КАК ПРОТИВОСТОЯТЬ мошенникам

А.Майстренко, Техносфера

В ноябре в Москве прошла пятая всероссийская конференция "Revenue Assurance, Fraud, InfoSecurity & Risk Management", организованная компанией Connectica Lab. В повестке дня стояли такие ключевые вопросы как гарантирование доходов, удержание абонентской базы, предотвращение мошенничества и борьба с ним, а также управление рисками в телекоммуникационных компаниях. Мероприятие собрало около 200 участников из Москвы, регионов России, ближнего и дальнего зарубежья.

В этом кратком обзоре остановимся только на одной секции конференции, посвященной весьма волнующему операторов связи вопросу – борьбе с мошенничеством в сетях связи.

Секция открылась выступлением начальника отделения Управления "К" МВД России Станислава Калинина. Он отметил, что на территории 24 стран мира, включая Россию, жертвами киберпреступников каждую секунду становятся 12 человек. Преступники, используя SIM-карты, приобретенные по ложным паспортным данным, получают доступ в глобальную сеть для распространения вредоносного ПО, совершения DDoS-атак и хищения денежных средств со счетов граждан. Расследование преступлений с использованием таких SIM-карт технически невозможно. Есть проблема с предоставлением лог-файлов соединения абонента небольшими региональными Интернет-провайдерами. Основная задача Управления "К" – устранение причин, способствующих киберпреступности. МВД России уведомило Министерство связи и массовых коммуникаций и Роскомнадзор о необходимости законодательного урегулирования данной проблемы, так как текущая ситуация позволяет преступникам уходить от ответственности.

Доклад руководителя управления по предотвращению мошенничества и потерь доходов компании МегаФон Сергея Хренова был посвящен борьбе с SMS-спамом. В рамках этой борьбы в 2014 году МегаФон провел ряд мероприятий, в результате которых к октябрю 2014 года МегаФоном в неделю блокировалось около 50 млн. спам-SMS. Была устранена проблема с рядом мошеннических схем, основанных на массовых рассылках. Существенно сокращен объем пострадавших от рассылок со ссылками на вредоносное ПО для ОС Android, нацеленного на кражу денег с лицевого счета телефона и банковских счетов. Докладчик отметил ключевую роль изменений ФЗ № 126 "О связи". Согласно им рассылки коротких текстовых сообщений по сети подвижной радиотелефонной связи могут осуществляться только при условии заключения договора между заказчиком рассылки и оператором связи и при условии получения предварительного согласия абонента. Однако спамеры не сдаются и ищут новые каналы рассылки, поэтому от оператора требуются постоянный мониторинг и быстрота реакции. Спикер отметил, что борьба со спамом невозможна без участия регулятора.

Старший менеджер проекта "Гарантирование доходов и борьба с мошенничеством" компании ARAXXE Лилиан Кисалита в своем докладе остановился на вопросе контроля терминации SMS. Он отметил большой объем рынка SMS (90 млрд. евро в 2013 году) и его бурный рост (вдвое с 2009 по 2013 год). Оптовые доходы оператора

от входящих SMS могут составлять до 5% его годового оборота, что привлекает мошенников. Защищая интересы оператора, фирма ARAXXE предлагает решение для контроля терминации SMS. Оно подразумевает генерацию тестовых SMS через большое число международных маршрутов и последующий контроль их маршрутизации. Эффективность решения доказывается статистическими данными о сроках службы незаконных SIM-карт: если у незащищенного оператора этот срок составляет от 20 до 150 дней, то у защищенного всего 0,1 дня.

Выступление начальника отдела по управлению фродом компании ВымпелКом Елены Аслановой было посвящено сценариям фрода и его мониторингу. Привычный сценарий подразумевал вывоз партии SIM-карт в другую страну с целью реализации фрода. В плане реагирования это было очень удобно, так как партию значительно легче отследить, чем единичный номер. Новый сценарий подразумевает реализацию фрода с украденного мобильного телефона. Риски фрода существенно возрастают, если на номере подключены услуги ожидания вызова, конференц-связи или переадресации, поскольку это дает возможность выполнять много звонков одновременно. Фрод на фиксированной сети представляет собой несанкционированный доступ к оборудованию абонентов фиксированной сети с последующей генерацией международного трафика, особенно на дорогостоящие международные номера. Мошенники используют шлюзы, подключенные, с одной стороны, к Интернету и бирже VOIP-трафика, а с другой стороны – к сети оператора по договору оказания услуг местной связи с безлимитным тарифом. Оператор несет финансовые потери, поскольку недополучает стоимость интерконнекта международных звонков, а также имиджевые потери, поскольку используются дешевые каналы с плохим качеством. Реагирование на фрод подразумевает предотвращение звонков на рисковые направления, которые часто используют мошенники, но практически не используют обычные абоненты. Для борьбы с фродом используется как автоматическое реагирование на подозрительный трафик, так и работа аналитиков – постанализ. Система фрод-контроля и дифференцированная система порогов для различных направлений позволяют выявлять фрод практически в реальном времени.

Директор направления "Противодействие мошенничеству и гарантирование доходов" компании МФИ Софт Сергей Васильев коснулся перспектив борьбы с незаконным пропуском трафика в РФ. Докладчик отметил изменение структуры незаконной терминации трафика в последнее время. Для этого есть несколько причин: продолжающийся рост доли трафика VoIP/OTT, изменение структуры абонентской базы фиксированных сетей (заметен рост абонентской базы альтернативных операторов, использующих СПД для передачи голоса), выравнивание тарифов на внутрисетевую и внешнюю терминацию и повышение “белых” цен терминации в России. Противодействие нелегальной терминации со стороны операторов предусматривает упорядочивание пропуска трафика, контроль за типом вызова и АОН на межоператорских стыках, блокировку возможности подстановки АОН на международных и межгородских вызовах, усиление борьбы с нелегальной терминацией крупных операторов и существенное сокращение времени жизни нелегальных SIM-карт. В качестве ответа "серые" операторы применяют спуфинг – подмену исходного А-номера на местный фиксированный или мобильный номер, а также оффнет-терминацию – вывод точки нелегальной терминации из-под контроля терминирующего оператора. Докладчик отметил увеличение доли альтернативных операторов в нелегальной терминации. Среди особенностей противодействия незаконной терминации в новых условиях он назвал сложность взаимодействия с операторами-источниками нарушений: отсутствие однозначной трактовки существующей нормативной базы при переходе из СПД в ТфОП, недостаточный объем положительной судебной практики и низкое качество судебной экспертизы в вопросах технологического мошенничества, а также отсутствие постоянного технологического контроля порядка пропуска трафика на уровне регулятора.

Спикер также остановился на недостатках нынешнего состояния контроля информационного обмена. Часть антифрод-систем не проводит достоверное подтверждение факта вызова. При передаче таких событий невозможно на 100% подтвердить факт фрода. Часто в ходе антифрод-мероприятий выявляются факты спуфинга, когда сознательно или из-за ошибок настройки оборудования оператор получает АОН, принадлежащий другому оператору РФ, а не реальному источнику трафика. Передача таких событий может приводить к ошибочной блокировке абонентов. Поступающая от другого оператора информация не обладает достаточной степенью детализации для выполнения сверки CDR на стороне "домашнего" оператора. Передача отчетов об оффнет-фроде, а также импорт и сверка этой информации не автоматизированы. Подключение регулятора к системе позволит создать единое информационное пространство для оперативных санкций в отношении фродеров и доказательную базу для действий органов правопорядка.

Начальник отдела анализа и контроля трафика Ростелекома Алексей Кулешов рассказал о предотвращении фрода в межоператорском бизнесе. Международный вызов можно завершить на Ростелеком четырьмя способами: это международное, междугороднее, межзоновое и местное завершение вызова. Цена местного завершения вызова самая низкая, затем идет цена международного завершения, несколько дороже зоновое завершение, а самая высокая цена у междугородного завершения вызова. Основную часть фрода составляет завершение российского трафика на международном уровне и завершение на местном уровне всех других видов трафика. Для выявления фрода Ростелеком использует несколько анти-фрод систем: Спайдер, Fraud View, собственную систему прозвонки Test Call System и систему МФИ Софт. С помощью Test Call System можно направить вызов в сеть любого международного транзитного оператора и проверить, на каком уровне завершился вызов. Выполняется также совместная прозвонка с альтернативными операторами. С большой тройкой операторов организован оперативный обмен информацией о выявленных фактах фрода. В случае выявления фрода уличенному оператору направляется обращение, а если это не помогает, то следует обращение в Роскомнадзор и ФСБ, а также применяется ограничение трафика. Заключая договор с оператором, Ростелеком оговаривает запрет на подмену номера А и подмену трафика с неуказанного диапазона под угрозой ограничения трафика и штрафных санкций в трехкратном размере.

Спикер отметил, что бороться с фродом тяжелее, чем формировать условия его предотвращения. В этом вопросе очень важное значение имеет взаимодействие с регулятором. ■