Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№7 (252)/2014

АНТИФРОД: ВСЕ ТАЙНОЕ СТАНОВИТСЯ ЯВНЫМ

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Редакция:
Дмитриев В.Ю.
vlad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Шедова Е.Л.

Дискина А.Л.
ashklyaeva@jet.msk.su

Верстка:
Кулешова Ю.В.

Корректура:
Макеева Е.И.

Над номером работали:
Жильцов Е.С.
Наумов Д.А.
Сергацков В.А.
Сизов А.Ю.

Издатель:
Компания
«Инфосистемы Джет»

Контакты:
тел.: (495) 411-76-01
http://www.jetinfo.ru

АЛЕКСЕЙ СИЗОВ,
руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»

Любая средняя или крупная компания в процессе своей работы сталкивается со множеством проявлений мошенничества. Способы реализации хищений различны, векторы атак неоднородны, едина лишь цель злоумышленников — хищения товарной продукции и денежных средств. Это неизбежно приводит либо к прямым убыткам, либо к недополучению прибыли от текущих продаж товаров и услуг. Так, риски мошенничества для компании enterprise-сегмента оцениваются в сотни миллионов рублей в год.

Где и как искать признаки и факты злоупотреблений и прямого воровства? Что нового изобретают злоумышленники в условиях сегодняшних принципов ведения бизнеса? Как обеспечить функциональную и процессную эффективность работ по борьбе с мошенничеством? Как добиться получения прибыли от развития функции противодействия мошенничеству? Ответить на эти и другие подобные вопросы — вот цель нашего номера.

СОДЕРЖАНИЕ

6 ОДИНАКОВО РАЗНОЕ МОШЕННИЧЕСТВО
АЛЕКСЕЙ СИЗОВ

8 А СЛОНА В КУСТАХ И НЕ ЗАМЕТИЛ…
АЛЕКСЕЙ СИЗОВ

10 НЕ ТУШИТЕ ПОЖАР ПИРОГАМИ
ДМИТРИЙ НАУМОВ

15 ВАКЦИНА ДЛЯ ТЕЛЕКОМ-ОПЕРАТОРОВ
ВАСИЛИЙ СЕРГАЦКОВ

3 От редакции

5 Новости

33 В тему номера

21 ПОЙМАЙ МЕНЯ, ЕСЛИ СМОЖЕШЬ
АЛЕКСЕЙ СИЗОВ

23 ОЛЕНЕВОДЫ В ПРЕДЕЛАХ САДОВОГО КОЛЬЦА
ЕВГЕНИЙ ЖИЛЬЦОВ

26 СКАЖИ МНЕ, КТО ТВОЙ ВРАГ…
АЛЕКСЕЙ СИЗОВ

30 МАТЕМАТИКА НА СЛУЖБЕ У АНТИФРОДА
АЛЕКСЕЙ СИЗОВ

Jet Info — лучшее клиентское издание в ИКТ-отрасли

Наш журнал победил в конкурсе корпоративных медиа ICT CORPORATE MEDIA AWARDS, участниками которого были несколько десятков изданий. Об этом рассказывает **ЕЛЕНА ШЕДОВА,** директор по маркетингу компании «Инфосистемы Джет»:

«Конкурс корпоративных медиа, организованный в июне 2014 года издательской группой ComNews, был призван выделить яркие и успешные СМИ ИКТ-отрасли, а также отметить успехи редакционных команд. Получив предложение поучаствовать в конкурсе, мы ни секунды не медля решили номинироваться на "Лучшее клиентское издание".

На первом, отборочном, этапе предстояло заполнить весьма внушительную заявку — подробное описание, достижения за последние годы, тематический план, рубрикатор, а также приложить отзывы заказчиков и партнеров. Через несколько дней, после пристального анализа всех пришедших заявок, конкурсная комиссия сообщила, что Jet Info прошел во второй тур и вошел в шорт-лист в своей «весовой категории». Оценивали такие критерии, как информационная насыщенность, визуализация, интерактивность, инновационность, медиапотенциал. Нашими соперниками стали "Outlook Аксенчер Россия" (Accenture) и "Резонанс-Ростов" (Ростовский филиал ОАО "Ростелеком").

Второй тур конкурса предусматривал краткую презентацию на II Стратегическом форуме "PR-Вектор. Развитие внешних

и внутренних коммуникаций в сфере ИКТ". На этот раз в качестве жюри выступили более 200 участников форума — ведущих экспертов ИКТ-отрасли — сотрудников пресс-служб, департаментов внешних и внутренних коммуникаций телеком-, digital- и ИТ-компаний, коммуникационных агентств и деловых СМИ.

Мы решили, что сделаем видеоролик с кодовым названием "20 лет за 150 секунд" и расскажем, как менялся Jet Info с 1994-го — года его основания — по наши дни. По результатам интерактивного голосования, организованного прямо во время форума, 75% аудитории отдали свои голоса Jet Info.

Победа в конкурсе — это официальное признание нашего журнала как одного из эталонов корпоративной ИКТ-публицистики. Но не менее приятно получать неофициальные отзывы: мы часто слышим от заказчиков и партнеров, что Jet Info является их "настольной книгой". Журнал меняется вместе с рынком. При этом наши принципы остаются неизменными — мы говорим о действительно "горячих" темах, наболевших проблемах и предлагаем реальные способы их решения». JI

ОДИНАКОВО РАЗНОЕ МОШЕННИЧЕСТВО

Честный и мошенник просто путают понятия «мое» и «твое». Один считает первое за второе, а другой — второе за первое.

Г. Лихтенберг

АЛЕКСЕЙ СИЗОВ,
руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»

Мошенничество многолико — оно принимает различные формы в зависимости от компании, в которой имеет место. В то же время итог всегда один: прямые финансовые потери денежных средств или товарной продукции, высокий объем недополученной прибыли, потери клиентов или партнеров. Последнее является весовым репутационным риском в условиях жесткой конкурентной среды. Наш опыт показывает, что соотношение прямых убытков и недополученной прибыли сильно зависит от отраслевой специфики компании (см. рис. 1–3). При этом совокупные объемы мошенничества составляют от 2 до 5% от операционной прибыли.

Мы, общаясь с десятками компаний из разных вертикальных рынков, видим различное отношение к мошенничеству. Одни принимают этот риск как неотъемлемую часть бизнеса, отводят на него весомую долю потенциальной прибыли и не инвестируют в развитие процессов защиты. Другие характеризуют противодействие хищениям как непримиримую борьбу: ее цели и задачи неразрывно связаны с принципом

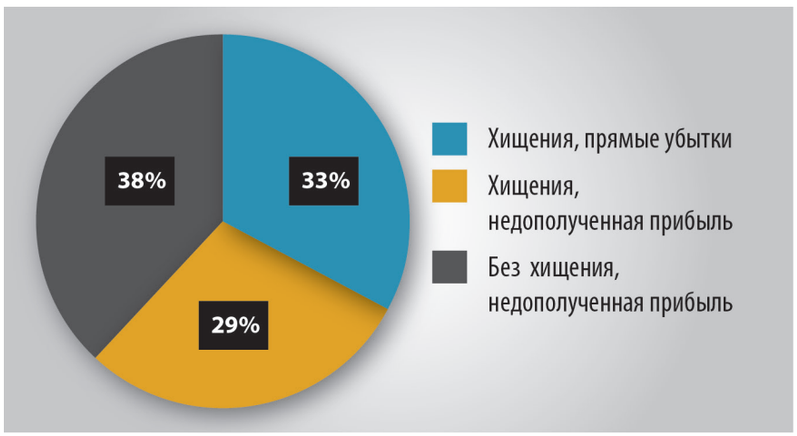


Рис. 1. Мошенничество в продуктовом ритейле

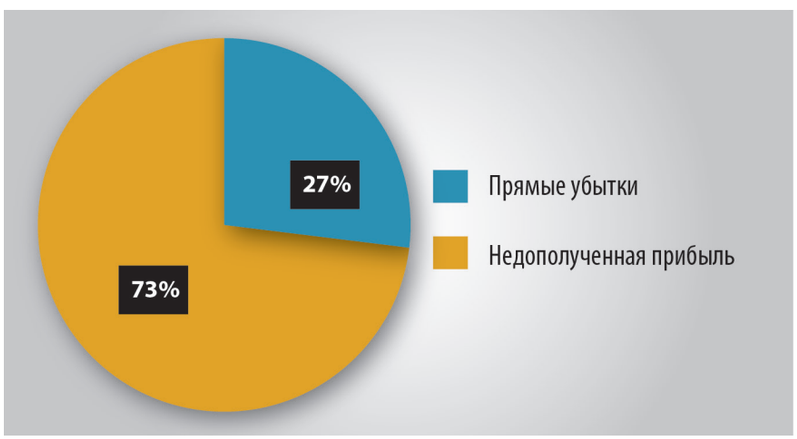


Рис. 2. Мошенничество у операторов связи

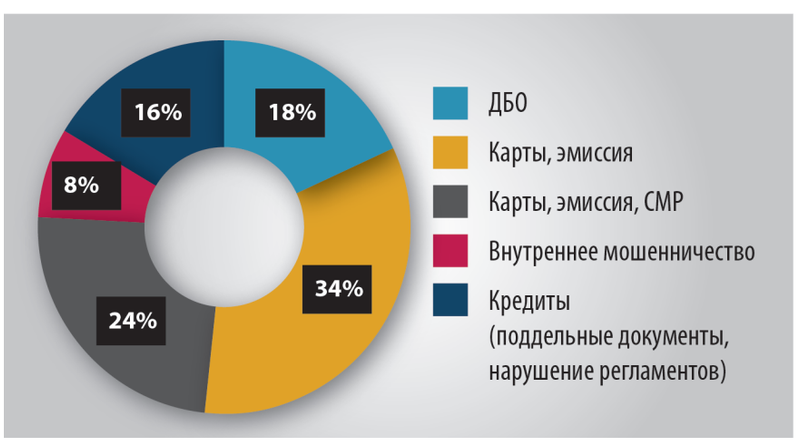


Рис. 3. Банковский фрод

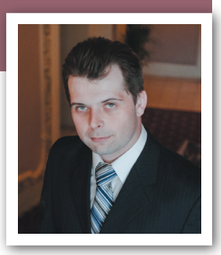
получения прибыли, а результат влияет на жизнеспособность компании. Но главное, что мошенничество само по себе — редко отрицаемый факт.

Можно констатировать, что внедрение средств и технологий борьбы с мошенничеством лишь по одному направлению деятельности компании в 99% случаев является инвестицией в увеличение прибыльности всей организации. Как правило, суммарные затраты на приобретение и внедрение системы, а также на обслуживающий или эксплуатирующий персонал покрываются за 8–9 месяцев ее работы. Другими словами, положительный экономический эффект достигается уже в первый год полноценной эксплуатации.

Но целью внедрения автоматизированных систем по борьбе с мошенничеством сегодня является не только снижение объема хищений. Эффективность решения может заключаться и в автоматизации текущих процессов предотвращения мошенничества (что приводит к сокращению штата, снижению влияния человеческого фактора на процессы защиты), и в повышении оперативности механизмов контроля (это позволяет внедрять новые услуги и, в конечном итоге, осваивать новые сегменты рынка).

На базе таких систем можно выстраивать комплексные процессы по контролю над мошенничествами и злоупотреблениями в рамках всех бизнес-процессов компании, а значит, формировать независимый контур безопасности бизнеса. Он будет обеспечивать «надзор» за всеми критичными процессами движения денежных средств и товарной продукции, обслуживания клиентов и внутрихозяйственной деятельности. JI

А СЛОНА В КУСТАХ И НЕ ЗАМЕТИЛ…



АЛЕКСЕЙ СИЗОВ,
руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»

Компании, оказывающие услуги физическим или юридическим лицам, т.е. имеющие большую клиентскую базу, сталкиваются с мошенничеством практически каждый день. Это кредитно-финансовые и микрокредитные организации, операторы платежных услуг, телекомоператоры и др. Активы клиентов — вот самый лакомый кусок для злоумышленников. В то же время ловить рыбу в мутной воде могут и клиенты, что приводит к убыткам уже самой компании. Большинство компаний в таких условиях стараются держать оборону — выстраивают технологический/организационный/нормативный уровни защиты. Но всегда ли она эффективна?

Периодически в СМИ появляется информация о фактах задержания злоумышленников, похищавших реквизиты банковских карт, ключи доступа к личным кабинетам, идентификационную и аутентификационную информацию. Нередки случаи и прямого взлома сервисов ДБО и электронных площадок. Казалось бы, пресечение деятельности таких организованных преступных группировок доказывает эффективность работы правоохранительных органов, а также корпоративных служб безопасности. Все было бы так, если бы не буйная фантазия злоумышленников, изобретающая все новые варианты атак, взломов и т.д.

Согласно официальной статистике VISA за 2013 год, объем мошенничества по банковским картам в России составляет более 50 млн руб.[1],

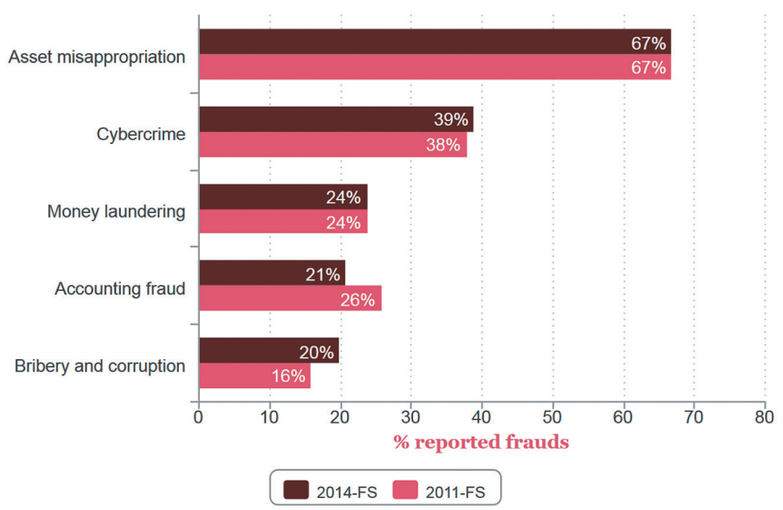


Рис. 1. ТОП 5 видов экономических преступлений, с которыми сталкивается сектор

[1] *http://www.klerk.ru/bank/news/331073/*

по оценке наших экспертов, эта сумма уверенно переваливает за 1 млрд руб. PricewaterhouseCoopers[2] констатирует, что объем мошеннических операций из года в год увеличивается с завидным постоянством. По оценкам того же аналитического агентства[3], в 2011 году от действий мошенников в России могли пострадать порядка 40% компаний.

К сожалению, такая ситуация объясняется 2 ключевыми факторами. Во-первых, если клиент со своей стороны не заботится о безопасности, он рано или поздно обязательно столкнётся с мошенничеством. Например, он может фокусироваться на формальном подтверждении банковской операции и не уделять должного внимания простым признакам, указывающим на факт мошенничества.

Во-вторых, некоторые компании стараются удовлетворять лишь требованиям регуляторов, минимально вкладываясь в безопасность клиентов. Причин здесь может быть несколько:

- Недостаток финансирования ИБ: бизнес считает безопасность «расходным подразделением» и не готов вкладывать средства.
- Сомнения в окупаемости внедрения антифрод-системы. Встречается мнение, что стоимость решения не должна превышать текущего объема убытков от мошенничества. С этим можно согласиться при условии, что точкой отчета будет не текущий убыток, а общая оценка рисков.
- Сложность внедрения. Большая часть антифрод-систем нуждается в глубокой интеграции для соответствия высоким требованиям бизнеса и предотвращения мошенничества в момент его непосредственного совершения. При этом серьезная модернизация продуктивных систем — процесс весьма трудоемкий, зачастую он не обходится без привлечения нескольких подразделений компании и производителей решений.
- Недостаток ресурсов. Как показывает многолетний опыт, ни одна служба безопасности не может похвастаться наличием «свободных», достаточно подготовленных специалистов, которые могли бы организовывать периодическую перестройку систем защиты бизнеса.

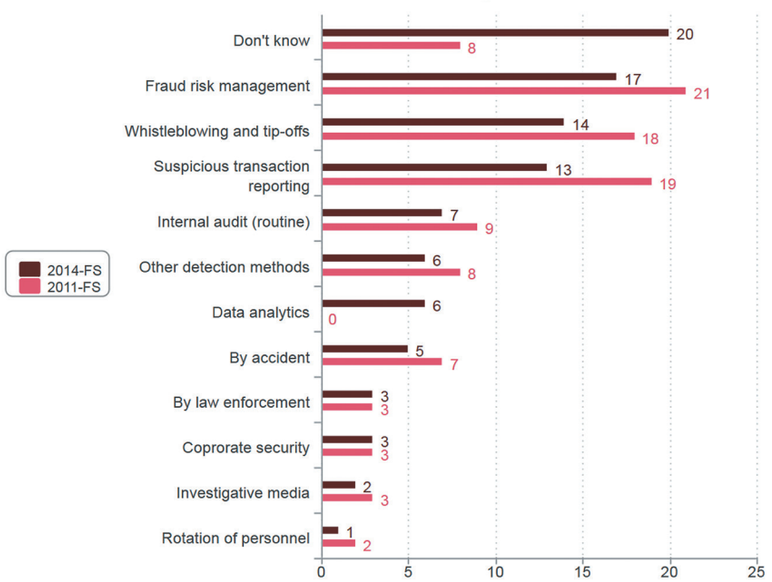


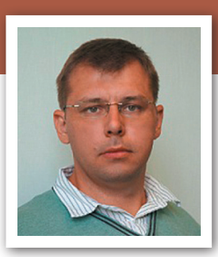
Рис. 2. Методы выявления экономических преступлений

> Отметим, что бизнес таких вроде бы разных компаний, как банки и телеком-операторы, стал очень близок по характеру некоторых оказываемых услуг. Поэтому данные организации зачастую используют идентичные системы и успешно масштабируют их функционал на новые сферы своей деятельности.

Так можно ли эффективно бороться с мошенничеством в условиях таких ограничений и оправданы ли вложения в антифрод-системы? По нашему опыту, да. Более того, развитию систем защиты от мошенничества во многом способствовало именно развитие бизнеса. Сегодня анализ $^{3}/_{4}$ клиентских операций должен проводиться online (а иначе будет нечего спасать), необходимо консолидированно контролировать все каналы обслуживания клиентов: от личного кабинета (интернет-банка или сервиса управления услугами) до операторов call-центра. В последующих статьях мы более подробно рассмотрим обозначенные нами отрасли — банки, телеком — с точки зрения реализации мошенничества и эффективной борьбы с ним. JI

[2] *http://www.pwc.com/gx/en/economic-crime-survey/index.jhtml*
[3] *www.computerra.ru/85084/fraud-bigdata/*

НЕ ТУШИТЕ ПОЖАР ПИРОГАМИ



ДМИТРИЙ НАУМОВ,
эксперт направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»

За последние 10 лет произошли существенные изменения в технологиях защиты банковских счетов и карт наших сограждан: токенизация юридических и физических лиц, распространение стандарта EMV (Europay + MasterCard + VISA), рост объемов операций с поддержкой технологий Verified by Visa и MasterCard SecureCode для обеспечения защиты интернет-транзакций. В то же время приходится констатировать, что в большинстве случаев внедряемые технологии являются не механизмами снижения рисков компании, а, скорее, попыткой потушить пожар, который разгорелся несколько лет назад и продолжает бушевать. Вспоминается стихотворение Корнея Чуковского, в котором огонь пытаются тушить не очень пригодными для этого средствами. Правда, в нашем случае инструменты ИБ становятся непригодными вследствие безграничной человеческой изобретательности. Дело в том, что злоумышленники постоянно «пишут» все новые сценарии мошенничества, прибегают к комбинированию известных схем, например:

- Friendly Fraud — операции, совершенные с применением легитимного платежного средства и/или его реквизитов аффилированным лицом (родственник, друг и т.д.).
- Кража средств и реквизитов, в том числе с применением методов социальной инженерии. Как следствие, мошенники с легкостью проходят любые проверки пользователя — кодовое слово, паспортные данные и пр., иногда такие операции совершают сами клиенты по указке злоумышленников.
- Использование вирусов и другого вредоносного ПО, инициирующего нелегитимные операции с рабочих мест пользователей.

Следует отметить, что одни виды мошенничества, такие как неправомерные операции по картам или каналам ДБО, являются вероятными рисками потерь, тогда как другие — кредиты и внутреннее мошенничество — в 95% случаев представляют собой фактические убытки. Потенциальные потери для канала ДБО банка из ТОП 15 в случае успешной реализации всех попыток мошенничества составляют 300–450 млн руб. в год, объем неправомерных CNP-операций (Card not present) — от 200 до 700 млн руб. в год в зависимости от применяемых технологий защиты.

КАКИМ ТЫ БЫЛ, ТАКИМ ТЫ И ОСТАЛСЯ

Поговорим о фрод-проблемах, которые в настоящий момент стоят перед банками, более подробно. Сегодня практически любой вид банковского фрода с высокой долей вероятности не будет оперативно детектирован классической системой обеспечения безопасности или выявления мошенничества. Дело в том, что схема анализа исключительно платежных транзакций на уровне АБС может отрабатывать только «медленные» операции, скорость исполнения которых на стороне банка или оператора ограничена спецификой технологий. Но бизнес сегодня требует режима real-time. И это относится не только к платежным операциям. Если 7 лет назад срок одобрения потребительского кредита мог составлять 3–5 рабочих дней, то сегодня банки дают на него «добро» за то время, пока покупатель идет от витрины до кассы.

Само мошенничество стало изощрённее, и только по характеру операции зачастую нельзя понять, насколько высок риск платежа.

В то же время в любой компании существует весомое количество регламентов действий при возникновении фактов мошенничества и сложившихся процедур взаимодействия подразделений. Прибавьте сюда требования к непрерывности

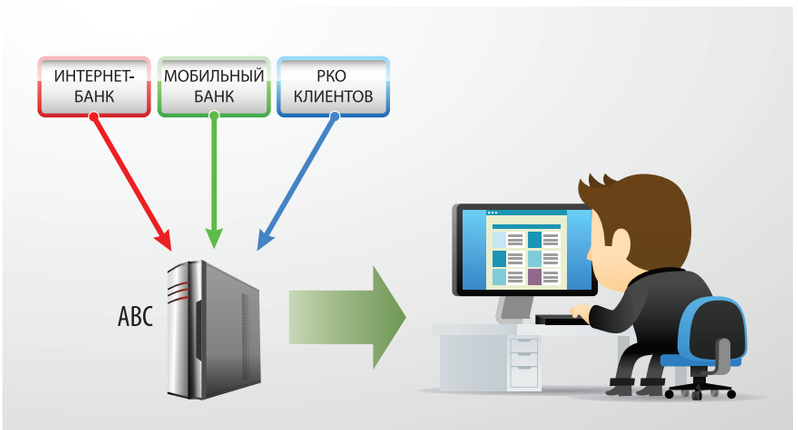


Рис. 1. Ручной анализ поступающих событий (изжил себя еще на заре формирования бизнеса ДБО и банковских карт)

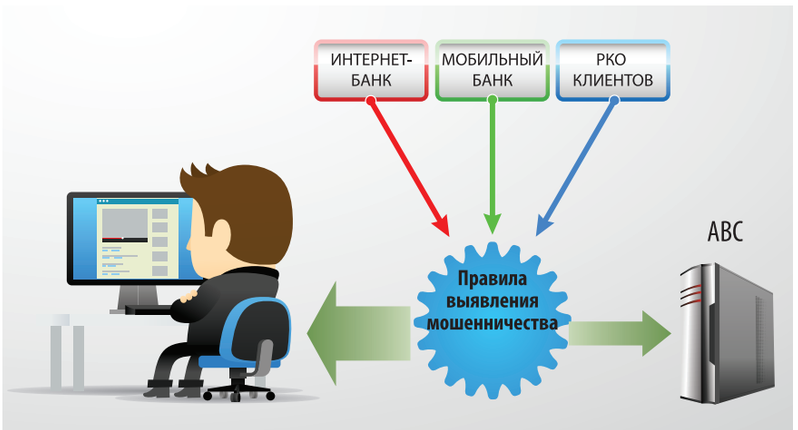


Рис. 2. Rule-based модели (все еще применяются в некоторых банках, формируют лишь оповещения о мошенничестве, запускающие внутреннюю машину расследований и процедур взаимодействия)

Приведем еще один пример того, что сложившиеся практики мало удовлетворяют требованиям: классический мониторинг операций по картам является обязательным для банков с 2003 года (вступление в силу требований Visa по мониторингу эмиссии и эквайринга). Но тот же эквайринг в своем развитии ушел далеко вперед, и сегодня транзакция по карте – это максимум 25% требуемой информации, особенно для обслуживания карт в интернете. Для формирования целостной картины банкам приходится дорабатывать существующие процессинговые системы, чтобы можно было анализировать параметры самой покупки, базовые элементы идентификаторов пользователя и пр. Решение этой задачи для многих компаний оборачивается заменой устаревшего ПО процессинга масштабируемыми и гибкими инструментами.

бизнеса, стандарты обслуживания клиентов. Все это накладывает дополнительные ограничения на реализацию средств защиты от мошенничества.

АХ, ЕСЛИ БЫ СБЫЛАСЬ МОЯ МЕЧТА

Какой же должна быть современная комплексная антифрод-система? Во-первых, она должна давать возможность открытого построения бизнес-правил, профилирования клиентов, обладать механизмами контроля среды выполнения операций (ПК/гаджет), быть самообучаемой. Во-вторых, необходима всеохватность: способность контролировать как кроссканальные атаки на клиента, так и операции, осуществляемые через операционные подразделения, call-центр. Последнее становится особенно важным в свете набирающего обороты внутреннего мошенничества. Контроль его реализации подразумевает «надзор» за несколькими взаимосвязанными процессами: за действиями операционного сотрудника и последующими операциями, совершаемыми от имени клиента или даже с использованием реквизитов его платежных инструментов.

В эффективный антифрод-комплекс целесообразно включать такие решения, как:

- систему защиты ДБО юрлиц. Это может быть отдельный модуль в составе ДБО-решения или реализованная схема анализа преимущественно финансовых транзакций на стороне АБС;
- систему защиты ДБО физлиц и мобильного банка (коробочное или кастомизированное решение, иногда система класса Web Application Firewall

(WAF) с ограниченной функциональностью по анализу транзакций);

• систему защиты карточного процессинга: в 99% случаев она представлена модулем от производителя, чье решение отвечает за процессинг, в составе модели мониторинга эмиссии и эквайринга. К сожалению, функции мониторинга интернет-эквайринга могут быть ограничены ввиду отсутствия интеграции с электронными торговыми площадками, идентифицирующими клиента, устройство и обладающими информацией о характере оплаты товара/услуги;

• систему защиты от внутреннего мошенничества (в первую очередь на базе мониторинга активности back-office систем и инструментария call-центров);

• систему оценки и анализа выдачи кредитов, определения связанных заемщиков и др.: на базе специализированного решения или мощного OLAP-инструмента.

Отметим, что это не полный список возможных решений.

Общая цель этих систем — предотвращать факты мошенничества в режиме реального времени, т.е. не просто оперативно выявлять инциденты, имеющие высокий риск реализации хищения, но и блокировать подозрительную активность до момента нанесения ущерба клиенту или компании. Эффективное антифрод-решение активно реагирует на высокорисковые операции вплоть до блокировки любых действий со счетами клиента при наступлении неблагоприятных событий. Прозрачные средства управления обеспечивают (причем в режиме 24/7) возможность изменения логики его работы даже в отсутствие архитектора, главного аналитика и пр. При этом влияние системы на текущие бизнес-процессы сведено к минимуму, а решения, находящиеся с ней в связке, от нее не зависят. Штат сотрудников, осуществляющий анализ подозрительных операций, минимизирован.

Одним словом, компания получает в свое распоряжение инструмент анализа рисков, способный аккумулировать действия разных подразделений, связывать транзакции различных учетных систем, объединять результаты работы прикладных комплексов информационной безопасности, таких как SIEM, Database Security, WAF.

Рис. 3. Идеальная система (работает 24/7, обеспечивает всесторонний анализ проводимых операций, пользователь системы получает лишь уведомления о блокированных случаях мошенничества)

ВЫ ТАК, А МЫ ВОТ ТАК

Теперь подробнее рассмотрим распространенные мошеннические схемы и механизмы противодействия им. Классический сценарий для канала ДБО или электронного кошелька таков: на компьютер клиента внедряется вирус для хищения данных. Если вирус прост, происходит хищение логина/пароля с их последующим использованием на компьютере злоумышленника (конечно, не на собственном, а из контролируемой сети — работа в ней гарантирует невозможность отслеживания). В этих случаях характера операций и реквизитов подключения вполне достаточно для понимания высокой вероятности мошенничества. Но, к сожалению, мошенники учатся на примерах противодействия их атакам, характер формируемых ими операций все более приближен к действиям клиентов, а значит, высока вероятность, что новый профиль атаки может быть пропущен существующим базисом правил анализа транзакций.

Сегодня наиболее сложной с точки зрения обнаружения является схема MITB (Man-in-the-Browser). В этом случае классическая система с обычным набором правил «IP, login, параметры операции» бессильна. И даже OTP (One-Time Password), отправленный клиенту, будет перехвачен, платеж по переводу денег родственнику будет переводом в карман злоумышленнику, а клиент этого и не заметит.

Для контроля такого класса мошенничества в современных

системах мониторинга применяются развитые механизмы анализа среды работы пользователя: рассматриваются все доступные реквизиты ПК, с которого осуществляется операция. Причем происходит это не только при входе пользователя, а более/менее дискретно, чтобы найти точку активации вредоносной программы, перехвата управления клиентской сессией и т.д.

Отличительной чертой наиболее передовых систем является применение механизмов FingerPrint и Trojan Detection — подобные решения имеют активные средства защиты от атак и позиционируются не только как логические инструменты.

Защита 24/7

Ни для кого не секрет: чем сложнее и продуманнее атака, тем больше вероятность того, что она нацелена на конкретную компанию. Многие банки сегодня могут «похвастаться» вирусами, принципы работы которых направлены именно на них. Но мошенники идут дальше. Представьте: подобная атака проводится в ночь с субботы на воскресенье, и текущие механизмы не могут достоверно выявить профиль мошенничества. В рабочее время была бы возможность экспресс-анализа ситуации, внесения корректировок в алгоритмы анализа. А в выходные?

По этой причине принципиальна возможность реализации плавающего управления критериями анализа и обучаемости системы по факту подтверждения мошеннических операций. Сегодня существуют и активно внедряются технологии обучаемости систем мониторинга. Это не простое профилирование клиентов, фокус анализа направлен на резолюции, фиксируемые операторами call-центра, — обработанные претензии. Формируемый массив данных является дополнительным источником для передовых систем, позволяющим контролировать краткосрочную историю обращений, выявлять тенденции и влиять на актуальные параметры детектирования текущих операций как мошеннических.

ОДНИ ВИДЫ МОШЕННИЧЕСТВА, ТАКИЕ КАК НЕПРАВОМЕРНЫЕ ОПЕРАЦИИ ПО КАРТАМ ИЛИ КАНАЛАМ ДБО, ЯВЛЯЮТСЯ ВЕРОЯТНЫМИ РИСКАМИ ПОТЕРЬ, ТОГДА КАК ДРУГИЕ – КРЕДИТЫ И ВНУТРЕННЕЕ МОШЕННИЧЕСТВО – В 95% СЛУЧАЕВ ПРЕДСТАВЛЯЮТ СОБОЙ ФАКТИЧЕСКИЕ УБЫТКИ. ПОТЕНЦИАЛЬНЫЕ ПОТЕРИ ДЛЯ КАНАЛА ДБО БАНКА ИЗ ТОП 15 В СЛУЧАЕ УСПЕШНОЙ РЕАЛИЗАЦИИ ВСЕХ ПОПЫТОК МОШЕННИЧЕСТВА СОСТАВЛЯЮТ 300–450 МЛН РУБ. В ГОД

Такой подход позволяет значительно снизить риск высокого ущерба от принципиально новой схемы мошенничества за счет быстрого реагирования на факт атаки счетов клиентов.

Клиенты не любят, когда борются с ними

К сожалению, любая система имеет погрешность в точности выявления мошенничества, причем объем детектируемого мошенничества прямо пропорционален объему ложных срабатываний, когда решение идентифицирует операцию как высокорисковую при легитимном характере транзакции. Неизбежны случаи, когда система блокирует операцию, которая является для клиента очень важной на текущий момент. Существует схема интеграции, позволяющая операторам call-центра ограниченно управлять логикой работы решения:

- Система мониторинга передает все результаты в back-офисное приложение, тем самым обеспечивается прозрачность осуществляемых действий — оператор call-центра может увидеть причины блокировки/приостановления транзакции.
- Оператор в случае обращения клиента проводит идентификацию по существующим правилам и алгоритмам.
- Если идентификация прошла успешно, проводится проверка принадлежности клиенту транзакции.
- Транзакция относится к списку правомерных.
- Этот статус интерпретируется дополнительным модулем обработки (специализированным сервисом) как информация о временном разрешении транзакции для клиента в соответствии с ее реквизитами.
- Информация о транзакции вносится в белый список временного разрешения, и клиент свободно проводит необходимую ему операцию.

Такой подход позволяет не только органично вписать решение в ИТ-ландшафт банка, но и обеспечивает высокий уровень сервиса, минимизацию негативной реакции со стороны клиентов на факты блокировки правомерных операций. JI

ВАКЦИНА ДЛЯ ТЕЛЕКОМ-ОПЕРАТОРОВ

ВАСИЛИЙ СЕРГАЦКОВ,
архитектор FMRA-решений Центра информационной безопасности компании «Инфосистемы Джет»

Любого оператора связи можно сравнить с человеческим организмом — в нем есть органы, отвечающие за поддержание жизнедеятельности, фильтрующие «кровь», он же трафик, и т.д. Соответственно, телеком-операторы могут «заболевать», если их иммунитет — функции противодействия мошенничеству и гарантирования доходов (FMRA, Fraud Management & Revenue Assurance) — ослаблен. Негативное влияние на реализацию FMRA оказывает несовершенство структурной и организационной составляющей. ТОП 10 источников потерь и рисков возникновения мошенничества выглядит следующим образом:

- мошенничество с интерконнектом (взаиморасчеты между операторами связи за приземление трафика);
- потеря CDR (Call Detail Records) — записей о вызовах, передаче данных, SMS и т.п.;
- некорректная тарификация услуг и списание абонентской платы вследствие ошибок, аварий и внутреннего мошенничества;
- мошенничество, связанное с вознаграждением (комиссия, бонусы и выполнение планов) дилеров и агентов по подключению и продаже МГ/МН-трафика;
- социальные виды мошенничества, направленные на клиентов оператора связи (SMS-спам, ботнет-сети и т.п.);
- мошенничество с использованием услуг роуминга;
- мошенничество с использованием мобильной коммерции;
- мошенничество в собственной розничной сети;
- некорректное предоставление скоростей доступа в интернет;
- внутреннее мошенничество.

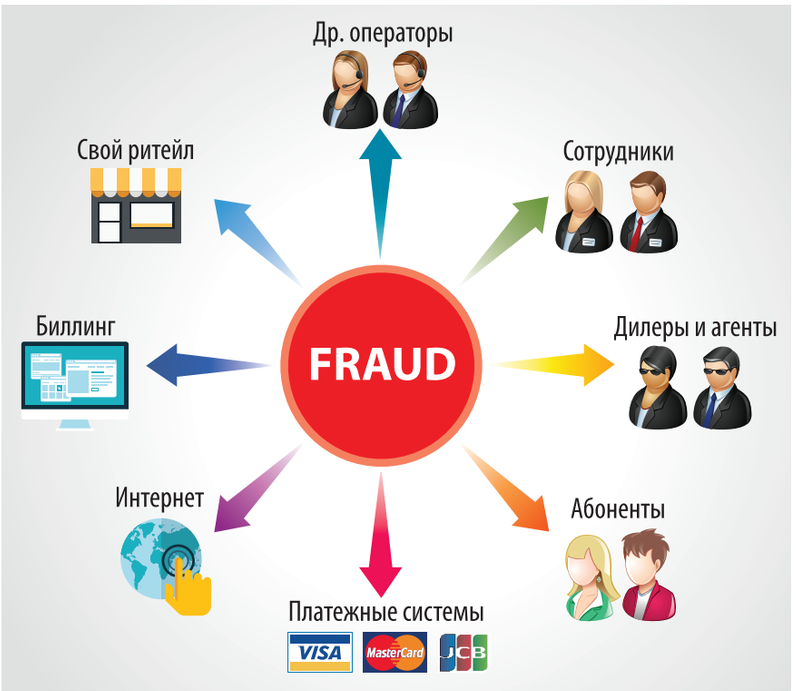


Рис. 1. Потенциальные объекты мошенников

ПРОСТЫЕ ПРИМЕРЫ

Мошенничество с интерконнектом представляет наибольшую угрозу и приводит к существенным потерям у операторов. Поэтому мы подробнее рассмотрим его виды, причем мало описанные в открытых источниках. Однако мы не будем приводить самые опасные способы из соображений безопасности.

Для начала опишем схему взаиморасчетов между операторами за голосовой трафик: когда абонент оператора А звонит абоненту оператора В, за каждую минуту оператор А платит оператору В от 0,2 до 3,5 руб., и наоборот. В случае вызовов на номера международных операторов себестоимость одной минуты может доходить до 300 руб. Это происходит, например, когда звонок идет на так называемые премиум-номера — аналоги наших коротких (четырехзначных), по своему виду они ничем не отличаются от обычных иностранных номеров в международном формате, т.е. состоят из 11–12 цифр.

Как же мошенники могут здесь «зарабатывать»?

Нелегальная генерация трафика из роуминга. Мошенник оформляет на компанию-однодневку или на «левые» данные физического лица комплект из нескольких десятков SIM-карт с postpaid тарифным планом. Большинство услуг на этих тарифных планах тарифицируются в офлайн-режиме, т.е. минимум через 10 минут с момента завершения вызова. Затем мошенник бесплатно оформляет несколько международных премиум-номеров. Теперь достаточно просто вывезти SIM-карты в международный роуминг и генерировать исходящие вызовы на оформленные номера

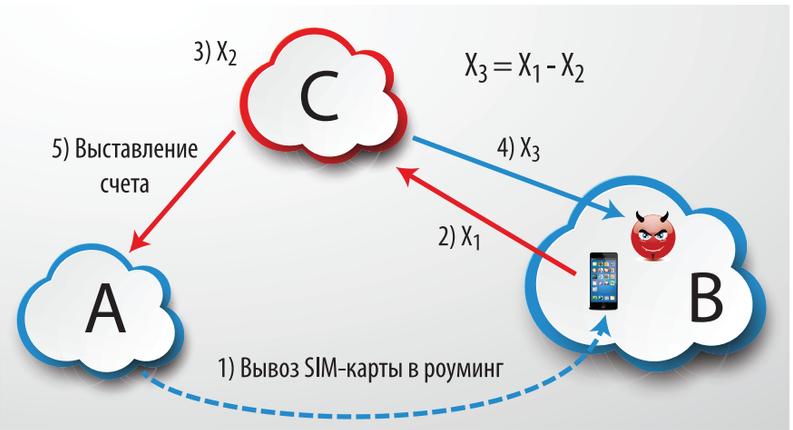


Рис. 2. Нелегальная генерация трафика из роуминга

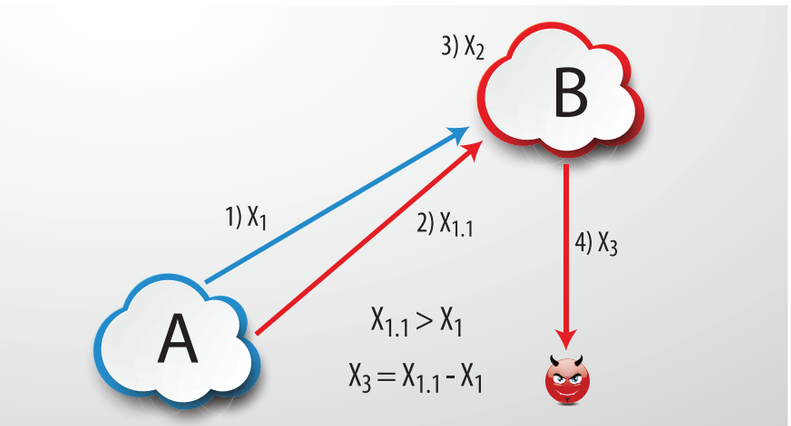


Рис. 3. «Легальная» генерация трафика

(одновременно по 5 вызовов с 1 SIM-карты) (см. рис. 2). Как следствие, на балансе SIM-карт образуется дебиторская задолженность, а мошенник получает прибыль: чем больше совершено вызовов, тем больше он «зарабатывает» (до 25 руб. за 1 минуту). В роуминге эта схема работает из-за особенностей взаимодействия между операторами связи: абонент одного оператора может обслуживаться другим, и тарификация происходит со значительной задержкой. Размер ущерба становится известен «родному» оператору только в момент выставления счета от его коллег, в сети которых обслуживался абонент. К слову, 2 года назад из-за этой схемы крупный российский оператор потерял более чем 9 млн рублей.

«Легальная» генерация трафика. Первым шагом к заветной цели мошенника является сравнительный анализ доходной и расходной частей за минуту на премиум-номера. Для этого осуществляется подборка стоимости звонков на международные премиум-номера у PRS (Premium Rate Services) и у операторов, которые предоставляют услуги связи по этому направлению. Допустим, 1 минута исходящего вызова на премиум-номер Литвы у оператора стоит 5 руб. (расходная часть мошенника – X_1 на рис. 3), а входящая минута у PRS – 7 руб. (доходная часть мошенника – X_3 на рис. 3). В итоге за каждую входящую минуту мошенник может легально «заработать» разницу – 2 руб. Злоумышленнику остается подключиться к оператору связи, арендовать премиум-номера и начать генерацию вызовов.

Петли. Мошенник – маленький оператор связи – перенаправляет входящий трафик от оператора-жертвы обратно на себя с подменой А-номера. Перенаправление проводится через третьего оператора или через самого оператора-жертву. Тем самым один вызов превращается в кольцо, состоящее из двух и более операторов связи. В результате мошенник искусственно увеличивает количество входящих в свою сеть вызовов и зарабатывает на разнице цен за входящую минуту.

Можно предположить, что внедрение систем оптимальной маршрутизации трафика отправило подобную схему в небытие, но тем не менее она продолжает жить и процветать. Практикуются в основном сложные петли с использованием 3-х и более операторов связи, находящихся в сговоре. Как правило, убытки исчисляются сотнями тысяч рублей за каждый инцидент, в месяц у крупного оператора набегает от 5 до 10 случаев «петляния».

Wangiri. Сначала в бой идет отработанная схема аренды международных премиум-номеров. Но здесь уже другая цель – не генерация вызовов на

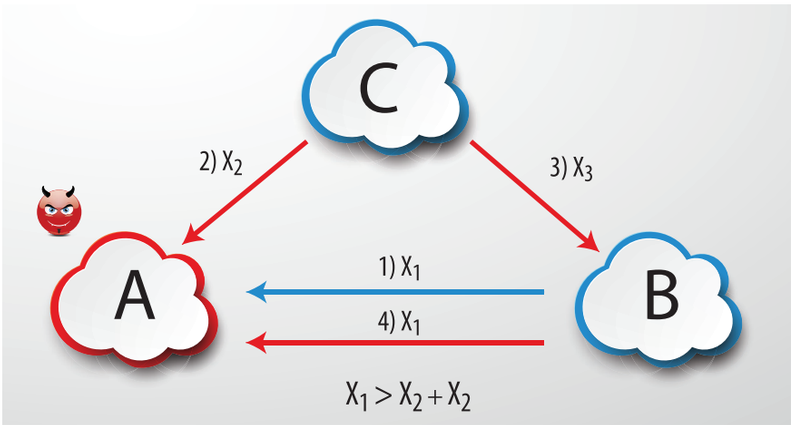


Рис. 4. Петли

Рис. 5. Wangiri

них, а провоцирование жертвы на совершение одного и более звонков. Мошенник с помощью подмены А-номера генерирует пропущенные вызовы на номера обычных людей, чаще всего по принципу ковровой бомбардировки (последовательный перебор). Абонент перезванивает и оплачивает дорогостоящий звонок, а злоумышленник получает прибыль с входящего трафика.

На первый взгляд, схема нежизнеспособна или малоэффективна, ведь практически каждый уже сталкивался с подобным и понимает, что это обман. Но мошенники знают слабые места абонентов. Прозвон может проводиться, к примеру, ночью, когда бдительность в прямом смысле слова спит. Встречаются и оригинальные случаи: в 2011 году мошенник арендовал номера из диапазона спутниковой сети Ellipso Satellite, которая имеет емкость +8812, и начал усиленно прозванивать мобильные номера, относящиеся к Санкт-Петербургу и Ленинградской области. Питер имеет схожий код города, разница лишь в том, что он начинается с кода РФ — «7». Сложно представить человека, который не перезвонил бы на определившийся номер своего региона. Стоимость каждой минуты для абонента составляла до 300 руб., а прибыль мошенника с нее — до 25 руб. Количество пострадавших исчислялось тысячами, а потери — несколькими миллионами рублей.

Мы рассмотрели всего 4 мошеннические схемы, но если представить, сколько различных сервисов, услуг, тарифов и т.п. существует у операторов связи, можно понять, что насчитывается несколько сотен известных сценариев и тысячи их вариаций.

МЕТОДЫ БОРЬБЫ: НЕОБХОДИМОСТЬ И ДОСТАТОЧНОСТЬ

У многих телеком-операторов существуют отдельные подразделения по противодействию/управлению фродом и гарантированию доходов. Как и у сотрудников правоохранительных органов, у фродоборцев есть свое оружие и амуниция, так сказать, на все случаи жизни. Множество участков, где могут «увести» денежные средства, требует наличия массы разнотипных систем защиты. Вот некоторые из них:

FMS — Fraud Management System. Название говорит само за себя. Существует множество систем этого класса, но все они устроены идентично и имеют схожие ключевые функции: сбор данных (действия абонентов, биллинговые данные, платежи, корректировки), нормализация и насыщение информации, выявление случаев мошенничества путем анализа в соответствии с настроенной логикой, Case Management.

RAS — Revenue Assurance System. Системы гарантирования доходов предназначены

для проведения проверок корректности загрузки данных в биллинг (в соответствии с ним выставляются счета абонентам). Набор основных сверок включает сверку данных о вызовах с коммутатора и биллинга для выявления вызовов, не попавших с биллинг, расхождений в длительности вызовов и т.д.; сверку статусов абонентов и услуг для выявления расхождений и несоответствий (к примеру, на коммутаторе абонент действующий, но в биллинге отсутствует) и т.д.

LCR – Least Cost Routing. Решение позволяет в автоматическом режиме выбирать маршруты передачи вызова с минимальной для оператора стоимостью или передавать вызов, опираясь не на цену, а на качество связи (речь идет об отдельных тарифах). LCR-системы могут обладать и дополнительными модулями противодействия мошенничеству, связанному с международными и междугородними вызовами, причем возможно принятие мер в режиме реального времени.

SMS Antispam System. Аналог антиспам-систем для электронной почты, который работает и в режиме реального времени. Благодаря подобным системам абоненты могут самостоятельно управлять черными и белыми списками номеров, отправлять и получать SMS-сообщения через ПК.

Генератор тестовых событий. Система позволяет имитировать использование различных услуг связи и передачи данных на тестовых SIM-картах как в домашней сети, так и в роуминге. Далее в автоматическом режиме проводится проверка корректности тарификации, длительности вызовов, объема сессий и т.д.

Генератор тестовых международных вызовов. Цель генерации вызовов – выявление случаев нелегальной терминации международного трафика. Для этого система генерирует вызовы на тестовые номера сети со стороны международных операторов мобильной и фиксированной связи, карт международной связи, VoIP-операторов. В случае нелегальной терминации определяется номер мошенника, а не реальный иностранный тестовый номер, либо вызов поступает через местное, а не через МГ/МН присоединение.

МОШЕННИЧЕСТВО С ИНТЕРКОННЕКТОМ ПРЕДСТАВЛЯЕТ НАИБОЛЬШУЮ УГРОЗУ И ПРИВОДИТ К СУЩЕСТВЕННЫМ ПОТЕРЯМ У ТЕЛЕКОМ-ОПЕРАТОРОВ

Отметим, что перечисленные нами инструменты не покрывают всех потребностей оператора в условиях наличия мобильной коммерции и других подобных сервисов. Поэтому развитие систем защиты от мошенничества должно идти не просто в ногу со временем, а опережать его. Это позволит не только бороться с известными видами мошенничества, но и обеспечит защищенность компании и ее абонентов от будущих противозаконных схем.

Безусловно, разрозненное управление перечисленными инструментами не может обеспечить необходимую оперативность выявления фактов мошенничества и потерь доходов. К примеру, выявление точек нелегальной терминации международного трафика наиболее эффективно при анализе косвенных признаков (количество исходящих вызовов, соотношение исходящих и входящих вызовов, число используемых IMEI, базовых станций, процент уникальности B-номеров и др.), но этот механизм частично теряет свою эффективность без поддержки генератора тестовых международных вызовов. Поэтому управление описанными системами, принятие соответствующих мер и составление отчетности (тем более в режиме, приближенном к online) могут проводиться только в рамках комплексного решения, объединяющего в себе перечисленные инструменты.

У FMRA-систем есть и ряд недостатков. Это частое отсутствие возможности работы в режиме online, анализа входящего трафика в скопе всех событий от внешних A-номеров, построения сложной логики для выявления мошенничества в дилерском канале, в ритейл-сегменте и т.д. Конечно, часть недостатков может быть снята в ходе доработок, но увы, фундаментальная архитектура некоторых распространенных и популярных FMRA-систем уже исчерпана и не позволяет отвечать новым требованиям. В ряде случаев стоимость масштабных доработок сопоставима со стоимостью нового решения.

В завершение рассмотрим основные факторы, которые могут негативно повлиять на функцию гарантирования доходов и управления фродом у оператора связи.

Раздробленность функции на несколько подразделений, находящихся в подчинении у раз-

ных департаментов, к примеру, противодействие фроду относится к безопасности, а гарантирование доходов — к финансовому департаменту. Получается, что вопросами классического мошенничества (SMS-спам, внутреннее мошенничество, мобильная коммерция и т.п.) занимается безопасность, а выявление потерь доходов и недополученной выручки (нелегальная терминация трафика, выявление искаженных и потерянных данных) курируют грамотные финансисты. С первого взгляда все логично, каждый занимается своим делом, но большинство видов мошенничества и потерь доходов требуют функционирования FMRA как единого целого, зачастую необходимо привлекать и технологические службы.

Сильная вертикаль и обширная иерархическая лестница влекут за собой дополнительные временные затраты на согласование тех или иных действий и документов (служебные записки/приказы), на подготовку отчетности на каждом вертикальном уровне и т.п. В случае формирования единого комплекса борьбы с мошенничеством появится реальная перспектива замены регламентов взаимодействия подразделений на автоматизированные инструменты реагирования. Они повысят эффективность и скорость принятий конпенсационных мер по фактам мошенничества и снизят нагрузку на человеческие ресурсы.

Отсутствие специалистов, обслуживающих и поддерживающих системы FMRA. Это существенно снижает эффективность работы подразделения FMRA, повышает риск форс-мажорных ситуаций с программно-аппаратным комплексом и увеличивает время, затрачиваемое на устранение неполадок.

Территориальная разрозненность подразделений FMRA. Зачастую существенная удаленность сотрудников подразделения друг от друга негативно влияет на его централизованное управление, оперативность принятия решений, а также на взаимодействие с другими подразделениями. К примеру, если у оператора 2 и более филиалов/дочерних компаний, но при этом круглосуточная дежурная смена находится лишь в одном регионе, это может привести к задержке в принятии решений в отношении инцидентов либо к некорректным действиям (специалисты дежурной смены не всегда могут знать специфику отдельных тарифных планов, услуг или маркетинговых кампаний, относящихся к анализируемому региону).

Отсутствие единой методологии определения схем мошенничества, потерь доходов, расчета KPI по выявленным инцидентам, базы знаний. Например, исторически сложившиеся методологии расчета KPI закрепляются в отдельных, «родных» регионах, это приводит к тому, что каждый регион рассчитывает ущерб, предотвращенные и восстановленные потери различными методами.

Отсутствие единого центра взаимодействия между подразделениями FMRA разных операторов. Подобный центр позволил бы не допускать к работе ранее скомпрометировавших себя сотрудников, включая персонал ритейловых сетей операторов. Не менее важным является обмен черными списками B-номеров, IMEI и т.п.

Влияние со стороны коммерческих подразделений. Возникает извечный вопрос «Что важнее: коммерческая составляющая или безопасность?». К сожалению, у бизнеса всегда есть дополнительная гиря для своей чаши весов в виде прогнозируемой выручки, особенно если планируется ввод нового потенциально опасного тарифа или услуги. Часто слова со стороны FMRA о возможных рисках потерь воспринимаются только по факту их наступления.

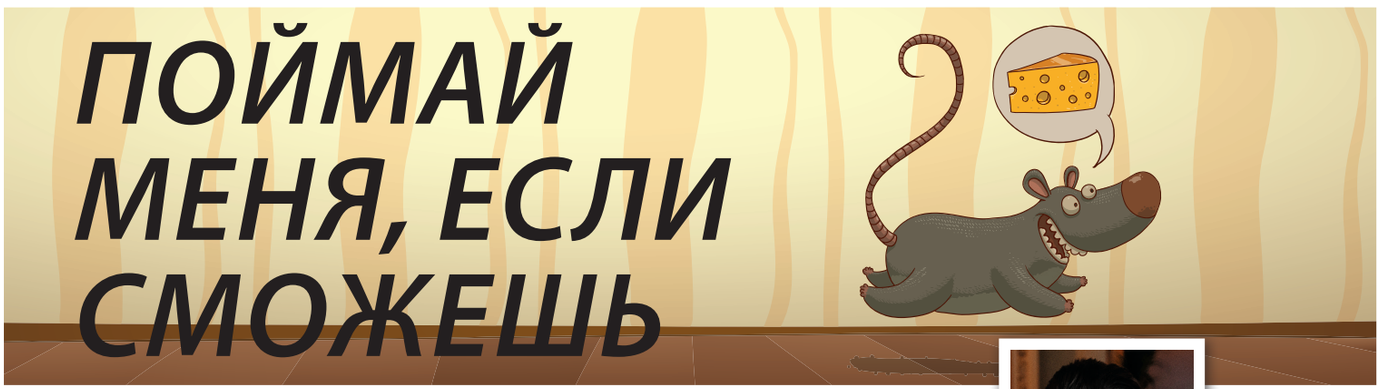
В качестве вывода определим верхнеуровневую стратегию создания/модернизации организационной структуры FMRA:

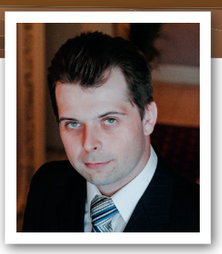
- Объединение функции FMRA в единое подразделение по троичному принципу (ИБ, финансы, технологические компетенции).
- Развитие горизонтальной организационной структуры.
- Развитие технической компетенции.
- Повышение независимости.
- Повышение целостности.
- Систематизированная методология определения инцидентов FMRA, расчета KPI, ведение единой базы знаний.
- Создание Центра взаимодействия между FMRA-подразделениями различных операторов России.
- Модернизация процедур взаимодействия с другими подразделениями.

***

Что же мы получаем на выходе в случае эффективного и оперативного использования FMRA-систем при наличии качественной организационной структуры? В среднем операторы сотовой связи перестают терять порядка 2–5% от общего оборота. В отдельных случаях уровень потерь может снижаться в 10 раз, это позволяет полностью окупить FMRA-систему в течение 6–12 месяцев. JI

ПОЙМАЙ МЕНЯ, ЕСЛИ СМОЖЕШЬ





АЛЕКСЕЙ СИЗОВ,
руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»

Ночь. Темно. Кухня. Открывается холодильник, и из него медленно выползает огромная крыса. В одной лапе у нее палка колбасы, в другой — здоровенный кусок сыра, а за спиной висит свиной окорок. Добирается эта крыса до своей норы, с трудом все это туда запихивает и, перед тем как скрыться самой, бросает взгляд в сторону и видит в углу мышеловку, а в ней маааленький кусочек сыра. Крыса вздыхает, качает головой и произносит: «Ну, просто как дети».

В одних компаниях мошенничество легко поддается оценке, выбрать способы защиты тоже не составляет труда. Например, банки и телеком-операторы могут определить объем и характер мошеннических действий исходя из обращений клиентов. Для других организаций — ритейлеров, топливно-энергетических, промышленных и производственных компаний — оценка уровня мошенничества является намного более сложной задачей. Дело в том, что действия злоумышленников нацелены не на процессы обслуживания клиентов, а на внутреннее движение денежных средств, товарной продукции и т.д. Если факты хищения не могут быть относительно просто выявлены компанией или ее клиентами, мошенниками обычно являются сами сотрудники этой организации.

Отметим, что отчетные документы, которые анализируются при инвентаризациях, инкассациях и пр., никак не помогают в деле обнаружения мошенничества. Совпадение данных из отчетных документов дает право ревизионным службам рапортовать об отсутствии хищений, в то время как их масштабы только увеличиваются.

Наиболее остро проблема гарантирования доходов стоит перед классическим ритейлом и ТЭК. Одним словом, если ваша продукция высоколиквидна и маржинальна, можете быть уверены — на нее найдутся охотники «без лицензии». Причем риски мошенничества особенно высоки при реализации гаджетов и высокотехнологичных товаров — мы установили это путем сравнения эквивалентных по обороту магазинов продажи электроники, продуктов питания, одежды.

Каким образом мошенники добиваются своих целей? Представим себе любую последовательность действий, например, бизнес-процесс реализации това-

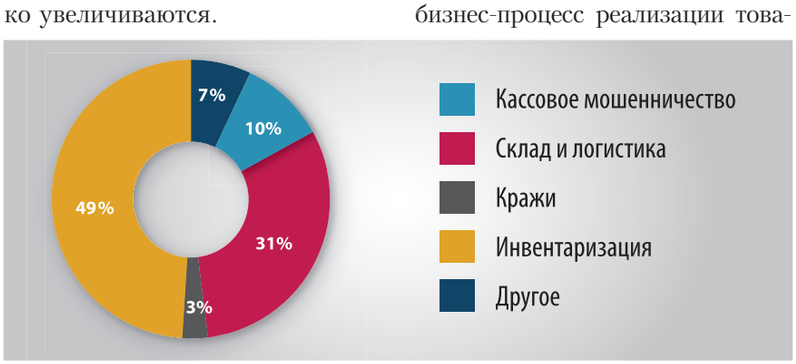
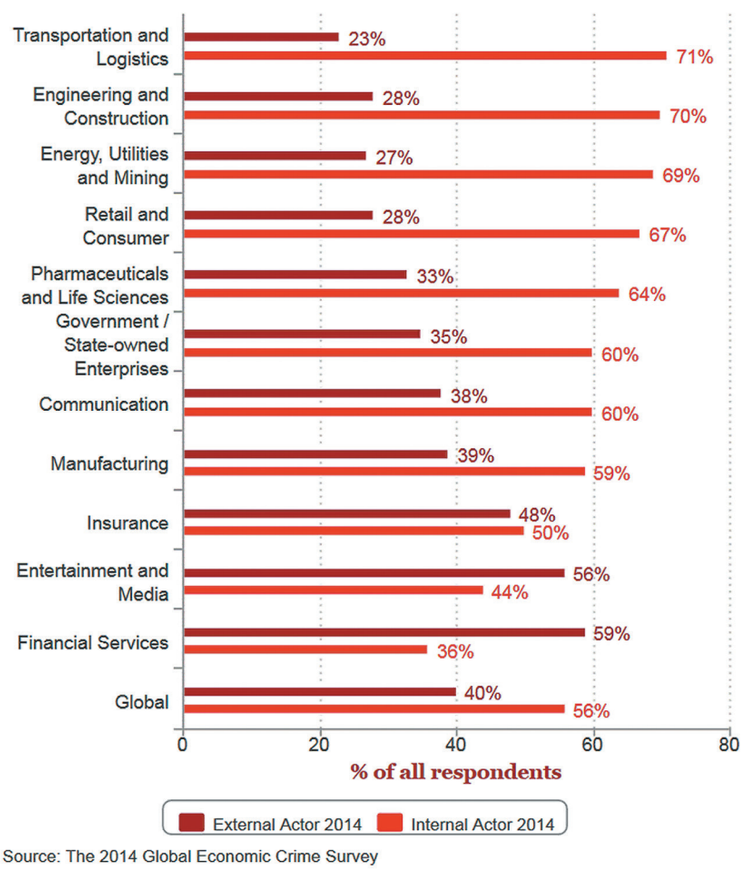


Рис. 1. Соотношение типов мошенничества в ритейл-сегменте

ра. Так или иначе это учет движения товарной продукции на всех этапах — от закупки до реализации. Очевидно, что если система является замкнутой с точки зрения движения денежных средств, прозрачной для определения конечной цены товара и защищенной от изменения учетных данных, отчетность по крайним точкам процесса будет однозначно указывать на наличие или отсутствие фактов мошенничества.

Но можно ли сегодня выстроить подобный процесс? Это очень сложно, а при текущих бизнес-потребностях и вовсе близко к утопии. Причина кроется в распространении современных технологий оплаты, разнообразных бонусных программ и программ лояльности, программ для агентов и партнеров, маркетинговых акций и др. Кроме того, бизнес-процесс выходит за рамки реализации товарной продукции в чистом виде — это и сложные логистические операции по хранению/учету/доставке, и сервисное/гарантийное обслуживание, и списание/уценка товара и т.д. Как следствие, расчет эффективной бизнес-модели, исключающей риски совершения мошенничества, — почти сверхзадача.

Если мошенничество так незаметно, а бизнес приносит прибыль, стоит ли вообще уделять внимание гарантированию доходов? Окупаются ли вложения в поиск мошеннических схем, организацию технологий и процессов по контролю действий злоумышленников? Каждая компания должна решать для себя эти вопросы самостоятельно. При этом есть вполне очевидный тренд: комплексы мероприятий, направленные на борьбу лишь с тривиальными схемами, окупают себя менее чем за год.



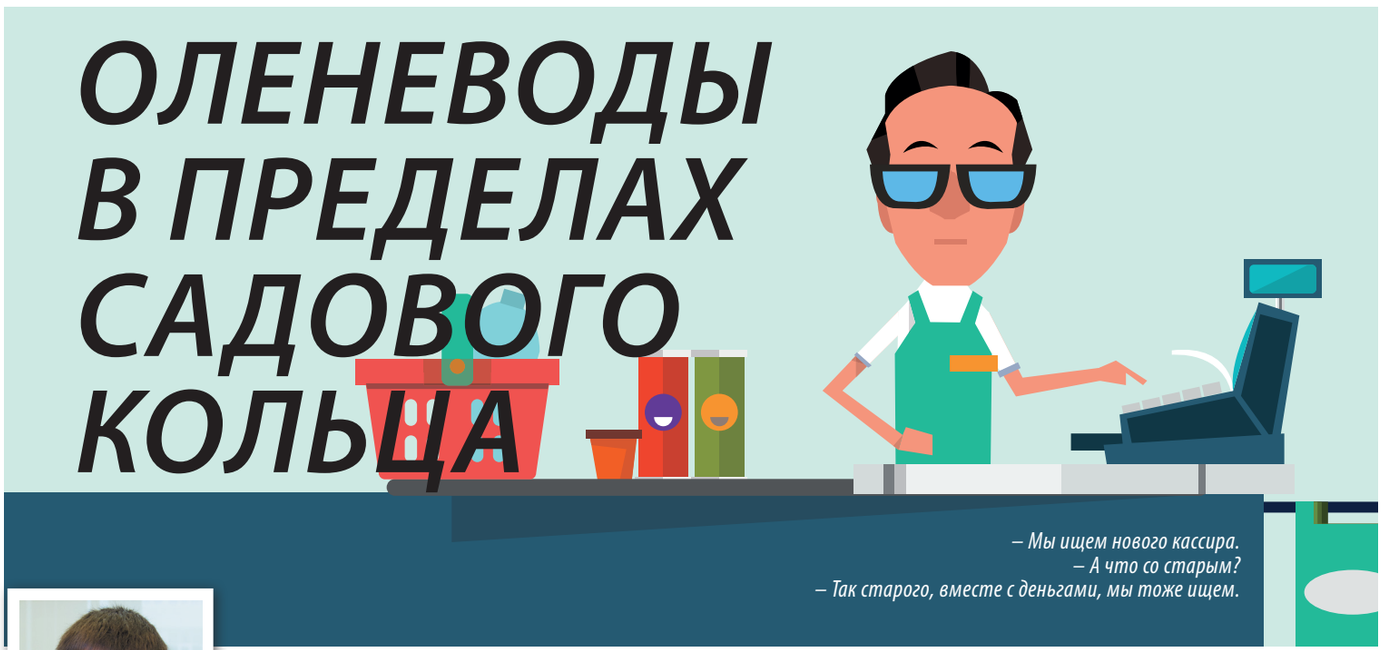
Source: The 2014 Global Economic Crime Survey

Рис. 2. Соотношение внутренних и внешних угроз мошенничества

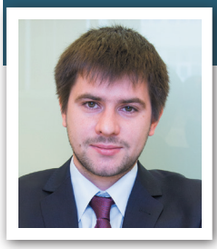
Причины высокого уровня хищений у любого ритейлера:
1) Бизнес-процессы, подспудно приводящие к потере прибыли. Любая маркетинговая акция, призванная стимулировать спрос и привлекать новых клиентов, воспринимается сотрудниками как способ подзаработать.
2) Формальная законность каждой отдельно взятой операции.
3) Невидимость убытка при классической инвентаризации.
4) Трудность и высокая стоимость контроля большинства процес сов – от закупки до продаж.
5) Высокая текучка кадров и низкая лояльность персонала.
6) Влияние человеческого фактора на процесс контроля мошенничества.

В то же время некоторые сотрудники — существа алчные, и если есть возможность иметь не совсем легальный, но дополнительный доход при отсутствии даже видимости контроля, аппетиты у них будут расти, как грибы после дождя. Тогда как можно эффективно контролировать подобную открытую бизнес-систему? Только реализовав комплексный проект по защите бизнеса и гарантированию доходов, который бы обеспечил компанию инструментом контроля критичных областей. JI

ОЛЕНЕВОДЫ В ПРЕДЕЛАХ САДОВОГО КОЛЬЦА



– Мы ищем нового кассира.
– А что со старым?
– Так старого, вместе с деньгами, мы тоже ищем.



ЕВГЕНИЙ ЖИЛЬЦОВ,
старший аналитик отдела разработки и внедрения прикладных решений Центра информационной безопасности компании «Инфосистемы Джет»

Стремительное развитие российского ритейла характеризуется автоматизацией кассовых операций, операций ценообразования и логистики, развитием области кредитования и функций платежных агентов. Как следствие, возрастают риски реализации мошеннических действий. Нет на свете человека, которого хотя бы раз в жизни не обвесили или не добавили ему в чек лишний товар. С другой стороны, нерадивые клиенты «обвешивают» магазин на кассах самообслуживания, выносят товары под одеждой и т.д. А какой урон наносит компании ее персонал: кассиры, менеджеры? Какая доля прибыли приходится на небольшое злоупотребление сотрудников на том или ином участке их работы?

Любой ритейлер — это сложнейший процесс организации производства и продаж: десятки учетных и оперативных систем, многоуровневые процессы оборота товарной продукции и денежных средств, функции управления и поддержки бизнес-деятельности и т.д. Среди всего этого многообразия есть узкие места, которые позволяют осуществлять хищения, лежащие за классическими границами воровства товаров или наличных денежных средств.

Например, **мошенничество с кассовыми операциями** — это и простое сторнирование/возврат товара по оставленному чеку, и модификация сумм/количества товара. Приведем классический пример мошенничества на кассе с применением функции возврата при наличии в компании программы лояльности:

- Покупатель приобретает, например, телевизор. Расплатившись, забирает покупку и покидает магазин с кассовым чеком, заполненной гарантией и пр.
- Сотрудник осуществляет фиктивный возврат, телевизор встает на остатки.
- После сотрудник продает ранее фиктивно возвращенный товар с применением бонусных карт, сохраненных купонов и иных возможных скидок.
- Разницу между первой и второй продажами кассир кладет себе в карман.

Нетрудно подсчитать, что скидка по бонусной карте в 10%, накопленные кассиром баллы на его бонусной карте и купоны на скидку в совокупности составля-

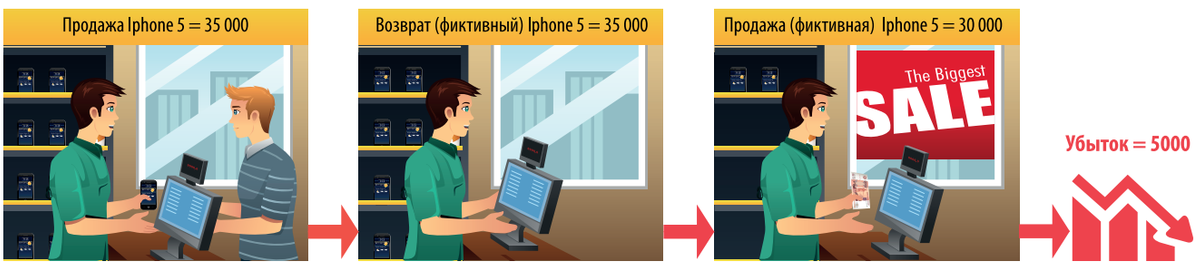


Рис. 1. Мошенническая схема в ритейле

ют 20–40% от стоимости покупки. При стоимости телевизора, равной 40 000 руб., это вполне ощутимый заработок только от 2 фиктивных действий.

Другой вариант — **манипуляции с ценами и ценообразованием**. Процесс ценообразования в современной ритейл-компании практически всегда централизован, а значит, рядовому сотруднику регионального магазина почти невозможно изменить прайс в свою пользу. При этом у многих ритейлеров менеджеры магазинов имеют возможность устанавливать скидку на товар независимо от текущего прайса. Задача компании в данном случае — ограничить соответствующий доступ узким кругом пользователей.

В настоящее время в большинстве ритейл-компаний действуют различные методы удержания клиентов путем предоставления скидок и бонусных баллов, которые можно использовать для обмена на товар в данной сети, в целом это называется — программа лояльности.

В то же время существует очень много разных вариантов схем мошенничества с картами программ лояльности. Например, встречаются бонусные карты с кредитным лимитом. В нашей практике были случаи, когда сотрудники, используя подобные карты, уводили их в глубокий минус. Сценарий прост: сотрудник пробивал товар и начислял себе баллы, далее приобретал на них другой товар, а в конце возвращал оба за наличные. Эта трёхходовка обеспечивала конвертацию начисленных баллов в реальные денежные средства. Вся тонкость в том, что при возврате товара начисленные баллы должны списываться, но на втором шаге сотрудник уже потратил их на товар, списываться нечему, следовательно, возникал отрицательный баланс.

Даже точечное внедрение системы борьбы с мошенничеством может сократить потери и повысить доходность ритейлера. Приведем пример влияния подобного внедрения (см. рис. 2).

Отметим, что система закрывает 4 направления: акции мотивации, программа лояльности, возвраты, подарочные карты. Оранжевый столбец на графике — это сумма убытков до внедрения, серый — сразу после него

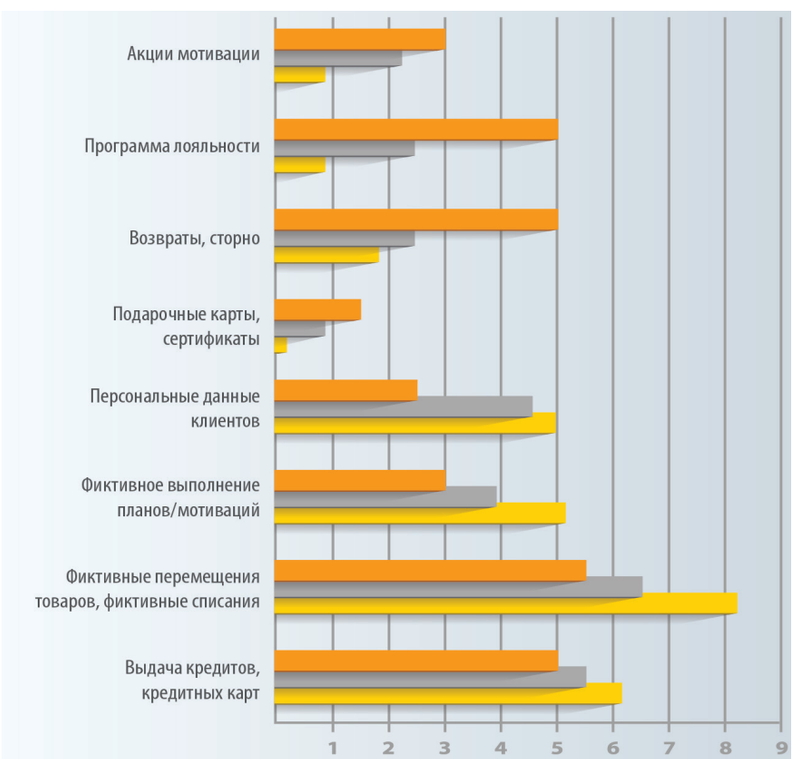


Рис. 2. Изменение величины ущерба по направлениям мошенничества при частичном внедрении антифрод-системы

(в течение 1 квартала), желтый — после 3 месяцев внедрения. Видно, что после начала контроля над частью направлений объемы убытков на других участках увеличились. Сотрудники почувствовали контроль и «переместились в серые зоны», не охваченные антифрод-решением.

ШАГ ВПЕРЕД, ДВА ШАГА НАЗАД?

Многие ритейлеры сегодня вышли за рамки обычных продаж и проводят в своих точках операции пополнения банковских карт, баланса сотовых телефонов и т.д. Продажи часто совмещаются с выдачей кредитов. К сожалению, это наиболее уязвимые сегменты бизнеса с точки зрения реализации мошенничества, поскольку их крайне сложно контролировать. Например, операция пополнения банковской карты контролируется в соответствии с реквизитами назначения платежа, остальной «надзор» — дело кассира, а значит, при его халатности или попустительстве осуществить фиктивный платеж не составляет труда. Сотрудник легко может пополнить карту знакомого без фактического внесения денежных средств. Именно такой способ мошенничества еще не так давно наносил миллионные убытки ведущим ритейлерам.

Еще более изощренными являются схемы выдачи кредитов. Живя в России, вы могли неоднократно слышать об оленеводах. Они занимаются разведением одомашненных животных — северных оленей. Но XXI век вносит свои коррективы в общепринятые понятия. Если бы настоящие оленеводы узнали, что у них есть лжеподражатели, а точнее, мошенники, работающие по схеме под кодовым названием «оленеводы», им бы это точно не понравилось.

В чем состоит их схема? Мошенники расклеивают объявления и размещают баннеры в интернете с рекламой «До 200 тыс. рублей за 5 минут по паспорту!». Желающие получить быстрый кредит всегда находятся. Затем для экономии времени и сил «оленеводы» собирают их в группы по 5 человек в условленном месте. Далее злоумышленники ведут группу в торговую точку ритейловой сети, в которой работают их братья по преступному умыслу, и оформляют на этих людей различную технику в кредит. Пришедшая группа получает не технику, а наличные в виде 50% от ее номинальной стоимости. Вот он — их быстрый денежный кредит.

Мошенники же осуществляют возврат товара за наличные средства или вовсе не проводят его продажу по кассе. В итоге желающие получить быстрые деньги удовлетворены, а мошенники в обличье вежливых продавцов-консультантов забирают оставшиеся 50% наличных, и это в худшем случае.

О каких суммах здесь может идти речь? Возьмем за основу плазменную панель стоимостью 20 тыс. руб., представим, что за месяц в одну торговую точку зашли 4 группы. Получаем до 500 тыс. руб. оборота в месяц и «надбавку» к зарплате недобросовестных сотрудников торговой точки в 250 тыс. руб. Неплохие бонусы «за вредность».

Теперь поговорим о механизмах, способных обеспечить защиту от подобных действий. Как показывает наш опыт, большинство компаний предпочитает проверенные временем меры:

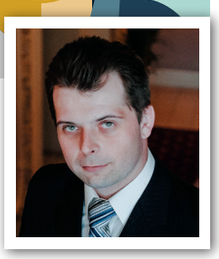
- техническое ограничение количества начислений в день (неделю);
- установление временных ограничений между начислением и списанием (т.е. списывать баллы можно только через несколько дней после начисления);
- выборочные проверки нескольких карт с максимальным количеством покупок и проведение ручного анализа всех транзакций по ним;
- блокировка всех карт, количество покупок по которым превышает определенный порог (зачастую это приводит к большому количеству жалоб от клиентов).

К сожалению, все перечисленное далеко не всегда эффективно. Очевидно, что сотрудник определит действующие фильтры (ограничения) после двух заблокированных карт либо узнает о нововведениях по сарафанному радио и больше не попадется на удочку. Например, на своем листе со штрих-кодами он проставит дни, когда и какую карту можно использовать, и будет продолжать в том же духе.

Внедрение системы противодействия мошенничеству обеспечит ритейлера технологической платформой для обнаружения событий, прямо или косвенно указывающих на возможные случаи фрода со стороны сотрудников или клиентов. В целом это позволяет предотвращать хищения с помощью применения средств детектирования и оперативного реагирования на попытки совершения мошенничества. Значительно снижается риск возникновения новых схем хищений, готовящиеся операции выявляются еще на этапах подготовки. Идет постоянный контроль над несанкционированными действиями сотрудников в режиме реального времени, оптимизируются процессы проведения проверок и расследований, связанные с превышением должностных полномочий или совершением противоправных действий. JI

СКАЖИ МНЕ, КТО ТВОЙ ВРАГ…

АЛЕКСЕЙ СИЗОВ,
руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»



Я скажу, кто ты. По такому принципу вполне можно определить, каким именно должно быть эффективное решение по противодействию мошенничеству для той или иной компании. Портрет злоумышленника (врага) здесь очень пригодится.

Антифрод-системы позволяют решать вполне прикладные бизнес-задачи — выявлять и предотвращать совершение мошеннических операций, также они служат источником первичной информации о выявлении злоумышленников и следах хищения. По этой причине их крайне сложно классифицировать без привязки к той области бизнеса, элементы которой необходимо защищать/контролировать. В то же время есть несколько общих черт, присущих практически всем подобным ИБ-инструментам. Такие решения (за исключением систем физической безопасности):

- используют информацию из других учетных систем, в рамках которых осуществляется бизнес-процесс, подверженный рискам мошенничества;
- обладают совокупностью сведений, определяющих профиль мошенничества;
- обладают механизмами сравнения текущей учетной информации с фиксированными схемами мошенничества и представления результата.

Другие функциональные возможности опциональны.

Основными критериями достаточности технологии для контроля мошеннических действий являются особенности защищаемого бизнес-процесса и характеристики злоумышленников. Наиболее важны такие свойства системы, как:

1) скорость функционирования;

2) развитые функции контроля, определяющие саму возможность выявления мошенничества;

3) оптимальные технологии сбора/получения данных из систем-источников, автоматизирующих бизнес-процесс;

4) оперативный сбор разнообразных данных, необходимых для формирования профиля мошенника (он будет использоваться для дальнейшего анализа);

5) наличие элементов обратной связи для системы мониторинга, позволяющих контролировать ее эффективность в оперативном режиме.

Для наглядности мы подробно рассмотрим основные характеристики антифрод-решений, применяемых в банках и у ритейлеров.

АНТИФРОД ДЛЯ БАНКОВ

В подавляющем большинстве случаев это система online-анализа, интегрированная с front-офисными системами (ДБО, процессинг). Они могут кооперироваться двумя способами.

Диалоговая схема подразумевает, что антифрод-решение взаимодействует с внешними приложениями в режиме запрос/ответ. То есть система функционирует в пассивном режиме до момента получения запроса от front-системы о необходимости анализа сведений об операции. Антифрод-решение возвращает результат анализа — это либо команда к дальнейшему действию (разрешение операции, ее запрещение, приостановка и др.), либо скоринговое значение, определяющее уровень риска или вероятность реализации мошенничества.

Шлюзовая схема подразумевает, что система работает как шлюз для пропуска и анализа всего трафика, формируемого между конечным пользователем и сервером приложения front-системы/между web-сервером и сервером приложения. При необходимости шлюз позволяет отклонять непосредственно запросы пользователей или дополнять реквизиты первичного запроса информацией, которая будет анализироваться сервером приложения front-системы наряду с параметрами пользовательской операции.

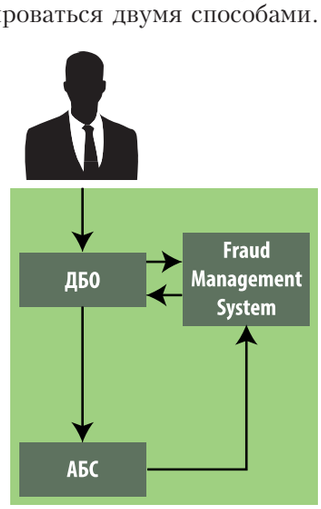


Рис. 1. Диалоговая схема

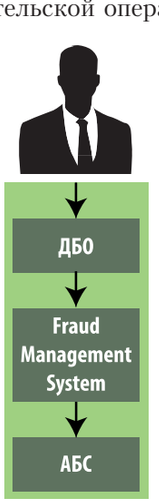


Рис. 2. Шлюзовая схема

В чем преимущества и недостатки этих схем: первый вариант подразумевает отсутствие прямого влияния антифрод-решения на основной бизнес-процесс, в то же время компании грозит длительный и сложный процесс его интеграции с front-системами. Второй способ как раз предполагает более простую интеграцию, не требующую доработок бизнес-приложений. Минусы здесь — более дорогостоящая схема обеспечения отказоустойчивости и зависимость от смены формата передачи данных между клиентами и сервером приложений.

Методология анализа операций антифрод-системой подразумевает несколько уровней:

1) Анализ реквизитов операции клиента и сопоставление текущей активности с сохраненной историей его операций.

2) Поведенческий анализ операции с применением схем профилирования активности (как платежной, так и сессионной), а также математических моделей анализа.

3) Контроль параметров операции, в том числе с помощью внешних глобальных источников: сервисов геолокации, баз Drop Zone, баз скомпрометированных реквизитов платежных инструментов и др.

Очевидно, что описанные уровни тяготеют к ограниченному набору правил, а также к логике профилирования и статистическим метрикам. Это связано с естественными ограничениями на скорость обработки операции (время ожидания клиента, требования платежных систем и пр.), что, в свою очередь, приводит к негласным ограничениям на размеры черных/белых списков, обработку сложной логикой и пр.

При этом результаты работы механизмов контроля должны обладать базовыми характеристиками: достоверностью, непротиворечивостью, полнотой и открытостью. Первый критерий отвечает за качество действий (автоматизированных или организационных), которые предпринимаются по факту формирования результата системой контроля. Второй позволяет формировать объективное заключение об эффективности функций контроля и возможности их более точной настройки.

АНТИФРОД-СИСТЕМЫ ПОЗВОЛЯЮТ РЕШАТЬ ВПОЛНЕ ПРИКЛАДНЫЕ БИЗНЕС-ЗАДАЧИ – ВЫЯВЛЯТЬ И ПРЕДОТВРАЩАТЬ СОВЕРШЕНИЕ МОШЕННИЧЕСКИХ ОПЕРАЦИЙ, ПО ЭТОЙ ПРИЧИНЕ ИХ КРАЙНЕ СЛОЖНО КЛАССИФИЦИРОВАТЬ БЕЗ ПРИВЯЗКИ К ТОЙ ОБЛАСТИ БИЗНЕСА, ЭЛЕМЕНТЫ КОТОРОЙ НЕОБХОДИМО ЗАЩИЩАТЬ

Подчеркнем, что функциональность современных систем контроля мошенничества становится все более бизнес-ориентированной, «заточенной» под конкретный сегмент. 5–7 лет назад любое антифрод-решение можно было определить как иерархичную модель, состоящую из 3 базовых уровней — интеграции, анализа и представления результата. Сегодня такая каноническая структура претерпела множество изменений: добавляются функции, необходимые представителям того или иного вертикального рынка. Например, для банков это механизмы контроля среды совершения дистанционных операций. Поскольку 100% операций ДБО совершаются с удаленных и недоверенных устройств, характеристики среды их выполнения оказывают большое влияние на анализ, выявление наличия удаленного управления и вредоносного ПО.

РИТЕЙЛЕРЫ

Выявление мошенничества в подобных компаниях является более трудоемкой задачей. Фактическое хищение определяется спустя длительный промежуток времени, а мошенничество в рамках снижения прибыльности (непрямые хищения) может быть не выявлено вовсе. Действия злоумышленников крайне сложно отличить от рядовых операций, свой отпечаток накладывает и более высокий уровень внутреннего мошенничества.

Контрольные функции зачастую не требуют online-анализа ввиду специфики процессов продаж (например, существует множество различных, эквивалентных друг другу и легитимных способов оформления продажи) и логистики. В то же время источников информации для системы контроля кассовых операций, например, в большинстве случаев в разы больше, чем для антифрод-решения в банке. Причина кроется в том, что кассовая система не является независимым процессом обслуживания клиента, она представляет собой бизнес-образующую операцию. Все эти факторы говорят о том, что нужен более сложный и глубокий анализ.

Схему интеграции антифрод-системы в ИТ-ландшафт

Рис. 3. Целевые источники данных

ритейлера можно назвать более классической. Она представляет собой набор модулей подключения к различным источникам данных: к Data Warehouse, СУБД бизнес-приложений и др. Кроме того, нужны специализированные интерфейсы работы с такими системами, как SAP, 1С, и их модулями.

Ключевая особенность решения — схема хранения и преобразования данных, обеспечивающая единое пространство для всей критичной информации компании, построение взаимосвязей и восстановление последовательности действий сотрудников, сложный статистический анализ за периоды, учитывающие сезонность продаж, показатели регионов и т.д.

При этом антифрод-система должна масштабироваться и охватывать большинство разрозненных процессов, процедур, а иногда и структурных подразделений компании. Сегодня это независимый инструмент контроля не только правомерности отдельной операции клиента, но и жизненного цикла товара с момента его закупки и до реализации. Функции детектирования мошенничества можно разделить на несколько основных блоков:

1. Контроль базовых схем мошенничества, его логика направлена на выявление частных злоупотреблений и схем хищений (например, поиск перекрестных возвратов, комбинирования скидок, возвратов ранее непроданной продукции).

2. Контроль статистических показателей и метрик направлений бизнеса, что позволяет осуществлять поиск закономерностей и предпосылок появления еще не известных способов хищения.

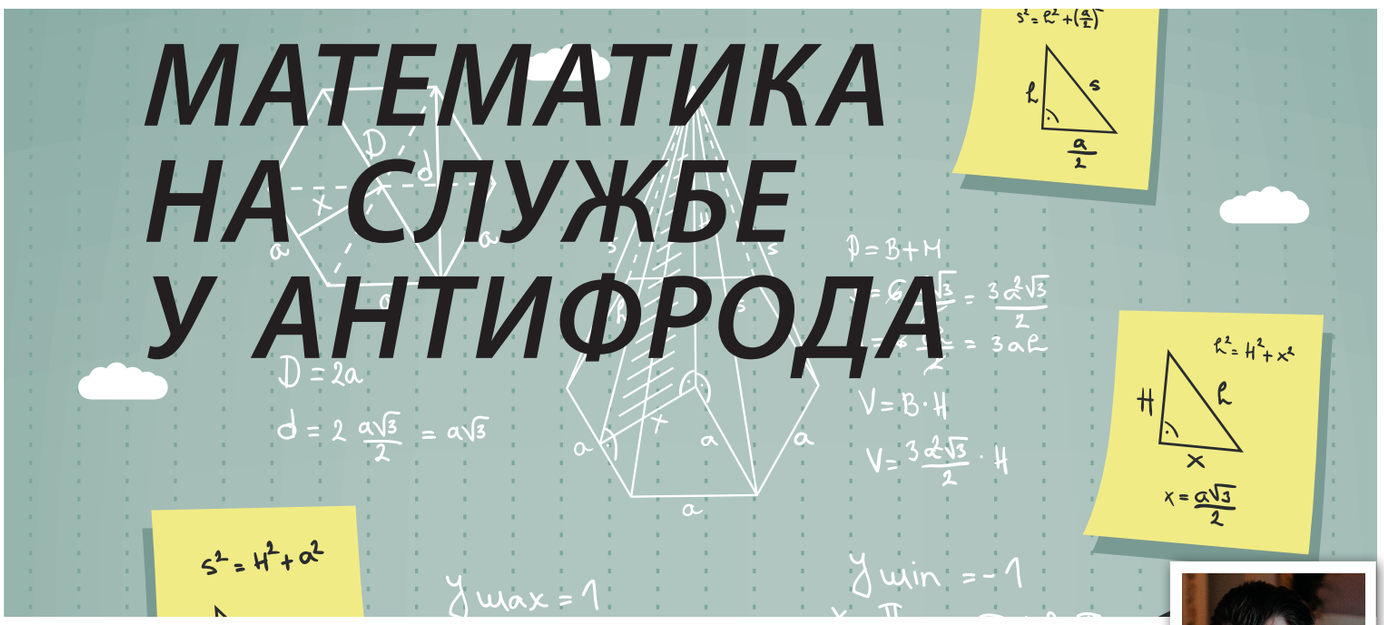
3. Контроль полного цикла движения товарной продукции сквозь различные структурные подразделения и учетные системы.

Любая система контроля мошенничества должна предоставлять интегрированную среду проведения проверок и административных расследований. Это позволяет автоматизировать формирование инцидентов мошенничества, регламентировать правила их обработки, ограничивать ролевую структуру, осуществлять контроль над процессами анализа инцидентов и предпринимаемыми мерами по минимизации потерь. Такой подход дает возможность реализовать функцию «одного окна» – предоставлять все сведения для проведения работ конечному исполнителю. Кроме того, он позволяет упорядочить и систематизировать деятельность аналитиков, специалистов по безопасности в регионах и удаленных офисах, внедрить метрики оценки эффективности работы сотрудников и мер по защите от мошенничества.

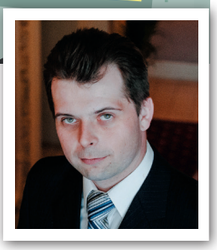
***

Ну, что же, осталось выбрать конкретную систему. Здесь главное — понимать, что предложение того или иного производителя — это своеобразный полуфабрикат, эффективное функционирование решения зависит от факторов, которые достигаются только на этапе внедрения. Это и построение адресных моделей обнаружения мошенничества, выявляющих максимум противозаконных действий при минимальном количестве ложных срабатываний, и создание архитектуры, обеспечивающей надежность и масштабирование решения при эксплуатации, и правильное построение самого бизнес-процесса эксплуатации, от которого в конечном счете зависят фактические объемы возвращенных средств. Без этих элементов антифрод-решение окажется лишь системой отчетности, а не полноценным инструментом предотвращения мошенничества. JI

МАТЕМАТИКА НА СЛУЖБЕ У АНТИФРОДА



АЛЕКСЕЙ СИЗОВ,
руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»



Определить вероятность и момент реализации хищения невозможно без наличия у антифрод-системы методологической основы. Именно она позволяет выделять из набора анализируемых сведений те, которые обычно характеризуют противоправные действия. Здесь не обойтись без базовых критериев мошеннических действий (профиля мошенничества — его вида или способа), критериев доверенных действий легитимного клиента/сотрудника (профиля пользователя) или статистических характеристик, определяющих глобальные аномалии текущих учетных операций.

НЕМНОГО ИСТОРИИ И ТЕОРИИ

Исторически выявление мошенничества шло по пути контроля заранее определенного вектора атаки. Так, некоторые правила контроля банковских карт основывались на тривиальных действиях злоумышленника: кража карты (зачастую вместе с PIN-кодом, если человек хранил эту информацию вместе с пластиком), проверка баланса и совершение операции на сумму, близкую к остатку, одновременное совершение операций в разных странах и т.д. То есть использовались базовые критерии, основа для них черпалась из тех случаев мошенничества, которые фиксировались при потере карты, ее краже или компрометации. Вполне очевидно, что со временем такие простые правила анализа становились менее эффективными ввиду более изощренных действий мошенников. На смену им пришли вариативные и поведенческие модели, динамические группы — методы, обеспечивающие некоторую степень самокорректировки системы на базе статистических показателей. День сегодняшний — это применение «тяжелых» аналитических алгоритмов, поддерживающих полновесные обучаемые модели: нейронные, байесовы сети и пр.

Здесь можно привести пример из жизни ритейлеров. Так, выявление перекрестных возвратов фактически сводится к контролю трех операций: продажи, возврата и новой продажи этого товара со скидкой. Как показывает практика, при стабильном числе ложных срабатываний в течение 1 года алгоритм анализа меняется: от простого контроля последовательности операций система переходит к сложному

статистическому правилу, контролирующему более 10 параметров каждой операции.

ОДНА РЕАЛИЗАЦИЯ МАТЕМАТИЧЕСКОЙ МОДЕЛИ

Основное, что нужно сделать для выявления мошенничества, например, в программе лояльности, — это создать модель, способную охватить весь бизнес-процесс. Она должна включать известные мошеннические схемы и в то же время уметь классифицировать «поведение» карты и указывать на вероятность того, что совершается противозаконие.

Конечно, схема не даст 100%-ной гарантии, что карта является мошеннической, но она может дать достаточно оснований для проведения расследования и передачи дела в службу физической безопасности. Степень сложности выявляемого мошенничества, а также его относительная доля являются основными критериями эффективности схемы. Теперь поговорим о том, что в нее входит.

Модуль анализа анкетных данных позволяет в автоматическом режиме выявлять мошеннические карты. Это достаточно эффективный метод, т.к. зачастую сотрудники не слишком перетруждаются и оформляют карту на себя, коллегу, клиента (приходившего утром и оформившего кредит, контракт и т.д.). Под словом «анализ» понимается не простое сравнение ФИО с существующей базой данных, а применение алгоритма нечеткого сравнения строк. Например, алгоритма Jaro–Winkler, который рассчитывает числовую величину схожести между двумя заданными строками, или алгоритма Левенштейна, рассчитывающего редакционное расстояние или дистанцию редактирования между двумя строками (минимальное количество операций вставки одного символа, удаления одного символа и замены на другой, необходимых для превращения одной строки в другую).

Транзакционный анализ позволяет выявлять отклонения от типичного поведения клиента в части начислений и списаний по картам. Для его проведения необходимо выбрать основные статистические показатели: количество чеков по каждой карте (рассматривается выборка за месяц), сумма списаний, начислений и т.д. В среднем рабочая модель может опираться на 30 показателей. Каждый клиент уникален, следовательно, и покупки по его карте будут отличаться. При этом 99% мошеннических действий не могут и не будут соответствовать нормальному поведению рядового клиента.

В то же время следует отметить, что формирование уникального профиля поведения для каждого клиента иногда является избыточной мерой. В таких случаях можно разбить всех на группы-кластеры и определить их основные различия. Кластеризация — многомерная статистическая процедура, выполняющая сбор данных, выборку объектов, а затем упорядочивающая объекты в сравнительно однородные группы.

На рис. 1 представлено распределение карт по осям, где x — количество чеков, y — количество посещений (в днях за период), z — частота посещений. Выборка данных рассматривалась по нескольким магазинам одного региона за 5 месяцев.

На рис. 2 приведены те же результаты, только после проведения кластеризации по 10 основным параметрам с разбивкой на 6 кластеров. Каждый цвет соответствует своему кластеру. Выделяются 4 основных цвета: красный, желтый, салатовый и синий. Синий кластер характеризует обычного клиента, который посещает магазин не более двух раз за месяц.

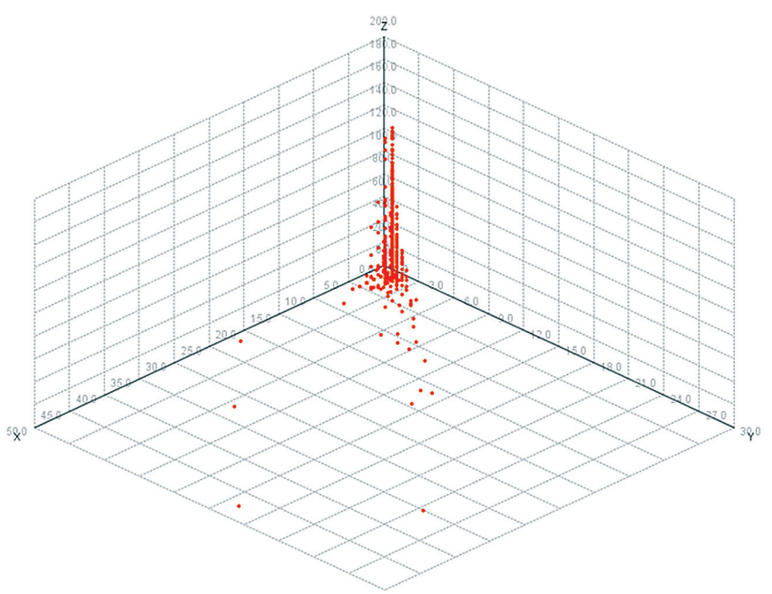


Рис. 1. Графическое представление распределения карт по активности использования

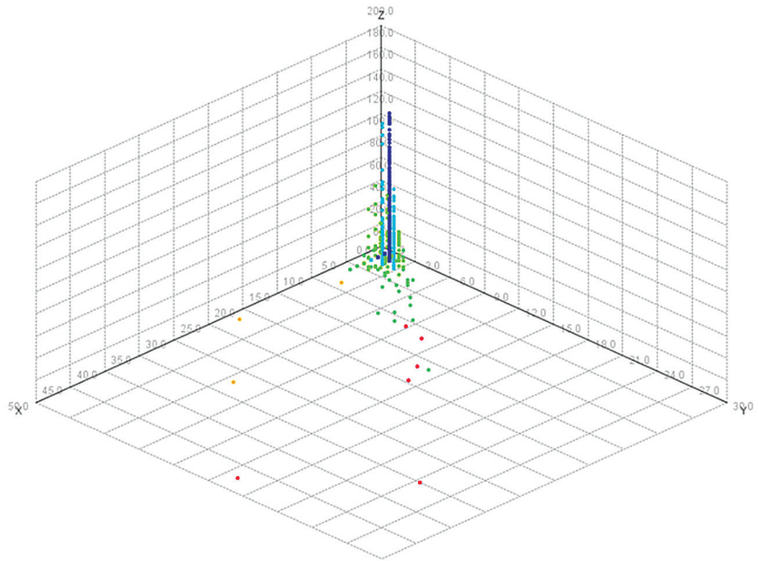


Рис. 2. Графическое представление распределения карт по активности использования после кластеризации типичности поведения клиентов ритейлера

Интерес представляют красный и оранжевый цвета: они с большей долей вероятности отражают мошеннические действия, что требует дополнительной проверки. Так, красный цвет подразумевает, что количество чеков, пробитых с участием той или иной карты в одном магазине, превышает 40%, а анкетный анализ показывает, что часть таких карт имеют общий номер мобильного телефона, оформлены на сотрудников и т.д. Интересна также салатовая точка, которая находится в красной группе: здесь практически все чеки были оформлены в различных магазинах и разными сотрудниками.

Транзакционный анализ покупательской корзины – это способ вычислить товары, которые в большинстве случаев продаются вместе. Для выявления мошеннических карт лояльности необходимо интерпретировать этот анализ, т.е. находить покупки, которые отклоняются от обычной статистики. Это не очень эффективно в случае продажи электроники – сложно выделить основную группу коррелирующих товаров. Положительные результаты есть в продуктовых сетях. Например, как показывает анализ, среднее время между приобретениями чистящих средств составляет чуть больше месяца, крупы приобретаются не чаще чем раз в две недели и т.п. Карты, по которым подобные покупки совершались в несколько раз чаще, после дополнительной проверки оказывались мошенническими (их находили у кассиров).

Интересные результаты были получены при анализе программы лояльности на автозаправочных станциях (АЗК). Основным товаром здесь является топливо, покупки в призаправочных магазинах составляют малую часть от общего числа транзакций. Профиль среднестатистического покупателя в этом сегменте прорисовывается более четко: это частота покупок, предпочтение определенного вида топлива, посещение АЗК в определенные временные интервалы и т.д. Карты, по которым заправлялись разным топливом (понедельник – 50 л АИ-92, вторник – 150 л дизеля, среда – 3 л АИ-98), в 90% случаях оказывались мошенническими, в остальные 10% попадали клиенты, имеющие несколько автомобилей, или организации.

Основные преимущества применения статистических методов выявления мошенничества:

- Внедрение таких алгоритмов дает большую гибкость учета лимитов в сравнении с классическим алгоритмом, тем самым снижается процент ложных срабатываний
- Статистические метрики дают возможность контролировать сезонные колебания совершения операций
- Статистические процедуры позволяют обеспечить самокорректирующуюся логику, т.е. формирование потенциальных ограничений на поток операций осуществляется без внесения правок в параметры алгоритма
- Настройка дополнительных источников информации позволяет выстраивать логику автоматизированного реагирования на любые негативные факторы: сбои в оборудовании и программном обеспечении, массовое мошенничество по принципиально новой схеме, не подконтрольной текущей базовой логике, и пр.

В конечном счете все это оказывает положительное влияние на основные параметры работы компании. За счет повышения уровня выявления мошенничества и снижения объема ручной работы возрастает финансовая эффективность. В то же время снижается влияние человеческого фактора при экстренных корректировках схем контроля мошенничества и обработки типовых инцидентов. JI

Правила безопасности «хорошего тона»

АВТОР: АЛЕКСЕЙ СИЗОВ

«Безопасность клиентов сейчас — не только конкурентное преимущество, но и продукт, пользующийся спросом, а пресловутый «авось» в контексте ИБ уверенными темпами исчезает из нашего обихода», — полагает **Алексей Сизов, руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет».** В своей статье он рассказывает о том, как без внесения больших изменений в текущие бизнес-процессы, не требуя дополнительных манипуляций или действий со стороны клиентов, банки могут повысить защищенность от мошенничества до 97—99%.

Источник: информационное агентство Bankir.ru, январь 2014 г.

Телекомы тоже плачут

АВТОР: АЛЕКСЕЙ СИЗОВ

Все мы хоть раз в жизни слышали о том, как разводят честных пользователей мобильной связи. Но только ли на абонентов направлен взор злоумышленников??? Отнюдь! **Алексей Сизов, руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»**, пошагово описывает наиболее популярный сценарий дилерского мошенничества, приводит расчеты возможных потерь оператора, дает рекомендации по противодействию мошенникам.

Источник: Comnews.ru, июль 2013 г.

Мошенничество — как много в этом слове?

АВТОРЫ: ДМИТРИЙ МИХЕЕВ, АЛЕКСЕЙ СИЗОВ

Жертвами мошенников сегодня часто становятся целые организации, само же мошенничество может быть внутренним, внешним и клиентским. О том, какую роль играют DLP-системы в борьбе с мошенничеством в современных организациях, рассказывают специалисты компании «Инфосистемы Джет» — **Дмитрий Михеев, эксперт Центра информационной безопасности, и Алексей Сизов, руководитель направления по борьбе с мошенничеством.**

Источник: Information Security, № 1, март 2013 г.

Незаметное мошенничество – заметные убытки

АВТОР: АЛЕКСЕЙ СИЗОВ

«Если факты хищений не отражаются в клиентских обращениях или не выявляются существующими механизмами оценки рисков, можно говорить о наличии мошенничества со стороны внутренних сотрудников или клиентов», полагает **Алексей Сизов, руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет»**. В своей статье Алексей рассказывает о наиболее эффективных способах их выявления и предупреждения, характерных для сферы ритейла.

Источник: : Connect! Мир связи, № 3, март 2013 г.

Массовый DDoS – челябинский метеорит для ИБ

АВТОР: ИГОРЬ ЛЯПУНОВ

«ИБ в современной экономике – это не просто довесок к ИТ, а отдельный вид деятельности, который очень сильно влияет на бизнес», – полагает **Игорь Ляпунов, директор Центра информационной безопасности компании «Инфосистемы Джет»**, рассуждая в своей авторской колонке о DDoS-атаках как о «большом инциденте», наглядно демонстрирующем бизнесу угрозы информационной безопасности.

Источник: : ComNews.ru, март 2014 г.

Деньги «уходят в небо», или Особенности мошенничества в ритейле

АВТОР: АЛЕКСЕЙ СИЗОВ

Какие сценарии мошенничества наиболее часто реализуются в ритейловых компаниях? Каковы могут быть потери от внутреннего фрода и как с ним бороться? Существуют ли технологии, позволяющие предотвращать хищения автоматизированно? На эти и другие вопросы в своей статье отвечает **Алексей Сизов, руководитель направления по борьбе с мошенничеством Центра информационной безопасности компании «Инфосистемы Джет».**

Источник: BISA-expert, май 2014 г.

Jet Info
NEWS-BULLETIN

Главный редактор Дмитриев В. Ю.

Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01 факс (495) 411 76 02
e-mail: Jetinfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**

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