позволяет выявлять актуальные уязвимости, которые могут возникнуть при изменении конфигурации сети и параметров сетевого оборудования, и оценивать риски, связанные с информационной безопасностью.

Помимо этого, требуется обеспечить постоянный мониторинг и анализ сообщений, пересекающих границы сети, в целях поддержания параметров безопасности в актуальном состоянии, своевременного выявления потенциальных угроз и реагирования на них. Указания использовать системы мониторинга для противодействия атакам содержатся и в рекомендациях GSMA<sup>1</sup>. Эта задача должна выполняться с использованием специальных систем обнаружения угроз, которые могут проводить интеллектуальный анализ сообщений в режиме реального времени. Такое решение позволяет выявлять нелегитимную активность внешних узлов на ранних стадиях и передавать информацию о них системе фильтрации сигнального трафика для повышения ее эффективности, например для обновления списков запрещенных узлов, а также позволяет обнаруживать ошибки конфигурации сетевых устройств и оповещать сотрудников оператора о необходимости их исправить.

Безопасность — это процесс, поэтому нельзя ограничиваться разовыми мерами (аудитами или внедрением средств защиты). Комплексный подход применяют специалисты Positive Technologies для защиты сигнальных сетей своих клиентов, узнать подробнее можно на сайте, задав вопрос через форму обратной связи или написав нам на [info@ptsecurity.com](mailto:info@ptsecurity.com).

В следующем разделе мы выясним, позволяют ли существующие средства защиты противостоять злоумышленникам в реальных условиях и как использование системы обнаружения и предотвращения угроз может обеспечить защиту сети.

<sup>1</sup> SG.11. SS7 Interconnect Security Monitoring Guidelines.



## АТАКИ НА СЕТИ SS7

Мы рассмотрели уязвимости, которым подвержены сети SS7, и возможные угрозы, связанные с их эксплуатацией. Остается открытым вопрос: как результаты исследований защищенности соотносятся с реальной жизнью, квалификацией и возможностями настоящих преступников? В этом разделе мы приведем результаты проектов по мониторингу безопасности в сетях SS7 и посмотрим, с какими атаками действительно сталкиваются операторы мобильной связи и эффективны ли на практике существующие меры защиты.

### Методика

Проекты по мониторингу безопасности в сетях SS7 проводились для крупных операторов связи Европы и стран Ближнего Востока. Целью этих работ была демонстрация возможностей системы PT Telecom Attack Discovery (PT TAD), которая предназначена для анализа сигнального трафика в режиме реального времени и выявления нелегитимной активности с возможностью блокировки несанкционированных сообщений или оповещения сторонних средств фильтрации и блокировки трафика. Такой подход позволяет своевременно выявлять потенциальные угрозы и реагировать на них, не оказывая негативного воздействия на функционирование сети.

PT TAD возможно использовать и в качестве пассивной системы обнаружения нелегитимной активности, в этом случае система позволяет анализировать проходящий трафик, но не влияет на него. В нашем исследовании представлены результаты мониторинга трафика в пассивном режиме.



Рисунок 21. Схема подключения оборудования для анализа сигнального трафика системой PT TAD в пассивном режиме

### Статистика по выявленным атакам

Во всех сетях, где проводились работы по мониторингу событий безопасности, использовалось оборудование SMS Home Routing, а та или иная система фильтрации и блокировки сигнального трафика была установлена в каждой третьей сети.

В ходе мониторинга мы получили результаты, свидетельствующие о том, что злоумышленники не только хорошо осведомлены о проблемах безопасности сигнальных сетей, но и активно эксплуатируют эти уязвимости.

В таблице для каждой угрозы по вертикали отражено распределение всех попыток атак по используемым методам. Доли успешных атак приведены по каждой угрозе и отдельно по каждому методу. Пустая клетка означает, что сообщение не ведет к реализации данной угрозы.

Например, попытка получить IMSI абонента в 79,9% случаев осуществляется нарушителями с помощью метода SendRoutingInfo. В целом нарушителю удается в 34,5% случаев успешно получить IMSI тем или иным методом. А сам метод SendRoutingInfo успешен в 22,6% попыток атак.

Таблица 3. Распределение выявленных атак по типам угроз

	Раскрытие информации об абоненте			Раскрытие информации о сети оператора	Мошенничество			Перехват SMS	Недоступность сервисов для абонента	Доля успешных атак
	Раскрытие IMSI	Определение местоположения абонента	Раскрытие информации о профиле абонента		Перенаправление вызова	Эксплуатация USSD-запросов	Уклонение от таргетирования в реальном времени			
SendRoutingInfoForSM	15,7%			5,2%						87,2%
SendRoutingInfoForLCS	3,3%			1,1%						1,1%
SendRoutingInfo	79,9%	27%		26,3%						22,6%
SendIMSI	1,1%									65,6%
AnyTimeInterrogation		69,3%		67,4%						13,3%
ProvideSubscriberInfo		3,7%								58,6%
RestoreData			84%							0,5%
UpdateLocation			0,9%		4,7%			100%	4,6%	100%
AnyTimeSubscriptionInterrogation			14,8%							0%
InterrogateSS			0,3%							58,8%
AnyTimeModification					0,6%		0,5%		0,6%	0,1%
InsertSubscriberData					93,2%		86,7%		90,6%	1,5%
RegisterSS					1,5%				1,4%	26,7%
ProcessUnstructuredSS						0,6%				53,3%
UnstructuredSSNotify						99,4%				31,1%
DeleteSubscriberData							12,8%			2,1%
PurgeMS									2,8%	53,3%
<b>Доля успешных атак</b>	<b>34,5%</b>	<b>17,5%</b>	<b>1,5%</b>	<b>20,1%</b>	<b>6,5%</b>	<b>31,2%</b>	<b>1,5%</b>	<b>100%</b>	<b>7,8%</b>	



Как мы выяснили, источником большинства атак являются не национальные операторы той страны, в которой проводился мониторинг безопасности, а международные операторы связи. Подозрительные запросы поступают преимущественно из стран Азии и Африки; вероятно, это связано с тем, что в этих странах злоумышленнику проще купить доступ к сети SS7. При этом физический доступ к оборудованию оператора, предоставившего возможность подключения к сети SS7, не требуется, злоумышленник может находиться в любой точке земного шара.

Для демонстрации среднего количества атак в сутки мы выбрали крупного оператора с абонентской базой более 40 миллионов человек, который дал согласие на публикацию данных без указания наименования компании.

Таблица 4. Среднее число атак в сутки по типам угроз

Угроза	Среднее число атак в сутки
Раскрытие информации об абоненте	4827
Раскрытие IMSI	3087
Определение местоположения абонента	3718
Раскрытие информации о профиле абонента	47
Раскрытие информации о сети оператора	4294
Мошенничество	62
Перенаправление вызова	2
Эксплуатация USSD-запросов	59
Уклонение от тарификации в реальном времени	2
Перехват SMS	1
Недоступность сервисов для абонента	4



## Утечка информации

Практически все зафиксированные атаки были направлены на раскрытие информации об абоненте и о сети оператора. Атаки с целью мошенничества, перехвата абонентского трафика и нарушения доступности абонентов в совокупности составили менее двух процентов<sup>2</sup>.



Рисунок 22. Распределение выявленных атак по видам угроз

Такое распределение связано с тем, что злоумышленнику в первую очередь требуется узнать идентификаторы абонентов и адреса узлов сети оператора. Только в случае получения необходимой информации на первом этапе можно проводить дальнейшие атаки. При этом сбор информации необязательно свидетельствует о готовящейся целенаправленной атаке на абонента. Вместо того, чтобы проводить сложные в техническом плане атаки, существует способ получить прибыль более простым путем, продавая сведения другим преступным группировкам. Массовые однотипные запросы могут указывать на то, что злоумышленники составляют базы абонентов, в которых сопоставлены телефонные номера и идентификаторы пользователей, а также собирают данные об операторе для последующей продажи полученных сведений на черном рынке.

Каждая третья атака, целью которой было получение IMSI пользователя, и каждая пятая направленная на раскрытие конфигурации сети — возвращали злоумышленнику искомую информацию.

Для получения информации использовались главным образом два метода — AnyTimeInterrogation и SendRoutingInfo. Помимо того, что оба метода раскрывают информацию о сети, а метод SendRoutingInfo возвращает IMSI абонентов, эти сообщения позволяют узнать и местоположение абонента. Как показывают результаты, в 17,5% случаев ответы сети на подобные запросы содержали данные о расположении абонента.

Параметры фильтрации на сетевом оборудовании (STP, HLR) или корректно настроенная система фильтрации сигнального трафика позволили бы полностью исключить возможность атак с использованием этих сообщений, а значит, и снизить риск остальных угроз. Тем не менее на практике параметры фильтрации сообщений не всегда установлены корректно. Так, процент ответов на подозрительные запросы с целью определения местоположения пользователя в сетях, защищенных системой блокировки сигнального трафика, оказался в два раза ниже, чем в остальных сетях. Приблизительно те же результаты были получены для атак, направленных на раскрытие конфигурации сети и идентификаторов абонентов. В целом это хорошие показатели, указывающие на эффективность принимаемых мер защиты, однако при правильной конфигурации доля успешных атак была бы сведена к нулю.

### В 87%

случаев подозрительные запросы миновали SMS Home Routing

<sup>2</sup> Процедура UpdateLocation возвращает информацию о профиле абонента. Тем не менее мы полагаем, что регистрация абонента в поддельной сети преследует в первую очередь иные цели: перенаправление входящего вызова, перехват SMS или отказ в обслуживании абонента.

Интересно заметить, что во всех сетях была установлена система SMS Home Routing, используемая для противодействия атакам методом SendRoutingInfoForSM. Сообщение SendRoutingInfoForSM запрашивает информацию, необходимую для доставки входящего SMS, — идентификатор абонента и адрес обслуживающего узла. При нормальном режиме функционирования за этим сообщением должно поступить входящее SMS, в противном случае запросы считаются нелегитимными. Каждый запрос должен направляться системе SMS Home Routing, которая возвращает в ответе виртуальные идентификаторы и адреса, однако из-за предположительно некорректной настройки сетевого оборудования этот способ защиты оказался недостаточно эффективен — в 87% случаев подозрительные запросы миновали SMS Home Routing. Схожие результаты мы отмечали и в ходе работ по анализу защищенности сетей SS7.

### 23% атак

с целью мошенничества  
успешно осуществляются  
злоумышленниками

### Мошенничество

Атаки с целью мошенничества как в отношении оператора, так и в отношении абонентов составили всего 1,32%, причем существенная их часть пришлась на эксплуатацию USSD-запросов. Несанкционированная отправка USSD-запросов позволяет осуществить перевод денег со счета абонента, подписать абонента на дорогостоящую услугу или отправить фишинговое сообщение от имени доверенного сервиса.

Около четверти всех попыток оказались успешны: сообщения были приняты сетью оператора как легитимные независимо от наличия средств фильтрации трафика.

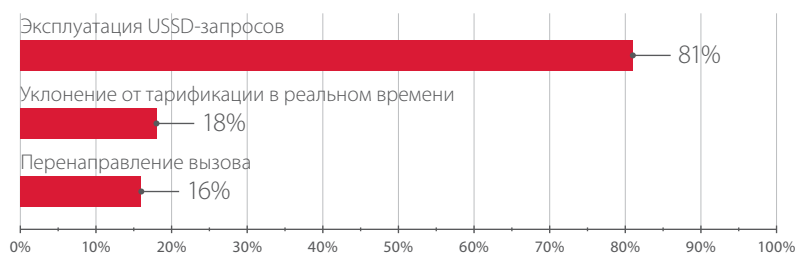


Рисунок 23. Атаки, осуществляемые с целью мошенничества

### 100% атак,

направленных на перехват  
SMS, являются успешными

### Перехват трафика

За время проведения работ были зафиксированы запросы UpdateLocation на регистрацию абонента в новой сети, исходящие из подозрительных источников. При этом ни одна попытка поддельной регистрации не была отклонена сетью оператора. Как показывают результаты работ по анализу защищенности и данные проектов по мониторингу безопасности, использование системы фильтрации и блокировки трафика не дает в этом случае существенных преимуществ — для защиты от такого рода атак необходимо принимать комплексные меры безопасности.

Нелегитимные запросы UpdateLocation составили всего 0,01% от общего числа атак, однако этот метод представляет особую опасность, поскольку позволяет перехватывать SMS абонента, содержащие конфиденциальную информацию, и перенаправлять вызовы на номера злоумышленников, что может быть использовано преступниками в мошеннических целях.

В 2017 году ярким примером атаки с использованием уязвимостей сетей SS7 послужил перехват SMS абонентов немецкого сотового оператора, в результате которого преступникам удалось похитить деньги с банковских счетов пользователей. Атака проводилась в два этапа. На первом этапе преступники отправляли пользователям письма, содержащие ссылку на фишинговый сайт, маскирующийся под официальный сайт банка, и похищали логины и пароли от банковских



учетных записей. Для прохождения двухфакторной аутентификации и подтверждения дальнейших операций им требовался доступ к одноразовым кодам, которые банк отправляет пользователю в SMS. Предполагается, что преступники заранее приобрели на черном рынке доступ к сети SS7. На втором этапе атаки они регистрировали абонентов в фальшивой сети, выдавая себя за роумингового партнера — иностранного мобильного оператора. После этого входящие SMS, содержащие одноразовые коды и уведомления о совершенных операциях, отправлялись на номер злоумышленников. Как считают эксперты, преступники проводили атаки главным образом в ночное время, чтобы снизить вероятность обнаружения своих действий.

### Отказ в обслуживании опасен для интернета вещей

#### Отказ в обслуживании

Атаки, направленные на отказ в обслуживании отдельных абонентов, также были немногочисленны, при этом лишь 7,8% подобных атак были успешны. Преимущественно использовался метод InsertSubscriberData, но 99% этих сообщений остались без ответа, то есть были проигнорированы сетью оператора. Наличие систем фильтрации и блокировки трафика оказало значительное влияние на итоговые результаты: процент успешно обработанных запросов в этих сетях был в четыре раза ниже, чем в остальных, однако полностью от таких атак защититься не удалось.

Отказ в обслуживании представляет серьезную опасность для электронных устройств интернета вещей. К сетям связи сегодня подключены не только отдельные устройства пользователей, но и элементы инфраструктуры умных городов, современные промышленные предприятия, транспортные, энергетические и иные компании.

Как мы уже отмечали, злоумышленник может провести атаку на нарушение доступности абонента таким образом, что восстановление связи будет невозможно без обращения за технической поддержкой, а среднее время недоступности пользователя превышает три часа. Утрата репутации надежного поставщика связи может лишить оператора существенной доли клиентов, которые предпочитают пользоваться услугами других компаний.



### Пример атаки

Как отмечалось выше, внедрения отдельных мер защиты без обеспечения комплексного подхода к безопасности недостаточно для противодействия всем атакам, эксплуатирующим уязвимости, причины которых кроются в самой архитектуре сетей SS7.

Рассмотрим реальный пример, выявленный во время проведения работ. Атака представляла собой ряд последовательных шагов, которые были объединены в логическую цепочку системой обнаружения атак, в то время как существующие системы защиты не смогли распознать отдельные запросы как нелегитимные. В первую очередь злоумышленники предприняли успешную попытку узнать IMSI абонента по телефонному номеру. Получив необходимые для дальнейших действий сведения, они попытались установить местоположение абонента, однако этот этап атаки завершился неудачей. Через день злоумышленники отправили запрос на регистрацию абонента в поддельной сети, который был выполнен сетью оператора, и получили возможность перехватывать входящие вызовы и SMS абонента, что, вероятно, и было их целью. Рассмотрим каждый шаг более детально.





Система обнаружения и предотвращения атак PT TAD зафиксировала сообщения SendRoutingInfoForSM в отношении абонента домашней сети оператора, которые были отправлены с внешнего узла. Сообщения были отмечены как подозрительные, поскольку за ними не следовала отправка SMS, как предполагается в случае легитимной активности. За каждым таким сообщением следовала попытка атаки ProvideSubscriberInfo, которая была заблокирована сетью. Система PT TAD выявила последовательную комбинацию атак SendRoutingInfoForSM и ProvideSubscriberInfo с интервалом в 1–2 секунды, что свидетельствует о том, что действия по определению местоположения абонентов автоматизированы.

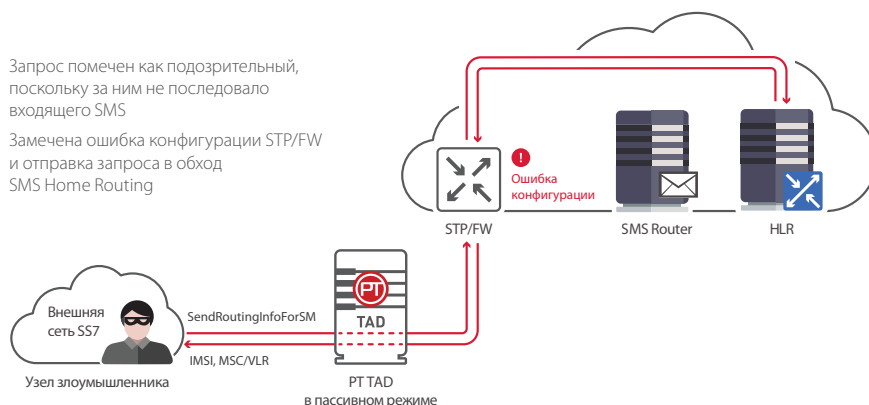


Рисунок 24. Обработка подозрительного запроса SendRoutingInfoForSM

Так как в сети оператора использовалась система SMS Home Routing, ответ на сообщение SendRoutingInfoForSM не должен был содержать реальный IMSI, равно как и адрес реального MSC/VLR. Однако определенным образом сформированный пакет позволял обойти не вполне корректно настроенный механизм работы SMS Home Routing. Пограничный STP должен направлять сообщения SendRoutingInfoForSM, полученные извне, на устройство SMS Router. Однако если в конфигурации STP маршрутизация по типу адресации имеет более высокий приоритет, чем проверка кода операции, то злоумышленник может отправить сообщение SendRoutingInfoForSM, адресуя его в плане нумерации (E.214), присущем операции регистрации абонента в роуминговой сети (UpdateLocation), и STP осуществит маршрутизацию сигнального сообщения без проверки кода операции. В результате атаки злоумышленник получал не адрес платформы и виртуальный IMSI, а действительный адрес MSC/VLR абонента и его реальный IMSI. Именно эти данные использовались для последующей попытки атаки ProvideSubscriberInfo с целью определения местоположения абонента.

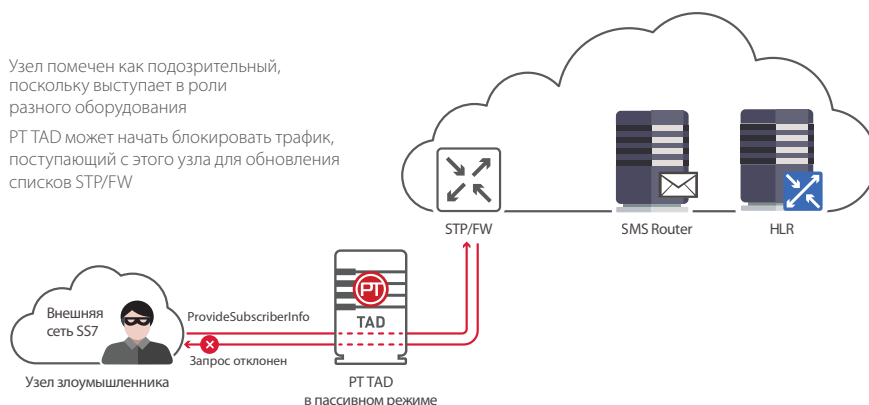


Рисунок 25. Попытка определить местоположение пользователя

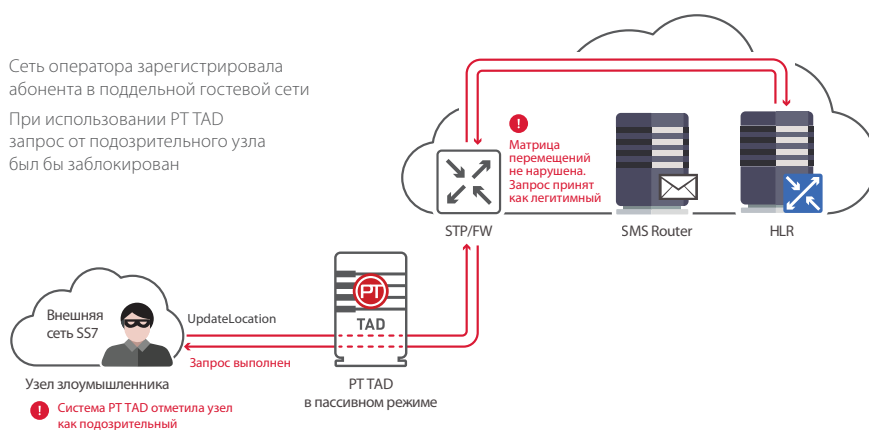


Рисунок 26. Регистрация абонента в поддельной сети

После обнаружения попыток атак с одного узла, который выступает в роли различного оборудования (MSC и HLR в данном случае), узел был помечен как подозрительный. На следующий день с данного узла поступил запрос UpdateLocation на обновление регистрации того же абонента. Запрос не нарушал матрицы перемещений абонента, поскольку предыдущее сообщение UpdateLocation было получено шестью часами ранее, и был пропущен системой фильтрации сигнального трафика как легитимный.

Если бы в сети применялся комплексный подход к безопасности, а именно мониторинг безопасности с интегрированной системой блокирования, то после успешной атаки SendRoutingInfoForSM и неуспешной ProvideSubscriberInfo система мониторинга немедленно оповестила бы модуль фильтрации о том, что необходимо обновить список запрещенных узлов для блокировки любого трафика, приходящего от данного узла.



## ЗАКЛЮЧЕНИЕ

Как показали результаты исследования, безопасность сетей мобильной связи все еще находится на низком уровне. Подавляющее большинство сетей подвержены уязвимостям, позволяющим перехватывать голосовые вызовы и сообщения абонентов, проводить мошеннические операции и нарушать доступность сервисов для абонентов.

О существующих уязвимостях прекрасно осведомлены злоумышленники, и мы уже увидели, к каким последствиям могут привести их атаки, на примере недавнего инцидента, затронувшего абонентов немецкого оператора связи: были похищены деньги с банковских счетов пользователей. Судя по уровню нелегитимной активности, которую выявляет система обнаружения и предотвращения атак PT TAD, мы можем ждать новых подобных инцидентов в ближайшее время.

Мы отметили, что операторы осознают недостатки безопасности сигнальных сетей и начинают внедрять дополнительные средства защиты для закрытия уязвимостей, в том числе системы фильтрации и блокировки сигнального трафика. Однако эти системы не могут полностью решить проблемы, связанные с особенностями архитектуры сетей SS7.

Для противодействия преступникам требуется комплексный подход к безопасности. Необходимо регулярно проводить анализ защищенности сигнальной сети с целью выявления существующих уязвимостей и разработки мер по снижению рисков реализации угроз, а после — поддерживать параметры безопасности в актуальном состоянии. Помимо этого, важно осуществлять постоянный мониторинг и анализ сообщений, пересекающих границы сети, для выявления потенциальных атак. Эту задачу может выполнять система обнаружения и предотвращения атак, которая позволяет на ранних стадиях выявлять нелегитимную активность и блокировать подозрительные запросы либо передавать информацию о несанкционированных подключениях сторонним системам, тем самым повышая эффективность существующих средств защиты. Такой подход позволяет обеспечить высокий уровень защиты, не нарушая нормальное функционирование мобильной сети.

---

### О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

© 2018 Все права принадлежат АО «Позитив Текнолоджиз». Любое использование, перепечатка, цитирование возможны исключительно при условии указания авторов и правообладателя.