ОСОБЕННОСТИ СЕТЕЙ МОБИЛЬНОЙ СВЯЗИ СТАНДАРТА LTE КАК ОБЪЕКТА ЗАЩИТЫ ИНФОРМАЦИИ

Рахимова Севара Санатжон kizi

аспирантка 2 ступени Ташкентского университета

информационных технологий имени Мухаммада Аль-Хоразми

АННОТАЦИЯ. Инфраструктура сетей четвертого поколения с LTE с точки зрения безопасности представляет собой совокупность нескольких защищенных компонентов и взаимосвязей между ними Защищенное пользовательское оборудование (UE) предоставляет пользователю доверенные приложения и услуги и отвечает за передачу данных в сеть и из сети. UE включает в себя универсальный модуль идентификации абонента (USIM) с аппаратной и программной защитой, в котором хранится международный идентификатор мобильного абонента (IMSI), который однозначно идентифицирует каждого пользователя. Кроме того, в USIM хранится секретный ключ K для получения дополнительных ключей, используемых во время процедуры аутентификации в сети LTE.

Ключевые слова: мобильные сети четвертого поколения, требования безопасности, информационная безопасность, LTE, технологические решения.

В настоящее время имеется широкий спектр публикаций по проблемам обеспечения безопасности беспроводных технологий, в том числе и сетей стан-дарта LTE которые необходимо проанализировать с целью определения ключевых осо-бенностей, учет, которых необходим в процессе проектирования архитектуры се-ти и выбора системы средств защиты от возможных угроз безопасности информа-ции.

Характерной особенностью проблемы защиты информации является

необ-ходимость полного описания множества угроз информационной безопасности. Каждый неучтенный дестабилизирующий фактор может существенно сни-зить эффективность защиты. Тем не менее, проблема описания полного множест-ва угроз в настоящее время в требуемой степени не формализована. Обусловлено это тем, что циркулирующая информация подвергается воздействию обширного ряда факторов, многие из которых идентифицируются как дестабилизирующие.

По причине отсутствия в имеющихся публикациях по проблемам защиты информации формализованного решения задачи формирования полного множест-ва угроз предлагается определить не полный перечень угроз, а пере-чень классов угроз. Отсюда первым этапом в оценке эффективности системы защиты является выявление и описание существующих угроз безопасности ССМС стандарта LTE с ИФ и их классификация.

В общем случае модель угрозы представляет собой набор характеристик:

$$My=(Ny,Sy,Vy,Ay,Dy,Tcy,Tpy),$$

где N - наименование угрозы; Sy - описание источника угрозы; Vy — опи-сание уязвимости объекта, которая используется для реализации угрозы; Ay описание атаки как способа реализации угрозы; Dy - описание деструктивных функций, выполняемых при реализации угрозы; 7^ - время существования угро-зы; Tpy - время реализации угрозы.

На рис. 1.1 приведена обобщенная классификация угроз безопасности ин-формации циркулирующей в ССМС стандарта LTE с ИФ.

Не все рассмотренные характеристики являются строго необходимыми при формальном описании угроз безопасности, поэтому выделяются только три из них: объект, источник и реализация, где объектом угроз являются фемтосоты ССМС стандарта LTE, в качестве источника угроз, например, антропогенный вид, а реализация угрозы - вид негативного воздействия (атаки), оказываемого на объ-ект угрозы посредством уязвимостеи, приводящих к негативному влиянию на свойства безопасности информации на объекте исследования.

Чтобы облегчить решение задачи классификации, целесообразно согласно документам международных организаций по стандартизации сгруппировать угро-зы безопасности по категориям.

В соответствии с данными рекомендациями и обобщенной классификацией угроз безопасности представляется целесообразным рассмотреть угрозы наиболее характерные для ССМС стандарта LTE с ИФ, разбив их на пять классов рис. 1.1.

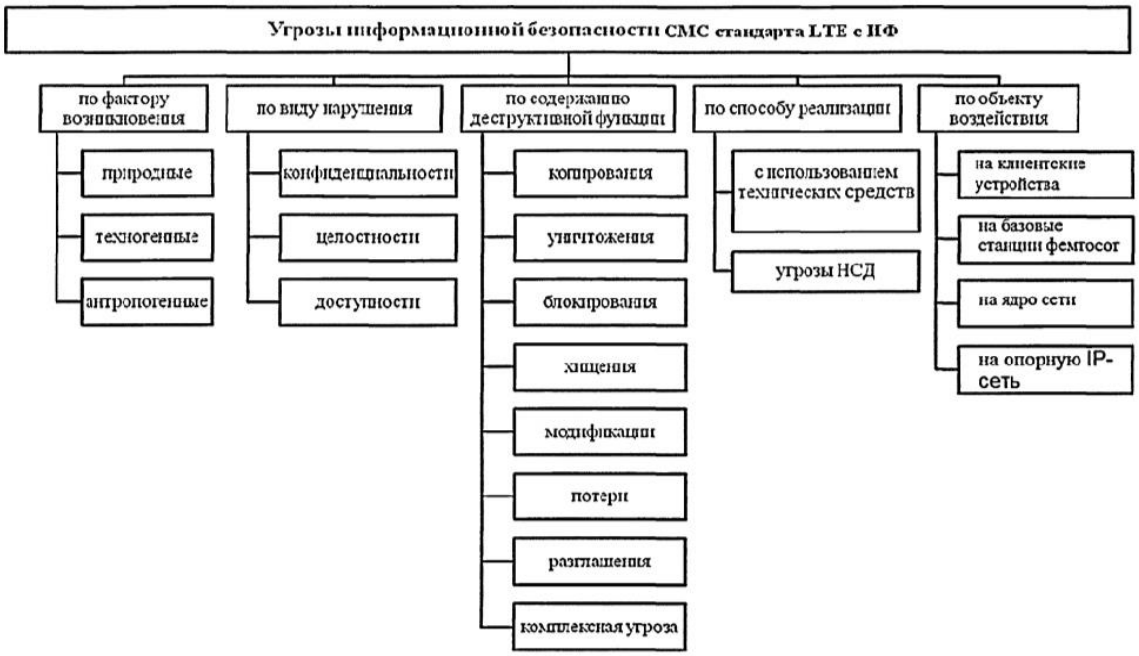

Рис.1.1 - Схема общей классификации угроз

Вопросы обеспечения безопасности в сетях четвертого поколения решаются на нескольких структурных уровнях: на физическом, так называемом воздушном интерфейсе, на уровне внутренней сети оператора, а также на уровне взаимодей-ствия различных операторов.

Рассмотрим основные разновидности атак как источники угрозы безопасно-сти ССМС стандарта LTE с ИФ. На рис. 1.2 представлены цели атак на ССМС с ИФ. На схеме стрелками обозначены три уязвимых элемента: (а) воздушный ин-терфейс между мобильным устройством (UE) и фемтосотовой БС; (б) непосредст-венно фемтосотовая базовая станция (H(e)NB); (в) широкополосное соединение между фемтосотой и шлюзом безопасности (SecGW).

Проанализируем ключевые виды атак на элементы ССМС стандарта LTE с ИФ, которые реализуются без взлома криптосистем или протоколов безопасности.

Атаки на воздушный интерфейс. В пассивном варианте злоумышленник прослушивает канал связи между мобильным устройством и базовой станцией; или активными - в дополнение к прослушиванию, злоумышленник вносит или оказывает воздействие на уже циркулирующий трафик. Хотя возможности актив-ных атак существенно снижены за счет применения криптографической защиты пере-даваемой информации, пассивные атаки, такие как анализ трафика и отслеживание местоположения пользователей, все еще возможны.

Проблема защиты идентификаторов пользователей поднималась еще в ран-них сетях GSM, и решение, которое было принято с тех пор, существенно не пе-ресматривалось. Учитывая тенденцию эволюции к плоским полностью IP-ориентированным ССМС с фемтосотами продолжение применения унаследован-ных решений становится не целесообразным.

Фактически стандарты GSM, UMTS и LTE для защиты идентификаторов мобильных устройств в воздушном интерфейсе предлагают исполь-зовать непригодные для редактирования временные идентификаторы (TMSI и GUTI), но капиллярное развертывание фемтосот делает эти меры недостаточными для обеспечения гарантированного уровня защиты для пользователей. TMSI (или GUTI) обычно постоянны для данного местоположения или контролируемой области, которая состоит из сотни смежных ячеек, и фемтосоты могут позволить злоумышленникам отслеживать передвижения абонентов с беспрецедентной точ-ностью в виду особенностей используемого диапазона частот.

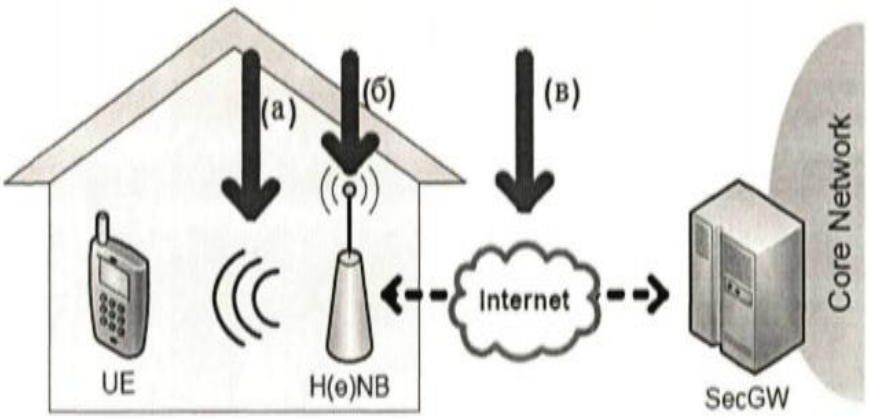

Рис.1.2 - Цели атак злоумышленников на сотовые сети с интегрированными фемтосотами

Идентификация абонента и прослеживание его маршрута передвижения яв-ляются новым классом угроз специфичным для ССМС с фемтосотами и обуслов-лено это уязвимостями, связанными с особенностями применяемого воздушного интерфейса.

Атаки на фемтосотовые базовые станции. Мобильное устройство под-ключено к обычной базовой станции (БС), поскольку применяются идентичные протоколы и стандарты безопасности [102]. Однако с точки зрения злоумышлен-ника фемтосота открывает новые возможности для реализации деструктивных воздействий. Например, злоумышленнику намного легче получить доступ к фемтосоте расположенной в помещении, чем к БС расположенной на крыше.

Физический размер, качество материалов, более дешевые компоненты и IP ин-терфейс фемтосоты делают ее более уязвимой для атак обратного проектирования и несанкционированного доступа, по сравнению с традиционными, более дороги-ми и высококлассными БС. Поскольку шифрование пользовательских данных транслируемых через эфир прекращается на уровне фемтосоты, аппаратное вме-шательство в устройство позволяет раскрыть конфиденциальную информацию ничего не подозревающего пользователя. Например, если злоумышленник деактивирует систему Closed Subscriber Group (CSG) и тем самым заставит фемтосоту принимать всех внешних пользователей без необходимости предварительной ре-гистрации, то он получит возможность несанкционированно анализировать их трафик. Кроме того, атаки типа подмена доверенного объекта, атаки на сетевые

службы с использованием протоколов Интернет, атаки-сообщения ложного ме-стоположения или атаки несанкционированной переконфигурация радиоаппара-туры усложняют оператору сети процесс управления интерференцией и средства-ми контроля питания, что неблагоприятно сказывается на качестве обслуживания.

Таким образом, для того, чтобы снизить вероятность реализации вредонос-ных манипуляций с программным обеспечением аппаратуры и перехват инфор-мации по техническим каналам, фемтосоты должны быть обеспечены доверенной контролируемой средой функционирования. Однако если будут применяться методы геолокализации только по IP-адресу, а фемтосоты санкционированы на работу только в определенных географических рамках, то атаки с ложными отче-тами о местоположении все еще могут быть реализованы, поскольку для манипу-ляции IP-адресом фемтосоты не требуется физического вмешательства в оборудо-вание.

Атаки на опорную широкополосную сеть. Крупномасштабное разверты-вание сравнительно недорогих фемтосот более выгодно для операторов мобиль-ной связи по сравнению с дорогостоящей глубокой модернизацией всей системы связи. Однако утечка информации о точке доступа ядра сети в сеть Интернет име-ет серьезные последствия: это провоцирует большое количество сетевых атак на операторов сотовой сети мобильной связи, таких как отказ в обслуживании (DoS) или подмена доверенного объекта. Рассмотрим последствия раскрытия IP-адресов шлюзов безопасности в Ин-тернет, которые необходимы большому количеству фемтосот для корректного функционирования всей системы. DoS и распределенные DoS (DDoS) атаки яв-ляются частым и хорошо известным явлением для крупных компаний предостав-ляющих большое количество сетевых сервисов.

Для того, чтобы разработчики систем и исследователи могли точнее выявлять и реагировать на различные по существу атаки одного вида, была пред-ложена общая классификация атак типа отказ в обслуживании и соответствующих средств защиты по их отличительным чертам. Если обнаружение факта реализа-ции в настоящее время крупномасштабной DDoS атаки лучше всего выполнять на стороне жертвы, то

процесс противодействия этой угрозе, эффектив-нее всего осуществлять распределенными мерами, не ограничиваясь только за-ключительной линией связи со злоумышленником. Причиной этому является тот факт, что механизмы противодействия являются наиболее эффективными, если они применяются на уровне непосредственных источников атаки, поскольку при фильтрации злонамеренного трафика от реальных подключений становится воз-можным избежать его прохождения до заключительной линии связи с целью ата-ки и предотвратить переполнение.

Для успешного функционирования описанных меры и решений по противо-действию DoS атакам необходимо, чтобы различные провайдеры интернет-услуг имели возможность и желание сотрудничать, причем отказ в достижении согла-шения может подвергнуть компроментации эффективность всей системы защиты.

Для оператора ССМС это означает, что эффективная система защиты от атак типа отказ в обслуживании должна охватывать не только провайдера, кото-рый обеспечивает доступ в Интернет, но также и ближайших провайдеров-конкурентов. Совместно они могли бы ограничить отказы в обслужива-нии в фемтосотах и шлюзах безопасности и гарантировать предоставление услуг абонентам фемтосот. Однако для достижения сотрудничества среди провайдеров необходимо создать условия, в которых все заинтересованные стороны будут иметь стимулы в совместной защите шлюзов операторов мобильной связи и оцен-ке эффективности этой защиты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Академик. Словари и энциклопедии [Электронный ресурс]. - URL: http://dic.academic.rU/dic.nsf/ruwiki/317301.

2. Архитектура системы безопасности в сетях LTE [Электронный ресурс] / Википедия. [2013 - 2013]. Дата обновления: 04.01.2013. URL:

http://ru.wikipedia.org/?oldid=51280381 (дата обращения: 04.01.2013).

3. Аналитический обзор защиты данных в сетях LTE по материалам NTT DOCOMO [Электронный ресурс] / Technical Journal Vol. 11 No. 3. - http://advancedmonitoring.ru/article/detail.php?ELEMENT_ID=56.

4. Анализ угроз информационной безопасности. Основные понятия и ана-лиз угроз информационной безопасности [Электронный ресурс] / Лаборатория Сетевой Безопасности. - URL: http://ypn.ru/106/analysis-of-threats-to-informationsecurity.

5. Батищев, Р.В. / Диссертация на соискание ученой степени кандидата технических наук. - Воронежский государственный технический университет. -Воронеж, 2002. - 198с.

6. Белов, Е.Б. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов - М.: Горячая линия - Телеком, 2006. — 544с.

7. Борисов, В.И. Помехозащищенность систем радиосвязи. Вероятностновременной подход / В.И. Борисов, В.М. Зинчук. - М.: РадиоСофт, 2008. - 260с.

8. Василик, О. Персональные базовые станции // Сети и телекоммуникации №7-8, 2008. -С.356-360