



# СТАТИСТИКА УЯЗВИМОСТЕЙ СЕТЕЙ DIAMETER

2018

## СОДЕРЖАНИЕ

Введение.....	3
Термины и обозначения.....	3
Резюме.....	4
Методика исследования.....	4
Портрет участников.....	5
Обзор угроз в сетях Diameter.....	5
Общая статистика.....	5
Утечка информации об абоненте.....	7
Утечка информации об операторе.....	9
Мошенничество.....	9
Отказ в обслуживании абонентов.....	9
Причины возникновения уязвимостей.....	11
Рекомендации по защите.....	13
Заключение.....	14

## ВВЕДЕНИЕ

Сети нового поколения 4G повсеместно набирают популярность, обеспечивая абонентам высокое качество связи, а также защиту передаваемых данных. Что мы имеем в виду, когда говорим о защите данных в телекоммуникационных сетях? Какие угрозы скрывает в себе привычная мобильная связь и в чем отличие сетей 4G от сетей предыдущих поколений с точки зрения информационной безопасности?

Для передачи служебных данных, например в процессе голосового вызова, в сетях 2G/3G использовалась сигнальная система SS7, которая разрабатывалась еще в те времена, когда безопасности не придавали особого значения. В связи с этим система SS7 оказалась подвержена ряду уязвимостей, о которых мы неоднократно говорили. Так, к примеру, злоумышленник мог с легкостью перехватить SMS абонента или прослушать чужой разговор.

В сетях 4G на замену SS7 пришел протокол Diameter, с помощью которого выполняется большинство служебных задач. Тем не менее, как мы рассказывали в одном из предыдущих отчетов, протокол Diameter отнюдь не является полностью защищенным. Теоретически мошенничество, перехват SMS, отказ в обслуживании и другие угрозы все еще остаются актуальными. Более того, абоненты сетей 4G так или иначе остаются абонентами сетей предыдущих поколений, поскольку большинство мобильных операторов на текущий момент используют 4G только для предоставления доступа в интернет, а передача SMS или голосовые вызовы осуществляются в режиме 3G.

В данном исследовании мы на примерах практических работ рассмотрим, какие атаки действительно может проводить злоумышленник в сетях Diameter и насколько такие сети безопаснее по сравнению с сетями на основе SS7.

## ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

Diameter — сигнальный протокол, используемый в телекоммуникационных сетях для передачи служебных данных.

DEA (Diameter Edge Agent) — пограничный агент. Обычно он функционирует на границе сигнальной сети оператора и служит в качестве прокси-агента для сигнального трафика из сетей других операторов.

DRA (Diameter Routing Agent) — агент маршрутизации. Осуществляет маршрутизацию Diameter-трафика.

HSS (Home Subscriber Server) — сервер абонентских данных. Один из важнейших элементов в инфраструктуре сетей четвертого поколения стандарта LTE, служит для хранения важной пользовательской информации и информации о действиях абонентов.

IMSI (International Mobile Subscriber Identity) — международный идентификатор абонента мобильной сети. Служит для уникальной идентификации абонента сотовой связи во всем мире.

MME (Mobility Management Entity) — узел управления мобильностью. Обеспечивает возможность переключения между базовыми станциями, работу в роуминге, аутентификацию пользовательских устройств путем взаимодействия с HSS, а также отвечает за выбор обслуживающего шлюза.

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

## РЕЗЮМЕ

**Все исследованные сети содержат критически опасные уязвимости**, позволяющие отследить местоположение абонентов и вызвать отказ в обслуживании. Риску мошенничества в отношении оператора подвержена каждая третья сеть.

**Абоненты сетей 4G подвержены тем же угрозам, что и абоненты сетей предыдущих поколений.** Как показывает практика, в сетях на основе протокола Diameter возможны атаки, направленные на отказ в обслуживании, раскрытие информации об абонентах и сети оператора, а также мошенничество в отношении оператора. Хотя спектр атак ограничен по сравнению с сетями предшествующих поколений, злоумышленник может принудительно перевести устройство абонента в режим 3G — и проводить дальнейшие атаки уже на менее защищенную систему SS7: прослушивать голосовые вызовы, перехватывать SMS и осуществлять мошеннические схемы в отношении абонентов.

**Для обеспечения защиты сети необходим комплексный подход к безопасности.** Большинство выявленных недостатков были связаны не только с некорректной настройкой или уязвимостями сетевого оборудования, но также с фундаментальными проблемами протокола Diameter, для решения которых требуются дополнительные средства защиты. Крайне важно, чтобы все меры по обеспечению безопасности принимались в комплексе и включали в себя регулярный анализ защищенности сети, поддержание параметров безопасности в актуальном состоянии, постоянный мониторинг и анализ сигнального трафика, своевременное выявление нелегитимной активности и реагирование на возникающие угрозы на ранних стадиях.

## МЕТОДИКА ИССЛЕДОВАНИЯ

В рамках анализа защищенности телекоммуникационных сетей специалисты Positive Technologies моделируют действия потенциального злоумышленника. Для эмуляции вредоносного узла используется специальное оборудование — PT Telecom Vulnerability Scanner. Чаще при проведении работ предполагается, что злоумышленник действует из сети, внешней по отношению к оператору, однако в некоторых случаях исследуются и возможности внутреннего нарушителя. На рисунках ниже представлены два стандартных варианта подключения комплекса к тестируемой сети.

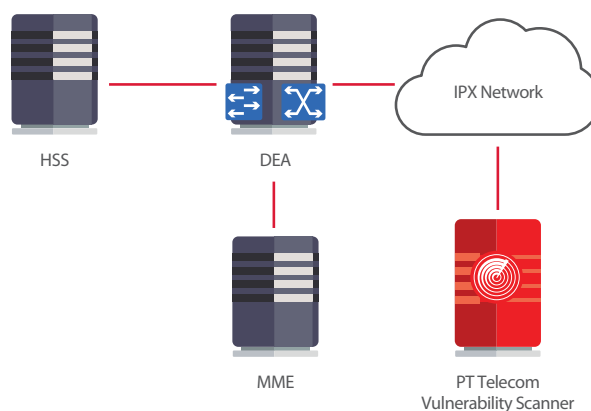


Рисунок 1. Схема внешнего подключения к исследуемой сети

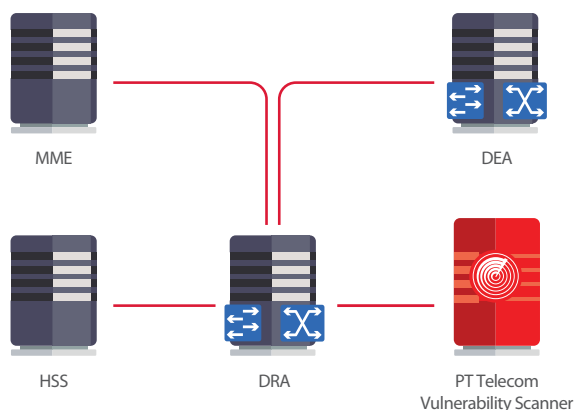


Рисунок 2. Схема внутреннего подключения к исследуемой сети

В настоящем исследовании представлены результаты анализа защищенности 15 телеком-операторов, в ходе которого эксперты Positive Technologies проводили максимально широкий перечень проверок.

### ПОРТРЕТ УЧАСТНИКОВ

В исследовании принимали участие операторы связи стран Европы и Азии. Большую часть (80%) составили крупные телекоммуникационные компании с объемом абонентской базы более 40 млн.

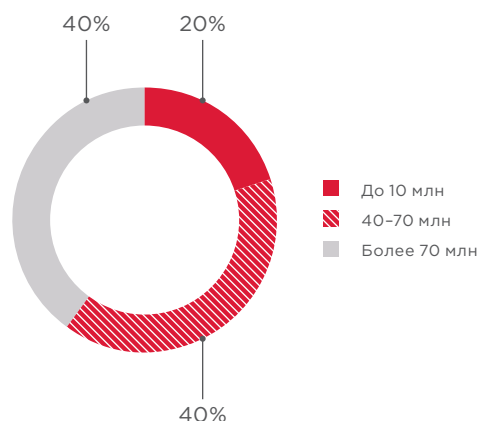


Рисунок 3. Распределение операторов связи по объему абонентской базы

### ОБЗОР УГРОЗ В СЕТЯХ DIAMETER

#### Общая статистика

В отношении сетей на основе сигнального протокола Diameter злоумышленник может проводить атаки с целью:

- + раскрытия информации об абоненте;
- + раскрытия информации о сети оператора;
- + перехвата абонентского трафика;
- + мошенничества;
- + отказа в обслуживании.

К раскрытию информации об абоненте мы относим те атаки, которые позволяют отследить местоположение абонента, узнать детали его профиля и определить IMSI — уникальный идентификатор абонента, требующийся для проведения дальнейших атак. Также злоумышленнику может понадобиться и информация о сети оператора — адреса устройств, конфигурация сети.

Перехват абонентского трафика (входящих SMS) в сетях 4G теоретически возможен, однако на практике его реализация затруднена, поскольку передача SMS зачастую осуществляется через сети предыдущих поколений либо с применением технологий, не использующих протокол Diameter. Установка соединения при голосовых вызовах также осуществляется при помощи иных протоколов.

Злоумышленник может проводить атаки с целью мошенничества для получения бесплатного доступа к услугам связи, что означает прямые финансовые потери для мобильного оператора.

В рамках анализа защищенности лишь небольшая часть операторов связи проводит тестирование своего оборудования на возможность отказа в обслуживании, поскольку это потенциально может привести к перебоям в работе мобильной сети. В связи с этим в данном отчете мы рассмотрим результаты только тех проверок, которые проводились с целью вызвать отказ в обслуживании отдельных абонентов. Нужно учитывать, что некоторые способы атак позволяют злоумышленнику реализовать массовый отказ в обслуживании, что чревато серьезными репутационными потерями, так как сразу тысячи пользователей могут остаться без связи на длительное время (до перезагрузки устройства или перехода в зону действия другого ММЕ).

Ранее в этом году мы проводили аналогичное исследование в отношении сетей SS7. Сравним, насколько сети 4G, в которых используется сигнальный протокол Diameter, безопаснее сетей предыдущих поколений, и рассмотрим доли успешных атак в отношении сетей разных поколений.

Таблица 1. Доли уязвимых сетей по типам угроз

Угроза	Сети SS7	Сети Diameter
Раскрытие информации об абоненте	100%	100%
Раскрытие информации о сети оператора	63%	75%
Перехват абонентского трафика	89%	— <sup>1</sup>
Мошенничество	78%	33%
Отказ в обслуживании абонентов	100%	100%

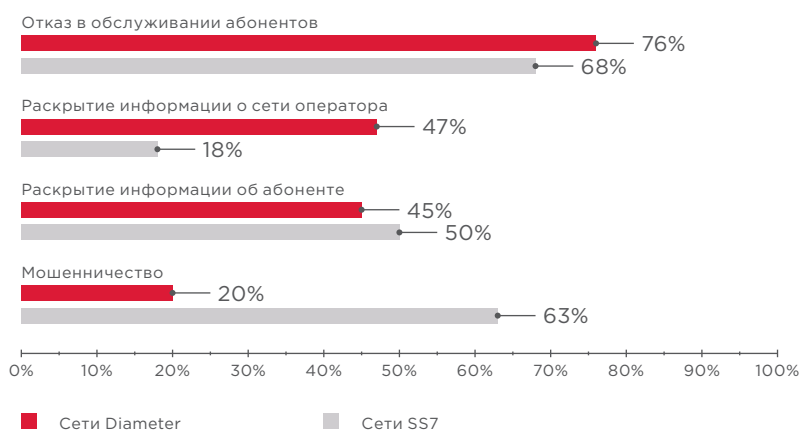


Рисунок 4. Доли успешных атак по типам угроз

<sup>1</sup> Передача SMS с использованием Diameter не осуществлялась. Для установления голосовых вызовов в сетях 4G используется протокол SIP.

Мобильные операторы плохо осведомлены о наличии проблем безопасности в сетях Diameter

Как и в сетях на основе SS7, во всех сетях, где применяется протокол Diameter, возможны раскрытие информации об абоненте и отказ в обслуживании абонентов. При этом доля успешных атак, направленных на отказ в обслуживании абонентов, несколько выше. Возможно, такие результаты связаны с тем, что операторы осведомлены о существующих проблемах безопасности в сетях SS7 и принимают меры для защиты.

В 75% сетей оказалось возможным раскрытие информации о сети оператора, что несколько хуже показателей для сетей предыдущих поколений. Это объясняется тем, что среди сигнальных сообщений протокола Diameter, позволяющих получить данные о сети оператора, выше доля тех сообщений, которые требуют дополнительных проверок для осуществления корректной фильтрации. Эти сообщения могут быть получены от любого узла, а единственный способ выявить подлог — сверять текущее сообщение с предыдущими, принимая во внимание местоположение пользователя и временной промежуток между сообщениями. Текущее оборудование в большинстве сетей Diameter не готово к этому — оно не позволяет гибко настроить правила фильтрации и осуществлять мониторинг соответствующей активности. Операторы не видят этих атак и, следовательно, не знают о том, что от них нужно защищаться.

Вдвое меньше сетей оказались подвержены риску мошенничества. Впрочем, причина такого снижения отчасти состоит в том, что на текущий момент известно лишь малое число атак, направленных на проведение мошеннических операций в сетях Diameter, в то время как для сетей SS7 хорошо изучены различные вариации таких атак (нелегитимная переадресация вызовов, эксплуатация USSD-запросов, манипулирование SMS, изменение профиля абонента).

Как показывают исследования, в сетях 4G существует возможность перехвата SMS абонентов. Однако во всех сетях, для которых проводился анализ защищенности, при передаче SMS устройства абонентов либо переключались в режим 3G (где используется сигнальная система SS7), и соответственно, провести тестирование новой технологии было невозможно, либо использовались методы передачи SMS, не позволяющие осуществить перехват сообщений.

Напомним, что в сетях SS7 удавалось перехватить 9 из 10 SMS, а значит, это справедливо и для текущей конфигурации большинства исследованных сетей 4G. В дальнейшем, с внедрением IMS (и, соответственно, технологий VoLTE/VoWiFi), передача SMS может осуществляться с использованием протокола SIP вместо протокола Diameter, поэтому атаки, направленные на перехват трафика абонентов, потенциально могут быть затруднены.

В процессе установления голосовых вызовов устройства абонентов также переключаются в режим 3G, реже применяется протокол SIP.

### Утечка информации об абоненте

Приватность абонентов остается под угрозой даже в сетях Diameter. Отследить местоположение абонента удавалось в 38% случаев. Для сетей SS7 этот показатель составлял 33%. Успешными были и подавляющее большинство попыток раскрыть детали профиля абонента.

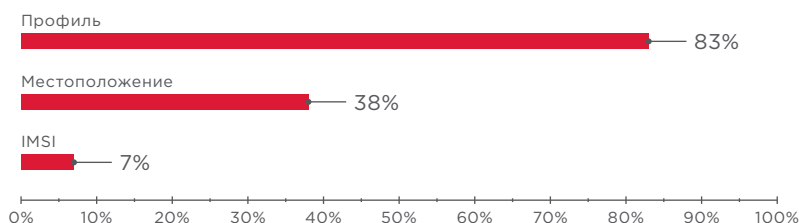


Рисунок 5. Раскрытая информация об абоненте (доли успешных атак)



Все сети 4G позволяют отследить местоположение абонентов

В то же время узнать IMSI абонента удавалось намного реже — всего в 7% случаев, и это связано с более безопасной конфигурацией исследуемых сетей: неиспользуемые в роуминге интерфейсы не были доступны из внешней IPX-сети. Этот показатель крайне важен с точки зрения безопасности; IMSI требуется для проведения других видов атак, поэтому снижение вероятности раскрытия идентификаторов оказывает влияние и на возможность реализации иных угроз. Тем не менее стоит учитывать, что получить IMSI абонента возможно и другими способами, например путем эксплуатации уязвимостей сети SS7, с помощью поддельных базовых станций и даже используя специальные сервисы в интернете.

Во всех случаях раскрыть IMSI получалось при помощи сообщения Sh UDR (User-Data-Request), которое используется сервером приложений для запроса различных данных об абоненте из HSS. Другой потенциальный метод атаки — при помощи сообщения S6c SRR (Send-Routing-Info-for-SM-Request), предназначенного для получения информации, необходимой для маршрутизации входящих сообщений, — не был успешен ни в одной исследованной сети.

Некорректная настройка сетевого оборудования и, в редких случаях, недостаточно эффективная фильтрация сигнальных сообщений позволяли отследить местоположение пользователей с помощью методов Sh UDR и S6a IDR (Insert-Subscriber-Data-Request). Сообщение S6a IDR предназначено для получения HSS текущей информации о местоположении абонента из MME. Злоумышленник может сфабриковать поддельные сообщения, выдав себя за легитимное оборудование роуминг-партнера.

Сообщение SLg PLR (Provide-Location-Request), которое используется GMLC для запроса информации о местоположении абонента из MME, было заблокировано сетью оператора в каждом случае и не позволило получить нужные данные.

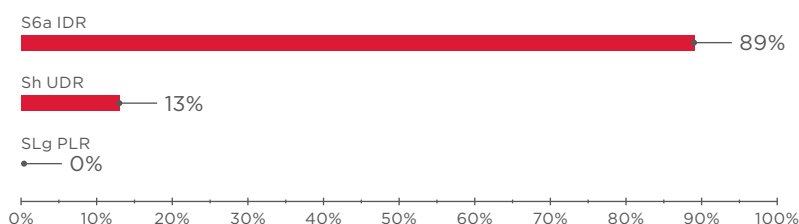


Рисунок 6. Методы раскрытия информации о местоположении абонента (доли успешных атак)

Узнать детали профиля абонента можно тремя способами — с использованием уже знакомого нам метода Sh UDR, а также методов S6a ULR и S6a AIR. Сообщение S6a ULR (Update-Location-Request) содержит запрос на регистрацию абонента в новой сети, однако после обработки этого сообщения источнику запроса возвращается дополнительно информация о профиле абонента, в том числе статус мобильного устройства, телефонный номер, конфигурация APN (точки доступа). Любую полученную информацию злоумышленник может использовать в своих целях. К примеру, телефонный номер — для составления базы абонентов, где сопоставлены IMSI и мобильные номера, а статус мобильного телефона — для выбора подходящего момента, чтобы провести мошенническую операцию в онлайн-банке. Как мы увидим далее, подделка этого сообщения чревата гораздо более опасными последствиями, чем простое раскрытие информации.

S6a AIR (Authentication-Information-Request) — это сообщение, предназначенное для получения ключей аутентификации абонента. Такое сообщение отправляет MME, в зоне действия которого абонент находится в роуминге. Используя данные из векторов аутентификации, злоумышленник может выдать свою поддельную базовую станцию за легитимную и проводить дальнейшие атаки: собирать информацию об абонентах, перехватывать SMS и исходящие голосовые вызовы, вызывать отказ в обслуживании абонентов.



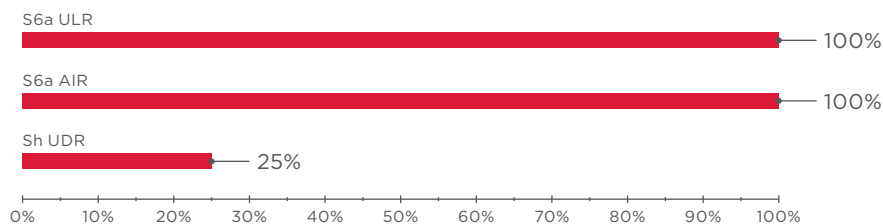


Рисунок 7. Методы раскрытия профиля абонента (доли успешных атак)

### Утечка информации об операторе

Информация о сети оператора — структура сети, адреса и функциональность сетевых устройств — также служит исходными данными для проведения других атак в целях мошенничества, перехвата трафика, отказа в обслуживании абонентов или оборудования.

В связи с тем, что крайне сложно отличить фальшивое сообщение S6a AIR от легитимного, при помощи этого метода необходимую информацию удавалось получить в 88% случаев. Метод SLh RIR (LCS-Routing-Info-Request), напротив, не приводил к нужным результатам: все сообщения были заблокированы благодаря корректно настроенной фильтрации.

Злоумышленник может пользоваться мобильной связью бесплатно и предоставлять услуги по снятию ограничений на связь третьим лицам

### Мошенничество

В сетях Diameter возможно проведение атак, позволяющих бесплатно пользоваться услугами связи. Существуют две разновидности таких атак, каждая из которых основана на изменении профиля абонента. Первый вариант — модификация параметров тарификации, хранящихся в профиле абонента, — достаточно сложно реализуем на практике, поскольку требует от злоумышленника знаний об устройстве сети оператора. Значения этих параметров не стандартизированы и зависят от конкретного оператора, а получить их из профиля абонента не удавалось ни в одной исследуемой сети.

Другой вариант атаки — использование сервисов в обход установленных ограничений, которое наносит оператору прямой финансовый ущерб.

Информация о профиле абонента и ограничениях передается в MME с помощью сообщения S6a IDR. Выдавая себя за HSS, злоумышленник может отправить специально сформированное сообщение, которое позволит снять установленные запреты на оказание услуг. В результате злоумышленник получит возможность неограниченно пользоваться услугами, не предусмотренными его тарифным планом, и не останется без связи даже в том случае, если у него закончились деньги на счету и оператор отключил его от сети. Такие атаки были успешны в 20% случаев. Злоумышленник может не только самостоятельно пользоваться такой возможностью, но и продавать подобные услуги третьим лицам.

### Отказ в обслуживании абонентов

Отказ в обслуживании абонентов возможен в 100% сетей 4G и является критически опасным для интернета вещей

Злоумышленник может лишить абонентов всех преимуществ технологии 4G — высокой скорости передачи данных и качества связи, которые предлагают телекоммуникационные компании. Рядовому пользователю замедление скорости доступа в интернет или недоступность сети могут причинить неудобство, однако вряд ли приведут к серьезным последствиям. Совершенно иная ситуация складывается в отношении интернета вещей. Если абонент — это система умного города, самоуправляемый автомобиль, промышленное оборудование и т. п., отсутствие связи даже в течение нескольких минут может привести к транспортному коллапсу, остановке промышленных процессов, авариям и даже человеческим жертвам.

Отказ в обслуживании абонентов возможен вызвать путем отправки шести типов сообщений: S6a IDR, S6a DSR, S6a ULR, S6a CLR, S6a PUR, S6a NOR.

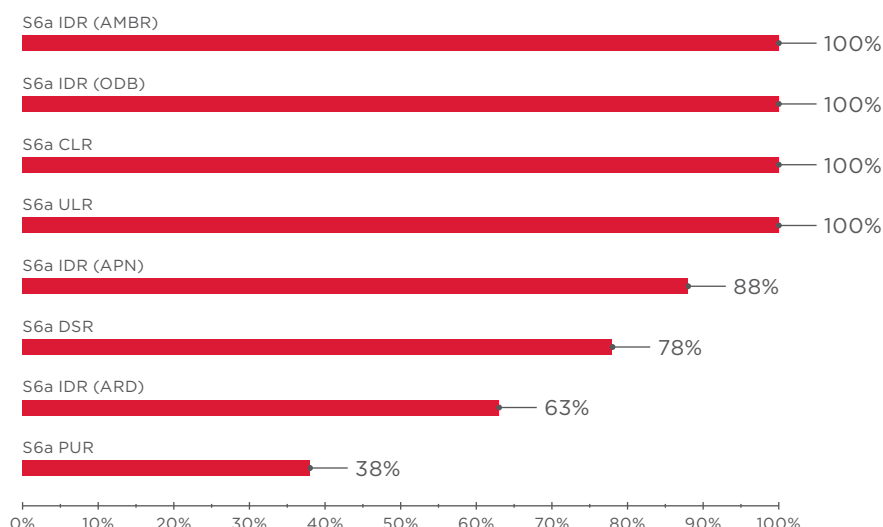


Рисунок 8. Доли успешных атак, направленных на отказ в обслуживании абонентов

Сообщение S6a IDR может быть сформировано разными способами, что позволяет манипулировать несколькими параметрами, хранящимися в профиле абонента:

- + Operator-Determined-Barring (ODB) — ограничения на предоставление услуг связи;
- + Access-Restriction-Data (ARD) — ограничения доступа к сетям связи;
- + Max-Requested-Bandwidth-UL и Max-Requested-Bandwidth-DL (AMBR) — максимальной пропускной способностью;
- + Access Point Name (APN) — точкой доступа, определяющей, через какую сеть (Packet Data Network, PDN) пользователь будет передавать данные.

Изменение значений этих параметров приводит тому, что абонент не может пользоваться интернетом, так как соединение недоступно или скорость передачи данных слишком мала, и сервисами 4G — устройство переключается в режим 3G. Дополнительная опасность заключается в том, что при переключении устройства абонента в режим 3G злоумышленнику становится доступен широкий спектр атак на менее защищенную сигнальную систему SS7.

Злоумышленник может зарегистрировать абонента в несуществующей сети путем отправки сообщения S6a ULR, тем самым отключив его от настоящего обслуживающего MME, и полностью оставить его без связи. К отключению абонента от обслуживающего MME приведет и отправка сообщения S6a CLR (Cancel-Location-Request), которое используется HSS для информирования MME о необходимости завершить работу с абонентом.

Сообщение S6a DSR (Delete-Subscriber-Data-Request) предназначено для удаления данных из профиля абонента, сохраненного на MME. Отправка сообщения с определенным набором флагов может привести к полному удалению профиля абонента и в итоге к отсоединению абонента от сети.

С помощью сообщения S6a PUR (Purge-UE-Request) MME уведомляет HSS о том, что устройство абонента больше не обслуживается данным MME. В результате HSS удаляет информацию об этом MME. Если отправить S6a PUR от имени MME, обслуживающего абонента в данный момент, в HSS не будет информации об MME, и абонент не будет доступен для входящих звонков и SMS.

Метод S6a NOR позволяет провести атаку, направленную на недоступность сервиса отправки и получения SMS, если передача SMS в сети осуществляется по интерфейсам SGd/GGd. Однако в тестируемых сетях данные технологии не использовались, поэтому эффективность метода атаки на практике не была установлена.

Злоумышленник может перевести устройство абонента в небезопасный режим 3G

## ПРИЧИНЫ ВОЗНИКНОВЕНИЯ УЯЗВИМОСТЕЙ

Рассмотрим основные различия между SS7 и Diameter и разберем, почему в сетях, использующих Diameter, могут быть возможны те же атаки, что и в сетях SS7.

Одним из недостатков SS7 является полное отсутствие шифрования. В Diameter же использование шифрования формально является обязательным, необходимо использовать TLS/DTLS (для TCP или SCTP соответственно) либо IPSec. Формально — потому что на практике операторы связи почти никогда не используют шифрование внутри сети и лишь иногда — на ее границах. Кроме того, шифрование осуществляется по принципу peer-to-peer, а не end-to-end. Другими словами, безопасность в сети строится на доверии между операторами и IPX-провайдерами, так как нет возможности отследить, что между двумя узлами шифрование не применялось или даже не происходило перехвата или изменения информации.

Другой недостаток — возможность подмены источника запроса — в Diameter стал еще более опасным в силу специфики маршрутизации ответов. На любой запрос должен быть получен ответ, который всегда идет тем же маршрутом, каким пришел запрос. В результате, несмотря на подмену источника, атакующий всегда получает ответ. Это облегчает сбор информации и позволяет проводить атаки более незаметно.

Заметим также, что, хотя большое количество процедур SS7 в сетях 4G выполняются с помощью Diameter, оставшаяся часть выполняется через другие протоколы. Так, например, непосредственное установление вызовов в VoLTE реализуется через SIP.

В основном сеть 4G сейчас используется только для предоставления доступа к интернету, в то время как голосовые вызовы и передача SMS осуществляются через сети предыдущих поколений. В результате многие действия, возможные в сети Diameter теоретически, оказываются невозможными на практике, а интерфейсы, соответствующие им, фильтруются просто в силу малой распространенности 4G-роуминга для этих сервисов.

Самым интересным примером являются, пожалуй, механизмы передачи SMS. В сетях 2G и 3G они содержат множество уязвимостей, в то время как в 4G сейчас широко не используются. Более того, в сетях 4G существуют три разные техники передачи SMS, и только одна из них задействует Diameter непосредственно для доставки сообщения.

На транспортном уровне разница состоит и в обязательном использовании IP в сетях Diameter, что может сделать атаки более доступными для злоумышленников благодаря большому количеству инструментов для проведения атак на IP.

Несмотря на перечисленные различия, выявленные в тестируемых сетях недостатки защиты во многом схожи с теми проблемами, которые мы отмечали в сетях SS7. В первую очередь это касается вопросов фильтрации отдельных сообщений. Категории фильтрации сигнальных сообщений определены в документе GSMA FS.19 Diameter Interconnect Security. Категории различаются в зависимости от требований, предъявляемых к перечню проверок. Категория 1 включает в себя настройку разрешенных интерфейсов и сообщений на DEA/DRA. В категории 2 определены требования к настройке на DEA или в системе фильтрации и блокировки сигнального трафика с целью определения легитимности сообщения для данного IMSI из соответствующего источника.

Поскольку обеспечить корректные проверки для этих категорий сообщений достаточно просто, были успешны лишь 9% атак, непосредственно связанных с недостаточной фильтрацией сигнального трафика.

Недостаток архитектуры Diameter, который также существовал и в SS7, — это принципиальная невозможность отличить поддельное сообщение от легитимного, так как процедура обмена некоторыми сигнальными сообщениями подразумевает, что сообщение может поступить от любого внешнего узла, если абонент находится в роуминге. К такого рода сообщениям должна применяться 3-я категория фильтрации. Она представляет собой более сложную

Протокол Diameter имеет архитектурные недостатки, которые нельзя компенсировать средствами фильтрации и блокировки трафика

техническую задачу, для решения которой необходимо использовать дополнительные средства защиты, такие как системы фильтрации и блокировки сигнального трафика или системы обнаружения атак. Оператор должен проверять, соответствуют ли поступающие сообщения матрице перемещений абонента (его последнему зафиксированному местоположению и времени, прошедшему с момента последнего обновления местоположения).

Предсказуемо, что практически все атаки, использующие сообщения, к которым должна применяться 3-я категория фильтрации (S6a ULR и S6a AIR), завершаются успешно. Отсутствие фильтрации объясняется тем, что блокировка легитимных сообщений приведет к нарушению связи для абонентов, которые действительно находятся в роуминге, а мобильный оператор потеряет потенциальную прибыль. Причем финансовый ущерб может оказаться весьма значительным: регулярные перебои со связью в роуминге могут вынудить абонентов сменить оператора.

Специализированные системы фильтрации и блокировки сигнального трафика были установлены в каждой третьей исследованной сети, однако их эффективность была крайне низкой, и проводить атаки удавалось даже с использованием сообщений, относящихся к 1-й категории.

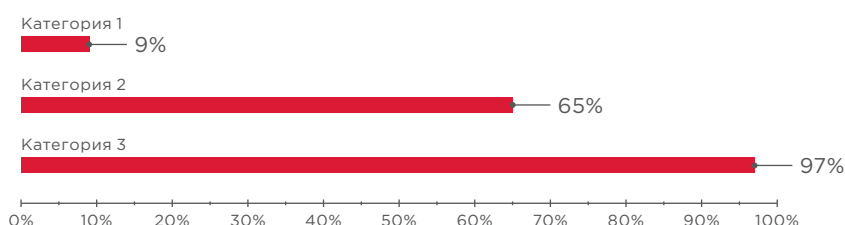


Рисунок 9. Доли успешных атак по категориям фильтрации

В документе GSMA FS.19 описана также нулевая категория, которая определяет базовые параметры фильтрации трафика на сетевом уровне (проверка адресов, формата сообщения), однако мы не будем ее рассматривать, поскольку соответствующие тесты (возможность отказа в обслуживании оборудования и проверка корректности фильтрации в частных случаях) редко используются при анализе защищенности сети.

Сетевое оборудование может содержать множество уязвимостей, которые приводят к некорректной фильтрации сигнального трафика (и потенциально к дальнейшим атакам), а также позволяют проводить атаки на отказ в обслуживании оборудования оператора. Распространены и недостатки защиты, связанные с некорректной настройкой сетевого оборудования оператором. Высокий процент успешных атак, для противодействия которым предусмотрена 2-я категория фильтрации, связан именно с некорректными параметрами оборудования.

Как мы видим, проблемы, характерные для сетей на базе сигнальной системы SS7, оказываются актуальны и для нового поколения сетей на основе Diameter. На следующей диаграмме представлены обнаруженные недостатки защиты и доли атак, которые были успешно проведены в результате их эксплуатации.

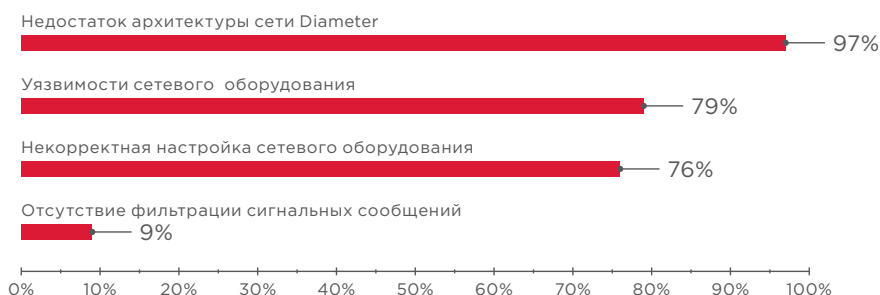


Рисунок 10. Уязвимости сетей (доли успешных атак)

## РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ

На данный момент операторы связи принимают лишь минимальные меры защиты в отношении сигнальных сетей Diameter. Возможно это происходит из-за того, что операторы не в полной мере осознают существующие проблемы безопасности и связанные с ними риски в сетях нового поколения, они уверены в том, что протокол Diameter достаточно защищен от атак в отличие от устаревшей системы SS7. Специальное оборудование, предназначенное для мониторинга сигнального трафика, которое позволило бы заметить атаки, попросту отсутствует в исследуемых сетях. Предпринимая только отдельные шаги по защите, операторы не имеют полного представления о ситуации и считают, что их сеть представляет собой безопасную среду, полагая установку дорогостоящего дополнительного оборудования излишней.

Для обеспечения защиты от рассмотренных в данном отчете атак необходим комплексный подход к безопасности, что также отражено в рекомендациях GSMA в документе FS.19 Diameter Interconnect Security. В первую очередь, следует регулярно проводить анализ защищенности мобильной сети для выявления уязвимостей, оценки текущего уровня защищенности и потенциальных рисков, выработки защитных мер и проверки их эффективности. Важно поддерживать параметры безопасности в актуальном состоянии и проводить анализ защищенности при любых изменениях в сети, например при изменении конфигурации или внедрении нового оборудования.

Кроме того, необходим постоянный мониторинг и анализ сигнальных сообщений, пересекающих границы сети, для своевременного выявления нелегитимной активности и реагирования на возникающие угрозы безопасности на самой ранней стадии. Специальные системы обнаружения атак позволяют выполнять анализ сигнального трафика в режиме реального времени и проводить блокировку нежелательных сообщений без риска нарушения доступности абонентов — либо передавать информацию об инцидентах безопасности дополнительным системам защиты.

Обеспечение безопасности не ограничивается единичными мерами, а представляет собой непрерывный процесс. Специалисты Positive Technologies применяют комплексный подход для защиты сигнальных сетей своих клиентов. Подробнее узнать об этом вы можете, задав вопрос через форму обратной связи на сайте [ptsecurity.com](http://ptsecurity.com) или написав нам по адресу [info@ptsecurity.com](mailto:info@ptsecurity.com).

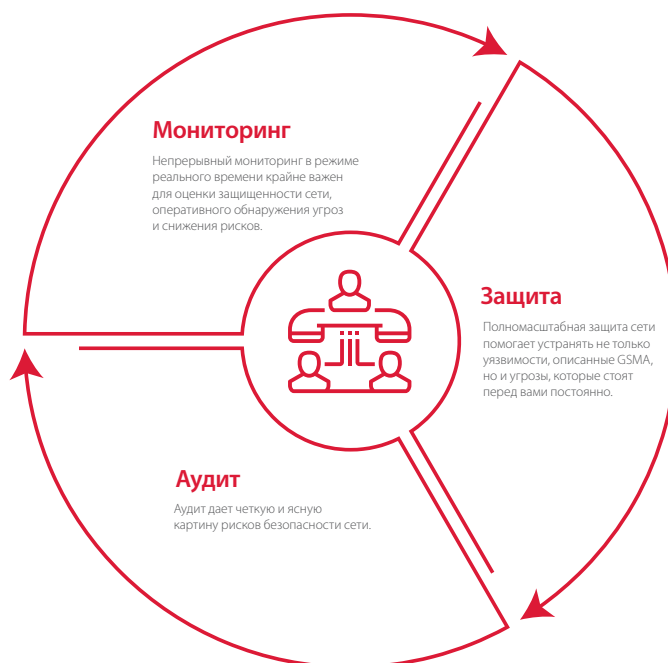


Рисунок 11. Рекомендуемый подход к обеспечению безопасности сигнальной сети

## ЗАКЛЮЧЕНИЕ

Несмотря на все механизмы защиты, заложенные в протокол Diameter, в исследованных сетях оказались возможными атаки в отношении абонентов и самого оператора. Злоумышленник может проследить местоположение абонента, вызвать отказ в обслуживании, оставив тысячи пользователей без связи, или перевести устройство абонента в режим работы 3G, чтобы воспользоваться многочисленными уязвимостями SS7.

Таким образом, абоненты сетей 4G подвержены тем же уязвимостям, что и абоненты сетей предыдущих поколений. Не защищены и операторы: злоумышленники могут получать бесплатный доступ к услугам связи, что ведет к серьезным финансовым потерям.

Выявленные уязвимости связаны как с недостатками настройки сетевого оборудования и механизмов фильтрации, которые устраняются относительно легко, так и с фундаментальными проблемами протокола Diameter, для решения которых необходимо специальное дополнительное оборудование. При этом осведомленность операторов о существующих угрозах пока невысока, а значит, принимаются лишь минимальные меры защиты, которые недостаточны для обеспечения безопасной и бесперебойной работы мобильной сети.

Эксперты Positive Technologies ежегодно проводят исследования актуальных угроз современных сетей мобильной связи с целью обратить внимание операторов на существующие недостатки защиты. Следуя приведенным выше рекомендациям, операторы могут значительно повысить безопасность связи для абонентов и минимизировать риски мошенничества и отказа в обслуживании в отношении своих ресурсов.

---

### О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. 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.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.