Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 8 (195)/2009

Большая стирка

КОРПОРАТИВНЫЕ СИСТЕМЫ

Большая стирка

СОДЕРЖАНИЕ

Новости 3

Тема номера

Большая стирка *(А.Герасимов)* 5

Наши проекты

Модернизация системы хранения данных и системы резервного копирования в ВТБ 19

От редакции

С момента публикации в JI статьи про систему Reveleus прошло совсем немного, однако за это время произошло достаточно значимое событие: Центральный банк решил внедрять первую компоненту Базель II со второй половины 2010 года, что предполагает необходимость расчета капитала под операционные риски. Сам по себе расчет капитала не сложен, однако подразумевает наличие у кредитной организации информационной системы по учету операционных рисков. Таким образом, банки, уже внедрившие у себя такие системы, получают двойную выгоду: они уже сейчас удовлетворяют требованиям законодательства и в состоянии строить управление на основании оценки рисков, которые могут возникнуть в ходе операционной деятельности. Остальным имеет смысл задуматься о внедрении систем риск-менеджмента — Центральный банк в очередной раз продемонстрировал, что будет и впредь ориентироваться на нормы Базель II.

В данном номере речь пойдет о другой составляющей комплекса GRC — Oracle Mantas AML, которая отвечает за выявление и расследование инцидентов, связанных с легализацией преступных доходов и финансированием терроризма, а также мошеннических операций в банковской деятельности.

Решение задачи унификации процессов ИТ – система автоматизации процессов управления инцидентами, работами и конфигурациями

Специалисты компании «Инфосистемы Джет» разработали и внедрили систему автоматизации процессов управления инцидентами, работами и конфигурациями.

Реализация данного проекта позволила национальной сети «Детский мир» решить задачу унификации процессов ИТ и повышения эффективности их работы в условиях географической распределенности объектов управления. При этом были учтены особенности в предоставлении одинаковых ИТ-услуг разным бизнес-подразделениям.

На этапе обследования специалисты компании «Инфосистемы Джет» зафиксировали текущую ролевую модель службы Help Desk, а также описали текущую деятельность в рамках процессов ИТ.

В рамках проектирования были разработаны регламенты и методические материалы по процессам управления инцидентами, работами и конфигурациями. Были разработаны метрики процессов, которые позволяют оценивать эффективность и качество работы ИТ-службы — в разработанных регламентах выделены роли, определены и разграничены зоны ответственности ИТ-специалистов. Также на данном этапе была разработана система показателей на основе CobiT[1] для внедряемых процессов.

Для руководителей и сотрудников ИТ-подразделений Группы компаний «Детский мир» быстрое и качественное решение оперативных вопросов пользователей является одним из приоритетных направлений улучшения работы. Поэтому в ходе проекта рабочая группа разработала инструменты контроля качества обслуживания на основе SLA.

Специалисты компании «Инфосистемы Джет» провели разработку, тестирование и развертывание на площадке ОАО «Детский мир — Центр» системы автоматизации на платформе программного обеспечения HP Service Manager 7.0. Система автоматизации интегрирована с другими информационными системами — Active Directory, MS SMS, Lotus Notes. На данном этапе выполнено обучение пользователей и запуск системы в опытно-промышленную эксплуатацию.

После запуска в промышленную эксплуатацию в ОАО «Детский мир — Центр» система управления была внедрена в региональном торговом предприятии компании в г. Санкт-Петербурге.

Система мониторинга и архивирования почтовых сообщений «Дозор-Джет» – решение для контроля и архивирования электронной почты

Компании «Инфосистемы Джет» и Hitachi Data Systems представляют решение для реализации корпоративной политики использования и долговременного хранения электронной почты на базе системы мониторинга и архивирования почтовых сообщений (СМАП) «Дозор-Джет» и платформы Hitachi Content Archive Platform (HCAP).

Данное решение позволяет в полном объеме реализовать корпоративную политику использования и долговременного хранения электронной корреспонденции: фильтрацию и архивиро-

1 Модель зрелости Управления ИТ в CobiT предназначена для контроля над ИТ-процессами организации с целью увеличения ценности ИТ, при соблюдении равновесия между риском и прибылью. Они базируются на определении уровня развития организации от несуществующего до оптимизируемого (от 0 до 5 уровня модели зрелости).

вание электронных сообщений согласно политике ИБ. Кроме того, оно позволяет предотвращать инциденты, связанные с утечкой конфиденциальной информации, выявлять нелояльных сотрудников, собирать и анализировать статистику использования почтового сервиса. Решение в настоящее время уже внедрено в ряде компаний.

Система мониторинга и архивирования почтовых сообщений «Дозор-Джет» — это специализированный программный комплекс, обеспечивающий фильтрацию и ведение архива почты в соответствии с требованиями компании. СМАП «Дозор-Джет» осуществляет мониторинг почтового трафика, проверяет сообщения на соответствие требованиям использования электронной почты, реагирует на их нарушения. Кроме того, система мониторинга и архивирования почтовых сообщений обеспечивает ведение оперативного архива электронной почты и управление им. СМАП «Дозор-Джет» включает в себя подсистему архивирования, использующую реляционные СУБД Oracle или PostgreSQL. Архив системы снабжен механизмами быстрого поиска писем по любым их атрибутам и механизмом индексирования, который позволяет осуществлять полнотекстовый поиск по архиву писем.

Платформа для построения электронного архива HCAP представляет собой программно-аппаратный комплекс, предназначенный для гарантированного хранения информации любого типа (неструктурированных данных): электронные письма, документы, изображения и т.п. Надежное долговременное хранение информации достигается за счет использования в составе отказоустойчивой платформы систем хранения данных Hitachi Data Systems, применения программно-аппаратных механизмов ограничения возможности удаления/изменения информации архива и средств проверки неизменности хранимых данных. HCAP, как и СМАП «Дозор-Джет», снабжен встроенными механизмами индексирования и поиска и предоставляет графический интерфейс для работы с архивом.

В совместном решении СМАП обеспечивает фильтрацию сообщений, обработку и расширенный поиск, HCAP — гарантированное долговременное хранение отобранных писем.

Дополнение функционала СМАП «Дозор-Джет» возможностями Hitachi Content Archive Platform позволяет:

- снять нагрузку с оперативного архива. Перенос редко используемых данных в HCAP позволит использовать быстрые и дорогие дисковые ресурсы оперативного архива по прямому назначению — для предоставления оперативного доступа к данным. Более медленные, но емкие и дешевые дисковые ресурсы в составе HCAP используются для долговременного хранения электронной почты пользователей и других неструктурированных данных;
- обеспечить соответствие стандарту PCI DSS (VISA), а также российским и международным стандартам в области ИБ, обязывающим компании иметь архив электронной почты (стандарт Банка России, HIPAA, Sarbanes-Oxley Act (SOX), Gramm Leach,Basel II, SEC);
- гарантированно хранить большие объемы информации длительный период времени;
- быстрее проводить поиск и выборку необходимых данных в долговременном хранилище.

Компания «Инфосистемы Джет» получила возможность миновать дистрибьюторов

Прямой договор с компанией IBM дает возможность компании «Инфосистемы Джет» размещать заказы на оборудование напрямую, минуя дистрибьюторов. Это признание результатов активной совместной работы продающих, технических и сервисных подразделений по продвижению решений IBM заказчикам компании «Инфосистемы Джет».

Кроме того, расширен перечень оборудования, на поставку которого сертифицирована компания. Теперь «Инфосистемы Джет» официально может поставлять оборудование System p (unix-системы) уровня high-end и System z (мэйнфрейм) уровня mid range.

ТЕМА НОМЕРА

Большая стирка

Александр Герасимов,
консультант по направлению FlexCube,
компания «Инфосистемы Джет»

13 мая 2004 года Центральный Банк РФ впервые отозвал лицензию за неоднократные нарушения федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Эта дата ознаменовала собой начало борьбы государства с теневыми доходами в финансовом секторе экономики. С каждым годом политика ЦБ по борьбе с легализацией преступных средств только ужесточалась, что явилось результатом отзыва лицензий еще у нескольких российских банков. На сегодняшний день существует целый ряд требований в этой области, которые кредитно-финансовые организации не могут реализовать в силу отсутствия необходимого функционала. Кроме того, это делает их беззащитными против атак различного рода мошенников, которым кредитные организации постоянно подвергаются. Как банку за счет правильного использования информационных технологий решить основные задачи по реализации требований законодательства в сфере противодействия легализации преступных доходов, пережить кризис с минимальными потерями и не лишиться лицензии? Именно на эти вопросы мы и постараемся ответить в рамках этой статьи.

Легализация преступных доходов и финансирование терроризма

Ежедневно международная банковская система сталкивается с беспрецедентным количеством рисков, при этом противодействие легализации (Anti Money Laundering или AML) является одной из наиболее актуальных проблем, с которой сталкиваются сегодня кредитные организации. Этот вид преступной деятельности считается одним из самых высокодоходных на теневом рынке и конкурирует, по различным оценкам, с незаконным оборотом наркотиков. Согласно данным ООН, в мире ежегодно легализуются более 3 триллионов долларов США. Первые попытки борьбы с отмыванием преступных доходов были предприняты в США еще в 1970 году, когда «Закон о банковской тайне» (Bank Secrecy Act) обязал финансовые институты формировать отчет обо всех операциях, превышающих лимит в 10 000 долларов США. В 1976 правительство США объявляет подобные операции государственным преступлением, а в 1994 году обязывает банки вырабатывать стратегии борьбы с легализацией преступных доходов.

Очень часто легализованные доходы идут на финансирование террористической деятельности. Обеспокоенность мировой общественности этим фактом наряду с отсутствием законодательного регулирования явились причиной принятия ООН «Конвенции о борьбе с финансированием терроризма» (резолюция 54/109 от 9 декабря 1999 г.), согласно которой акты международного терроризма ставят под угрозу безопасность и существование мира, поскольку их количество и тяжесть зависят от объемов и каналов финансирования, к которым террористы могут получить доступ. Трагедия, случившаяся в США 11 сентября 2001 года, выявила недостаточность мер, предпринимаемых в этой области. Это вынудило правительства влиятельных стран мира ужесточить финансовое законодательство и объединить свои усилия в целях предотвращения угрозы повторения подобных событий в будущем. Международная организация FATF (Financial Action Task Force on Money Laundering)[1] внесла коррективы в свои рекомендации по противодействию легализации, выработав в 2003 году 8 новых принципов по борьбе с финансированием террористической деятельности. Эти факты доказывают, что на западе борьба с этими явлениями является одной из приоритетных задач развитых стран.

В силу массы проблем в экономике в ее переходный период долгое время задача противодействия отмыванию незаконных доходов в России не была актуальной. Организация FATF исключила Российскую Федерацию из «черного списка» стран лишь в 2002 году. В настоящий момент эта сфера регламентируется Федеральным Законом 115-ФЗ («О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»), Положением Центрального Банка 321-П («О порядке представления кредитными организациями в уполномоченный орган сведений, предусмотренных ФЗ-115») и рекомендательным письмом ЦБ №99-Т («О внесении изменений в указания Банка России №179-Т и №278-Т»). На основе этих законодательных актов можно выявить следующие группы задач, которые стоят перед кредитными организациями, и проблемы, с которыми они сталкиваются в процессе их реализации:

1. Идентификация клиентов:
   - Сбор обязательной информации о клиентах. Ведение и периодическое обновление анкет клиентов;
   - Определение категории риска причастности клиента к «отмыванию» в зависимости от собранной информации, а в дальнейшем изменение категории риска в зависимости от деятельности клиента.

Банк может реализовать это требование двумя различными способами. Первый — предложить своим клиентам заполнение анкет, которые будут храниться в папках в хронологическом порядке. Способ неправильный как с точки зрения аналитики, так и эргономичности. Второй путь — ввод данных в информационные системы, так как это позволит унифицировать информацию и выполнить ее автоматизированную обработку. К сожалению, на сегодняшний день не все банковские системы предусматривают создание полей для всей необходимой информации, а если и предусматривают, то это, как правило, неструктурированные объекты, от которых невозможно добиться унифицированного ввода данных. Большая часть информации вводится при этом в различные формы и закладки системы, что затрудняет ее восприятие и анализ.

Вторая проблема — оценка риска в соответствии с требованиями ЦБ. Необходимо автоматизировать процесс присвоения клиенту группы риска, так как результат такой оценки учитывает все необходимые критерии (деятельность клиента, виды операций, состав контрагентов и т.д.). Многие банки параллельно классификации ЦБ имеют собственную классификацию рисков клиента, которую тоже было бы неплохо учитывать в рамках AML-системы.

2. Выявление лиц, причастных к террористической деятельности:
   - Проверка клиента на причастность к террористической деятельности в момент его регистрации в системе;
   - Проверка контрагентов в расчетных операциях клиентов на причастность к террористической деятельности. Приостановка расчетных операций. Отказ клиентам в обслуживании;
   - Ведение и обновление базы террористов.

Кредитные организации обязаны использовать в своей работе «черный список» стран, территорий, юридических и физических лиц, который подготавливается Центральным Банком РФ и

1 Группа разработки финансовых мер по борьбе с терроризмом и отмыванием денег. Организация была учреждена в соответствии с решением саммита «большой семерки» в Париже в 1989 году. В настоящее время в FATF входят 34 участника. Российская Федерация является членом FATF с 2004 года.

рассылается в формате dbf. Помимо этой базы данных, многие банки используют в своей работе собственные «черные списки» и «черные списки» международных организаций, которые могут иметь совершенно другие форматы. Возникает проблема интеграции и актуализации этих баз данных. Более того, если объединить эти списки в один, то получится база данных в несколько тысяч объектов. Следовательно, банк нуждается в автоматизированном решении, способном быстро и в режиме реального времени выполнять проверку клиентов и платежей на их наличие в такой базе данных, количество объектов которой подчас достигает ста тысяч сущностей.

3. Выявление операций клиентов, подлежащих обязательному контролю:
   - Операции на сумму, равную или превышающую 600 000 рублей;
   - Операции с недвижимостью на сумму, равную или превышающую 3 000 000 рублей.

Все виды таких операций подробно перечислены в ФЗ-115. Большинство таких операций ориентируются непосредственно на сумму платежа. Например, если клиент выполняет обменные операции на общую сумму в 25 000 долларов США, что превышает лимит в 600 000 рублей, банк направляет сообщение в Росфинмониторинг. В данном случае возникает задача отслеживания нескольких операций одного клиента, общая сумма которых может превышать контрольный лимит.

Другая часть обязательных операций предполагает контроль не суммы платежа, а суммы сделки (сумма договора по покупке/продаже недвижимости, акты приема-передачи по лизинговым операциям). Как правило, платежи по данным договорам совершаются несколькими траншами, что создает проблему суммирования платежей в разрезе договоров. Очень часто подобные операции не автоматизированы в банке и выполняются вручную.

4. Выявление необычных операций и сделок клиентов. В отличие от операций, подлежащих обязательному контролю, для необычных операций и сделок степень «необычности» каждый банк устанавливает для себя сам (основываясь на рекомендательном письме ЦБ №99-Т), при этом согласует порядок выявления с региональным департаментом ЦБ.

Сложность состоит в выработке методологии отнесения к необычным операциям. Раньше банки переписывали критерии и признаки необычных операций, сформулированные в рекомендательном письме ЦБ №99-Т, редактировали их таким образом, что в итоге они становились чисто формальными и не требовали реализации на практике. Это происходило в силу невозможности реализации контроля подобных операций в рамках существующих AML-систем.

Спасение банка заключается в использовании комплексного механизма, использующего сложные поведенческие и бизнес-модели, умеющего выявить различные последовательности, способного провести анализ текста и выявленных взаимосвязей. В настоящий момент российские разработчики не могут предложить автоматизированного решения для этих задач.

5. Выявление выгодоприобретателей клиентов:
   - Выявление выгодоприобретателей в расчетных операциях клиентов;
   - Идентификация выявленных выгодоприобретателей;
   - Ведение базы выгодоприобретателей.

В соответствии с требованиями законодательства кредитная организация обязана выявить операции с участием третьих лиц, после чего необходимо приостановить подобную операцию и идентифицировать третье лицо, направив клиенту соответствующий запрос. Так как операций много, то необходимо продумать систему направленных сообщений и полученных ответов, чтобы исключить случаи повтора. Большинство банков выполняют данные операции вручную, ведя учет в документах Word или Excel. Гибкий инструмент настройки бизнес-процессов мог бы помочь банку автоматизировать эту задачу.

6. Информирование ЦБ (в соответствии с требованиями 321-П):
   - Выявление террориста;
   - Приостановка расчетной операции;
   - Выявление операции, подлежащей обязательному контролю, или необычной операции и сделки;
   - Невозможность идентификации выгодоприобретателя клиента.

При формировании отчетности в стандартных AML-модулях банковских систем очень часто случаются различные ошибки, вызванные отсутствием структурного и логического контроля, неправильным вводом данных или неверным формированием файла. Наказанием для такого рода ошибок может стать отзыв лицензии банка.

В последнее время был разработан ряд проверочных программ, интегрируемых с механизмами отчетности, но это дополнительный модуль, очень часто еще и от стороннего разработчика, который нужно реализовать в существующей инфраструктуре.

Набор отчетов в стандартных AML-модулях банковских систем обычно ограничивается требованиями 321-П. У кредитной организации нет возможности создавать собственные аналитические отчеты и диаграммы, которые могли бы позволить руководству мгновенно оценить уровень противодействия легализации преступных доходов в банке и принять необходимые решения.

Мошеннические операции

Другая проблема, о которой хотелось бы поговорить в рамках данной статьи, это мошеннические операции. «Фишинг»[2], «скимминг»[3], хакерство — те явления, которые до сих пор внушают банкам страх. В условиях финансового кризиса эта проблема становится все более актуальной: с одной стороны, кредитные организации не могут себе позволить нести дополнительные убытки, а с другой — мошенники активизируют свои усилия в этой сфере, пользуясь финансовой нестабильностью. Кроме того, из всех секторов экономики финансовая индустрия остается наиболее уязвимой в силу того, что постоянно находится в фокусе внимания злоумышленников. Мошенничество становится ключевым операционным риском, который сказывается на репутации и доходах кредитной организации. Факты ужасают: согласно данным Ассоциации Региональных Банков (АРБ) РФ, потери, связанные с мошенничеством на российском рынке банковских карт, в 2008 году составили около миллиарда рублей. Это почти в три раза больше, чем в 2007 году.

С 2007 по 2008 год убытки транснациональных компаний от мошенничества составили 7,3 миллиарда долларов или по 8,2 миллионов долларов на компанию, что на 22% больше, чем в позапрошлом году (6,7 миллионов долларов). Такие данные содержатся в исследовании, проведенном Economist Intelligence Unit[4]. И чем крупнее компания, тем выше ее убытки: крупные корпорации потеряли из-за действий мошенников в три раза больше, чем средняя компания. Авторы доклада приходят к выводу, что слабеющий внутренний контроль и большая текучка кадров дают куда больше возможностей для преступников. «Эти факторы увеличивают вероятность мошенничества в полтора раза», — говорится в докладе.

И не всегда убытки от мошенничества можно выразить в стоимостном эквиваленте. Как правило, это еще и косвенные потери банка, которые могут иметь более серьезные последствия. Например, разрушается бренд, ухудшается репутация компаний, снижается уровень доверия клиентов, наносится ущерб контактам с партнерами. А финансовые структуры считают, что рыночная стоимость банка зависит в первую очередь от его репутации на рынке.

К сожалению, использование преступниками последних достижений технического прогресса и глобализация мошеннических операций ставят перед кредитными организациями целый ряд новых задач. Все чаще и чаще мошеннические операции совершаются организованными преступными группами, вступившими в сговор с партнерами и контрагентами, инсайдерами, в том числе и сотрудниками банка. Несколько месяцев назад консалтинговая компания Ernst & Young опубликовала исследование, согласно которому в период экономического кризиса 64% сотрудников крупных компаний ожидают увеличения числа случаев корпоративного мошенничества. Сотрудники находятся в постоянном страхе увольнения, что вызывает у них желание обмануть своих нанимателей и поддаться на уговоры мошенников. 31% россиян и 37% европейцев считают, что руководство их компаний не уделяет достаточного внимания вопросам противодействия мошенничеству.

Что делать?

Российские банки уже прошли этап формального исполнения обязательных требований и нормативов ЦБ, нарушение которых грозит отзывом ли-

2 Фишинг (от анг. phishing) - вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям. Общий размер убытков для банковской индустрии с января по июнь 2008 года составил 21,4 миллионов долларов по сравнению с 7,5 миллионами долларов в этот же период 2007 года.

3 Скимминг - мошенничество с пластиковыми картами, при котором используется скиммер - инструмент злоумышленника для считывания данных с пластиковой карты.

4 http://www.kroll.com/library/fraud/FraudReport_English-UK_Sept08.pdf

Agricultural Bank of China (Сельскохозяйственный Банк Китая)

В июне 2008 года китайское правительство раскрыло информацию о том, что в 2004 году в одном из крупнейших государственных банков было совершено более 50 мошеннических операций, в которых участвовало 174 человека. Общий ущерб от этих операций был оценен в 1.1 млрд. долларов. При этом финансовый аудит выявил и другие нарушения — при работе с депозитами (1,8 млрд. долларов) и кредитами (3,5 млрд. долларов). В результате инцидента 64 служащих банка были уволены, 20 отданы под суд, 1330 подверглись мерам дисциплинарного воздействия.

Это был очередной шаг правительства Китая, направленный на привлечение иностранных инвестиций в страну, которые возлагают большие надежды на развивающуюся, несмотря на кризис, экономику страны. В 2007 году Goldman Sachs Group Inc., American Express Co. and Allianz AG вложили около 4 миллиардов долларов в Индустриальный Коммерческий Банк Китая, выкупив 10% его акций. Этот шаг должен был показать зарубежным инвесторам, что правительство заинтересовано в улучшении практик управления в государственных банках. Однако аналитики отмечают, что много подобных фактов остается нераскрытыми, а их уровень очень велик в силу слабо развитого внутреннего контроля в китайских банках.

Banco Intercontinental

Banco Intercontinental функционировал на территории Доминиканской Республики и являлся вторым крупнейшим коммерческим банком страны. В 2003 году в этом учреждении была зафиксирована рекордная сумма убытков — 2.2 миллиарда долларов, что на тот момент составляло две трети государственного бюджета страны. Это отразилось на всей экономике Доминиканской республики: государство получило контроль над обанкротившимся банком, что привело к высокому уровню инфляции, девальвации национальной валюты и массовым беспорядкам населения.

Расследование причин понесенных убытков выявило, что незаконные операции совершались владельцем банка Рамоном Баец Фигуеро и рядом руководителей. Рамон Баец Фигуеро был очень влиятельным человеком: помимо банка, он владел крупнейшей медиакомпанией BANINTER Group, которая включала в себя старейшее печатное издание страны, 4 телеканала и более 70 радиостанций. В ходе судебного процесса были выдвинуты обвинения в легализации преступных доходов и сокрытии финансовой информации от органов власти. В результате решения суда Рамон Баец Фигуеро был приговорен к 9 годам лишения свободы.

Bank of Credit and Commerce International

На сегодняшний день преступление, совершенное в этом банке, считается крупнейшим мошенничеством в банковской сфере прошлого века, которое в 1991 году повлекло за собой банкротство Bank of Credit and Commerce International. Когда открылась правда о деятельности этого банка, мировое финансовое сообщество содрогнулось. В списке обвинений, звучавших в адрес банка после его краха, не только банальное финансовое мошенничество (правда, в особо крупных размерах), но и уклонение от уплаты налогов, отмывание денег, взяточничество, поддержка международного терроризма, запугивание свидетелей, причастность к торговле оружием и ядерными технологиями. А ведь незадолго до своего закрытия в 1991 году банк этот считался одним из флагманов мирового финансового сектора. Во времена своего расцвета филиальная сеть банка состояла из 400 офисов в 73 странах мира, и в нем работало около 14 тысячи сотрудников.

Сомнения в финансовом состоянии банка возникли в 1986 году. Именно тогда аудиторам и регулирующим органам стало известно об убытках в размере 500 миллионов долларов, понесенных банком, которые не были отражены в отчетности. В 1991 году аудиторская компания «Price Waterhouse» предприняла новое расследование. Ими было обнаружено 600 миллионов долларов, внесенных на депозит клиентами банка, но не нашедших отражения в отчетности. Вывод был налицо: масштабное мошенничество и подтасовки. Причем махинации, направленные на раздувание прибыли банка, были обнаружены уже с 1976 года, а их масштаб измерялся миллиардами долларов. После изучения этого отчета правительство Англии закрывает банк в июле 1991 года, после чего он прекращает свое функционирование и в других странах. На момент закрытия активы банка составляли 23 миллиардов долларов, но обнаружить удалось лишь половину этой суммы.

Декабрь 2008 года

ЗАО КБ «ФИА — банк» оказался замешанным в обналичивании денежных средств. Несмотря на то, что действия банка были признаны соответствующими 115-ФЗ, репутации банка был нанесен урон, повлекший массовый отток вкладов.

В декабре 2008 года следственное управление УВД по Автозаводскому району г. Тольятти возбудило уголовное дело по признакам состава преступления, предусмотренного ст. 159 УК РФ, против двух граждан России. Им вменяются мошеннические операции, связанные с обналичиванием денежных средств с использованием пластиковых карт на общую сумму 1.5 миллиарда рублей.

Любопытно, что «ФИА-Банк» уже не первый раз фигурирует в скандалах, связанных с незаконным обналичиванием средств и нарушением ФЗ-115. Так, по данным газеты «Коммерсантъ», летом 2007 года УВД города Тольятти направило в суд уголовное дело, возбужденное против бывшего главного бухгалтера «ФИА-Банка». Среди прочего в вину ей вменялось и участие в схемах по обналичиванию средств одной из компаний-клиента банка.

Примечательно, что «ФИА-Банк» также является одним из банков Самары и Тольятти, пользующихся государственной поддержкой в период кризиса. Так, осенью 2008 года банк получил кредит ЦБ под залог своего кредитного портфеля сроком на 6 месяцев, в декабре — 35-дневный беззалоговый кредит на 700 млн. рублей с датой погашения 14 января 2009 года.

Юлия Голышева, аналитик ИК «Финам»: *«...Основной причиной подобных нарушений является недостаточно высокий уровень внутреннего контроля и противодействия легализации преступных доходов. Кроме того, возможно, имеет место недостаточное обеспечение информационной безопасности данных клиентов»*[5].

цензии на осуществление банковской деятельности. Сейчас перед ними стоит задача минимизации рисков и предотвращения участия кредитной организации в сомнительных операциях. Многие приходят к тому, что нужно эффективно использовать результаты противодействия в интересах самого банка. Очень долгое время российские разработки в этой области были направлены исключительно на реализацию требований 115-ФЗ в рамках модуля АБС, используемой в банке. Вся работа по выявлению необычных операций выполнялась вручную или при помощи инструментов Microsoft Office, которые помогали не автоматизировать процесс, а лишь систематизировать обрабатываемые данные. Такое положение вещей могло устроить небольшой банк, а что делать финансовым организациям, объем операций которых превышает сотни тысяч в день? Ответ на самом деле очевиден: нужно использовать передовой опыт и наработки наших западных коллег. Ведь даже Центральный Банк РФ не придумывает ничего нового: многие из его нормативов и рекомендаций являются выдержками из международных документов по противодействию легализации.

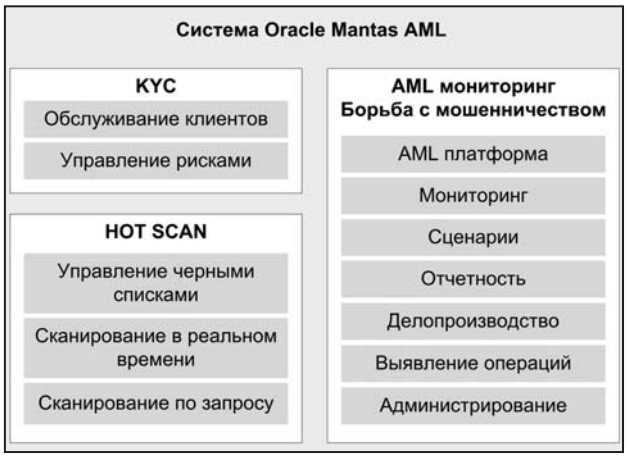

Рис. 1. Функциональная архитектура Oracle Mantas

В ходе детального анализа международного рынка AML-решений специалистами компании «Инфосистемы Джет» было рассмотрено несколько крупных игроков. Исследование показало, что наиболее полно с задачей финансового мониторинга в кредитной организации справляется система Oracle Mantas от компании Oracle Financial Services. Система дает банку целый ряд возможностей: консолидировать, очистись и интегрировать данные, полученные из разных источников; использовать сложные модели выявления преступных схем и необычных операций; сгенерировать предупреждения и снизить ошибочные результаты проверок («false positives») на 90%; произвести реинжениринг бизнес-процессов; получить в распоряжение современные инструменты делопроизводства и отчетности.

С точки зрения функционала можно выделить три основных блока системы (см рис. 1): модуль KYC («Знай своего клиента»), решение по работе с черными списками HotScan и, собственно, AML-платформа для противодействия легализации и выявления мошеннических операций.

Модуль KYC (см. рис. 2) отвечает за идентификацию клиентов банка. В момент заведения клиента или открытия счета в KYC передается информация о клиенте через SOAP[6]-интерфейс или

5 http://ibk.ru/48670.html

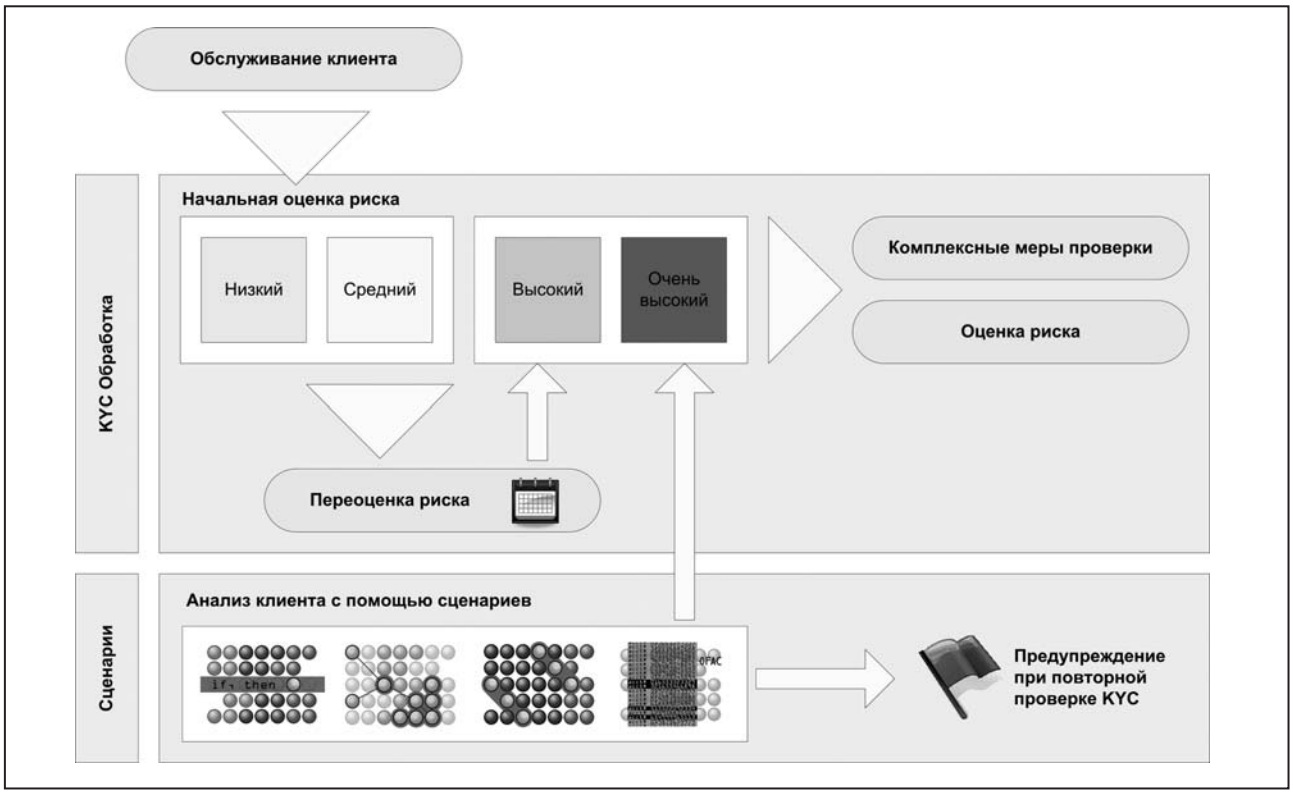

Рис. 2. Работа модуля KYC

посредством обмена файлами. Модуль отвечает за достоверность представленных документов, осуществляя сбор и проверку информации в публичных источниках (например, Factiva[7]), «черных списках» и внутренних базах данных. При этом система Mantas получает информацию, необходимую для того, чтобы идентифицировать клиента, и информацию, позволяющую определить его бизнес-профиль (ожидаемое поведение). Вся полученная модулем информация просматривается и может быть использована для подготовки заключений. Сведения, полученные таким образом от внутренних или внешних систем, могут быть приложены к аналитическим отчетам, могут быть сохранены в хранилище документов банка с соответствующей ссылкой на документы из модуля Mantas KYC. Здесь же решается задача отнесения клиента к группе риска: эта информация может быть загружена из системы риск-менеджмента или определена модулем KYC в соответствии с заданными настройками. В зависимости от присвоенного уровня риска к клиенту будет применяться различный ряд проверок. Чем выше уровень, тем чаще будет производиться переоценка риска для данного клиента. Интеграция с AML-платформой дает возможность использовать рейтинги рисков, устанавливая соответствующий уровень мониторинга для клиента, его операций и контрагентов. AML-платформа инициирует пересмотр клиентской информации в случае нарушения порогов, указывающих на значительные отклонения в поведении.

Решение HotScan предназначено для работы с «черными списками»: при этом у банка есть возможность использовать как собственные «черные списки», так и списки различных правительственных и международных организаций. В зависимости от требований банка автоматическое сканирование на наличие в «черном списке» может выполняться на любом из этапов обслуживания клиента: в момент сохранения его сведений, при изменении клиентской информации, в процессе периодического сканирования клиентской базы данных, мониторинга платежных сообщений и т.д. Более того, при наличии подозрений сотрудник банка может выполнить проверку клиента

6 SOAP — протокол обмена структурированными сообщениями в распределенной вычислительной среде. В настоящий момент протокол используется для вызова процедур и для обмена произвольными сообщениями в формате XML. SOAP является одним из стандартов, на которых базируется технологии веб-сервисов.

7 Factiva — подразделение компании Dow Jones, занимающееся предоставлением доступа к деловой и аналитической информации через свои информационно-аналитические службы. В своей основе службы Factiva имеют более чем 30 тысяч первичных источников из 159 стран мира на 22 языках.

в любой момент времени. Все предупреждения HotScan направляет в соответствующую экранную форму, где ответственный сотрудник может просмотреть их и принять необходимые действия. Что же касается объемов, то HotScan может обрабатывать в режиме реального времени более 720 000 платежных сообщений в час.

AML-платформа является основным функциональным блоком системы Oracle Mantas. Она является центральным хранилищем данных, которые поступают из различных внешних систем. Здесь же выполняются консолидация полученной информации, проверка на качество данных и их очистка. После этого обработанные данные прогоняются через сценарии — сложные логические модели, позволяющие выявить подозрительное поведение или возможное «отмывание» нелегальных средств. Именно сценарии дают банку возможность выполнять комплексный мониторинг операций и счетов в разрезе продуктов и направлений его деятельности. В системе есть специальный конструктор, который позволяет кредитным организациям создавать новые сценарии или вносить изменения в существующие без затрат на кастомизацию и программирование. В своей работе конструктор использует следующие инструменты:

- правила для представления линий поведения в качестве набора условий;
- профили клиентов для выявления необычного и подозрительного поведения;
- возможность связать реальные и производные названия и ассоциации в неструктурированном тексте;
- выявление последовательностей для взаимосвязей событий и операций в последовательном порядке;
- анализ связей для выявления комплексных линий поведения, когда отношения между объектами могут быть довольно сложными, неявными и намеренно скрытыми. Определяет и устанавливает связь с линиями поведения, выявленными другими инструментами, как несвязанные события возможного мошенничества, отмывания средств или воровства.

В настоящий момент компания Oracle готова предложить своим клиентам более 300 сценариев, которые можно применять в следующих областях: обслуживание юридических и физических лиц, брокерские операции, инвестиционные банковские услуги и контроль сотрудников банка. Как показывает опыт предыдущих внедрений компании Oracle, для реализации требований регуляторов достаточно 10-20 сценариев. Краткое описание AML-сценариев, применяемых в обслуживании физических и юридических лиц, можно посмотреть в Приложении 1 (см. стр. 18).

В случае обнаружения подозрительных операций система незамедлительно сформирует сообщение для ответственного сотрудника. Oracle Mantas предлагает гибкую настройку бизнес-процессов, подстраиваясь под организационную структуру банка и его регламенты. Необходимо отметить функционал делопроизводства, поддерживающий возможности «drill-down» и позволяющий заводить дела и отправлять инциденты на расследование как автоматически, так и вручную. А современный инструментарий отчетности поможет банку создавать не только обязательные отчеты, но и графические информационные панели. Создание отчета в системе не требует от аналитика навыков программирования, а выполняется простым нажатием кнопок мыши.

Не только выявлять, но и расследовать

Отличительное особенностью системы является наличие в ней механизмов делопроизводства и документооборота. Это означает, что система не просто выявляет возможные случаи отмывания денег и мошенничества, но и предоставляет развитые механизмы по их расследованию. Встроенная система документооборота позволяет настраивать порядок изучения события заданными лицами или группой лиц. На каждое расследование могут быть наложены ограничения по времени, как того и требует 115-ФЗ. Если необходимо информировать сотрудника банка, что ему поручены те или иные задачи в рамках расследования, система может автоматически отправить ему уведомление на электронную почту. Разумеется, все действия системы и пользователей фиксируются и могут быть впоследствии проанализированы.

Для того, чтобы инициировать расследование, система Mantas заводит новое дело. Как правило, дело заводится в результате обнаружения скриптами подозрительного поведения. Такое обнаружение называется инцидентом. Система позволяет объединить несколько однотипных инцидентов в единое делопроизводство. Созданное таким образом дело содержит всю информацию, инструменты для анализа и отчетности, которые могут пригодиться для его расследования. Преж-

де всего, в дело вносятся сведения о том, каким образом система распознала произошедший инцидент, каким скриптом и с какими параметрами это произошло. Такой подход позволяет быстро изменять настройки скриптов в случае большого количества ложных срабатываний. Во-вторых, дело содержит данные о состоянии всех относящихся к инциденту деталей, таких как: остатки по счетам, список операций, предшествующих инциденту, информацию о клиенте и т.п. Эта информация отражает состояние на момент события и поэтому остается в деле неизменной. Кроме статических данных, дело в таком же точно формате содержит актуальное состоянии всех основных сведений о клиенте и его счетах. Эта информация необходима для того, чтобы пользователь смог выявить динамику или проанализировать изменения в поведении клиента. Работа с делами организована очень гибко, например, закрытое ранее дело можно вновь открыть и инициировать на основании него специальное расследование и соответствующий документооборот. Для того, чтобы незначительные события (например, на небольшие суммы) не отвлекали внимание сотрудников, формирование дел по ним можно блокировать, однако если выставить порог суммарного срабатывания, при накоплении значимого количества таких событий, система все равно запустит расследование. Вообще говоря, все расследования в системе упорядочены, наиболее важные и критичные из них находятся выше по списку. Для выставления коэффициентов в системе есть настраиваемый многоуровневый скоринг, добавляющий баллы за те или иные характеристики произошедшего инцидента. Классическим примером ранжирования является приоритет при расследовании сделок на крупные суммы.

Для расследования инцидентов система Mantas содержит набор отчетов и специфических инструментов, таких, например, как анализ связей клиента, позволяющий идентифицировать все счета, вовлеченные в его сделки, всех корреспондентов, банки и т.п. Для анализа связей строится сеть, визуально показывающая направление движения средств и связи между корреспондентами. Схема представляет собой динамический объект, части которого можно удалять с помощью фильтров, что позволяет избавиться от «шума» мелких и незначительных операций и увидеть систему в поведении клиента. Кроме того, элементы схемы представляют собой ссылки на детальные отчеты, расшифровывающие сущность элемента.

В зависимости от описанного документооборота по результатам расследования система может автоматически сформировать отчет для последующей отправки в соответствующий орган по финансовому мониторингу, закрыть дело или подготовить отчет о результатах расследования. Результат расследования может быть экспортирован в любую систему в составе информационного комплекса, например, в Автоматическую Банковскую Систему или систему хранения электронных документов.

Таким образом, выявление операций по отмыванию средств и мошеннических операций в системе Mantas это только начало и основа для дальнейшего расследования. Помимо выявления подозрительного поведения, система Mantas гарантирует, что это поведение будет обязательно изучено и расследовано в установленные сроки с обязательной фиксаций всех выполненных в ходе расследования действий.

Архитектура

Система реализована в многоуровневой, масштабируемой и открытой архитектуре, что раскрывает перед банком широкие возможности интеграции и позволяет выбрать наиболее подходящую модель внедрения. Как правило, выбирается трехуровневая модель: сервер представлений, отвечающий за взаимодействие с пользователем; сервер приложений, отвечающий за бизнес-логику системы; сервер баз данных, отвечающий за сбор и хранение информации. Oracle Mantas — это веб-ориентированное решение: для работы обычного сотрудника необходимо лишь наличие рабочей станции с Интернет-браузером.

Многоуровневая модель безопасности Oracle Mantas (см. рис. 3, стр.14) позволяет банку гибко настраивать права доступа к системе. В соответствии с внутренними регламентами можно разграничить доступ сотрудникам к различным экранным формам, операциям и информационным объектам. Это достигается за счет механизма настройки ролей пользователей. Так, роль «аналитика», по умолчанию настроенная в системе, позволяет просмотреть предупреждения и связные с ними операции и данные, изменить их статус, ввести комментарий, отправить уведомление на электронную почту и назначить ответственного сотрудника. Помимо стандартного функционала аутентификации пользователей, система позволяет банку использовать возможности LDAP. За счет использования открытых интерфейсов

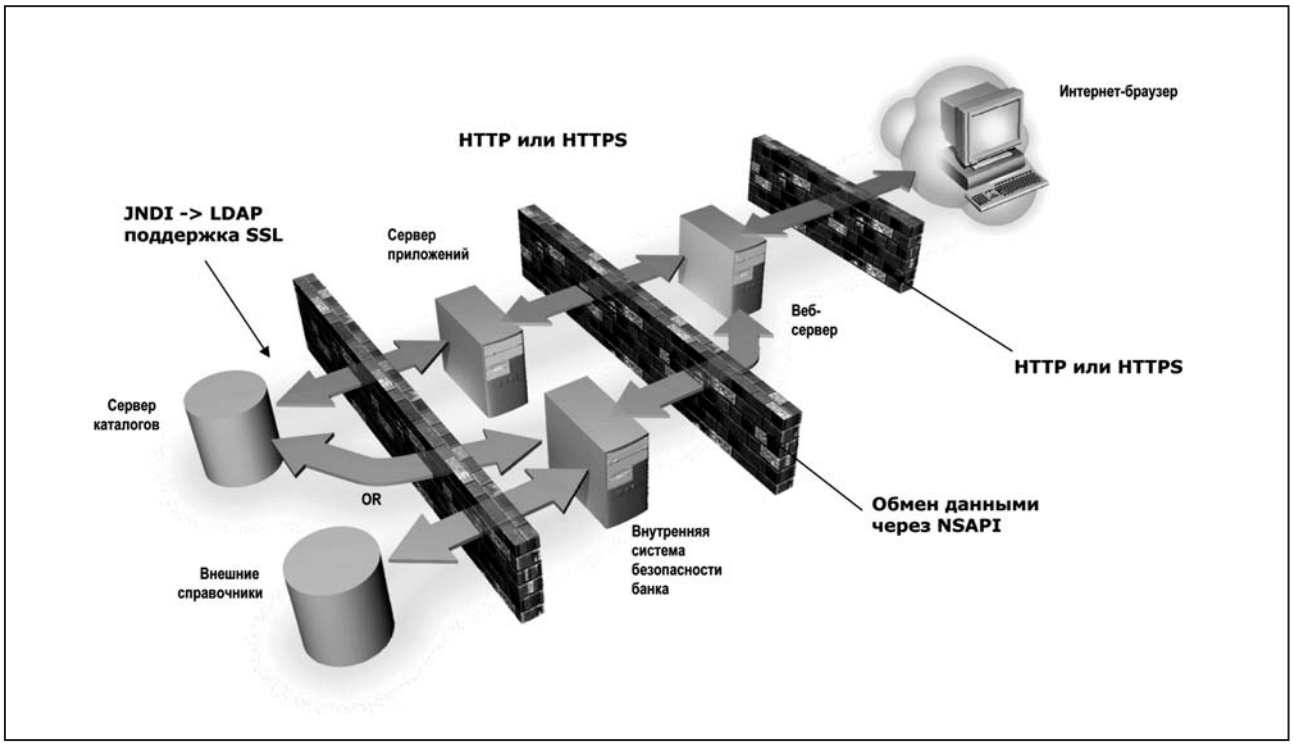

Рис. 3. Архитектура безопасности Oracle Mantas

Oracle Mantas может быть интегрирована практически с любой стандартной системой безопасности, используемой в банке. По умолчанию система использует протоколы SSL 3.0 для шифрования трафика, но при необходимости банк может использовать средства шифрования от других производителей. Все настройки системы защищены 128-битным цифровым ключом. Все эти инструменты надежно уберегут информацию банка от внешних посягательств.

Признание индустрией

Система Oracle Mantas пользуется большим спросом на финансовом рынке и ежегодно отмечается различными печатными изданиями и консалтинговыми агентствами. Решения были внедрены в 67 странах мира. О популярности системы среди кредитных организаций говорит хотя бы тот факт, что 5 из 11 ведущих банков (Deutsche Bank AG, ABN AMRO Bank N.V., Credit Suisse Group, Barclays Bank, Citibank N.A.), заложивших основные директивы по противодействию отмыванию преступных доходов в документе «Вольфсбергские принципы», используют Oracle Mantas в качестве основной AML-платформы. К тому же, клиентами Oracle Mantas являются такие крупные банки и инвестиционные компании, как: Merill Lynch, Charles Schwab, Goldman Sachs, BBVA, M&T Bank. Национальная ассоциация дилеров по ценным бумагам (NASD), организация, ответственная за соблюдение правил торговли на внебиржевом рынке, также использует в своей работе данную систему, которая анализирует более 150 миллионов сделок в день.

Издание Waters ежегодно проводит среди своих читателей опрос на лучшую AML-систему. За 7 лет существования этого опроса читатели журнала 6 раз выбирали платформу Mantas лучшей системой по противодействию легализации преступных доходов и предотвращению мошеннических операций. Примечательно, что в 2008 году система набрала рекордные 72,8 процентов голосов. Эта награда является неоспоримым доказательством надежных и взаимовыгодных отношений компании с ее клиентами. Более того, клиенты Oracle Mantas организовали собственную инициативную группу SMARTS, которая проводит встречи в режиме круглого стола четыре раза в год. Представители компании-разработчика принимают активное участие в этих семинарах, где они получают уникальную возможность детально обсудить первоочередные задачи кредитных организаций, поделиться своими знаниями и опытом, выработать лучшие методики для высокоэффективного мониторинга операций в рамках платформы Mantas.

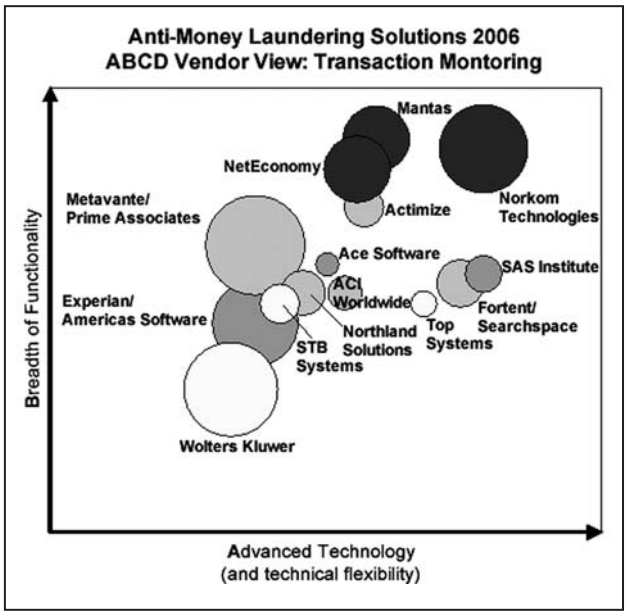

Рис. 4. Возможности AML-решений в мониторинге финансовых операций. Источник: Celent

В последнем отчете по AML-решениям известной консалтинговой компании Celent система Oracle Mantas была признана лидером рынка (см. рис. 4). Специалисты компании оценивали 19 поставщиков AML-решений, готовых предоставить своим клиентам возможности анализа сложных финансовых операций и умеющих работать с правительственными «черными списками». В своем исследовании Celent руководствовался такой информацией, как: клиентская база поставщика, набор функциональных возможностей, технологическая платформа, сроки внедрения и стоимость решения.

Mantas, как элемент GRC-модели

Противодействие легализации и мошенническим операциям является задачей комплаенс-контроля — одного из элементов относительно новой концепции управления GRC (Governance, Risk Management and Compliance), о которой мы уже рассказывали в публикациях нашего журнала («Jet Info», №7 (194) 2009). Governance (Управление) отвечает за выработку основных целей, задач и методик, а также включает в себя процессы принятия решений. Risk Management (Управление рисками) — это процесс, основными задачами которого является выявление, оценка, мониторинг, контроль и минимизация рисков компании. Compliance (комплаенс) отвечает за соблюдение принятых руководством решений, выработанных методик и требований регуляторов. На сегодняшний день это наиболее комплексный подход к менеджменту организации, который позволяет достичь высокого уровня культуры управления рисками, наиболее эффективно использовать имеющиеся в наличии ресурсы, принимать взвешен-

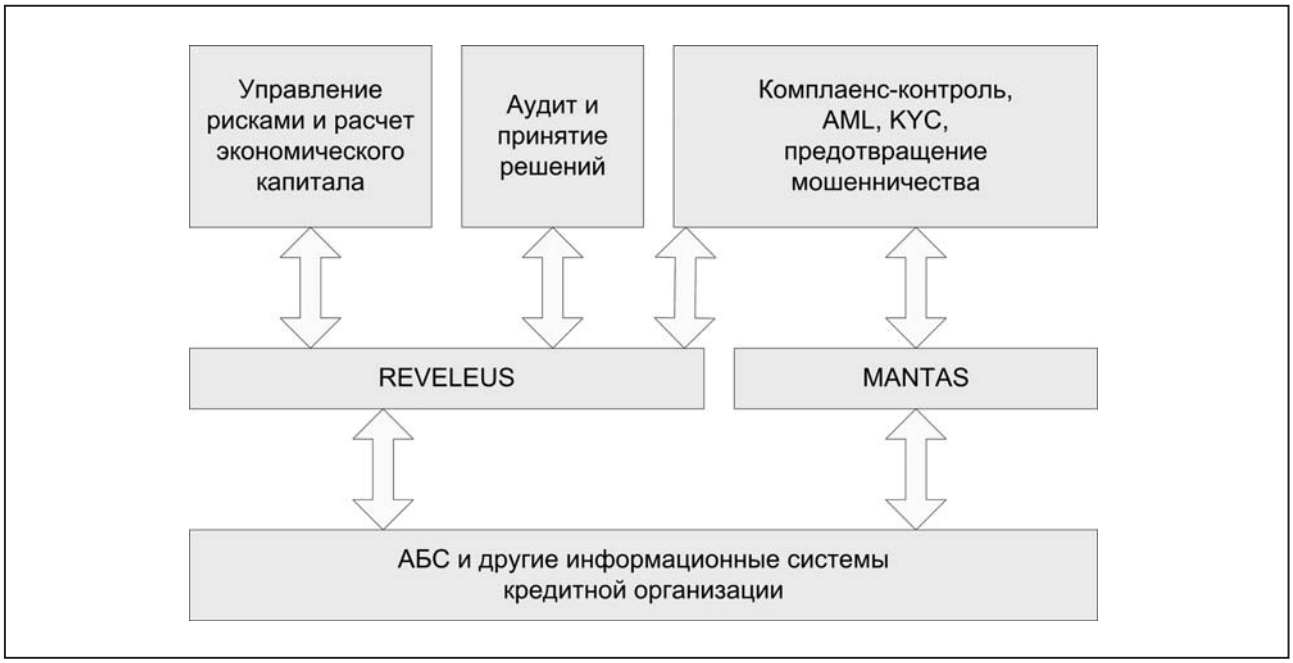

Рис. 5. Стратегическая GRC-модель

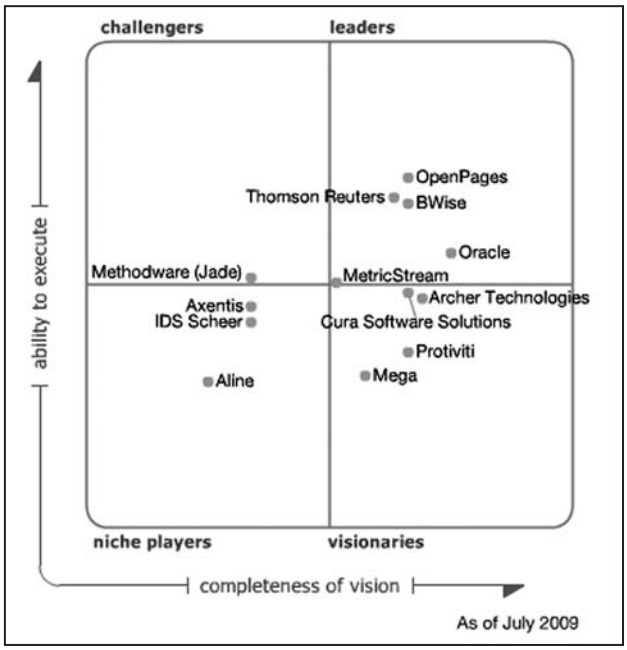

Рис. 6. Магический квадрат GRC-платформ. Источник: Gartner (июль 2009)

ные и правильные решения, а также полностью соответствовать требованиям законодательства и регуляторов. На рынке решений для банковской сферы GRC-продукт компании Oracle является наиболее полноценным. Помимо системы Mantas, он включает в себя решение Reveleus, предназначенное для управления рисками и расчета экономического капитала. За счет использования этих решений, а также международного опыта специалистов Oracle можно реализовать в банке полноценную GRC-модель (см. рис. 5, стр. 15).

Ряд авторитетных изданий и консалтинговых агентств по достоинству оценил решения Oracle в сфере GRC. Так, в своем последнем отчете (июль, 2009) Gartner оценивает компанию как лидера рынка GRC. При этом аналитики Gartner подчеркивают, что «среди всех поставщиков только Oracle может предложить наиболее полный набор GRC-решений для финансового аудита, комплаенс-контроля, управления компанией и ресурсами».

В 2008 году более 4 000 читателей издания OpRisk & Compliance приняли участие в опросе на лучшего поставщика GRC-решений. Им было предложено выбрать пять крупнейших поставщиков с точки зрения функциональных возможностей их систем, независимости технологической платформы, опыта сотрудников и конкурентных преимуществ. Согласно журналу «Oracle одержал убедительную победу среди программного обеспечения для реализации требований GRC, на 15 % опередив своего ближайшего противника».

Почему нужна система

После выхода Положения 115-ФЗ, практически все российские разработчики АБС встроили в банковские системы функционал, приводящий их к требованиям законодательства. Почему в условиях полного соответствия требованиям законодательства все же имеет смысл говорить об отдельной системе?

Во-первых. Заложенные в российские АБС алгоритмы по выявлению операций как правило точно следуют требованиям законодательства, не оставляя банку возможности дополнительной настройки или определения собственных правил. Кроме того, их алгоритмы не отвечают западным стандартам. Система Mantas позволяет реализовать требования 115-ФЗ с помощью комбинации существующих скриптов, при этом банк получает решение, которое он может самостоятельно улучшать с помощью настройки. Решение внедряется с готовыми скриптами, работающими в ведущих финансовых институтах всего мира, что позволяет кредитной организации соответствовать международным требованиям.

Во-вторых. Oracle Mantas в отличие от АБС позволяет не только выявлять операции, но и осуществлять их расследование. Встроенный в систему документооборот, механизмы скоринга и делопроизводство дают гарантию того, что все рискованные операции будут расследованы в заданные сроки и с необходимым результатом. В отличие от системы Mantas механизмы, реализованные в Российский банковских комплексах, занимаются лишь выявлением операций, оставляя банк решать вопрос с расследованием самостоятельно.

В-третьих. Помимо борьбы с отмыванием средств, добытых незаконным путем, система Mantas позволяет выявлять мошеннические операции. Как уже отмечалось в примере с КБ «ФИА», полное соответствие 115-ФЗ никак не связано с защитой от мошенничества. В результате отсутствия в банке механизмов по выявлению мошеннических операций, его репутация была потеряна. Такая система, как Mantas, могла помочь банку сохранить репутацию за счет раннего обнаружения подозрительной активности по карточным счетам.

В-четвертых. Очень часто мошеннические операции распределены территориально. Подобная тактика применяется с целью запутать службу безопасности банка и зачастую не подлежит выявлению без применения автоматизированных средств. Поэтому для крупного многофилиального банка эффективное выявление мошеннических операций возможно только в том случае, если

операции клиентов будут анализироваться в целом по организации. Система Mantas позволяет не только объединить данные всех филиалов, но и полноценно использовать эти данные для выявления нежелательного или подозрительного поведения. Например, в системе есть набор сценариев, позволяющих отслеживать открытия и пополнения множества счетов в различных филиалах банка одним клиентом. В сочетании с настройками пороговых сумм такие сценарии позволят выявить попытки разбиения клиентом крупных операций на мелкие части. В отличие от системы Mantas, российские наработки отвечают требованиям регулятора, но не в состоянии отслеживать подозрительное поведение клиента в целом по банку.

В-пятых. Помимо контроля за операциями клиентов, система позволяет анализировать внутренние операции банка с точки зрения соблюдения требований ЦБ или внутренних политик кредитной организации. Кроме того, такая система комплаенс-контроля позволяет следить, выявлять и расследовать операции банковских сотрудников, например, выполненных на рынке ценных бумаг и с использованием инсайдерской информации. Функциональность такого рода в российских АБС не предполагается.

В-шестых. Система по контролю за отмыванием денежных средств, финансированием терроризма, выявлению мошеннических операций и комплаенс-контролю является неотъемной частью системы управления операционными рисками. Любой выявленный инцидент является событием операционного риска и должен быть зафиксирован и изучен соответствующим подразделением. Как уже было сказано выше, система Mantas является частью GRC-комплекса, в который входит и система Reveleus, отвечающая, в частности, за управление операционными рисками. Таким образом, система Mantas принимает участие в общей картине того, что происходит в банке.

Можно сделать вывод, что автоматизированная банковская система не должна и не может комплексно и в целом по кредитной организации выполнять функции по контролю за отмыванием средств, финансированием терроризма, борьбе с мошенническими операциями и комплаенс-контролю. Можно провести аналогию с системой обязательной отчетности. Системы отчетности, работающие вне АБС, отличаются большей функциональностью, гибкостью, способностью загружать данные из нескольких источников и уменьшают нагрузку на основную банковскую систему. Аналогично, система по борьбе с незаконными и мошенническими операциями, выполняющая функции комплаенс-контроля, должна быть вынесена за рамки АБС. Такой подход обеспечивает необходимую гибкость, прозрачность для руководства и возможность интеграции системы по контролю за операциями в рамках единого механизма управления принятия решений на основе анализа рисков.

Заключение

Характерной особенностью легализации незаконных доходов является оперативное реагирование на изменения действующего законодательства и использование многоуровневых схем, существенно затрудняющих идентификацию истинного источника происхождения легализуемых доходов. Именно поэтому очень важно выбрать поставщика, обладающего международным опытом, который использует комплексный подход финансового мониторинга, выходящий за использование бизнес-правил, и своевременно реагирует на изобретательность мошенников и террористов. При этом необходимо учитывать наличие у него локального партнера, который будет оказывать услуги поддержки на территории Российской Федерации на русском языке. Не надо ждать ужесточения надзора со стороны Центрального Банка, а уже сейчас использовать международные наработки в этой области, повышая тем самым культуру рисков в кредитной организации. В конце концов, от этого зависит ее дальнейшее финансовое благосостояние и благополучие.

Приложение 1. Сценарии Oracle Mantas

Пакет сценариев	Описание
Территориальные единицы и юридические лица с высоким уровнем риска	Кредитные организации проводят дополнительные проверки в отношении стран и клиентов с высоким уровнем риска. Как правило, для выявления подозрительных клиентов банки пользуются собственными «черными списками», «черными списками» Центрального Банка, а также данными таких иностранных организаций, как Отдел по контролю иностранных активов Министерства Финансов США. Данный пакет сценариев предназначен для мониторинга операций, которые осуществляются клиентами с высоким уровнем риска или на территории из «черного списка». Сценарии этого пакета выполняют проверки операций, счетов клиентов, контрагентов, банков-корреспондентов на предмет их нахождения в используемых Банком «черных списках».
Скрытые связи	Сценарии, входящие в этот пакет, позволяют банку выявить неочевидные связи между счетами, клиентами, корреспондентами, которые могут свидетельствовать о возможной легализации преступных доходов. Система выполняет проверки денежных переводов с банками-корреспондентами, движения средств между внутренними счетами клиента, расчетов клиента с третьими лицами. В целях предотвращения попыток скрыть источники средств осуществляется анализ получателей и выгодоприобретателей. Эти сценарии помогают выявить сеть на первый взгляд несвязанных между собой счетов, клиентов и третьих лиц. Очень часто преступники пытаются скрыть свою личность путем изменения своего адреса или подделки документов. Так, например, они используют несколько различных удостоверяющих документов для отправления и получения денежных переводов, указывая при этом один и тот же адрес. Или, наоборот, используют несколько фиктивных адресов для одного паспорта. Сценарии позволяют выявить попытки скрыть истинную личность клиента и определить его фактический адрес.
Отклонения от привычного поведения	Внезапные денежные переводы с одного счета на другой, вывод средств за пределы кредитной организации и значительное увеличение объема операций на долгое время на неактивном счете могут свидетельствовать о возможном отмывании средств или деятельности мошенника. В ходе работы сценариев анализируются электронные денежные переводы, платежные документы, операции пополнения и снятия средств со счетов клиента, после чего идет сравнение с его средними или пиковыми объемами за месяц. В случае обнаружения значительного отклонения от привычного объема операций система направит инцидент на расследование комплаенс-офицеру. Быстрое движение средств между счетами обычно позволяет лицам, занимающимся отмыванием денег, интегрировать свои средства и придать им признаки легитимности. В ходе анализа операций клиента система будет принимать во внимание скорость перемещения средств, а также сумму перевода. Есть отдельный сценарий, который отслеживает снятие или пополнение счета приблизительно одинаковыми суммами, что может указывать на попытки структурирования (схема отмывания денег, когда несколько сумм депонируются подставными лицами).
Сценарии предотвращения мошенничества и утечки информации	Сценарии выявления фактов воровства и незаконного овладения счетом, подделки документов, мошеннических операций с банкоматами и пластиковыми картами и обналичивания недействительных чеков. А также сценарии предотвращения утечки инсайдерской информации и мошенничества со стороны персонала.
Сценарии, применяемые страховыми компаниями	В ноябре 2005 года Бюро по предотвращению финансовых преступлений США обязало страховые компании использовать в своей работе AML-программы, аналогичные финансовым организациям. Данный пакет сценариев предназначен исключительно для противодействия легализации через продукты страхования: заем средств под залог страхового полиса, купленного на нелегальные средства; досрочное расторжение договора страхования, заключенного на крупную сумму; переоформление полиса на другое лицо с его последующим обналичиванием.
Другие	Сценарии, входящие в данный пакет, предназначены для выявления попыток структурирования и анализа различных клиентских операций. Система очень тщательно проверяет транзакции, сумма которых близка к установленному Центральным Банком лимиту в 600 000 рублей, анализирует значительное списание средств со счетов клиентов, отслеживает операции, совершаемые в банкоматах. В своих попытках легализовать доходы лица, занимающиеся отмыванием, и преступные синдикаты берут в банках краткосрочные кредиты (потребительские кредиты, целевые кредиты для юридических лиц, ипотека и т.д.), после чего они погашают ссуду целиком или ее большую часть. Быстрое погашение кредита позволяет таким лицам получить от кредитной организации легальные средства, погашая кредит нелегальными доходами, чье происхождение очень сложно определить. Oracle Mantas анализирует краткосрочные кредиты банка, чей график погашения постоянно изменятся вследствие внесения больших сумм на досрочное погашение.

Модернизация системы хранения данных и системы резервного копирования в ВТБ

О заказчике

ОАО Банк ВТБ и его дочерние банки (группа ВТБ) являются международной финансовой группой, предоставляющей широкий диапазон банковских услуг и продуктов в России, некоторых странах СНГ и отдельных странах Западной Европы, Азии и Африки. Группа ВТБ работает в сферах корпоративного, розничного и инвестиционного обслуживания. Входящие в Группу банки ведут свою деятельность под единым брендом и руководствуются единым подходом к работе с клиентами.

Сегодня, будучи одним из крупнейших коммерческих банков страны по капиталу, ВТБ предоставляет весь комплекс банковских услуг высочайшего качества как юридическим, так и физическим лицам. ВТБ является одним из лидеров национального банковского сектора и занимает прочные конкурентные позиции на всех сегментах рынка банковских услуг. Главным акционером ВТБ с долей в 77,5% является Правительство РФ.

Дмитрий Назипов, старший вице-президент и CIO банка ВТБ: «Мы давно ощущали необходимость проведения модернизации систем хранения данных и резервного копирования. Благодаря проведенным работам нам удалось обеспечить требуемый уровень производительности, доступности и надежности работы систем. Наши системы способны работать в режиме 24x7x365. Внедренные решения позволят нам активно развиваться. Мы готовы к реализации новых бизнес-задач».

Сергей Удалов, заместитель начальника управления внедрения и сопровождения информационных систем банка ВТБ: «Специалисты компании «Инфосистемы Джет» предложили нам решение, которое позволило модернизировать системы хранения данных и резервного копирования, минимизировав при этом степень воздействия на имеющуюся ИТ-инфраструктуру. При таком подходе «жизнь» системы для ИТ-сотрудников банка осталась понятной и прозрачной, что обеспечило их быструю адаптацию к новой среде и позволило снизить затраты на внедрение системы на 30-40%».

Задачи

Банк ВТБ стремится предоставлять клиентам широкий комплекс услуг, принятых в международной банковской практике. Развитие и рост бизнеса, расширение спектра проводимых операций, необходимость гарантировать быстрое и бесперебойное обслуживание клиентов потребовали развития и модернизации ИТ-системы банка. В перспективе были поставлены следующие цели:

- осуществить переход к сервисно-ориентированной архитектуре;
- внедрить интеграционную платформу;
- создать и внедрить новые бизнес-приложения.

Достижение этих целей потребовало модернизации системы хранения данных (СХД) и системы резервного копирования (СРК).

В состав единой системы хранения данных ВТБ входили несколько дисковых массивов класса Midrange и Hi-End, производства компаний Hitachi Data Systems и Hewlett-Packard, расположенные на двух технологических площадках и объединенные единой сетью хранения данных (SAN). Связь между двумя площадками осуществляется по двум волоконно-оптическим каналам связи. По одному из каналов — с использованием оптической транспортной системы (ОТС) с применением технологии уплотнения DWDM, по другому — прямым соединением. Каналы связи использовались, в том числе, и для on-line репликации данных между технологическими площадками.

Для резервирования данных использовалась распределенная система резервного копирования. Ежедневный объем резервируемых данных составлял 4,5TB, общий объем зарезервированных данных, хранящихся на магнитных лентах, — 22TB. Ленточные библиотеки подключались к медиа-серверам через SAN. Передача данных при резервном копировании осуществлялась через SAN и LAN.

Несмотря на правильные архитектурные решения, заложенные при создании СХД и СРК, в процессе их эксплуатации накопились некоторые проблемы. В частности, на каждом этапе развития информационная инфраструктура банка

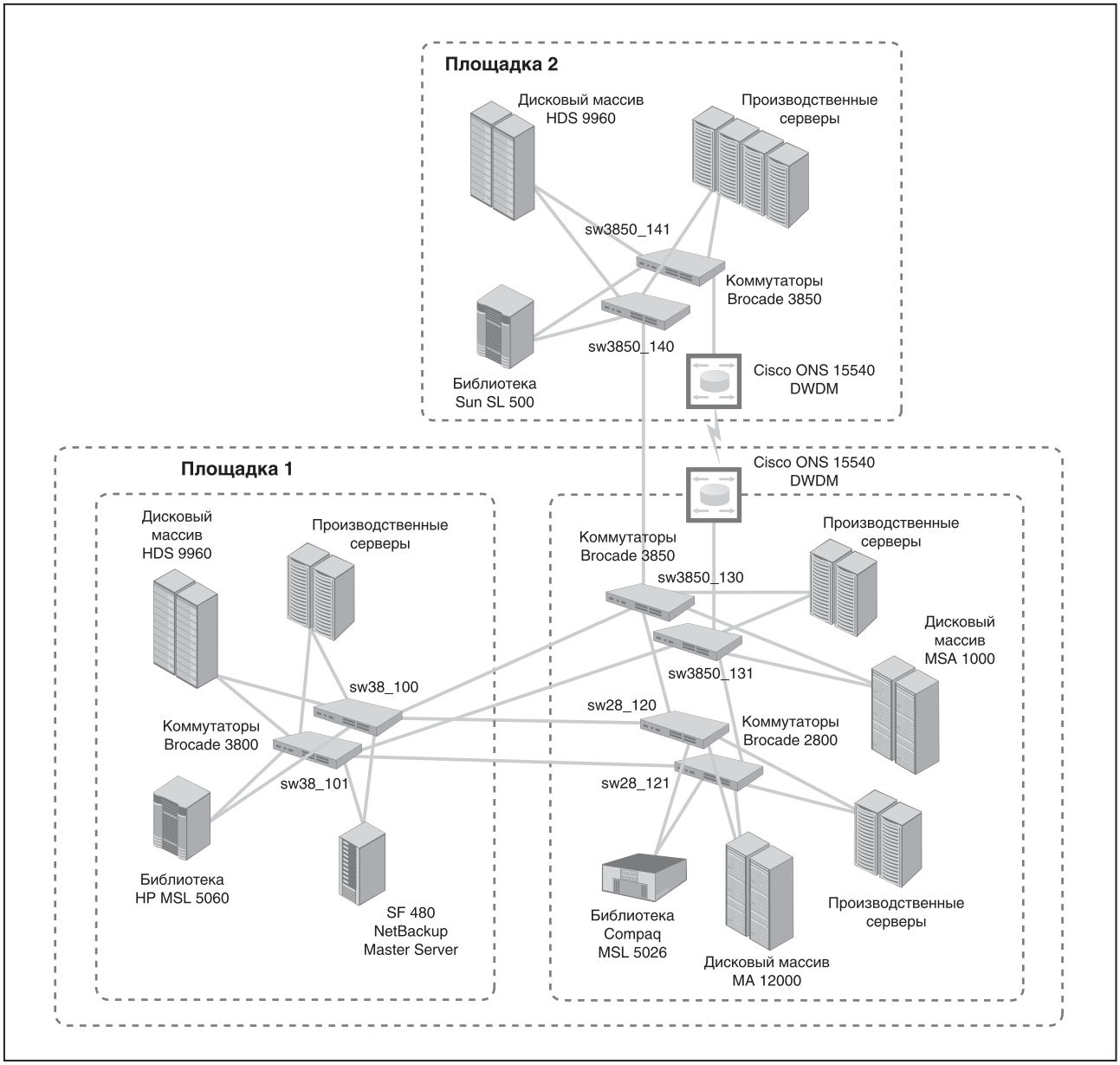

Рис. 1. Логическая схема СХД до проведения модернизации

дополнялась оборудованием актуальным на тот момент. С течением лет парк серверов и дисковых массивов постепенно становился все более разнообразным, часть оборудования со временем морально устарела. Это привело к увеличению времени копирования данных и снижению производительности.

Необходимо было предложить решение по модернизации СХД и СРК, которое позволило бы нарастить существующие объемы хранения, консолидировать хранимые данные на меньшем количестве дисковых массивов, обеспечив при этом необходимую производительность дисковой подсистемы для приложений, а также исключить из состава комплекса морально устаревшее оборудование. Помимо этого, СХД должна была обеспечить безболезненное подсоединение новых устройств без изменения архитектуры SAN, в полной мере используя имеющееся оборудование, и иметь возможность расширения в будущем, например, подключения новых технологических площадок.

Кроме того, необходимо было сохранить существующую ИТ-инфраструктуру и инвестиции, вложенные в СРК, СХД и каналы связи, а также учесть требования, предъявляемые к работе данных систем, как существующими приложениями, так и планируемыми к внедрению новыми прикладными системами.

Банк ВТБ провел тендер, по итогам которого исполнителем проекта стала компания «Инфосистемы Джет».

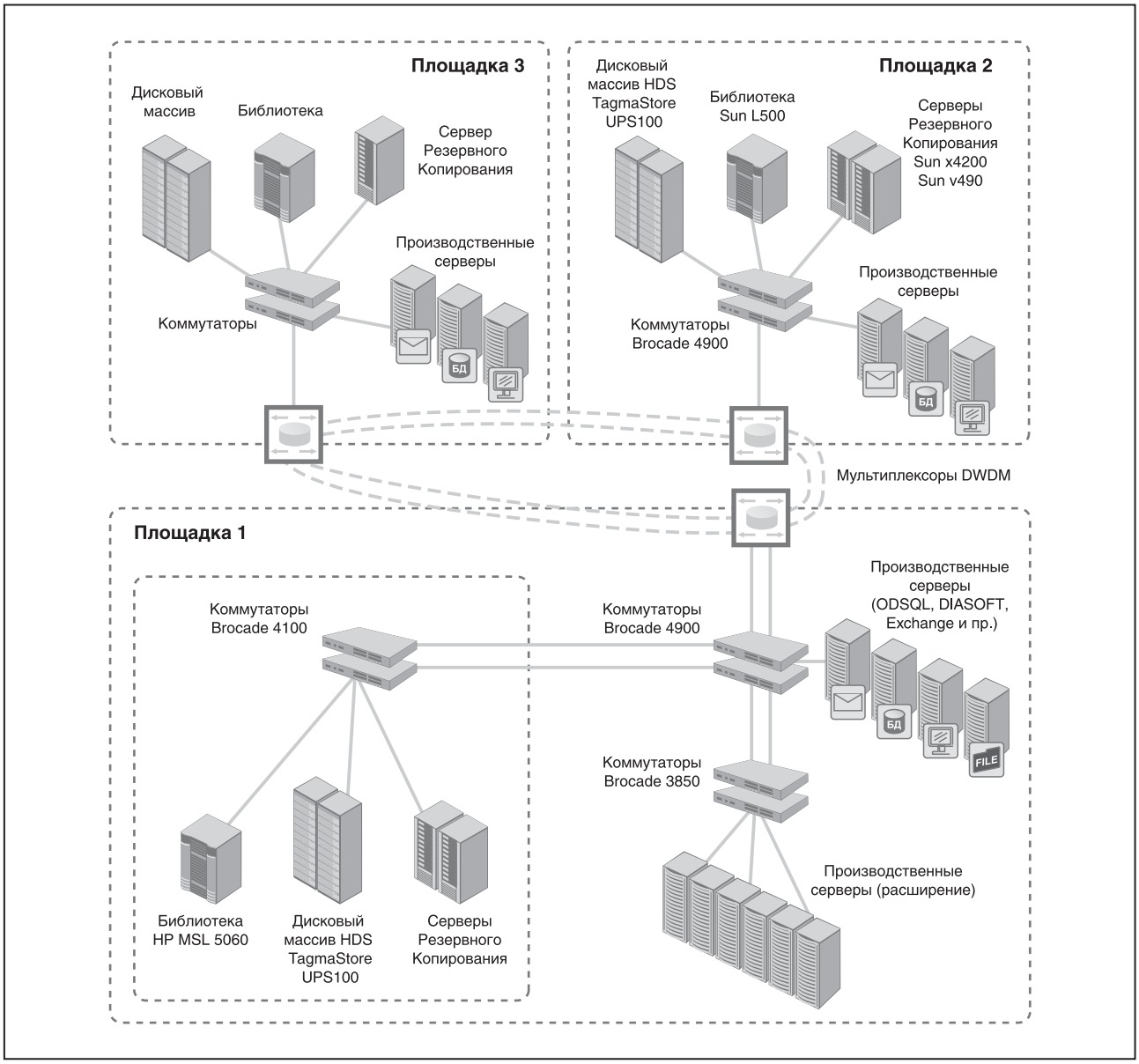

Рис. 1. СХД и СРК банка ВТБ (после модернизации)

Решение

Модернизация СХД

Специалисты компании «Инфосистемы Джет» предложили следующее решение по модернизации данной системы. Во-первых, в состав единой системы хранения данных ВТБ на обеих технологических площадках были введены новые дисковые массивы Hi-End класса USP100 и USP-V Hitachi Data Systems (суммарная «полезная» емкость составляет более 15 ТБ), на которых была консолидирована основная масса высококритичных данных. Массивы, используемые для этих целей ранее, были либо выведены из эксплуатации, либо задействованы для хранения менее ценных данных. Во-вторых, были произведены изменения в инфрастуктуре SAN. В частности, модернизировано каналообразующее оборудование, используемое для организации соединений между площадками (была произведена замена старых, снятых с производства и поддержки производителя DWDM-мультиплексоров, в работе которых периодически возникали сбои) и произведено подключение обоих каналов к отказоустойчивой ОТС. Также была изменена структура SAN внутри технологических площадок, в т. ч. были добавлены новые более производительные FC- коммутаторы(Inter-Switch Liks, ISL), за счет чего были увеличены портовая емкость SAN и ее пропускная способность.

DWDM на службе SAN

Для обеспечения требуемой производительности SAN при передаче данных в режиме on-line между 2-мя площадками были созданы 2 дублирующих друг друга канала связи с пропускной способностью не менее 8 GBit/s каждый. При этом оборудование, обеспечивающее связь между площадками, было совмещено с используемыми FC-коммутаторами Brocade. Также была предусмотрена возможность перспективного расширения по количеству линков, при этом как альтернатива прокладки новых оптических линий связи была использована технология оптического мультиплексирования. На существующие каналы связи была установлена система оптического уплотнения каналов DWDM от компании Nortel (Optera Metro 5200), которая сегодня позволяет передавать по одному оптическому каналу четыре сигнала FC400 и два сигнала GE. Таким образом, сегодня общая пропускная способность одного канала составляет 18 GBit/s. В случае аварии на основной оптической линии связи предусмотрено автоматическое переключение средствами оборудования DWDM всех оптических сигналов на дублирующий канал связи. Специалисты компании «Инфосистемы Джет» отработали решение по включению новых мультиплексоров компании Nortel в SAN и организации их взаимодействия с FC-коммутаторами Brocade в тестовой лаборатории — это позволило учесть все возможные ошибки и недочеты. Был разработан четкий план внедрения решения. Таким образом, несмотря на большое количество операций — установка оборудования, перекоммутирование, работы в банке были организованы четко, и связь между площадками при проведении модернизации отсутствовала менее одного часа. Все работы были проведены в выходной день.

Модернизация СРК

Специалисты службы ИТ банка и компании «Инфосистемы Джет» разработали решение, которое позволило банку без кардинальных изменений существующей системы резервного копирования интегрировать в нее новое оборудование.

В состав основной СРК был введен новый медиа-сервер, который обеспечил взаимодействие клиентов резервного копирования с новой ленточной библиотекой на второй технологической площадке, что привело к значительному сокращению трафика в LAN и SAN между площадками.

Результат

Модернизация СХД и СРК стала одним из фундаментальных проектов, реализуемых ИТ-службой банка ВТБ для обеспечения решения прикладных и бизнес-задач. В результате проекта была значительно увеличена производительность и расширена емкость систем хранения, повышена надежность хранения и эффективность управления данными. Банк ВТБ получил не только модернизированную сеть хранения данных, но и оптическую высокопроизводительную, масштабируемую сеть передачи данных. Проект позволит банку в дальнейшем развивать и совершенствовать ИТ-инфраструктуру, подключая новые офисы и Дата-центры, а также повышать уровень предоставления услуг.

Исполнение проекта с учетом тестирования решения в лаборатории компании «Инфосистемы Джет», поставок оборудования и запуска заняло примерно три месяца.

Константин Казаков, директор Центра банковских технологий компании «Инфосистемы Джет»: «В банке ВТБ очень грамотно выстроен процесс управления проектами: все работы были четко спланированы и достаточно последовательно реализованы.

На старте нами был подготовлен эскизный проект, который был защищен вначале на архитектурном совете внутри компании «Инфосистемы Джет», затем на архитектурном совете банка. Его дальнейшая реализация была уже достаточно тривиальным делом — совместной проектной командой был четко согласован план работ, грамотно спланированы ресурсы, разработан график закупок и внедрения».

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

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

Подписной индекс по каталогу Роспечати 32555

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