Построение системы информационной безопасности банка на основе управления рисками

Алексей Дроздов, *старший консультант компании IDS Scheer Россия и страны СНГ, д. т. н.*
Андрей Коптелов, *директор департамента ИТ-консалтинга компании IDS Scheer Россия и страны СНГ*

Банковские организации сегодня все чаще сталкиваются с широким спектром существующих угроз, таких как компьютерное мошенничество, компьютерные вирусы, взлом компьютерных систем, отказ в обслуживании и т. д. Высокая зависимость банковских организаций от информационных ресурсов, объединение корпоративных сетей и сетей общего доступа, совместное использование информационных ресурсов повышают уязвимость организаций от подобных угроз. Поскольку, многие существующие в банках информационные системы, изначально не проектировались с необходимым уровнем защищенности, то в большинстве случаев возможности обеспечения информационной безопасности (ИБ) ограничены. Поэтому сегодня для банков жизненно необходима комплексная система информационной безопасности, которая задействует не только технические, но и организационные ресурсы. Создание комплексной системы информационной безопасности может обойтись для банка значительно дешевле, чем ликвидация последствий угроз ИБ. Настоящая статья посвящена вопросам создания системы ИБ банка на основе управления операционными рисками в процессах банковской деятельности.

Общие принципы обеспечения информационной безопасности

Информационная безопасность – это состояние защищенности интересов организации в условиях угроз в информационной сфере. Информационная безопасность предполагает, что какую бы форму ни принимала информация (бумажная, электронная, видео- и аудиопредставление), она должна быть адекватно защищена. Защищенность информации достигается обеспечением совокупности следующих свойств ИБ:

- конфиденциальность: обеспечение доступа к информации только для авторизованных пользователей;
- целостность: обеспечение полноты и точности информации и методов ее обработки;
- доступность: обеспечение доступа к информации и смежным ресурсам авторизованных пользователей в любой необходимый момент времени.

Для создания эффективной системы ИБ необходимо определить требования своей организации к уровню информационной безопасности. Известны три основных источника таких требований [1]:

- результаты оценки рисков организации, на основании которых затем определяются ресурсы, оцениваются угрозы, уязвимости и вероятность их возникновения, а также величина возможного ущерба;
- требования законодательства, подзаконных актов и договоров, которые должна соблюдать организация, ее партнеры и поставщики;
- принципы и требования к обработке информации, разработанные внутри организации для обеспечения ее деятельности.

Требования к ИБ определяются путем систематической оценки рисков нарушения ИБ, при этом оценка рисков позволяет привести расходы на средства контроля в соответствие с размером ущерба, наносимого организации в результате реализации рисков нарушения ИБ. Оценка рисков предполагает определение вероятного ущерба для бизнеса, полученного в результате реализации риска нарушения ИБ, и оценку вероятности наступления рискового события.

Результаты оценки позволяют определять необходимые действия и приоритеты для управления рисками нарушения ИБ, а также объем внедрения средств и механизмов контроля и минимизации этих рисков.

Оценка рисков нарушения ИБ должна проводиться периодически для того, чтобы учитывать изменения требований и приоритетов, рассматривать новые угрозы и уязвимости, подтверждать эффективность и актуальность используемых в организации механизмов контроля. При этом проверки должны проводиться с различным уровнем глубины, в зависимости от результатов предыдущей оценки и изменения уровня риска, который руководство готово принять.

Необходимо отметить, что управление всеми рисками нарушения ИБ может оказаться экономически невыгодным, поскольку для части рисков проще согласиться с убытками, чем создавать и внедрять необходимую контрольную процедуру. Поэтому на начальном этапе оценки рисков обычно применяется метод качественных оценок, позволяющий ранжировать риски по критериям «вероятность» и «убытки» на основании экспертного мнения. И только потом производится уточнение качественных оценок в рамках количественной (стоимостной) оценки рисков, требующей больших временных затрат. Поэтому ключевой задачей качественной оценки, помимо определения значимости рисков, является «отсечение» тех рисков, которые с высокой степенью вероятности не оправдают дальнейших затрат на их минимизацию или не повлияют на критичную информацию.

Согласно [1], механизмы контроля, существенные для организации с юридической точки зрения, включают защиту данных и тайну персональной информации, охрану документов организации, права на интеллектуальную собственность.

Механизмы контроля, рассматриваемые в качестве лучших практических примеров в области обеспечения ИБ, включают политику ИБ, распределение ответственности за обеспечение ИБ, обучение и тренинги по ИБ, информирование об инцидентах безопасности, управление непрерывностью бизнеса.

В качестве критических факторов успеха построения в организации системы информационной безопасности можно рассматривать следующие:

- политика ИБ организации;
- принципы обеспечения ИБ;
- поддержка со стороны руководства;
- анализ и управление рисками в организации;
- информирование по проблемам безопасности руководителей и сотрудников;
- распространение разъяснений к стандартам и политике информационной безопасности организации среди сотрудников и контрагентов;
- проведение обучения и тренингов;
- сбалансированная система измерения эффективности и совершенствования системы менеджмента ИБ.

В качестве основных компонентов системы ИБ, присущих любым организациям, стандарт [1] рассматривает следующие:

- организационную безопасность (инфраструктура, безопасность доступа третьих сторон, аутсорсинг);
- контроль ресурсов;
- безопасность персонала (в должностных инструкциях и при найме на работу, обучение пользователей, реагирование на инциденты ИБ);
- физическая безопасность (в том числе безопасность оборудования);
- управление коммуникациями и операциями (включая операционные процедуры и распределение ответственности);
- контроль доступа;
- разработку и сопровождение систем.

Принципы построения системы менеджмента информационной безопасности банка

Основным нормативным актом Центрального банка России, регламентирующим создание системы информационной безопасности, является стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2006), введенный в действие в январе 2006 г. и заменивший собой стандарт Центробанка СТО БР ИББС-1.0-2004 (далее – стандарт ЦБ, [2]).

На сегодняшний день стандарт ЦБ носит рекомендательный характер: его положения применяются на добровольной основе, и российские банки пока не обязаны обеспечивать совместимость с данным нормативным актом. Тем не менее, в настоящее время в России и в других странах наблюдается тенденция к ужесточению законодательного бремени, поэтому со временем стандарт ЦБ может стать обязательным для исполнения.

Стандарт ЦБ, со ссылкой на ISO/IEC IS 27001, определяет систему менеджмента информационной безопасности (СМИБ) организации банковской системы РФ как часть общей системы менеджмента организации банковской системы, основанную на подходе бизнес-риска и предназначенную для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения информационной безопасности организации.

Стандарт содержит двенадцать глав, основной из которых является глава 5 – «Исходная концептуальная схема (парадигма) обеспечения информационной безопасности организаций БС РФ». Система менеджмента информационной безопасности (СМИБ) банка должна основываться на постоянном стремлении собственника информационных ресурсов к выявлению следов активности злоумышленника и превентивном противодействии им путем разработки моделей угроз и нарушителей.

В соответствии со стандартом ЦБ, обеспечение ИБ банковских организаций должно строиться с использованием процессного подхода.

Процессный подход применительно к ИБ – это представление деятельности по обеспечению ИБ в виде системы процессов организации вместе с их идентификацией, координацией и управлением. Согласно стандарту ЦБ, процессный подход к обеспечению ИБ банков требует:

- понимания требований ИБ бизнеса и потребности устанавливать политику и цели для информационной безопасности;
- реализации и надлежащей эксплуатации необходимых защитных мер (средств менеджмента ИБ) в контексте управления общим риском бизнеса организации;
- проведения мониторинга и анализа работы и эффективности СМИБ;
- непрерывного совершенствования СМИБ на основе объективных измерений.

В соответствии со стандартом ISO/IEC IS 27001, стандарт ЦБ предлагает модель непрерывного циклического процесса менеджмента организации, построенную в соответствии с моделью Деминга.

Стандарт ЦБ рассматривает следующие общие принципы обеспечения ИБ банковских организаций:

- своевременность обнаружения проблем;
- прогнозируемость развития проблем;
- оценка влияния проблем на бизнес-цели;
- адекватность защитных мер;
- эффективность защитных мер;
- использование опыта при принятии и реализации решений;
- непрерывность реализации принципов безопасного функционирования;
- адекватность и контролируемость защитных мер.

В дополнение к перечисленным, стандарт ЦБ рассматривает такие специальные принципы обеспечения ИБ банка, направленные на повыше-

Согласно стандарту ИСО 9000, процесс – это совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующих входы в выходы. Выход одного процесса может быть входом для другого процесса. Любой процесс имеет такие ключевые признаки, как повторяемость, наличие предварительно установленных правил выполнения цепочки взаимосвязанных операций процесса, наличие входов (таких как материалы и/или информация), выходов (продукт/услуга) процесса, а также ресурсов, используемых при его выполнении.
Согласно тому же стандарту, «систематическая идентификация и менеджмент применяемых организацией процессов, и особенно взаимодействия таких процессов, могут считаться «процессным подходом». Соответственно, организация, в которой деятельностью и ресурсами управляют как процессами, может считаться процессно-ориентированной.

ние уровня зрелости процессов менеджмента ИБ в организации, как:

- определенность функциональных целей и целей ИБ (с их фиксацией в специальном внутрибанковском документе);
- знание своих клиентов и служащих, персонификация и адекватное разделение ролей и ответственности;
- адекватность ролей функциям и процедурам и их сопоставимость с критериями и системой оценки;
- доступность услуг и сервисов клиентов и контрагентов в установленные сроки с их определением в соответствующих документах (соглашениях);
- наблюдаемость и оцениваемость обеспечения ИБ.

Фундаментальным документом СМИБ является политика ИБ. В этом документе должны быть описаны цели и задачи СМИБ, а также сформулированы правила, требования и руководящие принципы в области ИБ, которыми банковская организация руководствуется в своей деятельности. В частности, политика ИБ должна включать требования по обеспечению ИБ по следующим направлениям:

- при назначении и распределении ролей и обеспечении доверия к персоналу;
- в части стадий жизненного цикла автоматизированных банковских систем;
- при управлении доступом персонала и клиентов к активам банка;
- в части средств антивирусной защиты;
- при использовании ресурсов Интернета;
- при использовании средств криптографической защиты информации;
- в части банковских платежных/информационных технологических процессов.

Система менеджмента информационной безопасности банка, закон Сарбейнса-Оксли и соглашение Базель II

Стандарт ЦБ содержит большое число нормативных ссылок. В частности, он объединяет в себе основные требования стандартов по менеджменту ИТ-безопасности (ISO 13335, 17799, 27001), регламентирует описание жизненного цикла автоматизированных банковских систем и критерии оценки ИТ-безопасности в рамках ГОСТ Р ИСО/МЭК 15408, использует некоторые положения британской методологии оценки рисков CRAMM.

Sarbanes-Oxley Act (SOX) – определяет требования к системе внутреннего контроля и прозрачности финансовой отчетности компаний. Был принят в США в марте 2005 года как реакция на корпоративные скандалы и банкротства крупнейших мировых компаний (Enron, Parmalat и др.), вызванные недостоверной финансовой отчётностью и неэффективной системой внутреннего контроля. Данным законом руководству компаний вменена обязанность подтверждать правильность финансовой отчетности лично, а также подтверждать свою ответственность за эффективность системы внутреннего контроля и в первую очередь – при подготовке финансовой отчетности. Для соответствия закону необходимо получить заключение внешнего аудитора об эффективности системы внутреннего контроля компании.

Как отмечено в [3], прослеживается связь стандарта ЦБ с секцией 404 американского закона Сарбейнса-Оксли о средствах внутреннего контроля. Так в соответствии с п. 5.10 стандарта ЦБ «…все точки в банковских технологических процессах, где осуществляется взаимодействие персонала со средствами и системами автоматизации, должны тщательно контролироваться», что соответствует требованиям закона Сарбейнса-Оксли (правда, Комитет по надзору за отчетностью открытых акционерных компаний (PCAOB), созданный в США для контроля над исполнением закона Сарбейнса-Оксли, конкретизирует требования секции 404 в стандартах по аудиту механизмов внутреннего контроля, а в стандарте ЦБ данное положение не детализировано).

Другим важным международным документом, связанным со стандартом ЦБ, является соглашение Базель II, по которому финансовые организации обязаны рассчитывать кредитные, рыночные и операционные риски с целью обеспечения величины резервного капитала, достаточной для их покрытия. Важная особенность Базель II – требование учета операционного риска, определяемого как «риск потерь в результате неадекватности или ошибок (сбоев) внутренних процессов, людей и (или) систем, или в результате внешних событий». Согласно этому определению, в операционные риски попадают, прежде всего, действия инсайдеров (кража конфиденциальной информации, мошенничество, халатность и т. д.) и компьютерные угрозы (несанкционированный доступ, вредоносные коды и т. д.).

Очевидно, что угрозы ИТ-безопасности (и прежде всего, действия инсайдеров) не только являются неотъемлемой частью, но и представляют собой основной компонент операционных рисков. Поэтому стандарт ЦБ, позволяющий минимизировать риски ИТ-безопасности, дает банкам возможность организовать эффективную систему управления операционными рисками. Кроме того, реализация положений стандарта ЦБ сегодня позволит банкам упростить процесс перехода на соответствие требованиям Basel II завтра и сделать этот переход менее сложным и дорогостоящим (Россия планирует присоединиться к Basel II в 2009 году).

Базельский комитет по банковскому надзору при Банке международных расчетов был основан в г. Базеле (Швейцария) в 1974 году президентами центральных банков стран десяти крупнейших промышленно развитых стран (G10). Основная задача Комитета – внедрение единых стандартов в сфере банковского регулирования. Основными документами Базельского комитета являются:

- *Соглашение по капиталу «Базель-I» (1988 г);*
- *Основные принципы эффективного надзора (1997 г., пересмотрены в 2006 г.);*
- *Новые соглашения о достаточности капитала «Базель II» (2004 г.).*

Помимо трех названных (эффективная система ИТ-безопасности, эффективное управление операци-

онными рисками, совместимость с Базель II) существует еще один стимул к внедрению стандарта ЦБ – защита репутации банка. Дело в том, что при реализации любой из угроз ИТ-безопасности может пострадать репутация финансовой компании, что, в свою очередь, негативно скажется на ее клиентской базе. Поэтому неслучайно, что сегодня подавляющее число российских банков (по данным [3] – 78 %) высказываются за необходимость использования стандарта ЦБ кредитно-финансовыми организациями России.

Стандарт «Цели контроля при использовании информационных технологий» (Control Objectives for Information and Related Technology — CobiT) посвящен вопросам аудита соответствия используемых информационных технологий существующим бизнес-процессам и является основой для создания общих правил надежности и механизма контроля эффективности использования информационных систем. Применение COBIT позволяет использовать лучшую практику в области управления ИТ, определять зрелость ИТ-процессов и быть уверенным в существовании адекватного уровня надежности и контроля при использовании информационных технологий. Для аудиторов в области ИТ COBIT является основой для формирования мнения об эффективности внутреннего контроля. CobiT создается ISACF (Фонд Аудита и Контроля Информационных Систем), но продвигается и поддерживается ассоциацией ISACA (Ассоциации аудита и контроля информационных систем).

Уровни зрелости процессов менеджмента информационной безопасности

Для оценки зрелости процессов СМИБ стандарт ЦБ рекомендует использовать модель, основанную на универсальной модели зрелости процессов, определенной стандартом CobiT.

Модель зрелости процессов менеджмента ИБ включает шесть уровней:

1. Нулевой уровень характеризует полное отсутствие каких-либо процессов менеджмента ИБ в организации.
2. Первый уровень («начальный») характеризует наличие документально зафиксированных свидетельств осознания организацией существования проблем обеспечения ИБ. Однако используемые процессы менеджмента ИБ не стандартизованы, применяются эпизодически и бессистемно. Общий подход к управлению ИБ не выработан.
3. Второй уровень («повторяемый») характеризует проработанность менеджмента ИБ до уровня периодически повторяемых процессов ИБ. Однако отсутствуют регулярное обучение и тренировки по стандартным процедурам, а вся ответственность за их выполнение возложена на исполнителя.
4. Третий уровень («определенный») характеризует то, что процессы менеджмента ИБ стандартизованы, документированы и доведены до персонала посредством обучения. Однако применяемые процедуры не оптимальны, а порядок их выполнения оставлен на усмотрение персонала, что сохраняет возможность отклонений от существующих регламентов.
5. Четвертый уровень («управляемый») характеризует то, что выполняются мониторинг и оценка соответствия процессов менеджмента ИБ, в результате чего эти процессы находятся в состоянии непрерывного совершенствования и основываются на хорошей практике. Однако средства автоматизации менеджмента ИБ используются в ограниченном объеме.
6. Пятый уровень («оптимизированный») характеризует проработанность процессов менеджмента ИБ до уровня лучшей практики, основанной на результатах непрерывного совершенствования и сравнения уровня зрелости относительно других организаций. В результате организация может быстро адаптироваться при изменениях в окружении и бизнесе.

Содержание проекта по созданию системы менеджмента информационной безопасностью

Проект по созданию СМИБ в банковской организации, в соответствии со стандартом ЦБ, включает ряд этапов, схематически показанных на рис. 1.

На первом этапе определяются области действия СМИБ и выбираются подходы к оценке рисков ИБ; выполняется анализ и оценка рисков ИБ, определяются варианты обработки рисков ИБ для наиболее критичных информационных активов и бизнес-процессов организации; определяются или уточняются политики СМИБ; производится выбор целей ИБ и обоснование необходимых защитных мер; принимается решение о построении и эксплуатации (совершенствовании) СМИБ.

На втором этапе реализуется план создания СМИБ: производятся управление необходимыми работами и ресурсами; реализация программ по обучению и осведомленности персонала в части ИБ; обнаружение и реагирование на инциденты безопасности; обеспечение непрерывности бизнеса и восстановления после прерываний (обеспечение непрерывности бизнеса должно производиться с учетом требований раздела 14 международного стандарта ISO/IEC IS 17799).

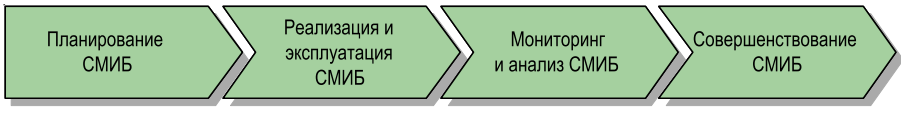

Рис. 1. Этапы создания СМИБ

На третьем этапе осуществляются мониторинг и контроль защитных мер, включая регистрацию действий и событий, связанных со СМИБ; анализ эффективности СМИБ; внутренний аудит СМИБ; анализ СМИБ со стороны высшего руководства; проведение периодического внешнего аудита СМИБ.

На этапе совершенствования системы производятся реализация стратегических и тактических улучшений в СМИБ (при этом стратегические улучшения требуют соответствующих решений на уровне руководства организации); информирование обо

всех изменениях и их согласование с заинтересованными сторонами (с клиентами, партнерами организации); оценка достижения поставленных целей и потребностей в дальнейшем развитии СМИБ.

Использование платформы ARIS при создании системы информационной безопасности

В качестве инструментального средства поддержки проектов по созданию СМИБ и повышению уровня зрелости процессов менеджмента ИБ может использоваться программный продукт ARIS Process Risk Scout [4], входящий в состав блока контроллинга платформы ARIS и предназначенный для разработки, внедрения и поддержания в рабочем состоянии системы управления операционными рисками (СУОР).

Process Risk Scout включает два основных компонента:

1. Risk Assistant, представляющий собой развернутое описание технологий, методик, этапов построения СУОР и используемый на этапе создания системы;
2. Risk Portal – портал операционных рисков компании, используемый на этапе контроля рисков в качестве основного инструментального средства СУОР.

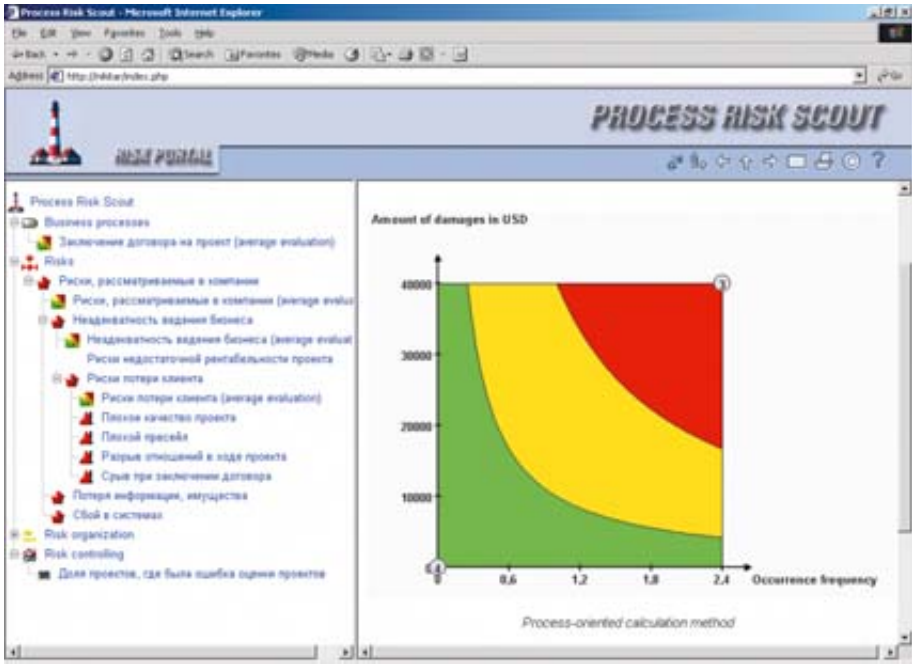

Рис. 2. Пример окна ARIS Process Risk Scout

Платформа ARIS представляет собой единый методологический и инструментальный комплекс, применяемый в течение всего жизненного цикла систем управления. Разработчик платформы – компания IDS Scheer AG – является признанным мировым лидером в области разработки инструментальных средств для описания, анализа, совершенствования и управления бизнес-процессами. Платформа ARIS объединяет более 20-и программных продуктов, относящихся, в соответствии со своим предназначением и областью использования, к одной из четырех платформ: стратегической, разработки, внедрения и контроллинга.

Портал рисков дает возможность посмотреть на риски организации с четырех различных точек зрения: с точки зрения процессов (какие риски связаны с процессами организации); с точки зрения категорий рисков, созданных в ходе их классификации; с точки зрения ответственных за риски; с точки зрения индикаторов рисков, используемых при их контроллинге.

Построению СУОР с использованием ARIS Process Risk Scout должны предшествовать описание процессов и классификация операционных рисков банка с использованием методологии и инструментария ARIS, например, программного продукта ARIS Business Architect. По окончании описания производится взаимная верификация моделей процессов и дерева рисков, в ходе которой, с одной стороны, риски из дерева позиционируются на моделях процессов, а с другой, новые операционные риски, выявленные в ходе анализа процессов, размещаются на дереве рисков. В результате получают:

- модели процессов с рисками, связанными с функциями,
- скорректированное дерево рисков,
- модели описания рисков, а также заполненные атрибуты рисков (объемы убытков и частоты возникновения), как текущие, так и целевые (уменьшенные в результате проведения необходимых корректирующих мероприятий).

Атрибуты рисков заполняются по информации, полученной в ходе изучения нормативной документации банка и проведения интервью с ключевыми сотрудниками.

Вся собранная таким образом информация далее используется для генерации портала рисков с использованием ARIS Process Risk Scout. Дальнейшее использование портала дает возможность получать актуальную информацию о состоянии операционных рисков, в том числе в графической форме (рис. 2).

Таким образом, использование стандарта Банка России СТО БР ИББС-1.0-2006, процессного подхода и инструментария ARIS может служить основой для создания в банке эффективной системы менеджмента информационной безопасности.

Литература

1. BS ISO/IEC 17799:2000 BS 7799-1:2000. Информационные технологии – Практические правила управления информационной безопасностью
2. Стандарт Банка России СТО БР ИББС-1.0-2006. «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». М.: 2006
3. А. Доля. Стандарт, ориентированный на консолидацию // Директор ИС, № 08, 2006
4. http://www. ids-scheer. com/en/Software/ARIS_Software/ARIS_Process_Risk_Scout/3753. html