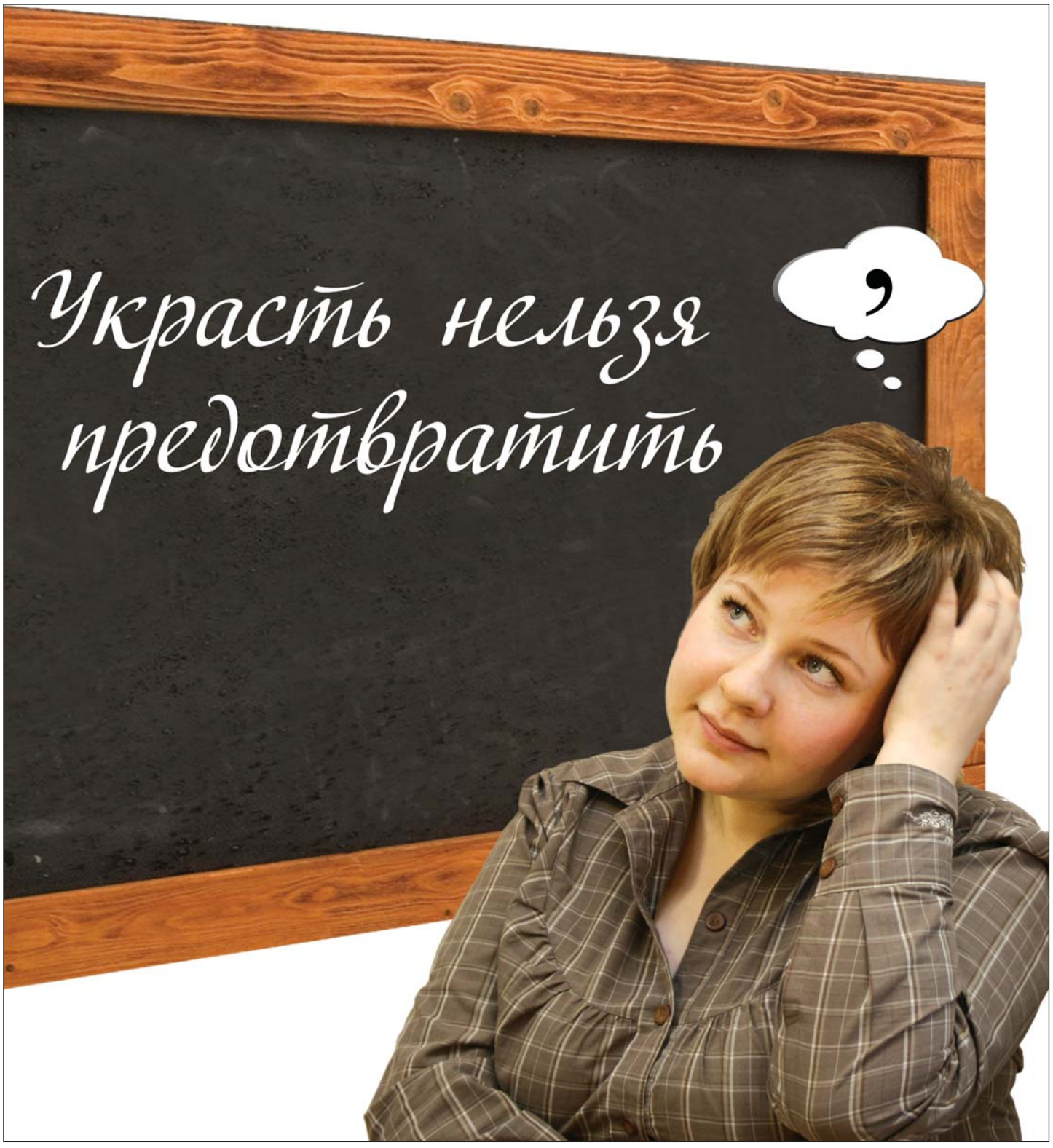
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 11 (209)/2010



Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Редакция:

Дмитриев В.Ю.
vlad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

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

Шедова Е.Л.
eshedova@jet.msk.su

Верстка:
Толоконникова Е.А.

Корректура:
Андрушко О.Ю.

Над номером работали:
Гуляев А. В.
Фефелов Д. А.
Шопин Д. В.

Издатель:
Компания «Инфосистемы Джет»

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

От редакции

Итак, в этом номере мы еще раз поговорим о фроде. Безусловно, тема не нова. Но не стоит забывать, что мошенники очень изобретательны и с завидной регулярностью «радуют» нас новыми способами того, как эффективнее для себя потратить наши с вами честнозаработанные. Поэтому чем чаще проводится апдейт информации по их деятельности и способах борьбы, тем эффективнее меры противодействия. Это как с антивирусом, который с заданной периодичностью обновляет свои базы, чтобы ваш ПК оставался «чист» и неприступен для различных вредоносных программ. С этой целью и мы решили провести своеобразную ревизию имеющихся на рынке схем мошенничества (не только в области телко, но и в нефтеперерабатывающей отрасли) и рассказать о вариантах противодействия им.

Помимо разговора о фроде в номере пойдет речь и о новых решениях в области построения сетей передачи данных — рубрика «О чем молчат проектировщики» расскажет о том, как сегодня обстоят дела в этой сфере и какие решения предлагает индустрия.

Берегите себя!

С уважением, Ваш JI

СОДЕРЖАНИЕ

Компания «Инфосистемы Джет» модернизировала ИТ-инфраструктуру компании «М.Видео» и осуществила миграцию бизнес-приложений

Компании «М.Видео» и «Инфосистемы Джет» завершили комплексный проект по модернизации ИТ-инфраструктуры и миграции бизнес-приложений SAP ритейлера на новую платформу — серверы Sun x64. Новый программно-аппаратный комплекс находится на аутсорсинге в компании «Инфосистемы Джет».

В связи с ростом бизнеса компании «М.Видео» потребовалось расширение системы SAP и добавление новых модулей. При этом существующая инфраструктура для работы бизнес-приложений SAP на базе hi-end серверов потребовала бы значительных финансовых затрат на масштабирование и эксплуатацию.

Поэтому ИТ-руководство сети «М.Видео» приняло решение о проведении проекта по модернизации серверных ресурсов с целью наращивания мощностей и оптимизации эксплуатационных расходов. В ходе проекта необходимо было произвести как межплатформенную миграцию данных и приложений и внедрение новых функциональных модулей SAP, так и переезд всей инфраструктуры из одного дата-центра в другой. На роль исполнителя, по результатам конкурса, была приглашена компания «Инфосистемы Джет», которая ранее сотрудничала с ритейлером и досконально знает ИТ-инфраструктуру компании.

Интегратор предложил несколько вариантов решения, один из которых — переход на blade-серверы Sun x64 — полностью удовлетворял требованиям как в части производительности, так и в части затрат на обслуживание, а также позволил бы масштабировать систему в дальнейшем с минимальным временем простоя.

Для соблюдения установленных сроков по запуску новых модулей SAP и минимизации времени простоя специалисты компании «Инфосистемы Джет» разработали ряд нестандартных решений, которые позволили внедрять новые бизнес-приложения в процессе модернизации инфраструктуры. С целью минимизации рисков миграция систем осуществлялась блоками (часть модулей еще работала на старом оборудовании, в то время как другая — на новом в другом дата-центре), в которые логически объединялись группы систем, интегрированных друг с другом. Такой подход позволил бы в случае возникновения нештатной ситуации осуществить «откат» к начальной конфигурации. Отметим, что в ходе реализации проекта таких действий производить не потребовалось.

Для сохранения самой возможности «отката» вся работа была построена так, что исходные системы фактически только «выключались», в них не вносилось каких-либо изменений. Все изменения производились на копиях данных, которые были заблаговременно подготовлены для каждой из систем. Это также способствовало осуществлению миграции БД больших объемов с кратчайшим временем простоя.

Переезд всей инфраструктуры комплекса систем SAP из одного дата-центра в другой, расположенный в противоположной части города, потребовал организации вспомогательных высокоскоростных каналов связи, по которым осуществлялись как миграция данных, так и взаимодействие систем, функционирующих на двух разных площадках, между собой. На случай возникновения сбоев на вспомогательном оборудовании и каналах передачи данных были разработаны решения и процедуры, которые смогли бы в кратчайшее время восстановить работу. С таким же расчетом был составлен план переезда, который обеспечил поэтапную миграцию таким образом, чтобы возможные сбои не могли нанести вред инфраструктуре SAP.

Новая инфраструктура вычислительного комплекса представляет собой кластер высокой доступности, состоящий из 14 узлов, и находится

под управлением ПО Symantec Veritas Cluster Server. Для удовлетворения строгих требований к восстановлению данных из резервных копий была проведена модернизация корпоративной системы резервного копирования.

«Перевод бизнес-приложений на новую платформу — значимый и довольно рискованный для любой компании шаг. Поэтому доверить его реализацию мы могли только профессионалам, на которых можно положиться. Команда специалистов компании «Инфосистемы Джет» смогла выполнить все задачи на самом высоком уровне и в строго определенные сроки. Отметим, что все работы по проекту проведены с минимальным временем простоя критичных для бизнеса систем, что позволило сохранить непрерывность важных бизнес-процессов компании и не допустить финансовых потерь», — комментирует Игорь Веселов, операционный ИТ-директор компании «М.Видео».

«Реализованный проект был по-настоящему сложным и интересным как с точки зрения технических решений, так и с точки зрения организационных работ. За такие проекты мы беремся с удовольствием, поскольку получаем возможность на деле продемонстрировать высокие профессиональные компетенции. Тесное взаимодействие со специалистами заказчика позволило четко и в срок реализовать все задачи проекта, в том числе осуществить нетривиальную процедуру миграции данных», — отмечает Виктор Новинский, директор по работе со страховыми компаниями и предприятиями торговли компании «Инфосистемы Джет».

Модернизированный комплекс передан на аутсорсинг сервисному центру компании «Инфосистемы Джет».

Компания «Инфосистемы Джет» интегрировала CRM-систему и контакт-центр в ОАО «Нордеа Банк»

ОАО «Нордеа Банк» и компания «Инфосистемы Джет» завершили проект по интеграции системы Oracle Siebel CRM с контакт-центром. Новое интегрированное решение позволило существенно повысить качество и скорость обслуживания клиентов банка. В рамках проекта также внедрен модуль «Маркетинг» системы Oracle Siebel CRM, который позволит банку эффективно проводить маркетинговые кампании и осуществлять кросс-продажи.

Нордеа Банк активно использует современные технологические решения. Так, например, для управления взаимоотношениями с клиентами внедрена система Oracle Siebel CRM, функционирует круглосуточный контакт-центр. С целью повышения оперативности работы специалистов банка, что особенно важно в период интенсивного роста розничных продаж, руководство банка приняло решение об интеграции CRM-системы с контакт-центром. Реализация проекта была доверена компании «Инфосистемы Джет».

Специалисты интегратора осуществили настройку и запуск специализированного ПО (интеграционный сервер), которое связывает Oracle Siebel CRM и программно-аппаратный комплекс контакт-центра. В рамках проекта был существенно расширен функционал контакт-центра и рабочего места операционистов. В частности, реализована функция автоматической идентификации звонящего и открытия карточки клиента с персональными данными и историей запросов. В зависимости от вопроса клиента система позволяет оперативно найти необходимую информацию или перенаправить звонок вместе с карточкой клиента компетентному сотруднику. Это не только сокращает время каждого диалога, но и повышает уровень удовлетворенности обслуживанием клиента, которому не требуется повторно объяснять суть звонка нескольким специалистам.

Специалисты компании «Инфосистемы Джет» внедрили и настроили модуль «Маркетинг» системы Oracle Siebel CRM. Новый функционал позволяет маркетологам банка производить анализ и точную сегментацию клиентов и проводить адресные маркетинговые кампании, учитывая индивидуальные потребности и интересы каждой группы клиентов. В результате эффективность маркетинговых кампаний выросла, а затраты существенно снизились. Система позволяет информировать клиентов о текущих акциях, новых услугах и сервисах, существенно повышая объем кросс-продаж. При этом выполнение звонков может осуществляться не только оператором, но и автоматической системой голосового оповещения (IVR).

«Высокое качество и скорость обслуживания клиентов сегодня являются обязательными составляющими банковского бизнеса, где уровень конкуренции традиционно очень высок, — рассказывает **Вячеслав Лясевич, Директор департамента розничного бизнеса ОАО «Нордеа Банк».** — Мы ценим время наших текущих и потенциальных клиентов. Использование возможностей CRM-системы в работе операторов контакт-центра позволяет сократить время на обработку запросов, увеличить скорость поиска и предоставления необходимой информации. Все это положительным образом отражается на уровне лояльности клиентов».

«Банковские услуги становятся все более высокотехнологичными — новинки в области телекоммуникаций, системы класса Hi-End, бизнес-приложения с развитым функционалом — все это уже сегодня можно найти в успешном банке. Но немаловажную роль играет интеграция различных технологий, которая позволяет достичь синергетического эффекта,— подчеркивает **Аркадий Затуловский, Директор по ИТ ОАО «Нордеа Банк».** — Специалисты компании «Инфосистемы Джет» успешно справились с поставленными перед ними задачами. В будущем мы планируем продолжить сотрудничество и вместе реализовать ряд проектов, требующих инновационного подхода и широкого набора знаний».

«Взаимопонимание и тесное сотрудничество со специалистами банка, неподдельная заинтересованность со стороны топ-менеджмента и руководителей функциональных блоков во многом определили успех этого проекта. Эксперты Нордеа Банка глубоко погружались в детали проекта, четко формулировали требования, активно помогали на всех этапах,— комментирует **Дмитрий Никитин, начальник управления продаж компании «Инфосистемы Джет».** — Мы передаем систему в руки профессионалов и уверены, что они смогут извлечь из нее максимум пользы для бизнеса».

Hitachi Data Systems упрощает и ускоряет внедрение «облачных вычислений» с помощью новой интегрированной инфраструктуры

Hitachi Data Systems Corporation, дочернее предприятие Hitachi, Ltd., объявила о выходе новых интегрированных технологий, призванных упростить и ускорить процесс внедрения «облачных» инфраструктур. Продукт Hitachi Content Platform (HCP) v4, который составляет основу линейки решений Hitachi для «облачных» инфраструктур, создан на основе передового интеллектуального хранилища данных, ориентированного на работу с контентом, и поддерживает такие функции, как новый, упрощенный автоматизированный механизм репликации, более тонкая настройка виртуальных сред хранения и возможности разнесения затрат по подразделениям. Продукт Hitachi Data Ingestor (HDI) представляет собой новый «адаптер» для платформы Hitachi Content Platform. Он поддерживает интеграцию с хранилищем HCP емкостью 40 петабайт (Пбайт), а также с новыми функциями управления данными и хранилищем, обеспечивая практически безграничные возможности хранения данных в распределенной среде без необходимости их резервного копирования. Оба предлагаемых продукта помогают провайдерам «облачных» услуг и департаментам ИТ спроектировать и построить собственную инфраструктуру для хранения, поиска и защиты данных с минимумом затрат, не прерывая работу пользователей или приложений.

Avaya выпустила программное обеспечение, предназначенное для виртуализации сетей

Avaya объявила об обновлении программного обеспечения своих коммутаторов, предназначенного для оптимизации работы в сети бизнес-приложений и сервисов за счет виртуализации.

Avaya Virtual Enterprise Network Architecture (VENA) является расширением программного обеспечения для Ethernet-коммутаторов Avaya 8600, 8800 и VSP 9000, поддерживающим новый стандарт IEEE 802.1AQ Shortest Path Bridging, который регламентирует процесс выбора множества активных маршрутов в коммутационной структуре ЦОД. Спецификация Shortest Path Bridging дополняет технологию Multiple Spanning Tree Protocol, предоставляя возможность использовать протокол маршрутизации с анализом состояния каналов передачи данных. Это позволяет коммутаторам получать информацию о кратчайших маршрутах в коммутационной структуре Ethernet и динамически адаптироваться к изменениям топологии сети.

Функциональность Virtual Services Fabric обеспечивает конфигурирование, позволяющее предоставлять сетевые сервисы «одним нажатием кнопки». Данная технология предназначена для создания «частного облака», упрощающего доступ к информации и приложениям. Кроме того, она способна исключить влияние ошибок персонала при ручном запуске, добавлении, удалении или изменении приложений в виртуальной среде.

В настоящее время программное обеспечение VENA доступно для коммутаторов Avaya VSP 9000. В феврале 2011 года им смогут воспользоваться и владельцы коммутаторов 8600 и 8800.

Экспертное мнение

Александр Гуляев, руководитель отдела сетевых проектов компании «Инфосистем Джет»: «К сегодняшнему дню большинство крупнейших сетевых вендоров выпустили или анонсировали реше-

ния, дополняющие стандартный функционал Ethernet-сети и предназначенные для удовлетворения нужд виртуализованных приложений и «облачных» дата-центров. У компании Cisco Systems это решение Unified Fabric и продукты Nexus, у Brocade — Virtual Cluster Switching (VCS) и новая серия коммутаторов VDX, Juniper заявил о создании продуктов в рамках концепции Stratus project. Все эти технологии и продукты позволяют говорить о том, что преобладающей топологией сетей дата-центра недалекого будущего будет Ethernet-фабрика.

Выпуск VENA для старших моделей коммутаторов Avaya позволяет говорить о том, что продукты, входившие в состав продуктовых линеек Nortel, продолжают развиваться в рамках рыночных трендов».

Cisco выводит на рынок новые устройства для создания виртуальной настольной среды

Cisco представила полномасштабное решение для виртуализации настольных систем и решения для организации совместной работы, создания сетей без границ и центров обработки данных, разработанные как корпорацией Cisco, так и экосистемой ведущих поставщиков решений в сфере виртуализации. Новая инфраструктура виртуализации под названием Cisco Virtualization Experience Infrastructure (VXI) решает проблемы, связанные с фрагментированностью существующих решений, которые существенно усложняют внедрение виртуальных настольных систем. Кроме того, новая инфраструктура расширяет возможности виртуализации традиционных настольных систем для обработки мультимедийных данных и видео.

Cisco также представила два не требующих клиентского ПО устройства. Они предоставляют пользователям все преимущества виртуализации настольных систем без ущерба для функций совместной работы в мультимедийной среде, присущих мощным персональным компьютерам.

Лазейка для вора

Потери на многочисленных участках процесса производства и продажи услуг телекоммуникационных компаний ежегодно складываются в общий недобор денег. Экспертные оценки доли потерь в доходах операторов сильно разнятся — от 3-4% до 25% от общего объема трафика в мире и до 4-15% в России. Сами операторы, по понятным причинам, скромничают, называя цифры в районе 1-5%.

Так видов мобильного мошенничества не счесть: GSM-пеленгаторы, локаторы, секретные диеты и тесты на IQ, перехватчики звонков и SMS-сообщений, калькуляторы точной даты смерти — все эти и многие другие использующие SMS-платежи за услуги помогают российским «мобильным» мошенникам зарабатывать более 160 млн долларов в год. И потери мобильных операторов от такой «активности» каждый год возрастают в среднем на 5-6%.

Но не только SMS-жульничество становится проблемой для операторов и абонентов. Относительно недавно по отношению к традиционным видам оплаты у абонентов сотовых операторов появилась возможность пополнять свой счет с помощью пластиковой карты.

Абоненты столкнулись с тем, что после оплаты услуг мобильной связи с их банковских карточек исчезают деньги. Дело в том, что схема привязки счета пластиковой карты к телефону уязвима, если кроме данных о номере банковской карты и срока действия не требуется для оплаты больше никаких данных. Более полная информация (CVC — код верификации, ФИО владельца) при оплате с карты во многом повышает уровень безопасности подобных операций. Нельзя сказать, что данный вид оплаты услуг уж очень популярен. По словам экспертов, его используют десятки или сотни человек, но никак не тысячи. Конечно, масштаб бедствия невелик, но это не значит, что следует оставить все как есть и не реагировать на такие случаи мошенничества. Ведь это явная прореха, которую нужно устранять.

Как бы там ни было, но утечка доходов объективно существует. И минимизировать убытки операторов призваны системы гарантирования доходов (Revenue Assurance Systems, RAS) и борьбы с мошенничеством (Fraud Management Systems, FMS). Фактически системы гарантирования доходов можно рассматривать как логическое продолжение систем анализа контроля операционных рисков и их развитие до уровня эксплуатации. В основе таких решений лежит анализ информации об оказанных услугах, потерях в системах коммутации, предбиллинга и биллинга. Не стоит пренебрегать такими иснтрументами. Ведь давно известно, что, скажем, в России мошенники всегда были хитры на выдумку. Каждый год они придумывают что-то новое. Так что, закрывая глаза даже на небольшие потери, можно просто не заметить, как количество подобных вырастет в геометрической прогрессии, а ведь это финансовые риски, не говоря уже о репутационных.

Подготовлено по материалам:
http://www.rian.ru/society/20091223/198407633.html
http://www.svem.ru/blog/likbez/747.html
http://netfraud.ru/publication/newspaper/21
http://finam.info/news/article212A900001/default.asp?id=need

Прагматическая классификация телекоммуникационного фрода

Дмитрий Шопин,
руководитель направления гарантирования доходов и борьбы с мошенничеством компании «Инфосистемы Джет»

«Вор не скрывал радости:
- Нет-нет, начальнички, не выгорит это делишко у вас, никак не выгорит. <...>
Нет, не придумали вы еще методов против Коти Сапрыкина...
Жеглов мрачно молчал всю дорогу и, когда уже показалось отделение милиции, сказал ему тусклым невыразительным голосом:
- Есть против тебя, Кирпич, методы. Есть, ты зря волнуешься...»

Братья Вайнеры. «Эра Милосердия»

Не будет откровением мысль, что невозможно составить исчерпывающий список всех существующих видов телекоммуникационного фрода. С одной стороны, постоянно возникают новые услуги, новые технологии и, как следствие, новые виды фрода. С другой стороны, телекоммуникационное мошенничество, в отличие от традиционных угроз информационной безопасности, весьма «операторо-специфично». Оно слишком сильно завязано на конкретные реализации тех или иных услуг у определенного оператора, на его системы, его процессы и т. д. Поэтому помимо общих проблем фрода, у каждой телекоммуникационной компании будет свой специфический набор фродовых схем, присущих только ей.

Оператору необходима классификация видов мошенничества, которая помогла бы ему упорядочить деятельность по борьбе с фродом в своих сетях.

В настоящее время существуют различные классификации телеком-фрода. Обычно в их основе лежит деление фрода по функциональным областям — роуминговый фрод, транзитный фрод, VoIP-фрод, SMS-фрод, PRS-фрод. Кроме того, в отдельные группы часто выделяют внутренний фрод и subscription-фрод. Практическая ценность таких классификаций неоднозначна. С одной стороны, некоторые комбинированные виды фрода трудно отнести к определенной категории в такой классификации. Например, smishing — использование SMS-рассылок с целью обманным путем вынудить абонентов сделать звонок на PRS-номер. Куда это отнести — к SMS-фроду или PRS? Или несанкционированная перемаршрутизация транзитного трафика злонамеренным сотрудником — что это внутренний фрод или транзитный?

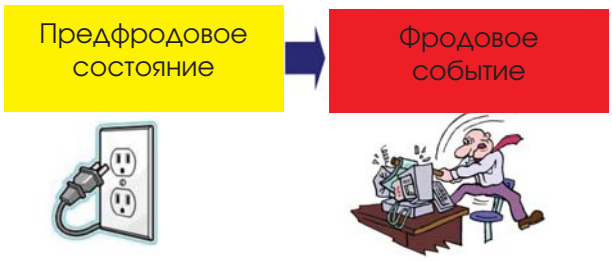
С другой стороны, такая классификация никак не облегчает оператору задачу развития у себя функции противодействия мошенничеству. Например, понятие «транзитный фрод» включает в себя большое количество мошеннических схем, которые, хотя и связаны с одной услугой — транзит трафика, тем не менее выявляются с помощью абсолютно разных методов и инструментов.

Поэтому, при планировании своей деятельности по развитию функции фрод-менеджмента, мы предлагаем операторам связи воспользоваться типологизацией фродовых схем на основе методов их выявления, детектирования. Такая классификация представляет собой законченный, ограниченный набор классов фрода. Каждая вновь возникающая, в том числе уникальная для данного оператора, фродовая схема может быть отнесена к одному из этих классов в зависимости от того,

какой метод можно использовать для ее детектирования.

В качестве отправной точки для такой классификации служит представление о любой фрод-схеме, как о сочетании двух составляющих. Первая из них: ПРЕДФРОДОВОЕ СОСТОЯНИЕ. Это некая ситуация, сочетание условий, создавшееся в настройках систем оператора, в его бизнес-процессах, которое делает возможным реализацию той или иной фродулентной схемы. Например, такой вид фрода как «фантомные абоненты». Это абоненты (или интерконнект-партнеры, или контент-провайдеры, т. е. кто-то, кто является пользователем услуг оператора связи), которые получили технологический доступ к услугам связи, но при этом не зарегистрированы в биллинговой системе. Это и есть предфродовое состояние — наличие рассинхронизации данных между сетевыми элементами и системами учета. Это еще не сам фрод, но теперь он легко может осуществиться — клиент воспользуется услугами, которые могут быть не оплачены.

Вторая составляющая — собственно ФРОДОВОЕ СОБЫТИЕ. Это то действие, ради которого и организована фродовая схема. В случае фантомных абонентов фродовым действием будет звонок, SMS, передача данных, транзит трафика, совершенные этим самым абонентом и неоплаченные вследствие его отсутствия в биллинговой системе.

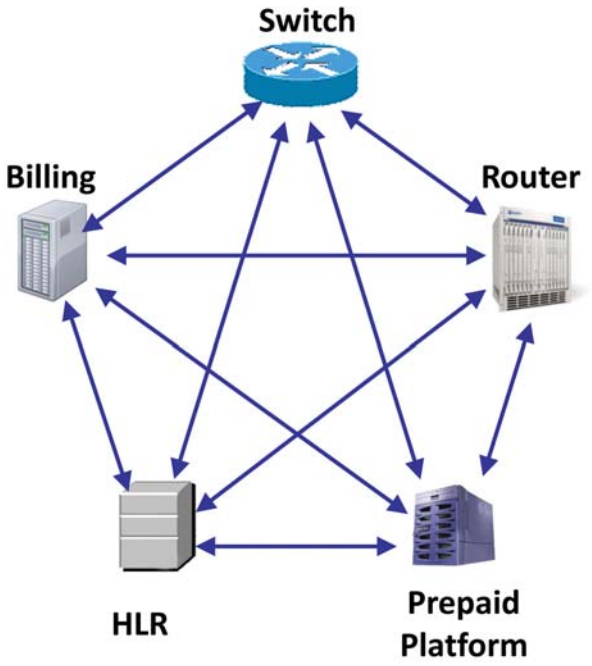


Нужно отметить, что далеко не всегда особое предфродовое состояние необходимо. Многие фродовые схемы не требуют никаких специфических ситуаций в системах и процессах оператора. Например, SMS-спам или клонирование SIM-карт, или всевозможные мошенничества с использованием социальной инженерии (fishing, vishing, smishing). Для того чтобы осуществить эти мошеннические действия, необходимо просто наличие оператора связи как такового и наличие у него необходимой телекоммуникационной услуги.

Такое разделение фродовой схемы на две составляющие служит отправной точкой для прагматической классификации телекоммуникационного фрода — классификации на основе общих методов детектирования мошенничества.

Первая большая группа видов фрода — мошенничества, которые можно детектировать на раннем этапе по их предфродовому состоянию. Здесь можно выделить два класса методов детектирования:

- **Первый – поиск рассинхронизации.**



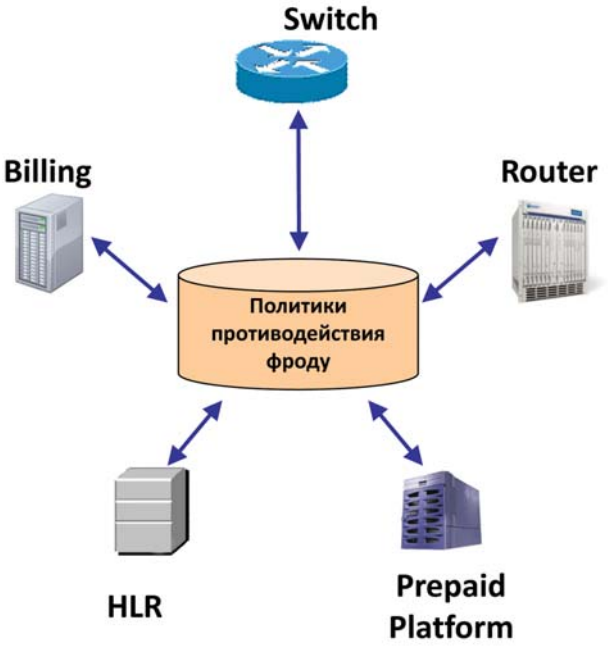
Этот метод направлен прежде всего на выявление рассинхронизации данных между системами NSS (сетевыми элементами) и системами, ответственными за тарификацию и оплату предоставленных сервисов.

Например, для детектирования уже упомянутых фантомных абонентов используется сопоставление данных HLR и биллинга (в случае мобильных операторов) или баз данных цифровых АТС, access-листов софтсвитчей для фиксированной или IP-телефонии. Подобные сверки, конечно, не ограничиваются простым поиском записей, имеющихся в одной системе и отсутствующих в другой. Этот же подход используется и для выявления расхождений в параметрах одного и того же абонента. Это актуально, например, для услуги широкополосного доступа, когда абоненту в биллинге установлен тарифный план со скоростью, скажем, 1Мбит/с с соответствующей оплатой, а на маршрутизаторе предоставлен канал 10Мбит/с. Аналогичная ситуация может возникать и у операторов, предоставляющих в аренду каналы другим операторам или корпоративным клиентам.

Решения, обеспечивающие детектирование фрода путем сверки данных из различных систем, называются системами класса Platform Integrity. Правильным системам Platform Integrity абсолютно безразлично, какие данные, из каких устройств в них сравниваются. Оператор может самостоятельно (или с помощью внешних консультантов) определить источники исходных данных, определить поля, которые нужны, и настроить необходимые сверки с нужной периодичностью.

Второй класс методов выявления предфродовых состояний:

- **Соответствие политикам безопасности.**



Методы данного класса направлены на выявление технологического фрода, связанного с внесением изменений в конфигурации систем. Например, отключение генерации xDR для групп абонентов, определенных направлений или присоединенных операторов. Другой пример — обнаружение потенциальных уязвимостей PBX — дефолтных паролей, незащищенных переадресаций с внешних линий на внутренние экстеншены, открытых удаленных доступов через модем и т. п.

Системы, в которых реализованы подобные методы детектирования фрода, это системы класса Compliance Management Systems.

Как уже говорилось, далеко не все виды технологического фрода определяются по их предфродовому состоянию. И поэтому можно выделить вторую большую группу методов детектирования телеком-мошенничества — обнаружение собственно фродовых событий.

По определению, такой метод требуется для анализа трафика. Причем здесь под трафиком следует понимать не только трафик как таковой, т.е. xDR голосовых вызовов, коротких сообщений, сессий передачи данных и так далее. Здесь понятие трафика более широкое и включает в себя вообще все данные, фиксирующее какое-либо событие в системах оператора связи — это и платежи, и заявки на активацию/деактивацию услуг, какие-то внутренние транзакции, например, корректировки счетов абонентов, выполняемые отделами обслуживания.

В данной группе методов — детектирование фродовых событий — можно выделить следующие классы методов:

- **Анализ отдельного события.**

Характерным примером фрода, детектируемого с помощью анализа каждой конкретной транзакции, является SMS-фрод в его различных проявлениях. К этому же классу следует отнести и все те фродстерские манипуляция, которые могут быть обнаружены и пресечены путем сравнения их параметров с эталонными значениями, стоплистами. Это, например, «черные списки» фродоопасных направлений звонков — Куба, Каймановы Острова и тому подобное.

Системы, реализующие данные методы детектирования, можно подразделить по двум критериям.

Первый критерий — режим противодействия. В этом смысле системы анализирующие каждое отдельное событие, могут обеспечивать либо активную защиту, либо пассивную. В первом случае, весь трафик определенного типа маршрутизируется в режиме реальном времени в систему,

которая анализирует каждое событие на предмет его фродулентности и, в случае выявления таковой, блокирует эту транзакцию (либо задерживает для рассмотрения аналитиком). Типичный пример такой системы — SMS-Firewall, обеспечивающий защиту в реальном времени от всех видов SMS-фрода. Такой же подход используется и для шейпинга IP-трафика, например, для того, чтобы исключить использование мобильного интернета для несанкционированных VoIP-звонков или запретить p2p-файлообмен для интернет-пользователей.

Второй критерий, по которому можно разделить системы, анализирующие каждую конкретную транзакцию, основан на том, анализируется ли реальный трафик реальных абонентов либо же специальным способом сгенерированные тестовые события. Дело в том, что существует целый ряд фродовых схем, характерных для межсетевого трафика, особенность которых в том, что и предфродовое состояние, и сами фродовые события создаются вне сетей и систем оператора-жертвы. Поэтому обнаружить эти признаки фрода в реальном трафике у оператора нет возможности. Типичный пример — нелегальный транзит и терминация трафика. Если присоединенный оператор на местном уровне пропускает МгМН-трафик, подменяя А-номера на свои собственные и т. о. выдавая этот трафик за свой собственный, обнаружить, а главное, подтвердить это можно только сгенерировав тестовый звонок из-за рубежа или другого региона страны и увидев, что этот звонок пришел как местный.

Другой пример интерконнект-фрода, выявляемого только с помощью тестирования — манипуляции транзитного оператора с длительностью вызовов. Выявить такое мошенничество можно только с помощью тестовых звонков с точным измерением длительности на сторонах А и Б.

Для этих целей существуют как программно-аппаратные решения (если у оператора есть возможность разместить элементы системы в других странах, сетях), так и сервисные продукты, когда сторонняя компания предлагает свои услуги по генерации тестового трафика, а также по дальнейшему сбору и анализу данных.

Следующий класс методов детектирования фрода, это:

- **Контроль целостности потоков данных «трафик->деньги».**

Это один из наиболее универсальных подходов (хотя и самых реактивных), применимых в тех случаях, когда никакими иными, более оперативными способами фрод обнаружить нельзя, и когда фрод связан с получением услуг оператора без надлежащей оплаты. (Рис. 1.)

Системы, реализующие данный подход, — это системы класса Revenue Chain Control или, как их еще называют, Switch-To-Bill Measuring Systems.

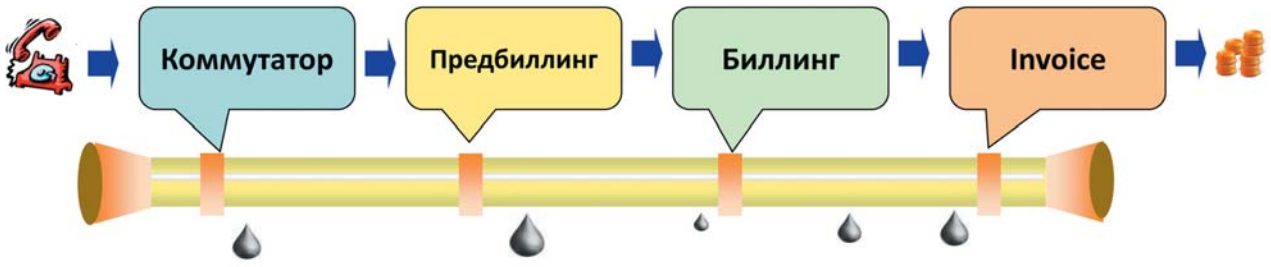
И, наконец, последний класс методов детектирования (и видов фрода):

- **Анализ профилей поведения.**

Это наиболее общий поход к выявлению фрода, ориентированный на косвенные признаки мошенничества — нестандартную активность, резкое изменение поведения абонентов или партнеров, превышение различных порогов и так далее. Такой метод, хотя и довольно неоперативный, часто является единственно возможным. Например, при выявлении спама методы статистического анализа являются незаменимыми, так как, с одной стороны выявляют спаммерский профиль поведения, а с другой — еще и предоставляют информацию другим системам, более активного действия. Например, модули анализа поведения абонентов, входящие в системы противодействия SMS-фроду, выявляя спаммерскую активность, обновляют «черные списки», библиотеки ключевых слов, с помощью которых уже системы активного действия могут предотвращать рассылки в реальном времени.

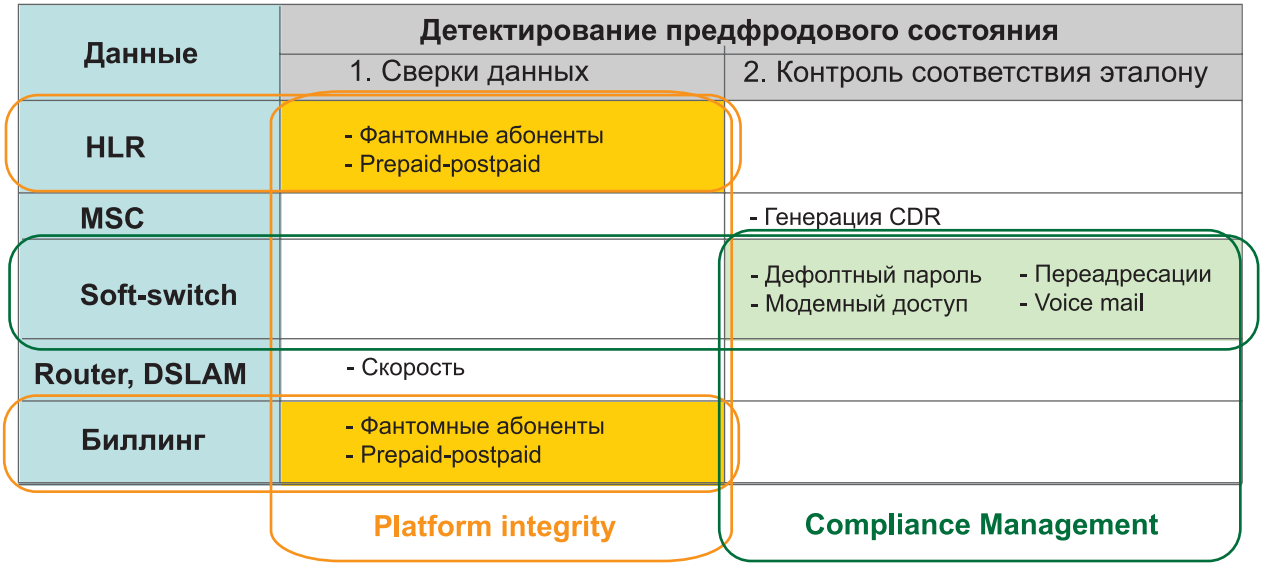
Таким образом, используя данный подход к классификации телекоммуникационного фрода,

Рис. 1.



оператор может построить осмысленную, экономически обоснованную стратегию развития у себя инструментов фрод-менеджемента. Для этого необходимо осуществить лишь несколько последовательных шагов:

1. Провести в компании фрод-аудит, определив существующие в своих сетях и системах мошеннические схемы.
2. Построить матрицу рисков фрода для своей компании, распределив виды мошенничества по кластерам, каждый из которых представляет собой сочетание определенного метода детектирования и необходимых для него исходных данных.
3. С учетом суммарного эффекта от всех видов фрода, попавших в один кластер, зависящего как от количества фродовых схем в нем, так и от критичности каждой из них, приоритезировать данные кластеры, а значит и системы, которые необходимо внедрить для контроля каждого кластера мошенничества.
4. Внедрять.



Статья опубликованна в № 10, 2010 журнала «Connect! Мир связи»

Борьба с потерями доходов на заправочных комплексах

Дмитрий Фефелов,
руководитель направления управления доходов в ТЭК компании «Инфосистемы Джет»

Современный бизнес-процесс реализации нефтепродуктов («Downstream») является сложным с точки зрения управления и контроля. Логистическая цепочка данного процесса состоит из множества различных объектов (НПЗ, нефтебаз, АЗК), удаленных друг от друга, и штаб-квартиры компании с большим количеством разнообразных ИТ-систем. Поэтому становится возможной потеря доходов на любом участке этой цепочки *(рис. 1)*.

Причины потерь могут быть различными — от простых утечек нефтепродуктов до весьма сложных сценариев мошенничества. Например, махинации с замерами и документами с последующим хищением «излишков», удаление транзакций в системах налива, неправильная калибровка и т.п. По оценкам различных экспертов средний уровень текущих потерь доходов можно оценить на уровне 1-5% выручки в «развитых» странах, где уже внедрены различные контроли для борьбы с потерями доходов, и около 20% выручки в «развивающихся», где контроли отсутствуют либо их внедрение только начинается. Естественно, компании заинтересованы в максимально возможном снижении потерь доходов при реализации нефтепродуктов.

Рис. 1. Потеря доходов в Downstream

Существующие на сегодня методы борьбы с потерями доходов, которые уже используют или могут использовать нефтяные компании, можно условно разделить на две группы.

К первой относятся так называемые «традиционные» методы — это инвентаризации, видеонаблюдение, контрольные замеры, инспекции, контролируемые поставки, сверки отчетности, выборки и анализ транзакций и т.п. К сожалению, «традиционные» методы имеют серьезные ограничения на применение. Во-первых, все они ориентированы на реактивное реагирование на проблему, т.е. обнаружение уже состоявшегося факта потери доходов со значительным отставанием момента обнаружения потерь от момента возникновения потерь. Очевидно, что объем реальных потерь доходов при этом может становиться существенным. Во-вторых, применение этих методов требует серьезных затрат ресурсов компании (в первую очередь — трудовых). И наконец, самые существенные ограничения, которые являются следствием предыдущего — выборочность и периодичность. Поэтому при попытке внедрения «традиционных» методов на полный постоянный контроль цепочки получения доходов, т.е. все существенные причины потерь («End-to-End»), затраты на осуществление контроля во многом превышают обнаруживаемые потери доходов. Таким образом, «традиционные» методы,

в силу описанных особенностей, не позволяют полностью контролировать весь процесс реализации нефтепродуктов.

Вторую группу составляют «современные» подходы. Они основаны на применении ИТ-систем. В качестве основы для системы борьбы с потерями доходов могут использоваться как BI-системы, так и специализированные системы оперативного контроля типа Revenue Assurance или Business Assurance (если контролируется не только поток выручки). Основными преимуществами первых являются экономия ресурсов при эксплуатации той же BI-системы, которой пользуются другие подразделения компании, и возможность анализировать большие массивы данных из различных источников. Для вторых — «заточенность» для оперативного создания контролей и выявления потерь доходов по любым векторам и большая независимость контрольного процесса от бизнес-процесса создания доходов. Кроме этого у компании есть возможность самостоятельно попробовать создать систему, подобную Business Assurance. Правда необходимо адекватно оценить трудозатраты и время для создания и отладки такой системы. Далее более подробно остановимся на системах Business Assurance, как наиболее проработанном на сегодняшний день инструменте борьбы с потерями доходов.

При использовании систем Business Assurance «рутинные» операции контроля автоматизируются. К таковым относятся выгрузка необходимых данных, их нормализация, сверка по заданным критериям и с заданной периодичностью, выявление несоответствий, накопление доказательной базы для передачи в правоохранительные органы, создание отчетов в необходимых срезах, отслеживание изменений и т.д. При этом обеспечивается сужение рисковых областей для применения «традиционных» методов, что позволяет существенно повысить эффективность администрирования всего процесса реализации нефтепродуктов и минимизировать потери доходов. Данные системы уже отлично проявили себя в различных компаниях: телекоммуникационных, финансовых, электроэнергетике и с недавних пор начали применяться в нефтегазовых компаниях. Принцип их работы прост: система с заданной периодичностью автоматически «собирает» данные из различных источников компании, которые, по сути, являются контрольными точками (датчики, уровнемеры, счетчики, системы налива, платежные системы и т.д.). Далее она интегрирует все собранные данные в сопоставимых форматах в центральной базе данных и затем с помощью настраиваемых сверок и правил производит анализ, и определяет несоответствия и ошибки, приводящие к потере доходов компании. *(Пример сверки, осуществляемой системой, приведен на рис.2.)*

Опираясь на опыт экспертов компании «Инфосистемы Джет» в развертывании систем Business Assurance, можно выделить следующие ключевые этапы при внедрении данных систем:

- аудит контролируемого бизнес-процесса или его частей и разработка адекватных дизайнов контрольных процессов, покрывающих все существенные риски потерь доходов;
- разработка технического задания на внедрение системы, описывающего необходимые источники данных (контрольные точки), реализуемые контроли и отчетность;
- внесение в систему потоков данных из контрольных точек и настройка бизнес-логики сверок;
- развертывание системы на выбранные участки бизнес-процесса *(пример развертывания системы для цепочки «нефтебаза — АЗК» можно увидеть на рис.3);*
- «тонкая» настройка системы в процессе эксплуатации, внесение дополнительных контролей, написание процедур и регулярный контроль за эффективностью использования системы (проверка отчетов системы о реагировании ответственных лиц на предупреждения, выдаваемые системой).

В результате использования системы Business Assurance собственники и топ-менедж-

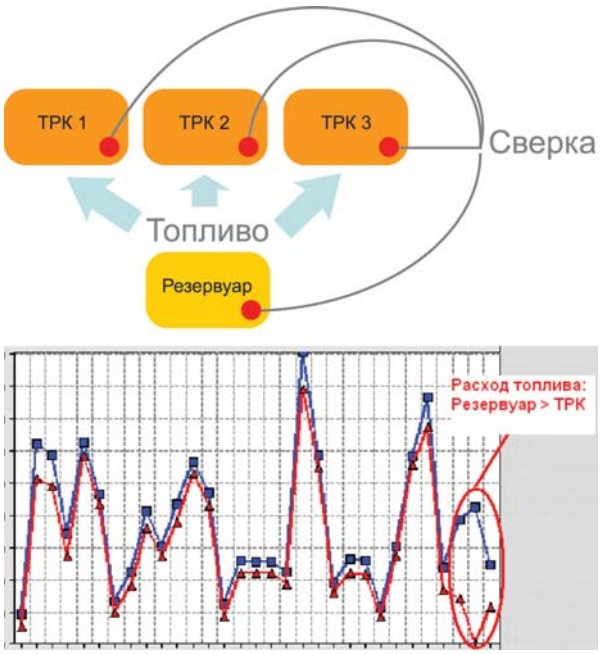


Рис. 2. Пример сверки счетчиков топливораздаточных колонок (ТРК) и расхода топлива в резервуаре на АЗК

мент компании обретают «мощный» объективный и оперативный инструмент контроля полной цепочки получения доходов от реализации нефтепродуктов.

Для специалистов по контролю реализации нефтепродуктов система Business Assurance — удобный инструмент анализа, выявления и оценки потерь. Конечные же потребители в результате получают более высокое качество обслуживания за счет снижения ошибок при заправке их автомобилей и сокращения заложенных в ценах потерь доходов. Таким образом, выигрывают практически все.

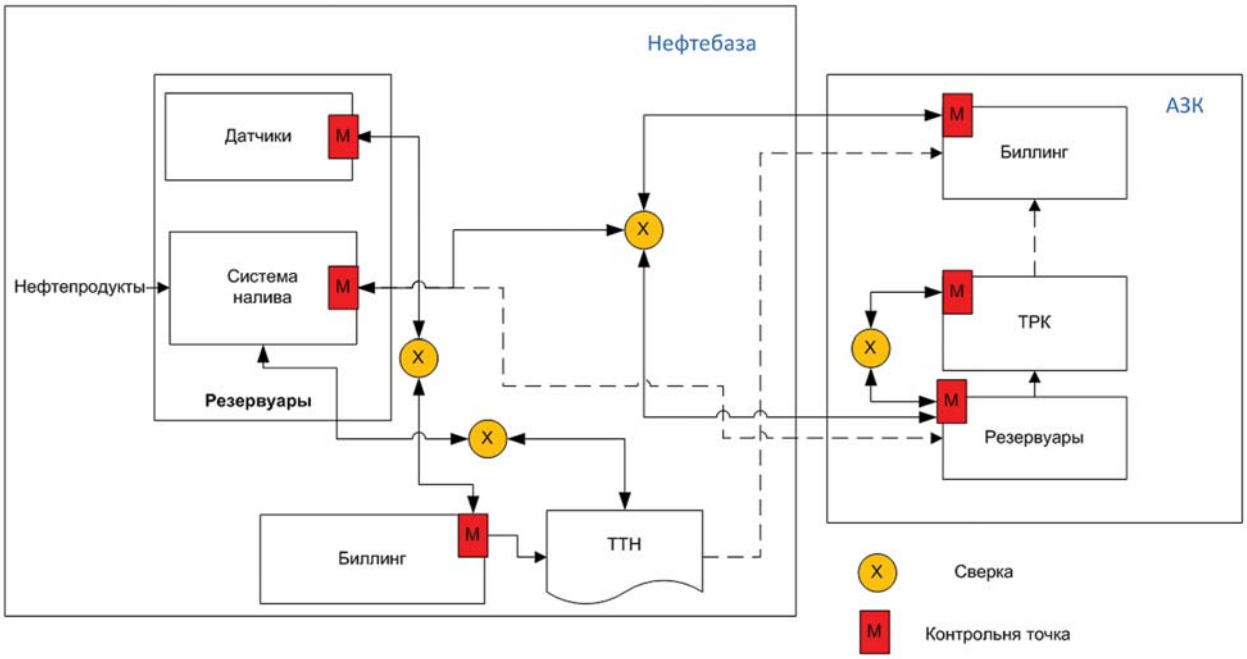


Рис. 3. Пример развертывания системы Business Assurance

Ускорение в 10 g

Александр Гуляев,
руководитель отдела сетевых проектов компании «Инфосистемы Джет»

Рост вычислительных мощностей серверного оборудования, тенденции перехода к виртуализации сервисов (размещение нескольких виртуальных серверов на одной аппаратной платформе) и связанное с этим увеличение объема сетевого трафика на сервер приводит к тому, что пропускной способности сетевых интерфейсов серверов (1 Гбит/с) зачастую оказывается недостаточно. Одним из решений данной проблемы является использование современных технологий Ethernet, позволяющих, кроме повышения скорости передачи данных до 10 Гигабит/с, обеспечить конвергентный транспорт (транспортные сети, которые могут сочетать оптическую коммутацию (на электрическом и на оптическом уровне), коммутацию SDH/SONET и пакетную коммутацию, предоставляя множество решений для транспортировки трафика) для трафика данных и систем хранения.

В настоящее время для дата-центров прорабатываются решения, в которых количество портов 10G составляет до 50%, а подключение к сети blade-шасси на скорости 10G — уже устоявшийся тренд.

Какие решения сегодня в этой области предлагает индустрия нам рассказал Александр Гуляев, начальник отдела сетевых проектов компании «Инфосистемы Джет».

J.I.: Какие недостатки существуют у «традиционных» решений по построению ЛВС дата-центра? Какова текущая ситуация в этой области?

А.Г.: Называя какие-либо решения «традиционными», следует сразу ожидать появления вопроса о «нетрадиционных» решениях, со всеми вытекающими последствиями. Поэтому я бы говорил, прежде всего, о том, что сегодня требуется современным дата-центрам от сетей передачи данных, и как сетевая индустрия отвечает на эти требования.

Первая тенденция касается магистралей ЛВС дата-центров. Объемы трафика между различными серверами в современных приложениях сравнимы с объемами трафика «клиент — сервер». При общении между серверами, расположенными в разных серверных и/или дата-центрах, трафик проходит через магистраль. Для дальнейшей виртуализации и «мобилизации» приложений необходимы магистрали, способные передавать все возрастающие объемы данных. Сегодня можно часто наблюдать, что скорость сетевых интерфейсов на доступе (соединения «сервер — коммутатор») и на магистрали (соединения между коммутаторами) одинаковая. Это может приводить к перегруженности магистрали трафиком и, как следствие, к проблемам в работе приложений. Если в ЛВС находятся production-сервера, что актуально для операторов связи, могут снизиться бизнес-показатели.

Конечно, существует «обходное» решение, позволяющее увеличить пропускную способность магистрали. Для этого несколько гигабитных портов объединяются в один логический канал большей пропускной способности. Но у такого решения есть свои минусы — нужны дополнительные порты и слоты коммутаторов, при этом используется большое количество кабелей, и трафик одного потока данных не может превышать 1 Гбит/с.

Отдельным вопросом в этой области стоит использование гигабитной ЛВС для решения задачи резервного копирования (РК). Backup серве-

ров, имеющих большие объемы хранимых данных, через такую сеть является неэффективным решением, т.к. время резервного копирования получается очень большим. К тому же, при выходе из строя аппаратной части серверов время восстановления сервиса зависит, в том числе от скорости восстановления резервной копии на сервер. Скорость восстановления backup-а зависит от скорости сети, т.е. время восстановления сервиса напрямую зависит от скорости сети. Поэтому для серверов с большими объемами данных часто применяют резервное копирование через SAN, что требует дополнительного оборудования и ПО. А это удорожает решение.

J.I.: Какие еще системы испытывают на себе недостаток пропускной способности? С какими минусами им приходится сталкиваться?

А.Г.: Относительно этой темы можно также говорить о системах хранения данных. Исторически СХД развивались на технологии FC (Fibre Channel). Этому способствовал и тот факт, что технология FC с решениями на 4G и 8G давала преимущества по скорости передачи данных. С появлением 10G Ethernet стали использоваться хранилища данных с файловым доступом (NAS[1]), имеющие 10G Ethernet-интерфейсы. Более того, сейчас на рынке уже есть хранилища с блочным доступом на базе технологии Fibre Channel over Ethernet (FCoE), также использующие указанные выше интерфейсы. Скорость передачи данных у таких устройств сравнима с СХД на базе FC.

Следует отметить, что NAS на технологии Ethernet ниже по стоимости внедрения и обслуживания, по сравнению с устройствами, имеющими интерфейсы FC. Очевидно, что устройства хранения бывают различных классов, и далеко не для всех приложений и систем можно применять «дешевые» NASы. Но в целом можно сократить вложения в системы хранения, если сеть дата-центра строится с достаточным запасом пропускной способности и имеет порты 10G Ethernet.

J.I.: Что можно посоветовать в сложившейся сегодня ситуации, как помочь решить проблему недостаточной пропускной способности?

А.Г.: Решение проблемы магистралей ЛВС лежит в использовании агрегированных 10G-каналов или в уже появляющихся на рынке 100G Ethernet-интерфейсов. Для соединения дата-центров, разнесенных на расстояние более 10 км, работоспособным на данный момент является первый способ. Но отметим, что предлагаемое ведущими производителями оборудование ядра сети уже сейчас поддерживает линейные платы с 100G интерфейсами. И в перспективе, когда стоимость этих плат упадет до разумных значений и появятся «дальнобойные» 100G оптические трансиверы, можно будет их добавить к вашим ЛВС.

J.I.: Что может измениться в части систем резервного копирования при построении сети с 10G-интерфейсами?

А.Г.: С точки зрения организации резервного копирования, подключение серверов к сети интерфейсами 10G Ethernet позволит, в ряде случаев, отказаться от использования сети хранения данных и ПО медиа-серверов, а также сократить время РК. При этом возможно существенное сокращение количества оборудования и ПО, а соответственно, и стоимости его поддержки.

Для систем хранения данных наличие 10G-подключения на уровне доступа позволяет внедрять СХД с 10G-интерфейсом, в том числе – поддерживающие протокол FCoE для быстрого блочного доступа к данным. Расширяются возможности использования более дешевых устройств файлового доступа на базе 10G-подключений и протоколов типа NFS, SAMBA.

В целом все эти действия могут повлечь за собой пересмотр существующих классов данных в сторону перевода самых низших из блочного доступа в файловый или создания новых классов данных. В любом случае, здесь могут быть заложены различные механизмы экономии средств.

J.I.: Можно ли сказать, что вся идея заключается исключительно в использовании более скоростного Ethernet – в 10 раз быстрее, чем один гигабит? Или есть какие-либо существенные инновационные изменения в самой технологии?

А.Г.: Безусловно, есть.

Прежде всего, это целый набор стандартов, разработанных и принятых IEEE[2], добавляющих сетям Ethernet новые качества – управление тра-

1 Network Attached Storage – сетевая система хранения данных

2 IEEE (англ. Institute of Electrical and Electronics Engineers) (I triple E - «Ай трипл и») – Институт инженеров по электротехнике и электронике. Международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки стандартов по радиоэлектронике и электротехнике. IEEE издает третью часть мировой технической литературы, касающейся применения радиоэлектроники, компьютеров, систем управления, электротехники.

I. Требования к сетевому оборудованию ЛВС современного дата-центра

1.Поддержка технологий:

- поддержка стандартов CEE как расширения Ethernet для дата-центров на уровне доступа и ядра/агрегации;
- поддержка возможности построения конвергентных сетей дата-центров с поддержкой FCoE на уровне доступа;
- наличие технологий кластеризации оборудования доступа и ядра/агрегации или виртуализации сети;
- поддержка архитектур типа Ethernet Fabric для уровня доступа;
- поддержка VLAN 802.1Q с большим количеством VLAN ID (4096);
- поддержка большого количества групп агрегации (802.3ad) и интерфейсов в группе;
- поддержка L3 на уровне ядра, протоколов FHRP (VRRP, аналогичные), протоколов динамической маршрутизации.

2. Пропускная способность, расширяемость, высокая плотность портов 1G/10G:

- минимальная блокируемость оборудования, желательно – коммутация wire-speed;
- возможность upgrade путем установки линейных плат с интерфейсами 100G/40G;
- гибкое наращивание функционала путем добавления лицензий;
- возможность наращивать производительность линков от доступа к уровню ядра/агрегации в соответствии с ростом нагрузки (трафика) с минимальным прерыванием сервисов.

3. Конструктив, размещение, управление, мониторинг:

- расширяемость за счет установки различных дополнительных линейных карт или модулей;
- удобство размещения в стойке, различные форм-факторы шасси.

фиком и перегрузками в сети, классы обслуживания и управление полосой пропускания для различных видов трафика, позволяющие избежать потерь фреймов и превращающих Ethernet из транспорта с негарантированной доставкой пакетов в среду без потерь (lossless). Эти стандарты часто объединяют под аббревиатурами CEE (Converged Enhanced Ethernet) или DCB (Data Center Bridging): IEEE 802.1Qbb – Priority-based Flow Control (PFC), IEEE 802.1Qaz – Enhanced Transmission Selection (ETS), IEEE 802.1Qau – Quantized Congestion Notification (QCN), DCBX – Data Center Bridging Exchange Protocol.

Следует отметить появление устройств, поддерживающих протокол IETF TRILL, представляющий собой эффективную замену традиционным протоколам резервирования типа xSTP в дата-центре и предоставляющий возможность доставки пакетов на уровне Layer 2 по множественным альтернативным маршрутам.

Кроме того, не так давно рабочей группой T11 института INCITS[3] была принята спецификация протокола FCoE (FC-BB-5), обеспечивающего конвергенцию трафика сетей передачи данных и СХД через 10G Ethernet-транспорт.

Помимо технологий, зафиксированных в виде стандартов, различные вендоры предлагают свои «фирменные» решения, например, обеспечивающие виртуализацию оборудования доступа, единое удобное управление оборудованием, организацию Ethernet- фабрики (Ethernet Fabric).

В последнее время на рынке появляется все больше решений, поддерживающих указанные выше технологии и стандарты.

Есть и некоторые исключительно технические новшества, например – медное соединение 10G, соединение на короткую длину (до 5 метров) с помощью кабелей Twinax или 10G-соединения с помощью активных оптических кабелей (AOC). Все они предназначены для снижения стоимости 10G-подключений.

J.I.: Какие пути перехода на новую технологию возможны для заказчиков, эксплуатирующих гигабитную ЛВС в своем дата-центре?

А.Г.: Начинать можно с поэтапной замены оборудования доступа в серверных на поддерживающие CEE и виртуализацию ToR (Top-of-the-Rack) коммутаторов доступа, расширения использования продуктов NAS, перевода на файловый доступ части объемов данных.

Затем перейти к организации интеграции с SAN через FCoE-коммутаторы, поддерживающие

3 Технический комитет T11, входящий в состав Международного комитета по стандартам в сфере ИТ (InterNational Committee for Information Technology Standards - INCITS), аккредитованного Американским национальным институтом стандартов (ANSI). Занимается стандартизацией протоколов высокоскоростной передачи данных.

подключение непосредственно к FC и multihop FCoE; перевести блочный доступ на FCoE/CEE-транспорт через естественную замену/модернизацию дисковых систем.

Для крупных дата-центров потребуется модернизация ядра ЛВС путем замены оборудования на новое ядро, поддерживающее CEE и имеющее высокую плотность 10G- портов.

Все эти мероприятия могут быть выполнены как в рамках утвержденной программы модернизации, так и в связи с «моральным» устареванием существующего оборудования.

J.I.: Так какие выгоды получает заказчик в случае применения подобных технологий?

А.Г.: Выгоды от применения 10G и конвергентных решений можно получить за счет сокращения объемов кабельных соединений (СКС) при строительстве новых и эксплуатации старых серверных. При использовании конвергентного транспорта существенно сокращается количество коммутаторов в СХД. Появляется уже упомянутая выше возможность перехода к упрощенной технологии резервного копирования с сокращением количества Media-серверов и ряда других устройств. Этому способствует повышение производительности ЛВС (10G), использование конвергированного транспорта. Снимаются возможные ограничения виртуализации вычислительных мощностей. А благодаря виртуализации и применению Blade-систем минимизируется количество физических подключений к сети, уменьшаются требования к занимаемому месту в серверных и, как следствие, — к количеству серверных помещений. Сокращается время восстановления серверов при аварии — время простоя бизнес-систем будет снижено. Уменьшается время простоя сети в случае сбоев за счет упрощения сетевой инфраструктуры и использования средств автоматического конфигурирования, предоставляемых Ethernet Fabric.

J.I.: Каков же экономический эффект от внедрения 10G-решений?

А.Г.: В целом происходит сокращение операционных расходов (OPEX) на эксплуатацию уже существующего ЦОД, а также капитальных затрат (CAPEX) в случае строительства нового дата-центра.

Модернизация ЛВС позволит существенно консолидировать ресурсы компании, уменьшить количество эксплуатируемых серверных и число физических серверов. В результате суммарная экономия OPEX может достигать 20-25%, а срок окупаемости модернизации — 3-4 года.

Учитывая наличие этапности модернизации, указанного эффекта экономии OPEX невозможно достичь сразу после реализации первых этапов. Приведенная оценка учитывает полное завершение всех работ. Это следует учитывать при анализе результатов расчета и построении бизнес-планов.

J.I.: Какие из представленных на рынке решений можно рекомендовать заказчикам ?

А.Г.: В качестве вендора для модернизации ЛВС, исходя из нашего опыта, можно рекомендовать решения компании Brocade или Cisco:

- для уровня ядра — маршрутизирующие коммутаторы Brocade MLX/XMR или Cisco Nexus 7010/7018.
- для уровня доступа — 10G ToR коммутаторы Brocade VDX 6720 или Cisco Nexus серий 5000/4000/2000.

J.I.: Как оценивать перспективы внедрения данных технологий?

А.Г.: В каждом случае — индивидуально. Готовых рецептов для всех не существует.

J.I.: Кому такие решения могут быть интересны? Кто типовой заказчик?

А.Г.: В данном случае речь идет о компаниях, имеющих средний или крупный дата-центр либо несколько дата-центров: операторы связи, особенно оказывающие Value Added Services (VAS[4]) своим клиентам, провайдеры услуг hosted дата-центров, в особенности — использующих «облачные» технологии, крупные корпоративные заказчики.

J.I.: На что стоит обращать внимание при выборе решения?

А.Г.: На различные варианты предлагаемых решений и расчеты, подкрепляющие эффективность выбора, особенно в части OPEX. Дата-центр строится не на год, а такие параметры как стоимость электроэнергии имеют тенденцию только расти, поэтому нужно обязательно прогнозировать ситуацию на будущее.

4 VAS — услуги, приносящие дополнительный доход

J.I.: Что может предложить компания «Инфосистемы Джет» в этой области?

А.Г.: Компания обладает штатом компетентных специалистов и опытом построения дата-центров, ЛВС и СХД. Кроме того, в центре сетевых решений установлено стендовое оборудование, поддерживающее 10G и FCoE. Таким образом, существует возможность демонстрации работы готового решения. Все это позволяет говорить о том, что необходимые по проекту работы будут проведены качество, с соблюдением всех сроков и максимально в соответствии с потребностями заказчика.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

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
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