АНАЛИЗ СПОСОБОВ МОШЕННИЧЕСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВИРТУАЛЬНЫХ СЕТЕЙ ОПЕРАТОРОВ СОТОВОЙ СВЯЗИ

УДК 621.391

В.Н. Максименко, *доцент кафедры «Информационная Безопасность» МТУСИ, к.т.н. vladmaks @yandex.ru;*
А.С. Беседина, *магистрант МТУСИ;*
К.М. Панской, *магистрант МТУСИ.*

Аннотация. Одним из возможных вариантов концепции сетей следующего поколения (*NGN*) предполагается бизнес-модель, которая предусматривает переход от вертикальной модели оказания услуг к горизонтальной, когда имеется множество сетей доступа, множество транспортных сетей и сетей услуг, и оказание услуги оказывается не одним, а, как минимум, тремя операторами сети. Среди несомненных достоинств такой бизнес-модели – возможность использования современных инженерных методов проектирования новых гео- инфо-телекоммуникационных услуг большим числом независимых групп разработчиков. Недостатком декомпозиции единой системы на независимые функциональные подсистемы является увеличение числа угроз, ухудшающих показатели качества и информационной безопасности. В данной статье рассмотрены способы мошенничества и их влияние на информационную безопасность в модели сетям *MVNO*, эволюция которых наиболее близка концепции *NGN*.

Ключевые слова: контакт-центр; фрод; мошенничество; информационная безопасность; доступность; целостность; конфиденциальность; сеть виртуального оператора сотовой связи.

ANALYSIS OF FRAUDULENCE METHODS IN THE FIELD OF INFORMATION SECURITY OF VIRTUAL NETWORKS OF CELLULAR COMMUNICATIONS OPERATORS

Vladimir Maksimenko, *associate professor of the «Information security» MTUCI, candidate of technical sciences;*
Alexandra Besedina, *graduate student MTUCI;*
Konstantin Panskoy, *graduate student MTUCI.*

Annotation. One of the possible variants of the concept of next-generation networks (NGN) is assumed to be a business model that provides for the transition from a vertical model of service delivery to a horizontal one, when there are many access networks, a lot of transport networks and service networks, and the service is provided not by one but at least by three network operators. Among the undoubted advantages of such a business model is the possibility of using modern engineering methods for designing new geo-information and telecommunication services by a large number of independent groups of developers. The disadvantage of decomposing a single system into independent functional subsystems is an increase in the number of threats that degrade the quality and information security indicators. This article discusses the methods of fraud and their impact on information security in the model of MVNO networks, the evolution of which is closest to the concept of NGN.

Keywords: contact center; fraud; fraud; information security; availability; integrity; confidentiality; network of virtual mobile operator.

Эволюция сетей виртуальных операторов сотовой связи

Фрод (с англ. *fraud*, обман, мошенничество) в системах сотовой связи – деятельность, направленная на использование услуг без надлежащей оплаты и обогащения с помощью незаконной деятельности.

Первый зафиксированный случай фрода в сетях связи в России произошел в 1993 г. С тех пор многое поменялось, изменились методики выявления, но и образовались новые типы мошенничества в сетях сотовой связи. В свою очередь развитие сотовых операторов не остановилось.

Еще в 1999 г. британский регулятор *OFTEL* предложил использовать термин *MVNO*. Под данным термином понималась компания, которая не обладает радиочастотами, но предоставляет услуги радиосвязи. После внесения данных изменений у любой компании появилась возможность создавать виртуальных операторов.

По данным от *GSMA Intelligence* от 2015 г. максимально развитие *MVNO*-операторы получили в Европе, Азии и Сев. Америке. *Transparency Market Research* прогнозирует что к 2023 г. весь рынок *MVNO* достигнет оборотов в 75$ млрд.

Для открытия виртуального оператора не потребуется покупка радиочастот и строительство собственной инфраструктуры. Все необходимое можно арендовать у опорного оператора *MNO*.

MVNO и *MNO* существуют рука об руку, один предоставляет свои услуги под собственным брендом, другие расширяют свою клиентскую базу, извлекают дополнительный доход из аренды инфраструктуры и занимают не освоенные ранее ниши.

MVNO подразделяются на несколько типов в зависимости от количества заимствований инфраструктуры у основного оператора. Чем меньше заимствований у виртуального оператора, тем более гибкую маркетинговую политику может проводить виртуальный оператор.

Бизнес модели *MVNO* подразделяются на [1, 2]:

- *Reseller MVNO* (Реселлер).
- *Service Provider MVNO* (Сервис провайдер).
- *Enhanced Service Provider MVNO.*
- *Full MVNO* (Полный *MVNO*).

Full MVNO отвечает за всю инфраструктуру, операции, клиентов и данные, обладая полный контроль над всеми услугами и продуктами, предлагаемыми на рынке, а также гибкостью при проектировании и развертывании новых услуг. В свою очередь оператор мобильной сети (*MNO*) обеспечивает доступ к сети.

Стандарты и спецификации в области информационной безопасности всегда следуют за изменениями в области информационных систем [2-5]. Критерии оценки доверенных информационных систем (оранжевая книга) предопределили «классы безопасности» компьютерных систем. В рекомендации *X.800* международного союза электросвязи отражены аспекты информационной безопасности распределенных систем. В стандарте *ISO/IEC-15408* (общие критерии) приведены критерии оценки безопасности информационных технологий. В отличие от оранжевой книги, в общих критериях не содержится предопределенных «классов безопасности», такие классы можно строить, исходя из требований безопасности существенных для конкретной организации или информационной системы. При этом, обмен информацией между программными модулями систем, построенных на основе одиночно вычислителя, осуществляется в виде блоков данных, а в распределенных системах обмен осуществляется в виде сообщений: блоков, данных снабженных информацией об адресе модуля-получателя и модуля отправителя. Обмен данными в сосредоточенной и распределенной системах существенно отличаются и зависят от архитектуры и характеристик каналов связи, соединяющих объекты информационной системы.

В зависимости от бизнес-модели выбирается архитектура распределенной информационной системы организации. В области телекоммуникаций бизнес-модель строится

на основе вертикальной модели информационно-телекоммуникационной системы, когда оператор СПС заключает договор с абонентом на предоставление услуг подключения к сети и оказывает инфокоммуникационные услуги только «своим» абонентам. При этом оператор сети (владелец информационной системы) владеет средствами доступа к сети, средствами услуг и средствами транспортной сети и система безопасности строится для одной распределенной информационной системы. Такая бизнес-модель имеет ряд недостатков, которые тормозят развитие информационных систем, ограничивая число разработчиков новых информационных услуг.

Концепция сетей следующего поколения (*NGN*) предполагает использование бизнес-модели, предусматривающей переход от вертикальной модели оказания услуг к горизонтальной, когда имеется множество сетей доступа, множество транспортных сетей и множестве сетей услуг. Каждая из сетей является независимой и их взаимодействие осуществляется только на основании договорных соглашений, включающих кроме финансовых, положения о качестве обслуживания и информационной безопасности. При заключении соглашение о совместной работе по оказанию услуг, оператор СПС должен учитывать риски, которые могут привести к неприемлемому ущербу в зависимости от несоблюдения партнерами условий соглашения. В основе стандарте ГОСТ Р ИСО / МЭК 27001-2006 лежит система управления рисками информационной безопасности, которая позволяет получить ответы на следующие вопросы: на каком направлении информационной безопасности требуется сосредоточить внимание и сколько времени и средств можно потратить на техническое решение для защиты информации [5]. Система управления рисками организации направлена на минимизацию возможного ущерба, связанного с использованием информационной технологии и выполнение основной бизнес-цели организации.

В области сотовой подвижной связи переход от вертикальной модели оказания услуг к горизонтальной модели наглядно проявляется на примере эволюционного развития сетей *MVNO*, от сетей, специализирующихся только на продаже и маркетинге услуг базового оператора под собственным брендом, к сетям *MNO – MVNE – MVNO*. Обязанности между операторами распределяются следующим образом: оператор *MNO* владеет радиочастотами и базовыми станциями и обеспечивает функции сети доступа, оператор *MVNE* владеет транспортной сетью и является посредником между базовыми (*MNO*) и виртуальными (*MVNO*) операторами, обеспечивая транзитные функции, оператор *MVNO* выполняет функции сети услуг.

Бизнес-модель *MVNO* является наиболее перспективной при выводе на рынок новых услуг, использующих информационные и навигационные технологии. Примером использования *MVNO* для оказания услуг экстренного реагирования при аварии автомобильного транспорта является *MVNO* под торговой маркой АО «ГЛОНАСС» [3]. Используя базовые станции федеральных операторов СПС МТС, Билайн и МегаФон при определении автомобильной аварии на дороге абонентский терминал «ЭРА ГЛОНАСС» в автоматическом или автоматизированном режиме передает данные о месте дорожно-транспортного происшествия в контакт-центр службы экстренного реагирования (112), оператор которой организует оказание экстренной помощи силами служб 01, 02, 03.

Разделение большой целостной информационной системы на небольшие независимые, связанные отдельными соглашениями, снижают защищенность как оператора связи, так и абонентов, открывая дополнительные возможности для мошенников.

Анализ угроз в виртуальных сетях операторов сотовой связи

На фоне увеличения количества правонарушений на сетях СПС необходимы опережающие разработки и внедрение процессов управления обеспечением информационной безопасности, отражающих атаки и выявляющих правонарушителей. В этих условиях обеспечение информационной безопасности сетей связи становится триединой задачей, включающей мониторинг функционирования, обнаружение атак и принятие адекватных мер

противодействия [6, 7]. Адекватные меры противодействия могут носить технический характер и предусматривать реконфигурацию информационной сферы сети. Они могут быть также организационными и предусматривать обращение операторов связи к силовым структурам с предоставлением информации для выявления и привлечения к ответственности нарушителей. Адекватность мер безопасности зависит от величины воздействия угрозы.

На основе анализа конкретных фактов мошенничества в сетях сотовой подвижной связи, а также на основе изучения специальной литературы предлагается следующая классификация способов совершения мошенничества в системе сотовой связи [2, 8]:

1. Доступ к системе сотовой связи с помощью использования знаний о процедурах ее функционирования.
2. Доступ к абонентскому терминалу.
3. Мошенничество с использованием заключенного контракта.
4. Мошенничество при использовании льготного тарифа.
5. Доступ к идентификационным данным.
6. Доступ к системе базовых станций.

Способы мошенничества с использованием заключенного контракта весьма многообразны, но все ситуации можно разделить на две категории:

- контракт (договор на оказание услуг связи) заключается без намерения оплачивать услуги;
- абоненты, заключившие контракт, принимают решение не оплачивать услуги в какой-то момент после начала действия контракта.

Мошенничество при использовании льготного тарифа включает два действия абонента-нарушителя: получение права пользования льготным тарифом некоторой службы и приобретение абонентом-нарушителем (или группой таких абонентов) нескольких номеров телефонов для того, чтобы звонить по номеру этой службы.

Доступ к идентификационным данным может осуществляться двумя способами:

- получение идентификационных данных пользователей с помощью сотрудников компаний сотовой связи (*Staff fraud)* для их последующего использования при программировании других телефонов (создания нелегального «двойника»).
- несанкционированное получение идентификационных данных пользователей с помощью технических средств (*Technical fraud*) с целью вмешательства, манипулирования или перепрограммирования идентификационных данных легальных пользователей.

В большинстве случаев преступниками используются различные количественные и качественные комбинации нескольких способов мошенничества. По мере их модификации и постоянного усложнения логических связей появляются новые способы мошенничества, отличающиеся наличием сложных алгоритмов действий преступника, которые все более совершенствуются и модернизируются.

С распространением сетей *MVNO* к уже известным способам совершения мошенничества добавились способы использующие:

- Вредоносное программное обеспечение.
- Уязвимости мобильных операционных сетей.
- Подмену точек доступа локальных сетей.
- Подписки на платный контент.
- Мобильный банкинг.
- *SMS*-шлюзы.

Вредоносное программное обеспечение. Одним из основных способов проведения атак является внедрения в систему *MVNO* вредоносного программного обеспечения. Основные цели вредоносного (вирусы, трояны) программного обеспечения:

- Получение доступа к индивидуальному счету абонента или банковскому счету.
- Использование уязвимостей в мобильных операционных системах.
- Кража персональных данных, контактов, параметры учетных записей – все эти полученные данные отравляются на сервер злоумышленников.
- Использование аппаратных мощностей телефонов для использования в сетях роботов (ботнет). Используется часть процессорной мощности для излечения собственной выгоды. Сюда же можно отнести программы, занимающиеся майнингом крипто валют без ведома пользователя.
- Выведение из строя телефонных аппаратов.

Уязвимость мобильных операционных сетей [9]. В 2015 г. исследователи информационной безопасности обнаружили ряд серьезных уязвимостей в ядре операционной системы *Android* под названием *Stagefright*. Был опубликован эксплойт, с демонстрацией в которой используется *MMS* сообщение. Для того чтобы воспользоваться данной уязвимостью достаточно только знать номер жертвы. После получения вредоносного сообщения код в сообщении исполняется автоматически. Уязвимость на тот момент распространялась на 950 миллионов смартфонов.

В том же году в операционной системе *IOS* была обнаружена уязвимость под названием «Арабская *SMS*», которая приводила к перезагрузке графического интерфейса. Поле перезагрузки при попытке открыть приложение «Сообщения», перезагрузка повторялась, так как операционная система пыталась прочесть приводящее к перезагрузке сообщение. В течении месяца было выпущено обновление от компании *Apple*, устраняющее данную уязвимость. Подвержены данной уязвимости были все смартфоны с *IOS* 8. Теоретически данное сообщение можно использовать для скрытия факта снятия денежных средств со счета, так как от пользователя будут скрыты сообщения о списании средств.

Методы борьбы с данным видом мошенничества [10]:

Со стороны пользователя:

- Осторожность пользователя при пользовании интернетом.
- Использование антивируса.
- Установка обновлений прошивок и патчей безопасности.
- Обращать внимание на технические сообщения от приложений при установке, дабы не предоставлять излишние права для приложения.

Со стороны сотового оператора:

- Заключение соглашений с контент-провайдерами для повышения уровня контроля за приложениями.
- Штрафные санкции по отношению к компаниям, допустившим нарушения интересов абонентов.

Подмена точек доступа локальных сетей. В связи с все большим развитием городской среды повсеместно распространены *Wi-Fi* сети общего доступа. А также множество магазинов и точек общественного питания организуют бесплатный доступ к интернету. Данный вид связи может быть легко использован злоумышленниками для получения паролей, номеров телефонов. Для этого достаточно создать точку доступа с *SSID* повторяющим название

известной сети или может быть очень похож. Большинство современных устройств будет подключаться автоматически к доверенной сети, если уже производилось подключение к сети с аналогичным *SSID*.

Способ защиты со стороны пользователя:

- Использование *VPN*.
- Не вводить пароли на ресурсах.
- По возможности не пользоваться сетями общественного доступа.
- Отключать автоотключение к общественным сетям.

Нежелательные платные подписки [11]. Злоумышленники в данном случае пользуются возможностью быстрого подключения платных услуг. Не добросовестные компании предоставляют различные контент услуги, при этом скрывая сам факт подключения. Обычно под кнопкой подключения мелким\трудно читаемым шрифтом указано, что данным действием вы подключаете платную услугу.

Методы борьбы со стороны пользователя:

- Обращать внимание на мелкий шрифт.
- Запретить подключение платных подписок на номер.

Методы борьбы со стороны оператора:

- Предоставление функции по запрету подключения платных подписок.
- Обеспечить возможность разделения счета на счет балансовый и для онлайн коммерции.
- Штрафы для контент-провайдеров при выявлении нарушений.

Дистанционное банковское обслуживание [12]. Достаточно большое распространение получила схема использования клонированных сим-карт по поддельным документам для получения доступа к счетам абонента, так как многие банки перешли на *SMS*-уведомления. Сотрудники точки продаж не в состоянии и не в их компетенции проверять достоверность предоставленных документов, будь то паспорт или доверенность. Еще один распространенный вид мошенничества – абонент перестает пользоваться сим-картой, на которую настроено смс-оповещение. Через 60 дней номер будет передан на реализацию, тем самым новый абонент получит доступ к уведомлениям от банка.

Методы борьбы со стороны пользователя:

- При прекращении пользовании сим-картой, закрыть договор и снять подписки.
- Своевременная реакции при пропадании связи.

Методы борьбы со стороны оператора и банка:

- Фиксирование смены *IMSI* и остановка проведения операций, требуются соглашения между оператором и банком.
- Обзвон клиентов при выявлении подозрительных операций.
- Смс-уведомления и рассылка на почту из контактных данных при запросе о замене сим-карты.
- Своевременное информирование.

SMS-шлюзы и SIP-Сервисы [13]. Мошенники используют в своих целях *SMS*-шлюзы, через которые можно добавить любой номер отправителя или закрыть номер буквенным

обозначением. Наиболее известные схемы – это сообщение о не корректном внесении средств на счет и просьбой вернуть эти средства и сообщение с блокировкой сим-карты. *SIP*-сервисы тоже обладают возможностью подмены номера, данный вид мошенничества так же строится на социальной инженерии.

Методы борьбы со стороны пользователя:

- Проверять баланс перед возвратом средств.
- Сверить номер, от которого поступило сообщение.
- Не сообщать конфиденциальных данных.

Методы борьбы со стороны оператора:

- Спам фильтры.
- Соглашения с контент провайдерами.

Проблемы обеспечения безопасности сетей *MVNO* охватывает широкий круг вопросов:

- аутентификацию (подтверждение того, что отправителем запроса является объявленный объект), защиту информации, хранимой на серверах;
- реализацию механизмов управления доступом и обеспечения целостности информации (защиту от несанкционированного доступа, исключение модификации, вставок и повторов);
- предотвращение вредительства от внесения помех, вирусов, дополнительного трафика и последствий других злонамеренных действий;
- устранение фрод-последствий (финансовых потерь от мошенничества).

Несанкционированный доступ к сетям *MVNO* может приводить не только к материальным убыткам и снижению качества обслуживания, но и нести угрозу экономической безопасности операторской компании и конфиденциальности внутренней информации.

При аутентификации в сети *MVNO* могут использоваться различные механизмы обеспечения услуги информационной безопасности. Например, согласно документам европейского института стандартизации, *ETSI* [14] в сетях *MVNO* могут быть использованы однопроходные и многопроходные механизмы аутентификации с использованием пароля, с изменением параметров (временных меток, случайного числа, счетчика), с третьим доверенным участником, с использованием симметричного или асимметричного шифрования.

При проектировании защиты информации от угроз несанкционированного доступа стоит задача определения характеристик качества механизмов аутентификации и шифрования [3].

Основные принципы построения защиты от фрода

1. Требуется подготовить программу управления уровнем мошенничества, работающую на основе принятой политики.
2. Необходимо периодически оценивать риск фрода для выявления потенциальных схем.
3. Повсеместное внедрение технических средств для снижения риска фрода.
4. Использование технических средств для выявления новых схем мошенничества.
5. Процесс подготовки отчетов должн быть включен в карту бизнес-процессов для контроля за уровнем фрода.

Уровень (или количественная характеристика) информационной безопасности сети *MVNO* определяется окончательной величиной риска безопасности. Под риском безопасности согласно терминологии, *ETSI* понимается результат и степень опасности воздействия угрозы безопасности. По всем видам угроз безопасности определяется порог риска, который состоит в решении, по каким видам угроз необходимо принять процедуры оценки риска, а по каким нет.

Выбор архитектуры безопасности сети *MVNO* (механизмов безопасности и средств управления безопасностью) в процессе проектирования позволяет составить окончательный остаточный риск (или уровень безопасности) для угрозы каждого вида [8, 15].

В зависимости от принятого способа количественной оценки угроз безопасности сетей *MVNO* может быть рассмотрено два подхода к концепции оценки уровня безопасности.

Первый подход состоит в оценке уровня безопасности по уровню воздействия (нулевой, средний и высокий) на каждый угрожаемый объект полной сети *MNO – MVNE – MVNO*.

В основу второго подхода положены характеристики, отражающие последствия всех видов угроз. К таким характеристикам угроз относятся: убытки из-за мошенничества; отток клиентов; потери из-за нарушения приватности; потери конфиденциальности; штрафы за нарушение закона; потери пользователей в оплате. При оценке потерь от мошенничества в первую очередь нужно учитывать позицию операторов. При больших доходах, возможно, что они допускают небольшой процент потерь от мошенничества, считая эти потери такими же неизбежными издержками бизнеса, как и налоги. Полное искоренение мошенничества, хотя и возможно, представляет для операторов невыполнимую задачу. Поэтому при составлении требований оператор *MVNO* должен найти баланс между затратами на защиту от мошенничества и убытками от него, включая потери клиентов.

Выводы

Обнаружение и предупреждение мошенничества – тесно связанные процессы. Предупреждение мошенничества, в основном, связано с организационными процессами, политиками, процедурами и др. В случае же с обнаружением акцент совмещается в сторону технологий и работ по обнажению фактов мошенничества, которое произошло или происходит. На данный момент предупреждение и обнаружение не позволяют полностью искоренить мошенничество в сетях сотовой связи, но являются первой линией обороны.

Литература

1. https://habr.com/ru/company/pt/blog/263903/
2. Артамонова Я.С., Максименко В.Н., Аналитическое моделирование ИК-услуг сетей NGN // Инновации и инвестиции, 2015. – № 6. – С. 136-142.
3. Максименко В.Н., Даричева А.Н. Методические подходы к оценке качества услуг контакт-центра // Экономика и качество систем связи, 2017. – № 1 (3). – С. 79-88.
4. Максименко В.Н., Особенности оценки качества инфокоммуникационных услуг контакт-центра // T-Comm: Телекоммуникации и транспорт, 2010. – Т. 4. – № 10. – С. 39-41.
5. Максименко В.Н., Ясюк Е.В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи, 2017. – № 2 (4). – С. 42-48.
6. Максименко В.Н., Васильев М.А. Методика расчета стандартизованных показателей качества дополнительных услуг на сетях подвижной связи // T-Comm: Телекоммуникации и транспорт, 2011. – Т. 5. – № 4. – С. 26-28.
7. Максименко В.Н. Услуга определения местоположения абонента как средство защиты в сети сотовой подвижной связи // Известия ЮФУ. Технические науки, 2007. – № 4 (76). – С. 151-155.
8. Нестеренко В.Д. Вопросы обеспечения безопасности сети ОКС7 ОАО «Северо-западный Телеком» // Тезисы доклада «Международный конгресс «Доверие и безопасность в информационном обществе» С-Петербург. 2001.
9. https://habr.com/ru/post/259007/
10. https://roem.ru/21-09-2015/207313/beeline-hustling/
11. https://habr.com/ru/post/267563/
12. https://habr.com/ru/post/267447/
13. http://lib.itsec.ru/articles2/focus/frod-realnost-sovremennogo-biznesa
14. Digital cellular telecommunication system (Phase 2+) GPRS ciphering algorithm requirements (GSM 01.61).

15. Бельфер Р.А., Максименко В.Н. Подход к разработке концепции оценки уровня безопасности мобильных систем // Сб. тр. Научно-практической конференции «Информационная безопасность» (28-31 мая 2002 г.) ТРТУ. – С. 205-207.