

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ 3 (201)/2010

FRAUD



ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Редакция:

Дмитриев В.Ю.
viad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Слободчикова Т.А.
slobodchikova@jet.msk.su

Шедова Е.А.
eshedova@jet.msk.su

Верстка:

Кулешова Ю.В.

Корректурa:

Андрушко О.Ю.

Над номером работали:

Шопин Д.В.

Фефелов Д.А.

Баталова Н.В.

Чередникова Ю.В.

Издатель:

Компания «Инфосистемы Джет»

Контакты:

тел. (495) 411 76 01

<http://www.jetinfo.ru>

От редакции

В первом весеннем номере *JI* мы заострим внимание на проблеме мошенничества в сфере телекоммуникаций (фрод — несанкционированный доступ к услугам связи, а также получение услуг в режиме неправомерного доступа). Конечно, тема фрода не нова, но все также актуальна. С началом нового года операторы связи активизировались в борьбе с этим явлением. Возможно, приход весны пробудил их от долгой спячки, а возможно, что с постепенным возвращением уровня инвестиций и витающими в воздухе отголосками кризиса, все чаще и острее встает вопрос о гарантировании и сохранении своих доходов.

По мере увеличения масштабов и сложности современных сетей связи растет и число попыток использовать широко разветвленную телекоммуникационную инфраструктуру в противоправных целях. Несанкционированные, сомнительные и откровенно мошеннические действия приводят не только к ощутимым потерям в доходах операторов, но и к снижению объемов и качества предоставляемых услуг. Такое развитие событий привело к появлению и в нашей стране отдельного направления по борьбе с мошенничеством и гарантированием доходов в телекоме — FM&RA (Fraud Management & Revenue Assurance).

Направление фрод-менеджмента (FM&RA) — новое для российского рынка, и пока отечественные телекоммуникационные компании не так легко идут на внедрение подобных решений. К тому же, рынок подобных систем представлен продуктами зарубежных вендоров, которые рассчитаны на некую универсальность и всеохватность, а потому стоят довольно дорого и не учитывают специфику российского рынка операторов связи. Та-

ким образом, по оценкам экспертов, сегодня стоит говорить о том, что в нашей стране в этой области господствует время локальных решений, нацеленных на выполнение конкретных задач. Такой подход, как показывает опыт компании «Инфосистемы Джет», позволяет не только сберечь средства от рук мошенников, но и экономит деньги и время на внедрении лишнего на данный момент функционала. А наглядный результат от работы такой системы будет виден практически сразу.

В этом номере мы не только расскажем о том, что такое фрод и как с ним бороться, но и обратим ваше внимание на то, насколько сложным может быть проект по борьбе с мошенничеством. Принимая решение о внедрении систем защиты у себя в компании, стоит серьезно подойти к вопросу выбора ответственных за его реализацию: сотрудники компании или привлеченные специалисты. Конечно, с одной стороны, вопросы информационной безопасности очень щекотливы, поэтому одним из наиболее безопасных способов может стать осуществление проекта своими силами. Но, с другой стороны, подобные проекты очень сложны, порой запутаны и требуют к себе большого внимания, опыта и знаний специфики. Поэтому, возможно, привлечение квалифицированных специалистов к реализации FM&RA-проектов поможет не только не утонуть в лавине решений, но и выбрать/внедрить продукт, который обеспечит вашей компании стабильный и, главное, гарантированный доход.

Берегите себя!

С уважением, редакция JI

СОДЕРЖАНИЕ

Статистика	5
Тема номера	
Гарантирование доходов и противодействие мошенничеству в телекоммуникационных компаниях (Д.Шопин)	6
Взломай свою офисную АТС до того, как это сделают другие (Д.Фефелов).....	12
Аудит функций Fraud Management & Revenue Assurance (Д.Фефелов)	15
Наши проекты	
Создание единой системы розничных продаж на платформе SAP CRM для Уральского Банка Реконструкции и Развития.....	19

Фрод – более 200 видов обмана в сетях связи

Мошенничество существует как на фиксированных, так и на мобильных сетях связи, причем вне зависимости от технологии передачи информации. Эксперты СФСА насчитали более 200 видов преступного обмана в сетях связи. Наиболее распространенными являются организация несанкционированных переговорных пунктов, получение доходов путем кражи PIN-кодов телефонных карт или взлома алгоритмов их генерации, клонирование SIM-карт мобильных телефонов, использование реквизитов подставных лиц при регистрации в сети, подключение к телефонным линиям, принадлежащим другим физическим или юридическим лицам. Одним из наиболее опасных видов мошенничества считаются преступные действия сотрудников самого оператора, которые умышленно активируют не оплаченные сервисы. По некоторым данным, доля потерь от внутреннего мошенничества достигает 23%.

В городской телефонной сети наиболее распространенный вид мошенничества – незаконное подключение к линиям связи. Как отмечает пресс-служба МГТС, основной целью таких подключений является осуществление за чужой счет международных и междугородних вызовов. Страдают при этом абоненты ГТС, которым приходится платить за разговоры неизвестных собеседников.

Напомним, что АТС и магистральные кабели городских сетей защищены и физическими, и техническими средствами, на этих уровнях несанкционированные подключения к линиям связи практически исключены. Зато подсоединение на участке от распределительного шкафа до квартиры абонента вполне возможно. Злоумышленни-

ки могут не только бесплатно звонить в дальние города и страны, но и незаконно прослушивать чужие переговоры. Иногда так можно «выудить» информацию стоимостью в миллионы рублей.

Телефонные аферисты стали подключаться к альтернативным операторам фиксированной связи под видом вновь созданных провайдеров услуг IP-телефонии. Они запускали карточные платформы и, проработав месяц-другой, исчезали в неизвестном направлении. После них оставались неоплаченные счета на громадные суммы. Со временем крупные операторы научились избегать подобного обмана, и мошенники переключились на взлом офисных АТС. Удаленно подчиняя себе корпоративную АТС, они звонят через нее в дальние страны за счет какой-либо компании. Впрочем, этот вид телекоммуникационного злодейства необходимо рассматривать отдельно – как нарушение безопасности корпоративной сети.

Аналитики дружно предсказывают новую волну мошенничества в сетях связи. Если раньше основной целью преступников был нелегальный доступ к каналам связи, то теперь они переориентируются на контент, цена которого нередко многократно превышает стоимость минут соединения. В будущем мошенники проявят себя, прежде всего, в области электронной коммерции. Уже сегодня активно действуют электронные службы заказа билетов, оплата товаров и услуг через Интернет, перевод денег с одних банковских счетов на другие.

*Подготовлено по материалам сайта
<http://netfraud.ru/publication/ttk/2>*

Гарантирование доходов и противодействие мошенничеству в телекоммуникационных компаниях



Дмитрий Шопин,
руководитель направления систем борьбы с мошенничеством,
компания «Инфосистемы Джет»

«...Свести бой по дороге от завода до магазина к приемлемой цифре: пятьдесят литров на тонно-километр водки и двадцать пять килограммов на тонно-километр коньячных изделий...»

М. Жванецкий

В лексиконе крупных компаний, занимающихся розничной продажей товаров народного потребления, существует такое понятие как «shrinkage», (пер. с англ. — «сокращение, усушка, уварка»). Это термин означает потерю части товара (а значит, и потенциальной выручки) в результате его порчи, утери, воровства и т. п. Компании предпринимают более или менее успешные меры по снижению уровня «shrinkage», но полностью исключить это неприятное явление не удается.

Телекоммуникационные компании не продают товары народного потребления. Они торгуют электромагнитными импульсами. И тем не менее, понятие «усушки» и «утруски» применимо и к ним.

У операторов связи превращение «товара» в доход представляет собой длинный и сложный процесс, на протяжении которого информация о его продаже (телефонного звонка, SMS, доступа в интернет и т. д.) последовательно обрабатывается множеством систем. Цепочка формирования дохода начинается с сетевого оборудования, обеспечивающего собственно предоставление услуги связи и фиксирующего это событие. Затем эта информация проходит через разнообразные про-

межуточные программные и аппаратные комплексы, агрегирующие и трансформирующие данные. И завершается все биллинговой системой, которая, в свою очередь, также состоит из нескольких модулей, ответственных за тарификацию услуг, прием платежей, выставление счетов и т. д. Если к этому еще добавить системы обслуживания клиентов, отчетности, управления услугами и т. д. и т. п., то становится понятно, насколько сложна и терниста дорога от предоставления телекоммуникационной услуги до получения за нее денег оператором. На каждом участке этого пути информацию поджидают сбои, конфликты оборудования, ошибки настройки систем и, конечно же, воровство или фрод (fraud), как принято называть мошенничество в телекоммуникационной сфере (рис. 1).

По данным CFCA (Communications Fraud Control Association) мировые потери телекоммуникационной отрасли в 2008 г. составили \$72-80 млрд., увеличившись на 34% по сравнению с 2005 г.

ТОП3 видов фрода в 2008 г.:

1. «Подписочный» фрод (subscription theft) — использование чужих учетных данных для доступа к услугам.
2. Взлом УАТС — несанкционированное использование УАТС (PBX) клиентов операторов связи.
3. Фрод с использованием Premium Rate-сервисов.

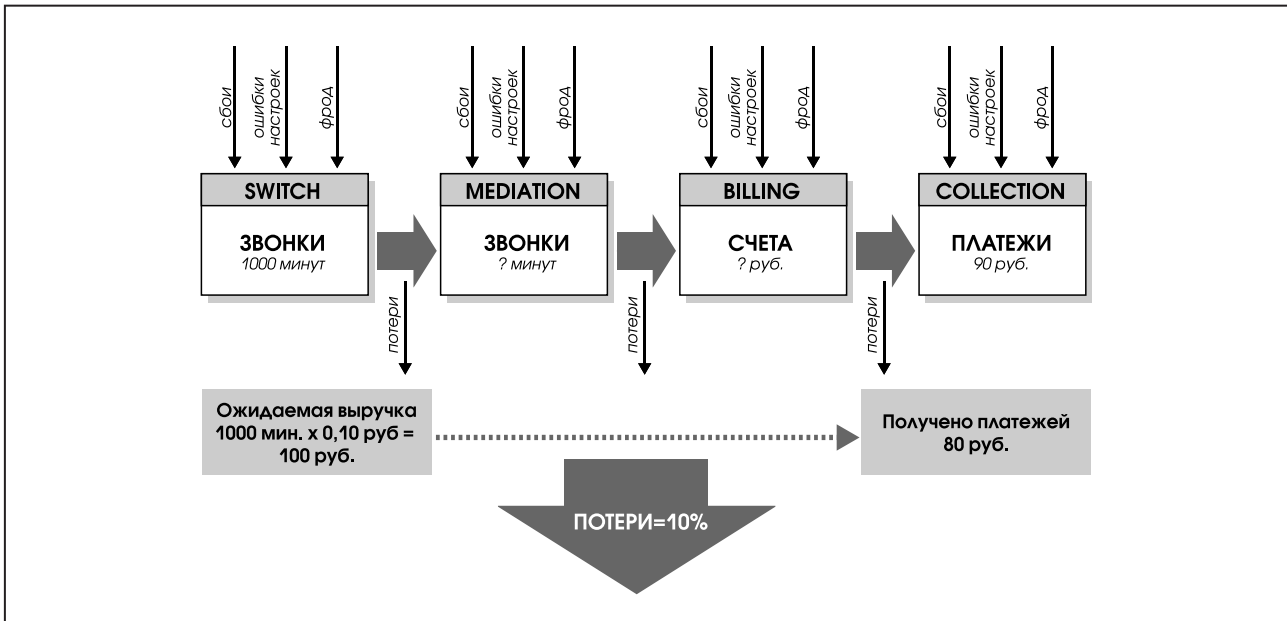


Рис. 1. Потери оператора связи

Так, по данным исследования, которое ежегодно проводится британской аналитической компанией Analysys Research, общемировой уровень потерь телекомов в 2007 году достиг 13,6% от выручки, по сравнению с 12,1% в 2006-м и 11,6% в 2005-м. В абсолютном выражении это составляет более \$200 млрд. При этом примерно треть этих потерь — последствия фрода, как абонентского, так и внутреннего.

Задача противодействия мошенничеству и гарантирования доходов (fraud management & revenue assurance, FM&RA) актуальна для телекоммуникационных компаний с тех пор, как был изобретен телефон. Но сегодня эта тема выходит на новый уровень значимости по нескольким причинам:

- мировой финансово-экономический кризис, выдвигающий особенно жесткие требования к эффективности ведения бизнеса;
- насыщение рынка телекоммуникационных услуг и обострение конкуренции;
- новая волна интереса государственных регуляторов к тому, как компании осуществляют мониторинг и как отчитываются о своей выручке (речь идет, например, о требованиях Sarbanes-Oxley Act);
- стремительное развитие технологий и маркетинговых инноваций, за которым развитие методов и инструментов контроля просто не успевает.

Непосредственных (корневых) причин утечки выручки великое множество, так как каждый оператор обладает своим уникальным набором

сервисов, систем, бизнес-процессов, а значит, характеризуется и уникальным набором ошибок, сбоев, мошеннических схем. Однако все это многообразие проблем приводит в итоге к последствиям всего трех типов:

1. Услуга предоставлена, но информации об этом нет (или она неполная, искаженная). Например, не сформированы или утеряны CDR звонков (**Call Detail Record (CDR)** — детальная запись о вызове), совершенных абонентом.
2. Информация об услуге есть, но обработана она некорректно. Типичный пример — ошибки настроек тарификации услуг.
3. Информация об услуге есть, обработана она корректно, но деньги не получены. Примерами такой проблемы могут служить отказы абонентов оплачивать счет или фиктивные платежи.

Какие же существуют решения проблемы утечки выручки в телекоммуникационных компаниях?

Сегодня разработчики BSS/OSS-систем предлагают операторам связи большой выбор FM&RA-решений. Традиционно эти решения подразделяются на два больших класса (см.рис.2):

- Fraud Management System (FMS);
- Revenue Assurance System (RAS).

В основе работы FMS лежит анализ поведения каждого абонента оператора с целью выявления активности, которая может расцениваться

как аномальная по сравнению с обычной активностью среднего абонента либо по сравнению с активностью данного конкретного абонента в прошлом. Так совершение 10 международных вызовов в час не является типичным поведением абонента — физического лица и может свидетельствовать, например, о том, что с тарификацией этих вызовов есть проблемы. Или неожиданное увеличение объема трафика абонента в несколько раз по сравнению с предыдущим периодом также может вызвать подозрения в том, что пользователь нашел способ увеличить потребление услуг без повышения своих финансовых затрат. Конечно, это только подозрения, которые далее потребуют детального исследования ситуации аналитиком.

В RAS используется иной подход. Системы такого класса собирают агрегированные данные на различных участках цепи формирования выручки и сопоставляют их, пытаясь выявить расхождения. Например, если за определенный период времени коммутатором сформировано записей на 1 000 000 мин. телефонных разговоров, а в биллинговой системе за тот же период в счетах оказалось 999 000 мин., то налицо «усушка», приводящая к недополучению оператором выручки.

Вследствие такого деления FM&RA-систем, противодействие фроду и гарантирование доходов иногда рассматриваются операторами как две отдельные отрасли, каждая из которых имеет свою собственную проблематику и свои собственные методы и инструменты идентификации этих проблем. Часто это отражается даже на организационной структуре компании —

функции Fraud Management и Revenue Assurance осуществляются различными подразделениями.

В принципе такое независимое сосуществование FM и RA возможно, но это не обеспечивает всеобъемлющего и максимально эффективного покрытия всех областей риска. Более верным является представление о единой функции FM&RA, где фрод — это всего лишь одна из причин или, наоборот, одно из возможных последствий проблемы потери доходов. Поясним на примере.

Предположим, к АТС какого-либо оператора фиксированной связи подключены абоненты, не учтенные в биллинговой системе. Подобная ситуация вполне реальна и может быть как следствием внутреннего фрода, так и результатом технического сбоя (или человеческой ошибки), когда при отключении ранее существовавшего абонента в биллинге, на станции его отключения не происходит. В результате абонент пользуется услугами связи, которые при этом не тарифицируются и не оплачиваются.

Если какой-либо из этих абонентов, пользуясь бесплатностью услуги, начнет генерировать значительный объем трафика, то он будет обнаружен FMS. Однако стопроцентной гарантии этого дать нельзя, так как уровень активности абонента может ничем и не отличаться от среднего по абонентской базе, и таким образом он останется незамеченным для FMS. С другой стороны, система гарантирования доходов (RAS) теоретически должна обнаружить эту проблему путем сверки объемов трафика, сформированного коммутатором и поступившего в биллинговую систему. Правда, если таких абонентов немного и соз-

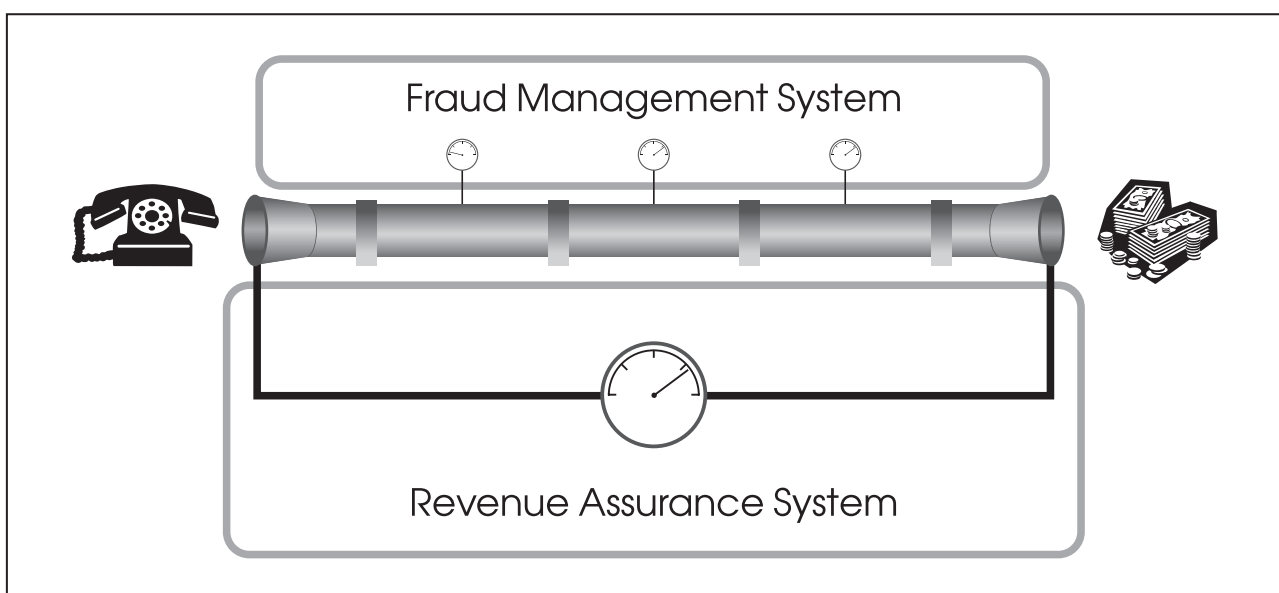


Рис. 2. Решение FM&RA

даваемое ими расхождение незначительно на фоне общего трафика, то чувствительности RAS будет недостаточно для его обнаружения.

Таким образом, одна и та же проблема потери доходов может иметь как фродовый (мошеннический), так и нефродовый характер. Причем фрод может быть как корневой причиной потери (преднамеренное создание расхождений между коммутатором и биллингом внутренними фродстерами), так и ее следствием (повышение активности абонентов, осознавших, что теперь их звонки бесплатны).

Одну и ту же проблему могут обнаружить и FMS, и RAS, при этом заранее нельзя предсказать, какая из них выявит утечку раньше.

И FMS, и RAS реагируют на проблему потери доходов тогда, когда она уже состоялась и проявила себя тем или иным образом. Т. е. они не обеспечивают превентивных мер борьбы с утечками выручки.

Профилактика фрода – Loss Prevention Center

Получается, что совместное использование FMS и RAS существенно повышает вероятность обнаружения различных утечек выручки, но скорость их реагирования уже не отвечает современным требованиям к эффективности гарантирования доходов. Можно ли решить эту проблему?

Возвращаясь к рассмотренному ранее примеру с отсутствием тарификации вызовов, легко заметить, что предотвратить данную проблему можно было бы простой регулярной сверкой данных, позволяющей выявить всех абонентов, отсутствующих в биллинговой системе, но присутствующих в базе данных АТС. Все, что для этого необходимо, — это выгрузка двух таблиц из биллинга и АТС и несложный SQL-запрос. Помимо простоты и минимальных затрат средств и ресурсов, у такого метода есть еще одно важное преимущество — превентивность. Теперь оператор может устранить проблему еще до того, как абонент сам обнаружит ее и сможет воспользоваться ей, нанеся тем самым экономический ущерб компании.

Однако подобные контрольные процедуры, ориентированные на корневые причины конкретных проблем потери выручки, т. н. «локальные контроли», могут быть реализованы только

в том случае, если FM&RA-подразделение оператора заранее знает о возможности возникновения такой утечки и ее корневых причинах. Конечно, на данный момент специалистами уже накоплен немалый опыт в области FM&RA, и известно достаточно много характерных для большинства операторов связи источников потерь. Тем не менее, прогресс не стоит на месте, и вслед за стремительным развитием технологий также стремительно развиваются и схемы фрода, возникают новые, ранее неизвестные «дыры» в системах и процессах.

Поэтому встал вопрос о необходимости такого решения, которое, с одной стороны, позволяет выявлять любые проблемы, приводящие к потере выручки, независимо от их природы и знания их корневых причин, а с другой — обеспечивает максимальную скорость реагирования на известные «дыры» еще до того, как выручка будет потеряна.

В процессе изучения данного вопроса и поиска оптимального решения, учитывающего все вышеперечисленные требования, специалисты компании «Инфосистемы Джет» разработали систему **Loss Prevention Center**, сочетающую в себе как сильные стороны традиционных инструментов FM&RA, так и превентивность локальных контролей.

Loss Prevention Center (LPC) представляет собой комплекс организационных, процедурных и программно-аппаратных средств противодействия мошенничеству и целостности всей цепочки формирования выручки оператора связи — от момента предоставления услуги абоненту до момента оплаты выставленного счета.

Программно-аппаратная или инструментальная часть LPC представляет собой кастомизированный для каждого конкретного оператора связи набор инструментов, обеспечивающий как постоянный мониторинг сети в целом при помощи традиционных решений FMS и RAS, так и превентивное противодействие всем известным источникам потерь, возникновение которых возможно в данной компании.

Структура инструментальной составляющей LPC представляет собой двухуровневую систему (см. рис. 3 на стр. 10).

На I уровне находятся традиционные системы FMS и RAS, обеспечивающие «глобальный» контроль всех потоков данных, формирующих выручку компании. Системы FMS и RAS работают по принципу «черного ящика», обнаруживая любые потери выручки либо по аномальному по-

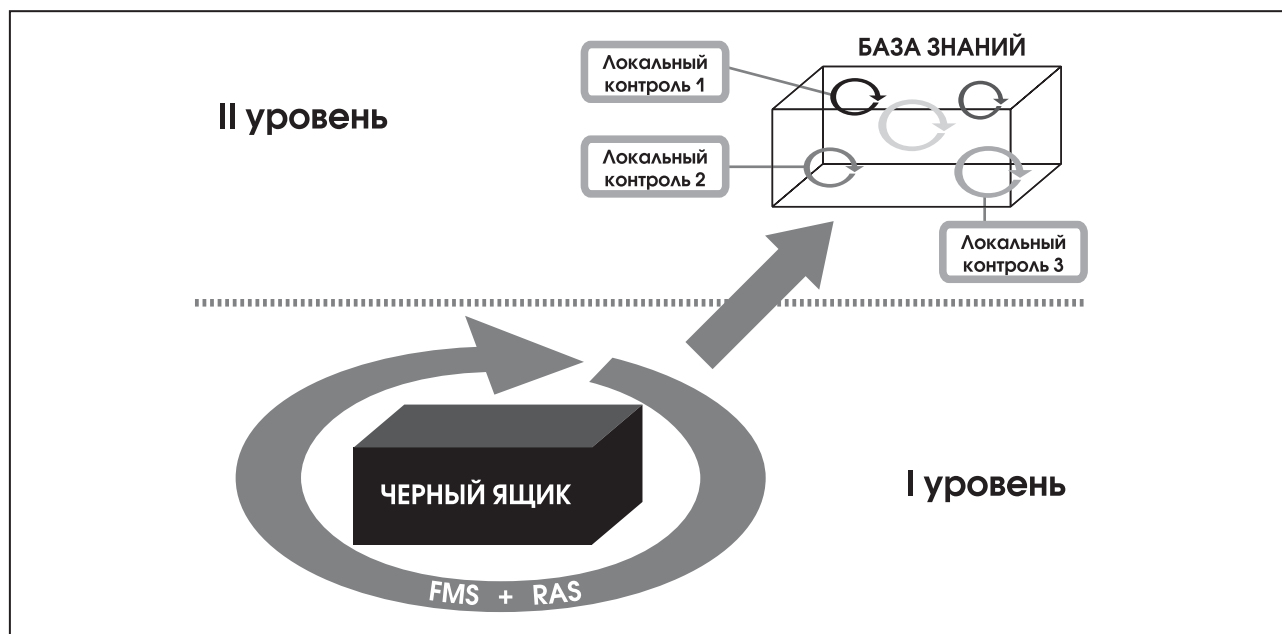


Рис. 3. Структура инструментальной составляющей

ведению абонентов и/или процессов, либо по расхождениям в объемах данных, проходящих через различные участки цепи получения выручки.

Обнаруживаемые на I уровне аномалии и расхождения анализируются на предмет их корневой причины, принимаются меры по устранению проблемы, и, если есть вероятность повторения последней, то разрабатывается локальный контроль, ориентированный на данную конкретную проблему. Проблема из элемента «черного ящика» превращается в элемент «базы знаний», и мониторинг ее перемещается на II уровень — уровень контроля корневой причины или «локального контроля». Соответственно изменяется и степень защищенности компании от данного вида риска — теперь проблема устраняется еще в момент зарождения.

Как показывает практика, зачастую нет необходимости внедрять промышленные системы уже на начальной стадии создания LPC. FMS и RAS — системы далеко не дешевые, их внедрение требует приобретения высокопроизводительного «железа», объемных массивов памяти и является достаточно длительным и ресурсоемким процессом. Часто оказывается, что на первом этапе создание нескольких дополнительных отчетов в уже существующих BSS/OSS оператора либо внедрение недорогой системы выгрузки и хранения данных (с возможностью проведения аналитических выборок и сверок) позволяет закрыть львиную долю наиболее критичных проблем утечки доходов и мошенничества.

Например, хорошо знакомым всем без исключения операторам фиксированной связи ви-

дом фрода является взлом PBX — несанкционированное использование злоумышленниками УАТС клиентов оператора для совершения междугородных вызовов. Все традиционные FMS борются с этой проблемой одинаково — регистрируя всплеск трафика с номеров «жертвы». Но оказывается, что за время, необходимое FMS для обработки данных и реагирования, мошенники успевают увеличить счет клиента на весьма значительные суммы. Поэтому в рамках LPC существует решение, обеспечивающее предотвращение данного вида фрода еще до того, как будет осуществлена попытка взлома (более подробно см. статью «Взломай свою офисную АТС до того, как это сделают другие», стр. 12).

Следовательно, если основным и самым критичным для оператора связи риском на данный момент является взлом PBX, то нет необходимости «стрелять из пушки по воробьям» и начинать создание LPC с приобретения FMS. Достаточно внедрить соответствующий «локальный контроль».

Внедрение систем защиты

Конечно, создание такого «индивидуального» набора инструментов для телекоммуникационной компании требует тщательного обследования последней. Необходимо проанализировать

действующие в компании системы, процессы, предоставляемые услуги и т. д. Цель такого обследования (FM&RA-аудита) — выявить в компании существующие на данный момент проблемы потери доходов и фродовые схемы, приоритезировать их в соответствии с масштабом потерь и вероятностью их возникновения и разработать поэтапный план развития инструментальной части LPC (более подробно см. статью «Аудит функции Fraud Management & Revenue Assurance», стр. 15).

Естественно, что сложноорганизованный инструментальный комплекс FM&RA требует и соответствующей *организационной и процедурной поддержки*.

Для этого в LPC существует **организационная составляющая**, которая подразумевает формирование в компании подразделения, ответственного за реализацию функций FM&RA. В его задачи должны входить координация выполнения процедур FM&RA всеми вовлеченными в них структурами компании, разработка новых процедур, управление внедрением и эксплуатация программных комплексов FM&RA, формирование и предоставление отчетности высшему руководству по специально разработанным KPI, характеризующим как ситуацию с гарантированием доходов в компании в целом, так и эффективность работы самого FM&RA-подразделения.

К процедурной составляющей LPC относится набор формализованных описаний процессов обнаружения и противодействия мошенничеству и потерям выручки. Большинство таких

процессов является кросс-функциональными, т. е. в них вовлечены другие подразделения компании. Поэтому необходим так же ряд документов, регламентирующих кросс-функциональное взаимодействие при выполнении процедур и направляющих отдел FM&RA необходимыми для этого полномочиями.

Все это позволяет наиболее оптимально использовать внедренное решение и добиться наибольших результатов в борьбе с фродом.

Отметим, что правильно реализованная концепция Loss Prevention Center позволяет решить три основные задачи современной функции Fraud Management & Revenue Assurance:

1. Поэтапное внедрение — от закрытия самых критичных и/или «лежащих на поверхности» проблем утечки доходов к стопроцентному покрытию всех возможных рисков потерь.
2. Экономическая целесообразность — затраты на создание FM&RA-функции не должны превышать экономическую выгоду от ее внедрения.
3. Превентивность — проблемы должны предотвращаться, а не обнаруживаться.

Такой подход в борьбе со фродом на данный момент является наиболее универсальным для различных компаний и позволяет обеспечить достижение целей гарантирования доходов в любой сфере — от сокращения боя дорогих коньячных изделий при транспортировке до максимально полного сбора выручки за услуги связи.

Взломай свою офисную АТС до того, как это сделают другие



Дмитрий Фефелов,
старший консультант по управлению фродом и гарантированию доходов, компания «Инфосистемы Джет»

Современные компании для организации связи все чаще используют офисные автоматические телефонные станции (УАТС или Private Branch Exchange, PBX), обладающие большим количеством «продвинутых» функций. Одновременно с этим, одним из наиболее распространенных видов мошенничества (фрода) для операторов фиксированной связи остается взлом и использование PBX их клиентов для совершения бесплатных вызовов.

Очень часто фризеры (мошенники, специализирующиеся на взломе телефонных сетей) создают нелегальные переговорные пункты и, используя взломанные PBX, начинают продавать по очень низким ценам звонки на международные направления для всех желающих. Естественно, счет за эти вызовы приходит к «организациям-жертвам». Суммы таких счетов для одной организации могут колебаться, в среднем, от 1 000\$ до 50 000\$ в месяц.

Как фризерам удастся взломать PBX?

В настоящее время существует много способов взлома PBX:

- «грубая сила» (Brute force). Фризер с помощью специальных программ-сканеров, путем прямого перебора возможных паролей к различным функциям PBX пытается

получить доступ к внешней телефонной линии;

- «социальная инженерия». При этом способе фризер пытается получить доступ к внешней телефонной линии с помощью «человеческого фактора». Например, звонит сотрудникам компании и, представляясь инженером ИТ-подразделения, просит набрать на телефонном аппарате определенную комбинацию цифр, которая приводит к переводу вызовов на нужное мошеннику направление;
- физическое подключение к нужной PBX;
- внутренний фрод со стороны собственных сотрудников компаний и т.д.

Нельзя сказать, что компаниям нечего противопоставить мошенникам. Для борьбы со взломами PBX используется несколько, ставших уже традиционными, методов. Например:

- регулярный просмотр сотрудниками компании детализации вызовов через PBX, с целью обнаружить «подозрительные» звонки (в нерабочее время, длительные вызовы на международные или дорогостоящие развлекательные направления, множество входящих коротких вызовов с одного номера и т.д.);
- мониторинг оператором трафика на международные направления и поиск его неожиданных всплесков;
- применение специализированных систем борьбы с мошенничеством (Fraud Management Systems, FMS), в которых настраиваются правила срабатывания предупреждений

Отвечая на давление, с целью защитить и повысить прибыли, операторы связи сосредотачивают свое внимание на выявлении и предотвращении утечки доходов.

Результаты опроса 96 мировых операторов связи показывают, что различные типы мошенничества все больше «отъедают» от операторской прибыли, и операторы связи все более обеспокоены последствиями мошенничеств и связанных с ними проблем в потоках доходов.

Опрос был проведен независимой исследовательской фирмой, изучающей причины распространения утечек доходов, наилучшие подходы операторов связи по предотвращению проблемы.

Основные результаты анкетирования

Аналитики сообщают, что в среднем утечка доходов составляет около 13,6% от годового оборота оператора связи. Это значительно больше по сравнению с 1,8% от годового оборота оператора связи, который игроки рынка связи считают максимально допустимым лимитом утечки доходов.

при превышении абонентом определенных порогов использования сервиса (например, длительные международные вызовы).

Общим недостатком вышеперечисленных методов борьбы является их реактивный характер. Проблема выявляется уже по факту, когда мошенник успел воспользоваться «дырой» РВХ в своих целях (с момента взлома и до момента обнаружения нелегального трафика). Чаще всего фрикер успевает совершить некоторое количество длительных международных вызовов. Получая счет за месяц от оператора на огромную дополнительную сумму за эти вызовы, корпоративные клиенты обычно не спешат его оплачивать. Оператор, чтобы не потерять клиента, вынужден идти на уступки и «списывать» эти суммы задолженности либо добиваться оплаты всеми возможными способами, что требует затрат ресурсов.

Более того, последние примеры громких судебных дел показывают, что при «продуманности» процесса взлома РВХ вычислить группу мошенников достаточно сложно. Например, в одном из обвинительных актов № 2005R00946¹ в США, с которым можно ознакомиться на официальном сайте Министерства Юстиции США, по делу международных телефонных мошенников, успешно действовавших несколько лет, говорится о подтвержденных убытках на сумму около 55 млн.\$.

Суммарная утечка доходов возрастает ежегодно, начиная с 2004 года. Основной причиной увеличения утечки доходов с 2006 года по 2007 год был значительный скачок, связанный с тремя видами мошенничества:

1. мошенничество через других операторов связи;
2. внутреннее мошенничество;
3. внешнее мошенничество.

Анкетирование показало, что мошенничество является самым распространенным источником утечки доходов операторов, на долю которого приходится больше потерь, чем в любой другой категории утечки доходов.

Согласно результатам, убытки от мошенничества выросли от 2,9% доходов в 2006 году до 4.5% в 2007 году.

По материалам
<http://netfraud.ru/publication/ttk/4>

Фрикеры специализировались на взломах РВХ методом «грубой силы». Далее они продавали трафик через колл-центры и при вызове обычного клиента маршрутизировали звонок через взломанные РВХ. Основными причинами их «успешного бизнеса» в течение столь длительного времени стали:

- широкая (международная) география бизнеса;
- изучение РВХ самых популярных производителей;
- проработанная технология взлома (с учетом особенностей РВХ и систем контроля);
- достаточное количество слабо защищенных РВХ;
- реактивный характер борьбы со взломами РВХ со стороны компаний-владельцев РВХ и операторов (достаточно времени до момента обнаружения, чтобы «зарабатывать»).

Выход есть!

Тем не менее, некоторые из видов взлома РВХ и последующие счета за «чужой» трафик могут

1 <http://www.justice.gov/usao/nj/press/press/files/pdffiles/PBX%20Hacking%20Indictment.pdf>

быть легко предотвращены как самими пользователями (например, ограничение физического доступа к РВХ, написание внутренних инструкций для сотрудников), так и специализированными компаниями.

Альтернативный подход к борьбе со взломами РВХ, которого придерживается, например, компания «Инфосистемы Джет», позволяет проактивно проверить уязвимость РВХ. Данный подход основан на хорошо зарекомендовавшем себя в области ИТ-безопасности методе — тестах на проникновение в систему или «пентестах» (Penetration tests).

Используя сценарии потенциального взлома во время «пентестов» (например, «brute force»), можно обнаружить слабо защищенные РВХ в сети оператора и предпринять необходимые меры по устранению выявленных уязвимостей еще до попытки атаки фрикеров на РВХ.

Основными преимуществами такого альтернативного подхода являются:

- минимальные затраты ресурсов оператора связи — все попытки «дружественного взлома» осуществляются профессионалами «снаружи»;
- любая необходимая периодичность сканирования РВХ клиентов позволяет легко проверить все РВХ на устойчивость к новым сценариям взлома либо к появлению уязвимостей после изменения их настроек;
- проактивность — оператор не успевает потерять свою выручку (не придется «списывать» долги);
- высокая эффективность — использование сценариев взлома, аналогичных мошенническим, и постоянное их обновление позволяет находить уязвимости, которые фриеры еще не успели обнаружить.

В заключение хочется напомнить менеджерам и ответственным за безопасность сотрудникам компаний о том, что безопасность системы определяется ее самым слабым звеном и что вопросам защищенности РВХ следует уделять не меньше внимания, чем безопасности другой ИТ-инфраструктуры. Иначе об уязвимостях в РВХ вашей компании побеспокоятся фриеры.

Материал был опубликован в журнале «Вестник связи» № 2, 2010

Аудит функции Fraud Management & Revenue Assurance

Дмитрий Фефелов,
старший консультант по управлению фродом и гарантированию доходов,
компания «Инфосистемы Джет»

На современном этапе развития телекоммуникационных операторов уже не подвергается сомнению тезис о необходимости особого контроля собираемой ими выручки. Функция контроля выручки у операторов связи реализуется в виде Fraud Management & Revenue Assurance (далее, FM&RA). Одновременно с этим на рынке консалтинговых услуг различными компаниями предлагается такая услуга как аудит функции FM&RA, которая позволяет провести независимую проверку соответствия FM&RA компании известным требованиям стандартов и лучших практик и выработать рекомендации по устранению выявленных несоответствий.

В рамках данной статьи мы расскажем, как правильно подойти к процессу аудита FM&RA.

Когда необходим аудит FM&RA?

Различные виды аудита FM&RA предполагают разные цели и объемы работ, что влияет на его продолжительность и стоимость. Поэтому, прежде, чем заказывать и проводить аудит FM&RA, оператору связи следует определить: зачем это нужно?

Четкое определение целей и задач позволит как достичь требуемого результата, так и сэконо-

мить затраты на аудит, оставив только необходимые активности. В противном случае, оператор получит отчет консалтинговой компании о несоответствии его функции FM&RA какому-либо стандарту и рекомендации по внедрению решений различных вендоров для устранения этого несоответствия. Но, возможно, цели и задачи аудита FM&RA были совсем другими. Например:

Необходимо было выявить причины неэффективной работы существующей функции FM&RA оператора. Вы, как менеджер, видите или подозреваете, что функция FM&RA не решает поставленных ей задач или решает их не достаточно оперативно. Признаки этого – регулярные инциденты, связанные с потерей выручки; проблемы потери выручки быстро не выявляются, а влияют на финансовую отчетность в виде роста дебиторской задолженности либо существенного падения выручки и т.д. В этом случае аудит необходим для выявления как причин неэффективной работы FM&RA (возможно, нужно просто более качественно настроить выгрузку данных из систем оператора или изменить существующие ключевые показатели эффективности), так и проверки покрытия существенных рисков потери выручки текущими контролями (например, этих контролей просто пока нет).

Или снизить затраты на FM&RA при сохранении приемлемого уровня оперативности и эффективности контролей. В этом случае необходимо провести аудит бизнес-процессов и текущих

контролей FM&RA и определить пути их оптимизации (возможно, часть контролей следует передать в операционные подразделения компании).

Возможной причиной аудита может стать поиск скрытых резервов увеличения выручки. Например, выявление определенных видов фрода и потерь выручки, которыми компания пока не занималась, но которые выявлены у других операторов связи, и оценка их влияния на бизнес. Аудит в этом случае будет направлен на выявление этих резервов и создание соответствующих процессов FM&RA.

А также обоснование необходимости внедрения автоматизированной системы FM&RA. У оператора по какой-либо причине (опыт у других операторов, рекомендации форумов и т.д.) возникает потребность внедрения системы FM&RA. В данном случае аудит будет строиться как на проверке необходимости внедрения (создания) такой системы или ее отдельных частей (при определенных условиях аналогичный результат может достигаться, например, построением системы контролей на выгрузках данных и их интеграцией в существующую систему отчетности оператора), так и на сравнительном анализе эффективности решений различных производителей.

К целям проведения аудита может относиться и определение направлений дальнейшего развития в части FM&RA. Для этого потребуются объективная оценка покрытия существенных рисков потери выручки текущими контролями и определение непокрытых областей, что и будет сделано в рамках аудита FM&RA.

Все рассмотренные нами случаи показывают, насколько важно четко сформулировать цели и задачи аудита, чтобы ваши ожидания от его результатов совпали с полученными сведениями. Только в этом случае средства, затраченные на его проведение, не будут потрачены впустую.

Что понимается под услугой аудит FM&RA?

«Классический» аудит предполагает независимую проверку соответствия чего-либо (процесса, отчетности и т.д.) известным требованиям (стандартов, нормативных документов и т.д.) и рекомендации по устранению несоответствий. Таким образом, в широком смысле аудит FM&RA можно определить как независимый процесс оценки эф-

фективности функционирования FM&RA или ее отдельных частей и разработки мероприятий по устранению неконтролируемых существенных рисков потери выручки.

Чему должен соответствовать эффективный FM&RA? В FM&RA предпринимаются попытки внедрения стандартов (на основе лучших практик). Вспомним такие известные стандарты как TM Forum («TR 131», «GB 941») и GRAPA («The Revenue Assurance Standards»). Одновременно с этим, так как сама функция FM&RA является частью системы внутреннего контроля оператора за выручкой, для нее актуальными являются также и стандарты внутреннего контроля и управления рисками (COSO, FERMA и т.д.).

Таким образом, проведение аудита FM&RA должно выявить те несоответствия стандартам и практикам в системе FM&RA, управлении рисками и внутреннем контроле, которые снижают эффективность функции и не позволяют контролировать все существенные риски потери выручки. Например, в результате аудита FM&RA у оператора связи может быть обнаружено отсутствие регулярного контроля за полнотой формирования записей о совершенных вызовах (далее, xDR) на уровне коммутационного оборудования. Тогда, в результате сбоя или ошибок настроек и не формирования xDR, тарификация вызовов производиться не будет. Оператор данную ошибку сможет обнаружить только после существенного роста бесплатного трафика (более 10-15% от всего трафика). В финансовой отчетности это отразится в виде отсутствия роста или падения выручки компании (если это падение не компенсируется ростом выручки по другим коммутаторам).

Каковы основные различия у компаний, предлагающих услугу аудит FM&RA?

Как правило, если вы диагностировали признаки проблемы (ответили на вопрос — зачем нужен аудит FM&RA), то дальнейшее ее решение собственными силами организации может быть достаточно сложным в силу:

- отсутствия достаточных компетенций в проведении аудита FM&RA;
- необходимости дополнительных затрат (трудовые ресурсы, программно-аппаратные доработки, консультации экспертов и т.д.);

Согласно исследованиям всемирной Ассоциации по борьбе с мошенничеством в телекоммуникациях (Communications Fraud Control Association, CFCA), в 2005 году потери отрасли электросвязи от этого вида преступлений составили \$54,4-660 млрд. За три года эта цифра выросла на 52% и составила около \$90 млрд. Эксперты Ассоциации указывают, что в 2007 году убытки от мошенничества составляли 5% совокупного оборота всех операторов мира. Пару лет назад значение данного показателя было вдвое меньшим. В российских компаниях связи, по мнению некоторых аналитиков, потери от мошенничества достигают 10%

операционной выручки. Однако в лидеры мы все же не попали. По данным CFCA, максимальный размах мошенничество приобрело в Пакистане, на Филиппинах, Кубе, в Индии и Бангладеш. Ассоциация опросила операторов связи в разных регионах и получила удручающие результаты: 85% респондентов заявили, что их потери от мошенничества увеличились или остались на прежнем уровне. Почти половина (47,3%) глобальных потерь от этих преступных действий обусловлена махинациями в момент идентификации пользователей.

<http://netfraud.ru/publication/ttk/2>

- ограниченности времени на решение проблемы (например, если проблема затрагивает выручку компании, то чем дольше будет длиться ее решение, тем больше выручки компания недополучит/потеряет).

Поэтому для более эффективного достижения необходимого результата возможно привлечение консалтинговой компании.

«Классическая» схема аудита, применяемая большинством консалтинговых компаний, включает следующие основные этапы:

1. **Подготовительный.** Сбор и анализ информации о существующей функции FM&RA оператора, ее целях и задачах, месте и роли в организации, стратегии развития, используемых методиках и ключевых показателях эффективности. Кроме этого необходимо изучить потоки выручки, генерируемые компанией, и ИТ-решения, применяемые для этого и т.д.
2. **Планирование аудита.** После анализа полученной на предыдущем этапе информации и с учетом целей и задач предстоящего анализа составляется план и детальная программа аудита FM&RA (выбираются его целевые области и направления).
3. **Проведение аудита.** Проводится анализ и оценка отобранных на предыдущем этапе областей рисков, а также существующих контролей. Общие для различных видов аудита методики включают:
 - выборочные тесты (например, проверка того, что предупреждения, которые создаются в контрольной системе, кто-то обрабатывает);
 - опросы и наблюдения;
 - «чек-листы» (проверка наличия/отсутствия у оператора того, что написано в стан-

дарте. Например, наличие документально оформленных процедур контроля).

4. **Завершение и оформление результатов аудита.**

Но, несмотря на общие положения, тем не менее, услуги аудита FM&RA существенно отличаются у различных консалтинговых компаний.

Консалтеры могут отличаться имеющимися компетенциями в FM&RA. Специалисты компании либо имеют практический опыт длительной работы в подразделениях FM&RA операторов связи, либо используют только рекомендации различных стандартов.

Различия также могут лежать в сфере используемых методик. Некоторые консалтинговые компании помимо общих могут применять и специальные методы, «заточенные» под определенные виды фрода и потерь доходов, которые не выявляются *группами методов аудита*.

Так, например, компания «Инфосистемы Джет» использует в своих проектах следующие специальные методы, которые основаны на опыте реализованных проектов, лучших практиках и стандартах аудита FM&RA (например, TM Forum, COSO, FERMA):

1. выгрузка и сверка данных по собственным алгоритмам из различных систем оператора;
2. прямые тесты систем оператора – совершение тестовых вызовов для определения реальных маршрутов терминирования, потерь записей о вызовах и корректности тарификации;
3. тесты на проникновение (или «пентесты») – дружественные попытки взлома офисных АТС (или PBX) клиентов фиксированного оператора связи для определения незащищенного выхода на телефонную сеть общего пользования.

В основе методики компании «Инфосистемы Джет» для обнаружения некорректной терминции¹ трафика лежит следующий способ тестирования: осуществление большого количества тестовых звонков из различных точек России, СНГ и дальнего зарубежья, совершаемых как с сетей фиксированной и мобильной телефонии, так и через VoIP-провайдеров.

По завершении тестирования эксперты компании собирают и при помощи специализированного программного продукта анализируют протоколы состоявшихся тестовых соединений. В результате формируется детальный отчет о маршруте каждого тестового звонка.

Это позволяет выявить точки некорректной терминции, через которые на сеть направлялись существенные объемы входящих МН/МГ-вызовов под видом местных звонков, что является нарушением порядка пропуска трафика, регламентированного условиями действующих договоров о присоединении.

Таким образом, вы можете получить полную картину происходящего, включая те сведения, которые невозможно выявить с помощью стандартных методик проведения аудита.

И, конечно же, консалтинговые компании отличает друг друга опыт реальных проектов в FM&RA.

Подводя итог, отметим, что рассмотренные в данной статье вопросы к проведению аудита FM&RA направлены на то, чтобы компании, принявшие решение о проведении такого проекта, смогли наиболее правильно и четко определить цели и задачи аудита, грамотно подойти к выбору консалтинговой компании, обладающей лучшим набором характеристик, необходимых для качественного выполнения задания. Все эти факторы призваны помочь оператору связи с наименьшими для себя потерями и наиболее эффективно реализовать проект аудита FM&RA.

¹ Некорректная терминция - завершение звонков на сеть оператора связи, выполненное с нарушением действующих нормативно-правовых актов, договорных отношений между операторами связи и/или экономических интересов оператора.

Создание единой системы розничных продаж на платформе SAP CRM для Уральского Банка Реконструкции и Развития

О заказчике

Уральский Банк Реконструкции и Развития — ровесник современной банковской системы России. Сегодня УБРИР является одним из лидеров рынка финансово-кредитных услуг УрФО, входит в первую сотню российских банков.

Задачи

В 2000 году УБРИР становится членом международных платежных систем MasterCard Europe и VISA Int. С 2004 года, когда была принята концепция развития розничного банка, УБРИР активно растет. Открываются новые офисы продаж, увеличивается число клиентов, расширяется спектр услуг. Большое внимание Банк уделяет повышению лояльности клиентов: улучшению качества обслуживания, созданию индивидуальных схем работы. В 2005 году после внедрения ERP-системы от SAP Банк запланировал переход на новый уровень взаимоотношений с клиентами. Это стало логичным продолжением реализации стратегии Банка, направленной на повышение прозрачности и управляемости всех бизнес-процессов.

Проект по созданию единой системы розничных продаж на базе SAP CRM стартовал в 2005 году — это первое внедрение SAP CRM для банков в России.

Партнером по внедрению была выбрана компания «Инфосистемы Джет». К моменту старта проекта у обеих компаний уже был опыт совместной работы — общая «история успеха». Кроме того, в компании «Инфосистемы Джет» сложилась профессиональная команда специалистов, обладающая знаниями не только в области ИТ, но и в банковской сфере.

Решение

У проекта было несколько основных целей: создание единой системы розничных продаж, увеличение числа продаж банковских продуктов, повышение качества обслуживания клиентов. Работа над проектом строилась, исходя из этих целей, и была разбита на четыре крупных этапа. Каждый из них обладал завершенностью и самостоятельной ценностью, этапы шли с некоторым наложением друг на друга.

«Это был первый проект подобного рода и масштаба в России. На момент подписания договора с УБРИР у нас даже не было детального технического задания. Многие трудности, которые присущи таким масштабным проектам, проявились и здесь. Но нам удалось справиться с поставленной задачей. Во-первых, благодаря активному участию всех заинтересованных подразделений на всех этапах реализации проекта. Во-вторых, в подобных проектах очень важно, чтобы обе стороны понимали задачу одинаково, чтобы совпадали взгляды на уровне идеи, на уровне концепции. Совместно нам удалось создать такую эффективную команду единомышленников. И конечно, знания и опыт специалистов обеих компаний позволяли быстро находить решение текущих задач, в том числе нетривиальных», — отметил Константин Казаков, директор Центра банковских технологий компании «Инфосистемы Джет».

Единая база клиентов

К моменту старта проекта количество клиентов УБРИР достигло полумиллиона, насчитывалось более 50 офисов продаж, которые работали со всеми клиентами по одной схеме. При этом Банк одновременно использовал несколько автомати-

зированных банковских систем (АБС), в каждой из которых велась своя база клиентов.

На первом этапе проекта специалисты Банка и компании «Инфосистемы Джет» создали единую базу клиентов (ЕБК), где была консолидирована информация обо всех клиентах Банка. Для этого был разработан модуль очистки данных, загружаемых из внешних источников. Этот модуль, помимо обеспечения корректности занесения атрибутов клиента Банка и его адресной информации, позволил выявлять и обрабатывать дублирование записей о клиенте. Модуль интеграции обеспечил синхронизацию информации о деловых партнерах Банка со всеми автоматизированными банковскими системами.

Также на этом этапе проекта была решена задача интеграции общероссийского справочника адресов (классификатор адресов России — КЛАДР) и SAP CRM. Сотрудники компании «Инфосистемы Джет» разработали и реализовали уникальное для российского рынка решение, которое позволяет загружать и обновлять справочник адресов SAP CRM, используя КЛАДР.

В результате проделанной работы создана единая клиентская база и единый профиль по каждому клиенту. Независимо от места или способа обращения в офис продаж, клиенты Банка обсуживаются теперь по определенному в соответствии с клиентским сегментом алгоритму, получают полный необходимый набор услуг и уровень обслуживания, соответствующий единым высоким стандартам Банка.

Единое место продаж

Следующим этапом проекта стала организация «Единого места продаж» (ЕМП). ЕМП позволяет выполнять полный набор операций по обслуживанию физических лиц от открытия вклада до перевыпуска пластиковой карты. Ранее при обработке запросов клиента операционисты УБРИР пользовались различными банковскими приложениями — «Кредиты», «Вклады и депозиты», «Пластиковые карты», — и это существенно увеличивало время обслуживания клиентов. С помощью нового унифицированного интерфейса специалист получает полную информацию о клиенте (данные, история взаимоотношений, договоры и пр.) и может быстро и четко произвести все необходимые операции по его обслуживанию. Помимо повышения скорости и качества обслуживания клиентов, ЕМП позволило избавиться операционистов и других сотрудников фронт-зоны от выполнения рутинных операций.

«Раньше операционисту приходилось знать и помнить фактически весь перечень продуктов Банка и набор услуг, условия и характеристики каждого продукта. Теперь этого не требуется — система подскажет и выведет на экран всю необходимую информацию. Сотруднику нужно уметь поддержать разговор с клиентом, при необходимости предоставить дополнительную информацию. И конечно, быть приветливым», — комментирует Юрий Миронов, вице-президент, директор департамента операций, банковских и информационных технологий, ОАО «УБРИР».

На этом этапе было также разработано уникальное решение — интерактивные сценарии, — позволяющее правильно выстроить диалог с клиентом. Предварительно настроенные интерактивные сценарии включают такие функции, как информирование клиента о продуктах и услугах (в соответствии с его профилем и на основе сведений об истории его взаимоотношений с Банком), сбор необходимой информации, поиск оптимального предложения и т.д. Внедрение этого решения привело к существенному повышению качества сервиса, а также позволяет Банку выдерживать корпоративные стандарты обслуживания клиентов.

«Очень важным результатом проекта стало соединение операционного и аналитического CRM в точке продаж. Аналитики УБРИР, используя мощный инструментарий, базирующийся на возможностях аналитического хранилища, могут выделять различные клиентские целевые группы, определять уникальные для данных групп продуктовые предложения и создавать для каждой группы сценарии взаимодействия, которые будут использованы сотрудником точки продаж при взаимодействии с клиентом. Данный подход позволяет делать клиентам предложение, которое они ожидают от Банка, что повышает и уровень лояльности клиентов к Банку и, соответственно, объем продаж», — отметил Илья Небесный, директор Департамента прикладных финансовых систем компании «Инфосистемы Джет».

Помимо прочих преимуществ, решение «Единое место продаж» позволяет Банку минимизировать затраты на проведение дорогостоящих тренингов для сотрудников: в случае ввода нового банковского продукта или маркетинговой программы легко настраивается новый сценарий, и

работа продолжается в привычном режиме. Все настройки сотрудники Банка могут выполнять самостоятельно.

Бизнес-аналитика

Следующим этапом проекта стало внедрение хранилища данных на платформе SAP BW; были интегрированы аналитическая система и CRM-система, создан ряд аналитических отчетов. На базе хранилища данных производится анализ финансовых результатов и готовится необходимая информация для принятия управленческих решений.

Юрий Миронов подчеркнул: *«Мы очень быстро почувствовали пользу от инструментов аналитики. Например, перед запуском одной из маркетинговых акций мы решили протестировать ее действие на небольшой группе клиентов. За короткий промежуток времени нам удалось выявить негативную реакцию и скорректировать планы».*

Аналитические приложения позволили Банку также получить ясное представление, каким образом влияют на поведение клиентов новые экономические условия, и оперативно отреагировать на изменения. Например, Банк внес корректировки в маркетинговую стратегию, что позволило не только сохранить, но и приумножить количество частных и корпоративных клиентов в непростых экономических условиях.

Маркетинг

Завершающим этапом проекта стало внедрение модуля «Маркетинг». У маркетологов УБРиР появился инструмент для анализа и сегментации клиентской базы, планирования, настройки и проведения маркетинговых кампаний. Кроме того, сотрудники фронт-офиса получили возможность регистрировать отклик клиента на маркетинговые сообщения и предлагать ему услуги Банка, которые в наибольшей степени соответствуют его потребностям. Маркетинговые кампании стали более адресными, эффективными и менее затратными. Возможности, заложенные в CRM, позволяют делать проактивные предложения для клиентов в ходе их обращения в Банк. Это приносит существенную экономию.

Результат

Внедрение CRM позволило Банку существенно повысить конкурентоспособность, лучше понимать потребности клиентов и, главное, предоставить качественные и доступные услуги. Теперь специалисты Банка разрабатывают продукты и услуги, не просто опираясь на клиентские предпочтения, но и во многом превосходя их.

Изначально целью проекта было не только внедрение очередного ИТ-приложения, а перестройка системы управления взаимоотношениями с клиентами. Стоимость привлечения нового клиента, стоимость удержания действующего клиента, оборот на одного клиента — лишь некоторые из показателей, которые рассматривались при расчете финансовой составляющей проекта и сроков окупаемости. Согласно предварительным расчетам, проект должен был окупиться в течение 2-х лет.

«По результатам опытной эксплуатации в Банке были произведены уточнения в расчетах. Срок окупаемости составил 1 год. Это еще раз подтверждает правильность выбранной стратегии реализации данного проекта. Мы гордимся тем, что одними из первых среди российских компаний осознали необходимость такого проекта. Правильность концепции, которую мы разработали по CRM, подтвердилась по прошествии времени не только результатами работы нашего банка, но и тем, что во многих решениях новых версий CRM большинства разработчиков ПО реализуется то, что мы для себя приняли несколько лет назад», — подчеркнул Юрий Миронов.

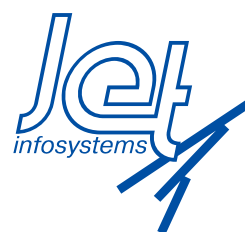
«Для организации работы с клиентами УБРиР использует лучшие технологические решения — такой подход демонстрирует высокий уровень зрелости компании, нацеленной на создание долгосрочных конкурентных преимуществ. Для нашей компании это был сложный, инновационный, но интересный проект», — отметил Константин Казаков.

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Главный редактор: Дмитриев В.Ю.
Редактор: Слободчикова Т.А.
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su <http://www.jetinfo.ru>



Издатель: компания «Инфосистемы Джет»

Подписной индекс по каталогу Роспечати

32555

Полное или частичное воспроизведение материалов, содержащихся в настоящем издании, допускается только по согласованию с издателем