**В. ЗИНКЕВИЧ**, руководитель отдела консалтинга компании «Франклин & Грант. Финансы и аналитика»
**Д. ШТАТОВ**, консультант компании «Франклин & Грант. Финансы и аналитика»

# Информационные риски: анализ и количественная оценка

Обеспечение информационной безопасности — тема, далеко не новая для российских банков. Наши банкиры прекрасно понимают стоимость информационной безопасности и её взаимосвязь с риском потери деловой репутации и стратегическим риском, а также эффект масштаба — чем крупнее банк, разветвлённее его территориальная сеть, чем активнее он развивается, тем более нелинейно могут возрастать его информационные риски. Однако понятие обеспечения информационной безопасности не совсем совпадает с управлением информационными рисками как частью операционных рисков, а включается в него. Дело в том, что в рамках обеспечения информационной безопасности, как правило, оценивается только часть потерь, а именно ожидаемые потери, тогда как предметом риск-менеджмента являются как ожидаемые, так и неожидаемые потери, которые банк будет вынужден покрывать собственными средствами. В настоящей статье мы посмотрим на основные аспекты анализа, оценки и снижения информационных рисков в коммерческом банке глазами риск-менеджера.

## Информационные риски и сложности их оценки

Определим сначала, какой областью рассмотрения мы ограничимся. Можно привести как минимум три определения информационных рисков, использование каждого из которых будет оправдано решаемыми задачами. Самое узкое определение информационных рисков — это риски утраты, несанкционированного изменения информации из-за сбоев в функционировании информационных систем или их выхода из строя, приводящие к потерям. В данном случае информационный риск соответствует категории I уровня операционных рисков (ОР) в классификации Базельского комитета «Остановка бизнеса и сбои в системах». Наиболее широкое определение включает риск возникновения убытков из-за неправильной организации или умышленного нарушения информационных потоков и систем организации. Такое расширенное понимание информационного риска совершенно оправданно, если задаться целью оценить риски в широком контексте информационной безопасности банка, включая организацию работ службы безопасности, PR-центра, информационных технологий и др. Однако при этом в круг рассмотрения попадают довольно разнородные риски, подходы при оценке и управлении которыми должны быть разными. Мы же в данной статье будем рассматривать информационные риски как риски возникновения потерь в результате воздействия людей и внешних событий на информационные системы, а также из-за сбоев и неадекватной работы информационных систем. Таким образом, информационные риски — мы их будем для краткости также называть IT-рисками — связаны с применением банками информационных систем и технологий. Применение информационных технологий является одним из важных факторов, определяющих конкурентоспособность банка. Однако наряду с очевидными преимуществами, такими как повышение скорости и качества обслуживания клиентов, доступности банковских услуг, снижение издержек, использование информационных технологий привносит новые существенные риски. Именно они приобретают всё большее значение по мере развития конкуренции в банковской сфере и расширении географического присутствия банков.

Однако количественная оценка IT-рисков затруднена и зачастую оказывается неточной и ненадёжной по нескольким причинам, часть из которых относится ко всем операционным рискам, а часть специфична именно для этого типа рисков. Во-первых, данные, необходимые как входные параметры практически для всех типов количественных оценок IT-рисков, зачастую очень сложно собрать. Сбор таких данных требует исчерпывающего понимания всех угроз и их воздействия на очень многие «активы» банка, начиная от IT-активов и заканчивая репутацией банка. При этом требуется точность регистрации, её непрерывность и достаточно длинный период, чтобы данные были пригодны для построения модели, имеющей предсказательную силу. Во-вторых, информационная среда современного банка насчитывает сотни объектов риска — IT-активов, которые к тому же претерпевают постоянные изменения, так как банки стремятся модифицировать IT-среду, совершенно справедливо рассматривая операционное совершенство как одно из важнейших конкурентных преимуществ. Таким образом, необходимо построить максимально гибкую модель IT-среды банка, которую можно было бы настраивать по мере изменения входящих в неё систем. И в-третьих, затраты времени и людских ресурсов на анализ уязвимости к рискам и собственно риск-анализ могут быть довольно высоки, что не позволяет проводить его с необходимой периодичностью. И если за-

падные банки обладают уже достаточно полными базами данных по IT-рискам, то для большинства российских кредитных учреждений процесс грамотного систематизированного сбора данных, их отслеживания и проверки, периодический анализ и налаживание отчётности — пока нерешённая задача. Для того чтобы реализовать этот процесс, необходимо сначала провести идентификацию IT-рисков.

## Идентификация IT-рисков

### Рамки рассмотрения и уровень детализации

Первым этапом в идентификации IT-рисков является выбор анализируемых объектов и уровня детализации, на котором они будут рассматриваться. Небольшая кредитная организация может рассматривать всю информационную инфраструктуру, но для большого банка такая единовременная и детализированная оценка может потребовать неприемлемых затрат времени и человеческих ресурсов. Необходимо в таком случае установить приоритеты и рассмотреть в первую очередь совокупность наиболее важных информационных активов, отдавая себе отчёт в том, что оценка будет ограниченной. Как указано во введённой Банком России в конце января 2006 года второй версии стандарта информационной безопасности[1] (далее — Стандарт ИБ), «собственник должен знать, что он должен защищать. Собственник должен знать и уметь выделять (идентифицировать) наиболее важный для его бизнеса информационный актив (ресурс)». При этом целесообразно создать карту информационной инфраструктуры банка, с тем чтобы видеть, какие объекты IT-инфраструктуры выбраны для анализа рисков, а какие остались за его рамками. Карту следует поддерживать в актуальном состоянии, чтобы при изменении IT-инфраструктуры или более глубоком анализе рисков легко можно было оценить, какие объекты нуждаются в рассмотрении. Карта информационной инфраструктуры создаётся в рамках инвентаризации IT-активов банка.

### Инвентаризация IT-активов

Поясним вначале, что мы будем понимать под IT-активами банка. Это, во-первых, информационные активы, т. е. нематериальные активы, к которым относятся различные виды банковской информации (платёжная, аналитическая и пр.), и программное обеспечение, рассматриваемое вне его носителя (аппаратных средств), и, во-вторых, технологические активы, т. е. материальные активы, включающие аппаратные средства ЭВМ, локальных вычислительных сетей и пр. При идентификации IT-активов, т. е. тех ценностей, которые банк хочет защитить, следует учитывать и поддерживающую инфраструктуру, и персонал, и такие нематериальные ценности, как репутация банка. Вершиной пирамиды, которая определяет нижележащие слои, является представление о миссии банка, т. е. об основных направлениях деятельности и способах их реализации (рис. 1) посредством определённых бизнес-процессов. Выбранные банком технологии и технологические активы — это уже зона прямого воздействия факторов IT-рисков. Программное обеспечение, носителем которого являются технологические активы, служит для работы с информацией — платёжной, финансово-аналитической, клиентской, управляющей и т. д., которая является своеобразной основой банковской деятельности. Ведь не зря современные банкиры шутят, что по роду своей деятельности имеют дело не с деньгами, а с информацией о них.

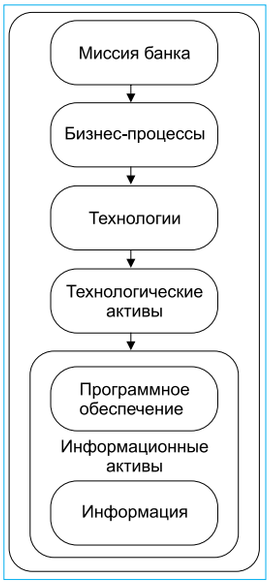


**Рис. 1**

Анализ IT-инфраструктуры предназначен для формирования и документирования целостной картины технологических и информационных активов банка, т. е. состава и структуры аппаратных и программных средств, взаимосвязей между ними, их физического местоположения, включая носители информации, а также потоков данных.

Банк России в Стандарте ИБ выделяет следующие уровни информационной инфраструктуры:

1) физические (линии связи, аппаратные средства и пр.);

2) сетевые (сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);

3) сетевые приложения и сервисы;

4) операционные системы (ОС);

5) системы управления базами данных (СУБД);

6) банковские технологические процессы и приложения;

7) бизнес-процессы организации.

На наш взгляд, на верхнем уровне классификации оптимально с точки зрения анализа выделить следующие группы:

- аппаратные средства, включающие оборудование (собственное и предоставленное поставщиками услуг, партнёрами банка), локальную вычислительную сеть (проводные и беспроводные участки), носители электронной информации;
- программное обеспечение (приобретённое, используемое по лицензии и разработанное банком);
- данные и информацию в электронной форме.

При этом особое внимание следует уделить программным интерфейсам, т. е. приложениям, которые обеспечивают взаимодействие внешних пользователей и персонала со средствами и системами автоматизации. Национальный институт стандартов и техно-

[1] «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0–2006) // Вестник Банка России, 2006. № 6 (876).

логий США[2] рекомендует выделять интерфейсы взаимодействия в отдельную группу объектов риска ввиду их высокой значимости и потенциальной подверженности угрозам, поскольку именно через них осуществляется взаимодействие человека и информационных систем. Стандарт ИБ также подчёркивает, что «все точки в банковских технологических процессах, где осуществляется взаимодействие персонала со средствами и системами автоматизации, должны тщательно контролироваться», рассматривая именно персонал как основную категорию источников операционного риска (не имея сравнительной статистики по категориям «внешнее и внутреннее мошенничество», мы не можем прокомментировать обоснованность невключения интерфейсов с внешними пользователями).

IT-риски банка являются частью операционных рисков, поэтому их следует рассматривать в рамках единой с ОР методологии. Если банком за единицу портфеля ОР выбран бизнес-процесс, то все IT-активы должны описываться с привязкой к бизнес-процессам, чтобы иметь возможность получения консолидированной оценки ОР каждого бизнес-процесса. Тот же подход должен применяться и в случае других способов структурирования портфеля ОР. С точки зрения оценки рисков важен анализ не только повреждения IT-актива, например сбоя программного обеспечения, но и его влияния на выход бизнес-процесса, т. е. на поставки внешним и внутренним пользователям «продуктов» бизнес-процесса.

Каждый из элементов IT-активов должен описываться группой параметров, из которых можно выделить параметры, общие для всех описываемых элементов IT, и специфичные параметры. К общим параметрам относятся:

- основное назначение элемента (компьютера, программы и т. д.), т. е. что именно элемент производит в бизнес-процессе;
- состав лиц, поддерживающих его функционирование;
- состав лиц, использующих данный элемент;
- уровень значимости элемента для обеспечения бизнес-процесса и в конечном счёте миссии банка;
- чувствительность элемента, под которой понимается необходимый уровень защиты IT актива (высокой чувствительностью обладают, например, данные, связанные с конкурентными стратегиями и преимуществами банка, клиентская информация).

Определение значимости и чувствительности IT-активов на данном этапе позволяет оценить рамки рассмотрения и уровень детализации информационной инфраструктуры с целью оценки рисков. Если ресурсов недостаточно, в первую очередь необходимо защитить наиболее приоритетные активы. Приоритетность определяется значимостью IT-активов для достижения целей банка.

Опишем некоторые специфические параметры. Для инвентаризации программных средств (ПО) — это информация по управлению версиями и обновлениями, встроенные в ПО средства обеспечения информационной безопасности, такие как средства шифрования, пароли, средства сетевой защиты. Инвентаризация локальной сети банка основывается на построении топологии (диаграммы) сети с указанием внешних каналов связи (например, с интернет), аппаратных компонентов сетевой инфраструктуры, уровня защищённости отдельных внешних и внутренних каналов (шифрование и др.), установленных средств контроля сетевой безопасности (сетевые экраны, системы обнаружения проникновения и т. п.). Описание информации и её носителей должно проводиться взаимосвязано, чтобы установить, какая информация сохраняется на каких носителях, какие средства резервного копирования применяются (с указанием частоты резервирования и местонахождения резервных копий).

Результатом инвентаризации должна стать карта информационной инфраструктуры с документированными потоками электронных данных внутри банка, а также входящих и исходящих потоков. Эффективным инструментом документирования потоков данных являются, например, диаграммы потоков данных (Data Flow Diagrams, DFD).

Планирование, проведение и документирование результатов инвентаризации IT-инфраструктуры банка, а также поддержание актуальности собранной информации входит в обязанности специалистов отдела информационных технологий. Роль риск-менеджеров заключается в формировании единиц портфеля ОР и выработке совместно с бизнес-подразделениями банка шкалы для оценки значимости и чувствительности элементов IT-активов. Значимость и чувствительность каждого должны оцениваться по заранее подготовленной формализованной шкале, чтобы каждая из категорий одинаково понималась всеми опрашиваемыми экспертами и обеспечивалась перекрёстная сравнимость полученных оценок. Например, методика CRAMM[3], которую приводит Банк России в качестве хорошей практики в Стандарте ИБ, оперирует десятибалльной шкалой, при этом при низкой оценке (3 балла и ниже) по нескольким используемым критериям рекомендуется базовый уровень защиты системы/информации, который не предполагает подробной оценки рисков.

Для инвентаризации IT-активов могут быть использованы следующие инструменты:

- специально сконструированные для каждого подразделения опросные листы;
- специально подготовленные для каждого подразделения интервью;
- анализ документации;
- автоматизированные сканирующие системы для оценки ОР, если они имеются у банка.

Поскольку инвентаризация является процессом, в котором в той или иной мере задействованы практически все подразделения банка, ключевым фактором успеха для её результативного проведения является

[2] NIST Special Publication 800–30. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology, July 2002.

[3] CRAMM UK Government's Risk Analysis and Management Method.

*Таблица 1*

| № | Категория событий возникновения ОР | Примеры действия ОР |
|---|---|---|
| 1 | Внутреннее мошенничество | Несанкционированное использование информационных систем<br>Преднамеренное искажение (сокрытие/раскрытие) важной информации, повлёкшее денежные потери (убытки) |
| 2 | Внешнее мошенничество | Незаконное проникновение в информационные системы, в том числе посредством сети интернет (хакерские атаки)<br>Причинение ущерба информационным системам<br>Кража информации, повлёкшая денежные потери |
| 4 | Клиенты, продукты и ведение бизнеса | Связанное с недостаточностью систем неправомерное раскрытие конфиденциальной информации и нарушение банковской тайны |
| 5 | Ущерб материальным активам | Ущерб материальным ценностям (в данном случае информационным системам) в результате воздействия внешних «натуральных» событий<br>Ущерб информационным системам от актов терроризма, вандализма |
| 6 | Остановка бизнеса и сбои в системах | Выход из строя информационных банковской системы, отдельных модулей и элементов её функционала<br>Отказы и сбои в работе автоматизированных систем<br>Сбои в работе каналов связи<br>Поломка оборудования (компьютеры, терминалы самообслуживания клиентов, другое оборудование) |
| 7 | Проблемы с управлением и исполнением операций | Отсутствие (несовершенство) системы защиты или порядка контроля доступа к информации<br>Неправильная организация информационных потоков внутри банка<br>Невыполнение обязательств перед банком поставщиками, провайдерами<br>Ошибки при вводе и обработке данных по операциям и сделкам<br>Ошибки (моделей и) систем |

поддержка высшего руководства банка. Высшее руководство должно обеспечить ресурсы (людские, временные, денежные) и понимание важности процесса инвентаризации как отправной точки для развития системы управления IT-рисками и, более широко, для повышения эффективности и надёжности работы банка. В ходе функционирования системы менеджмента IT-рисков высшее руководство должно контролировать качество проведения инвентаризации, периодически проверяя, что она носит систематический характер, а её результаты документируются в стандартизованной форме. Частота актуализации информации об IT-среде должна быть зафиксирована во внутренних документах банка, учитывая необходимость её обновления при существенных изменениях информационной инфраструктуры или возникновении новых типов угроз информационной безопасности.

## Выявление угроз

Для оценки операционных рисков необходимо выявить угрозы IT-активам банка, т. е. факторы риска. Однако это будет иметь мало смысла без классификации этих факторов, поскольку для оценки риска нужно систематически собирать статистику, строить качественную или количественную модель. Сложность классификации[4] операционных рисков в полной мере присуща и IT-рискам, к тому же здесь возникает и проблема согласования взглядов сотрудников информационных подразделений, которые занимаются вопросами информационной безопасности банка, и риск-менеджеров, которым необходимо оценивать капитал под операционный риск, проводить самооценку (self-assessment), мониторинг ключевых показателей операционного риска в рамках банка. Классификация IT-рисков должна быть единой, полной и непротиворечивой, и задача её создания с точки зрения методологии ложится на риск-менеджеров. Конечно, каждый банк может ввести свою классификацию IT-рисков, поскольку регулятор не вводит единой системы, однако лучше основываться на классификации Базельского комитета, которая является результатом многолетнего анализа источников и типов потерь западных кредитных организаций. Согласно базельской классификации[5] категорий событий и примеров действий, которые могут приводить к реализации операционных рисков, к IT-рискам можно отнести указанные в табл. 1.

Основываясь на классификации факторов риска, необходимо далее для каждого из принятых в рассмотрение элементов IT-активов выявить потенциальные рисковые события, которые могут на нём реализоваться. Хорошей практикой является разработка моделей угроз и нарушителей информационной безопасности для банка. Стандарт ИБ — Банк России рекомендует каждой кредитной организации разработать модель угроз информационной безопасности, которая включала бы «описание источников угроз, уязвимостей, используемых угрозами, методов и объектов нападений, пригодных для реализации угрозы, типов возможной потери (например, конфиденциальности, целостности, доступности активов), масштабов потенциального ущерба». По сути, разработать на основе сценарного анализа полноценную модель риска. При этом особо подчёркивается, что такая модель должна обладать прогностической силой. Подход «угроза — уязвимость» (модель угроз и нарушителей в терминологии Банка России), являющийся на Западе стандартом при оценке IT-рисков, предполагает сопоставление каждому элементу IT-активов определённых источников угроз (факторов риска), которые могут на-

[4] Штатов Д., Зинкевич В. О разработке положения по управлению операционными рисками коммерческого банка // Бухгалтерия и банки, 2006, № 10.

[5] International Convergence of Capital Measurement and Capital Standards A Revised Framework, Basel, Switzerland, November 2005.

нести ущерб организации посредством использования существующих в этом элементе уязвимостей. Источник угрозы (фактор риска) определяется как намерение и способ умышленного воздействия на уязвимости либо ситуация и способ, который может непредумышленно привести в уязвимость действие, т. е. это совокупность мотивов и условий, которые могут стать причиной нарушения целостности, доступности, конфиденциальности информации. Целостность, доступность и конфиденциальность информации являются выражением стоимости информационного актива, рассматриваемого как объект риска. Поясним эти понятия, отражающие свойства информации, важные для осуществления миссии банка.

Целостность отражает необходимость защиты информации от несанкционированного изменения и утраты. Целостность нарушается при неразрешённых действиях с данными или системами независимо от того, были ли они умышленными или случайными. Часто именно нарушение целостности являются первым шагом в атаке на системы. Если целостность вовремя не восстановлена, это может приводить к ошибкам в расчётах, реализации мошеннических действий, принятию неверных решений менеджментом банка.

*Доступность* — это обеспечение получения требуемой информационной услуги (информации) в нужное время. Информационные системы внедряются для предоставления определённых информационных услуг внутренним пользователям (сотрудникам банка) и внешним пользователям (клиентам, партнёрам банка). Если предоставить эти услуги в приемлемый срок невозможно, это влечёт за собой потери, начиная от снижения операционной эффективности банка и вплоть до оттока клиентов, связанного с риском потери деловой репутации.

*Конфиденциальность* — это обеспечение защиты от несанкционированного доступа к информации, её несанкционированного использования, воспроизводства и распространения. Конфиденциальность имеет большое значение именно для банков, поскольку её нарушение может привести к раскрытию банковской тайны, реализации риска потери деловой репутации, нанося репутации банка значительный ущерб.

*Источники угроз,* которые могут привести к нарушению целостности, доступности и конфиденциальности информации, должны быть выявлены и описаны с уровнем детализации, определяемым реальными потребностями в защите, т. е. в зависимости от соотношения между стоимостью защиты и стоимостью риска. Поэтому процесс идентификации риска является циклическим. Первоначально составляется грубая схема цепочек «угроза → ...→ величина риска» без детализированного описания моделей угроз, проводится сравнительная стоимостная оценка экспертным способом с привлечением данных по потерям банка, если они есть, и других кредитных учреждений, например, с помощью карт рисков или скоринговых карт[6].

[6] Зинкевич В., Штатов Д. Методы измерения операционного риска // Бухгалтерия и банки, 2006. № 12.

*Таблица 2*

| Уровень I | Уровень II | Уровень III |
|---|---|---|
| Компьютерный преступник | Проникновение в компьютерную сеть банка | Несанкционированный доступ к конфиденциальной информации |

На основе этой оценки выделяются наиболее значимые факторы риска и для них уже строятся детальные модели нарушителей.

Наиболее разнообразными являются угрозы, исходящие от человека, что определяет необходимость высокой детализации в их описании. При описании этого типа факторов риска рекомендуется выделять несколько уровней (категорий риска), упрощённый пример такого выделения на трёх уровнях приведён в табл. 2.

Факторы риска, связанные с действиями внешних (хакеры, спамеры, промышленные шпионы и пр.) и внутренних нарушителей (персонал), желательно описывать наиболее детально, включая возможную мотивацию, стереотипы поведения и типичные действия нарушителей в связке с уязвимостями в IT-инфраструктуре.

## Выявление уязвимостей

Термин «уязвимость» характеризует отсутствие или слабость (недостаток) предохранительных мер, позволяющих снизить риск. К ним могут относиться процедуры обеспечения безопасности IT-систем, проектирование систем и их разработка и внедрение или процедуры внутреннего контроля. Уязвимость — это состояние, которое позволяет угрозе осуществиться (случайно или преднамеренно), результатом чего будет большая частность потерь и (или) более тяжёлые последствия от реализации риска — величина потерь. Например, отсутствие антивирусной защиты увеличивает как частоту рисковых событий (большее количество заражений), так и тяжесть потерь, так как заражение будет выявлено с существенным запаздыванием и распространение вируса может привести к необходимости восстановления информации, переустановки операционной системы или отдельных приложений и т. д.

Рассмотрим схему формирования моделей «угроза → ...→ величина риска» на примере влияния факторов риска на частотность потерь (рис. 2). Риск — функция частотности потерь и величины потерь, что отражено стрелками, идущими от двух соответствую-


**Рис. 2**

щих сущностей к сущности «риск». На частотность потерь будет влиять частота воздействия угроз, например, вирусных атак и уязвимость IT-среды банка, которая зависит от уровня контроля (области контролируемого банком риска, см. рис. 1 статьи[4]) и мощности угрозы, которая не зависит от банка (банк не может её контролировать).

Мощность угрозы (фактора риска) определяется в рамках построения модели нарушителя. Поясним это на примере хакерских атак. Сообщество хакеров является неоднородным по своему составу и может быть разделено на кластеры, которые обладают сходными характеристиками. Кластер «профессиональные хакеры» характеризуется высокой мощностью, так как они имеют большой опыт, обладают, как правило, высокими или выдающимися способностями в своей сфере, используют продвинутые разработки для совершения действий, постоянно изучают слабости (уязвимости) своих потенциальных «клиентов». Кластер «непрофессиональные начинающие хакеры» характеризуется тем, что они имеют небольшой опыт, обладают способностями от средних до выдающихся, редко используют продвинутые разработки, пока не знают своих «клиентов», и обладает самой низкой мощностью. Кластер «непрофессиональные продвинутые хакеры» занимает промежуточное положение. Соответственно по-разному они будут влиять и на частоту воздействия угроз, которая зависит от частоты контактов и частоты действий нарушителей. Понятие «действие» характеризует вероятность того, что если контакт произошёл, то нарушитель будет действовать против IT-актива. Это понятие применимо при анализе «интеллектуальных» угроз — людей и созданных ими подручных средств, например специальных программ. Действие, в свою очередь, будет зависеть от мотивации нарушителя, вероятности отрицательных последствий для него и стоимости IT-актива для нарушителя (говоря о нарушителе в единственном числе, мы везде понимаем выделенный кластер с определёнными вероятностными характеристиками).

Для целей сбора информации об уязвимостях и их анализа уязвимости можно разбить на две большие группы:

- уязвимости, специфичные для программных и аппаратных средств, примером которых могут быть слабости конкретных версий программного обеспечения или моделей оборудования, допущенные в них производителем;
- специфичные для процессной и контрольной среды банка уязвимости, которые являются следствием слабостей практик, используемых банком для организации и управления IT-инфраструктурой и для контроля IT-безопасности.

Сбор информации об уязвимостях первого типа, как правило, не представляет особых сложностей, поскольку соответствующая информация обычно размещается в свободном доступе на сайтах производителей; по условиям сервисных соглашений производятся уведомления об обнаружении дефектов и обновление версий, установка «заплат». Источником информации об уязвимостях также могут служить сайты компаний, специализирующихся на обеспечении информационной безопасности (например, производителей антивирусного ПО), и специализированные порталы, объединяющие пользователей соответствующего оборудования и программ. Выявление уязвимостей первого типа — прерогатива информационно-технологических служб банка.

При выявлении уязвимостей второго рода набор внешних источников информации, как правило, чрезвычайно ограничен. Хорошей практикой является составление таблиц пар «источник угроз — уязвимость» и использование этой информации, в совокупности с результатами работ по аудиту безопасности систем, для составления списка требований к обеспечению безопасности. Отсутствие элемента контроля, соответствующего определённой угрозе, должно считаться уязвимостью, даже если вероятность реализации угрозы достаточно мала, поскольку ущерб (величина потерь) от данной угрозы может быть весьма существенным. Дальнейший вопрос о применении тех или иных способов снижения уязвимости — процедур контроля (минимизации риска) должен решаться в рамках стоимостного анализа.

Анализ уязвимости IT-инфраструктуры банка желательно проводить регулярно, но не реже одного раза в год. Эта процедура осуществляется в рамках самооценки (self assessment) среды контроля рисков банка, которая была описана ранее. При составлении опросников — проверочных листов для самооценки можно руководствоваться положениями стандарта COBIT[7], определяющего модель зрелости процессов информационной безопасности. Чтобы процедуры самооценки были более эффективными, рекомендуется выделить не менее трёх областей анализа (групп факторов, влияющих на контрольную среду) — менеджмент, операционную среду и технологии безопасности. Менеджмент информационной безопасности касается таких вопросов управления, как обязанности и разграничение прав, разделение полномочий и ролей, обеспечение непрерывности поддержки, наличие процедур измерения рисков и независимого контроля системы менеджмента рисков, обеспечение непрерывности деятельности, регулярное обучение персонала и т. п. Среда доступа к данным и их расположение, доступ к аппаратным средствам (сервера, центр данных и пр.), контроль внешней среды (пожароопасность, контроль влажности и температуры), обеспечение бесперебойности электропитания и пр. — это вопросы раздела «операционная среда безопасности». К группе «технологии безопасности» можно отнести вопросы о наличии средств криптографической защиты, антивирусной защиты, контроля доступа, процедуры идентификации и установления подлинности, наличие средств обнаружения вторжения в сеть банка и пр.

*Окончание следует*

[7] Control Objectives for Information and Related Technology, 3rd Edition, July 2000.

**В. ЗИНКЕВИЧ**, руководитель отдела консалтинга компании «Франклин & Грант. Финансы и аналитика»
**Д. ШТАТОВ**, консультант компании «Франклин & Грант. Финансы и аналитика»

# Информационные риски: анализ и количественная оценка[1]

## Оценка стоимости IT-активов и величины потерь

Для количественной оценки рисков необходимо оценивать частотность потерь и стоимость потерь (распределение величины потерь), зависящую от стоимости информационных активов банка. Но сама стоимость информационных активов банка не ограничивается стоимостью замены данных, аппаратных средств или программного обеспечения. Если для кредитного риска величина активов, находящихся под риском (Credit Exposure), очевидна, то в случае операционных рисков, включая IT-риски, её довольно сложно определить. Помимо этого можно привести ещё несколько существенных причин, затрудняющих оценку возможных потерь:

- IT-активы имеют, как правило, не одну и не две ценностные характеристики, как, например, в случае рыночного риска;
- потери могут принимать разные виды;
- реализация одного рискового события может приводить к потерям многих видов;
- между возникновением потерь различных видов существуют сложные системные взаимосвязи;
- множество факторов влияет на величину потерь.

При оценке величины потерь необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и величину ущерба, нанесённого бизнес-процессам банка, посредством которых он осуществляет свою миссию. Ещё более отдалённые от факторов риска по причинно-следственной цепочке, но и более сильные по воздействию последствия — потеря деловой репутации, ослабление конкурентной позиции.

Для первичной оценки можно ограничиться, как мы уже упоминали, построением карты рисков или скоринговой оценкой, которые строятся на основе экспертных шкал.

Для стоимости информационных активов это может быть, например, шкала типа:

- низкая стоимость — от актива не зависят критически важные процессы, он может быть восстановлен с небольшими затратами денег и времени;
- средняя стоимость — от актива зависит ряд важных функций процессов, актив может быть восстановлен за допустимое время, стоимость восстановления средняя;
- высокая стоимость — от актива зависят критически важные процессы, время восстановления превышает критически допустимое и (или) стоимость восстановления очень высока.

Оценив возможную частотность потерь и уязвимости, можно далее построить скоринговую матрицу, которая позволит принимать решения в отношении выбора средств для контроля за той или иной категорией IT-рисков. Достоинство методологии в том, что она позволяет довольно быстро и с точностью, зависящей от квалификации экспертов, расположить риски по приоритетам (отранжировать) и выявить те области, где незамедлительно требуется принять решение по контролю над рисками собственными силами или передать его. Однако если банк ставит целью оценку экономического капитала под информационные риски, то этого будет недостаточно, так как карты риска и скоринговая оценка не позволяют рассчитать его величину.

Используемые в документах по информационной безопасности методы оценки тоже не помогут, поскольку они оперируют только ожидаемыми потерями. Классический количественный алгоритм для оценки риска информационных потерь был разработан[2] ещё в 1974 году и используется по сей день. Согласно ему:

$$Asset\ \ Value \times Exposure\ \ Factor \times$$
$$\times Annualized\ \ Rate\ \ of\ \ Occurrence =$$
$$= Annualized\ \ Loss\ \ Expectancy.$$

И если в подходе внутренней оценки (Internal Measurement Approach — IMA) Базель II, где первоначально также оценивается величина ожидаемых потерь для каждой пары «бизнес-линия — категория потерь», вводится множитель, позволяющий перевести ожидаемые потери в неожидаемые, то для информационных рисков, которые являются «смесью» многих категорий, его ввести на основе отраслевой статистики затруднительно ввиду существенного различия как в типах IT-активов, так и в бизнес-процессах. Поэтому, на наш взгляд, если банк настроен на последовательное внедрение количественной оценки величины операционного риска на основе продвинутых подходов, следует выбирать способы моделирования, которые позволяют учесть как исторические данные о потерях, так и экспертные знания.

## Количественная оценка IT-рисков

В предыдущей статье мы рассмотрели основные подходы и модели для оценки операционных рисков. Ка-

[1] Окончание. Начало см. в «Б&Б» № 1 за 2007 г.

[2] Guidelines for Automated Data Processing Physical Security and Risk Management, NIST FIPSPUB-65, 1974.

кие же основные свойства сферы IT определяют способы и модели, применимые для количественной оценки IT-рисков?

Во-первых, это высокая динамичность. Технологии постоянно обновляются и становятся всё более продвинутыми и сложными, автоматизируются бизнес-процессы и отдельные их участки, изменяются потоки данных, внедряются и обновляются информационные системы, модернизируется оборудование — в течение одного–двух лет информационно-технологическая среда банка существенно изменяется. Новые информационные технологии несут новый риск. С точки зрения оценки рисков это налагает ограничения на использование методов, основанных только на статистике прошлых убытков банка, поскольку соответствующая информация в базе данных операционных потерь быстро устаревает и остающейся актуальной статистической информации оказывается недостаточно для использования статистических методов. Даже если банк выполняет требования Базеля, согласно которым статистические подходы к оценке ОР должны быть основаны как минимум на 3–5 летней истории операционных потерь, эта база лишь отчасти поможет построить адекватную статистическую модель IT-рисков.

Во-вторых, это высокая комплексность взаимосвязей в IT-среде. Большинство технологических компонентов банка связано между собой компьютерными сетями, бизнес-процессы используют в качестве ресурсов многие IT-активы, потоки данных разных систем и разных бизнес-процессов интегрируются в аналитических и отчётных модулях. При оценке IT-рисков это выводит на первый план методы и модели, позволяющие отразить причинно-следственные связи, поскольку в полностью автоматизированной среде реализация одного фактора риска может приводить к «эффекту домино».

В свете этих особенностей идеальным для оценки IT-рисков был бы метод, позволяющий использовать разнородные по своей природе данные (экспертные оценки и численную информацию о понесённых банком убытках), а также подходящий для моделирования причинно-следственных взаимосвязей. Такой метод существует — это построение каузальных моделей оценки ОР, в частности, байесовских сетей. Дополнительной мотивацией для применения банком этого подхода к оценке ОР в IT-сфере может служить также то, что он очень органично позволяет встроить в общую модель IT-риска модели нарушителей, проводить их своевременную модификацию.

Напомним, что байесовская сеть представляет собой графовую модель, в которой рисковые события и причины этих событий (факторы риска) обозначаются в виде окружностей (называемых концептами графа), а причинно-следственные взаимосвязи между ними — в виде направленных стрелок (рёбер графа), соединяющих концепты. В основе методологии байесовских сетей лежит теорема Байеса, ценность которой применительно к оценке ОР заключается в её способности комбинировать данные о вероятности событий, получаемые экспертным и статистическим путём. Для отдельных факторов риска (угроз), для которых нет статистики потерь, оценки вероятности рисковых событий могут быть основаны с использованием теоремы Байеса, только на экспертных знаниях; а для других — на статистике потерь, если объём собранных данных достаточен для целей моделирования.

Построение байесовской сети для оценки IT-рисков разумно ввиду трудоёмкости данного процесса проводить для наиболее значимых факторов риска и наиболее ценных и обладающих высокой чувствительностью IT-активов банка. Источники угроз, уязвимости IT-активов банка и установленные средства контроля, взаимосвязи в IT-среде, возможные рисковые события, выявленные в процессе идентификации рисков, составляют основную часть концептов байесовской сети. Они дополняются моделями нарушителей (см. рис. 2, где, по сути, применён тот же подход, который используется для построения сети). Кроме того, в модель необходимо включить события, которые могут стать последствиями реализации риска в IT-активах банка. При реализации этих событий банк и несёт основные потери, поскольку наибольший ущерб банку наносят не сами сбои IT-систем, а именно связанная с ними остановка или нарушение работы бизнес-процессов, важных для осуществления миссии банка. На этом этапе построения модели риск-менеджерам необходимо привлечь к работе не только IT-специалистов, но и менеджеров подразделений, осуществляющих основные процессы (процессы основной деятельности), вспомогательные процессы (процессы по видам обеспечения), процессы управления банком. На основе данных отчёта по идентификации IT-рисков строится «скелет» сети, небольшой фрагмент которой в упрощённом виде представлен на рис. 3.

После того как «скелет» сети (направленный граф) создан, проводится оценка характеристик включённых в неё концептов. Для уровня контроля (пример — периодичность обновления антивирусного ПО), который отражает уязвимость (чем выше уровень контроля, тем ниже уязвимость), допустима балльная оценка. Для рисковых событий (пример — хакерская атака) проводится оценка вероятности их реализации и, по цепочке, связанных с этим операционных потерь. При оценке вероятности реализации событий или состоя-

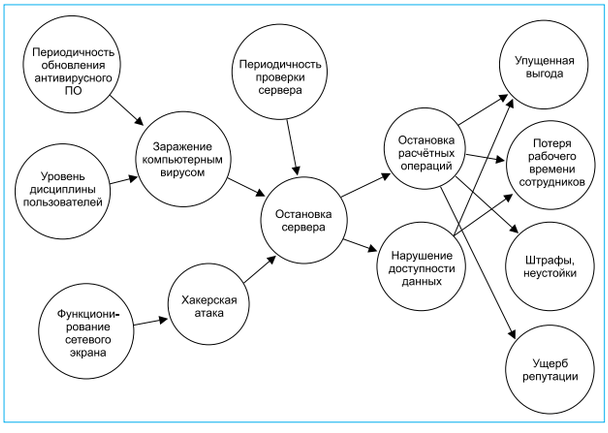


**Рис. 3**

ний факторов риска можно основываться на реальных статистических данных для каких-то типов событий, на полностью экспертных оценках для других и на смешанных оценках для третьих, например, с целью учёта поправок на будущие тенденции. Вероятность реализации событий может быть указана в байесовской сети в виде непрерывной функции распределения или в виде таблицы вероятностей, т. е. в виде дискретных вероятностей. Поскольку непрерывные функции распределения удаётся получить лишь в редких случаях из-за недостаточности статистики, мы далее будем рассматривать дискретные распределения.

Для концептов, которые на графе не имеют входящих стрелок, например, событий, которые являются драйверами (факторами) риска, должна быть указана абсолютная вероятность каждого из возможных исходов события. Для тех концептов, на которые влияют другие концепты, указывается условная вероятность для каждой комбинации связанных концептов. Пример экспертного задания таблицы условной вероятности показан в табл. 3.

*Таблица 3*

| | Исходы — условия | | | |
|---|---|---|---|---|
| Хакерская атака | Да | | Нет | |
| Заражение вирусом | Да | Нет | Да | Нет |
| Вероятность исхода события «Остановка сервера» для различных условий | | | | |
| Произойдёт | 0,3 | 0,15 | 0,10 | 0,02 |
| Не произойдёт | 0,7 | 0,85 | 0,90 | 0,98 |

Затем с помощью теоремы Байеса составляется композиция указанного экспертами распределения с распределением, построенным на основе фактических данных. Полученное распределение-композиция принимается для дальнейших расчётов по сети как наиболее точно описывающее поведение концепта. Из таблицы условной вероятности (как видно из табл. 3), не вполне очевидно, с какой частотой будет происходить остановка сервера. Чтобы провести количественную оценку, необходимо вычислить абсолютные вероятности реализации этого события. Для этого применяется формула условной вероятности, позволяющая провести расчёт на основе заданных условных вероятностей и известных вероятностей реализации событий (причин) рассматриваемого события. Таким образом, последовательно продвигаясь по сети и применяя теорему Байеса в связке с формулой условной вероятности, можно вычислить вероятность каждого исхода для каждого рискового события. Осталось определить для каждого события ещё одну характеристику — величину возможных потерь от его реализации, которая может определяться на основе статистики, экспертно, по данным других организаций с учётом эффекта масштаба. При оценке этого параметра задача существенно облегчается, если концепты определены верно, т. е. присутствуют все необходимые типы потерь и нет лишних. Классификация типов последствий может быть составлена с различных точек зрения, при построении графа полезно рассматривать два взаимосвязанных уровня классификации. Так, на первом уровне классификации можно разделять последствия с точки зрения изменений в технологических и информационных активах. Для информационных активов традиционно приняты три категории последствий — нарушение целостности, доступности, конфиденциальности, а для материальных активов ущерб определяется по шкале — от полной утраты актива до сбоя (остановки, неполадки) на несущественный промежуток времени. Возможна балльная оценка. В качестве второго уровня классификации возможных потерь могут рассматриваться: упущенная выгода; штрафы, пени, неустойки; потеря рабочего времени сотрудников, снижение производительности труда; потеря репутации и др.

Использование такой двухуровневой классификации позволяет соотнести ущерб в понимании технических специалистов со стоимостной оценкой, необходимой в целях управления рисками. Величина прямых финансовых потерь может быть оценена на основе профессионального опыта экспертов или на основе данных базы операционных убытков, при этом потери также могут оцениваться в вероятностных терминах, т. е. на основе доверительных интервалов или распределений. Стоимость нематериальных потерь, таких как ущерб репутации, оценить сложнее. На Западе они оцениваются по изменениям в рыночной стоимости компании, однако в России такой подход практически неприменим, поскольку абсолютное большинство банков не имеют свободно обращающихся на рынке акций. Выходом из положения может быть экспертный подход, основанный на измеримых характеристиках, таких как отток клиентов, снижение темпов открытия новых счетов, депозитов и т. п. Инструментом таких оценок может выступать модифицированный метод Дельфи, позволяющий вырабатывать обоснованные и согласованные оценки для группы экспертов (более подробное описание этого метода выходит за рамки нашей статьи).

Когда построение баейсовской сети закончено, её можно использовать для оценки риска в различных разрезах. Если требуется оценить совокупный риск какого-либо IT-актива, например информационной системы, то можно произвести суммирование распределений потерь по нескольким рисковым событиям, потенциально способным реализоваться в этой системе. Суммирование распределений потерь по отдельным рисковым событиям, кроме того, необходимо для определения ожидаемых и неожидаемых потерь, получаемых на основе расчёта математического ожидания и VaR — агрегированного распределения IT-риска банка. Такое суммирование по байесовской сети проводится, как правило, с помощью Монте-Карло-симуляции, которая заключается в имитации случайного возникновения различных исходов событий-драйверов, которые подаются на входы сети. Существует и другой аналитический подход к суммированию распределений, однако его применение затруднено из-за высокой трудоёмкости.

В целом, как видно даже из краткого описания методики построения байесовской сети, это достаточно трудоёмкий процесс, поэтому его лучше проводить с помощью специально разработанных программных средств. Их использование, по различным оценкам, позволяет сократить временные затраты на оценку

риска в 5–10 раз. Оценка риска завершается выработкой предложений по техническим, технологическим, организационным средствам контроля риска, направленным на его минимизацию.

## Снижение IT-рисков

Поскольку снижение IT-рисков сопряжено с затратами, при рассмотрении возможных действий по снижению риска необходимо разработать различные варианты средств минимизации для каждой единицы портфеля рисков, оценить потенциальный эффект от их внедрения (например, используя сценарный анализ в построенной байесовской сети) и стоимость этого внедрения, т. е. провести анализ «издержки–выгода» (cost-benefit analysis). Выработать реалистичный и эффективный план снижения IT-рисков можно путём комплексного анализа структуры портфеля IT-рисков банка и сравнения возможных действий, направленных на снижение риска, между собой по ряду значимых характеристик. В этом смысле разработка такого плана является типичным примером многомерной управленческой задачи выбора, которую разумнее всего решать в рамках поэтапного процесса, по своей сути схожего с методологией дерева решений.

Группы возможных методов снижения риска для каждой единицы портфеля IT-рисков стандартные для риск-менеджмента.

- **Принятие риска.** Банк признаёт потенциальные потери приемлемыми для себя и не реализует специальные меры по снижению риска.
- **Избежание риска.** Банк принимает решение, направленное на удаление данной единицы риска из портфеля IT-рисков, в частности, устраняя причину соответствующей угрозы (например, отказывается от использования установленного ПО, существенно нарушающего требования информационной безопасности).
- **Ограничение риска.** Банк внедряет специальные средства контроля, снижающие вероятность реализации угрозы IT-активам и (или) уменьшающие последствия этой реализации.
- **Передача риска.** Банк создаёт условия для компенсации потенциальных потерь путём передачи риска третьему лицу, например, используя страхование или отдавая отдельные функции на аутсорсинг.

Указанные способы не являются взаимоисключающими и часто применяются в комплексе. Основная цель ограничения риска — это его снижение до приемлемого для банка уровня, но поскольку риск при этом не устраняется полностью, то его часть, оставшаяся после ограничения, должна быть принята банком. При выборе мер воздействия на каждую единицу портфеля рисков необходимо разделить все выявленные IT-риски на подконтрольные и неподконтрольные банку. Эта характеристика, по сути, разбивает портфель IT-рисков на два субпортфеля с различным составом возможных методов снижения рисков. Так, банк не может воздействовать на неподконтрольные ему риски (такие, как природные угрозы и некоторые угрозы технологической среды), и, следовательно, он может либо принять их, либо передать путём страхования. Для субпортфеля подконтрольных IT-рисков применимы все из описанных методов воздействия на риск, но для этого субпортфеля. Если мы далее сравним денежную оценку каждого элемента портфеля рисков с порогом принятия риска, определяемым на основе «аппетита на риск», установленного высшим руководством и акционерами банка, то это позволит нам выделить ещё один субпортфель — субпортфель приемлемого риска. Для каждой единицы этого субпортфеля величина потенциальных потерь не превосходит порог принятия риска, поэтому эти риски могут быть полностью приняты банком. Хотя банк может пожелать ещё больше снизить риски из этого субпортфеля, в силу существующих ограничений по ресурсам, до этого доходит чрезвычайно редко, поскольку в первую очередь средства из бюджета разумно направлять на самые значимые для банка риски.

Таким образом, область анализа после первых двух этапов сузилась до одного субпортфеля подконтрольных, но неприемлемых для банка рисков, которые следует минимизировать наиболее подходящими средствами контроля. Необходимым шагом, предшествующим ранжированию средств контроля, является составление списков инструментов контроля (ограничения) риска для каждой единицы субпортфеля. Средства контроля делятся на три категории по применяемым в их рамках методам воздействия на источник риска:

- организационные (управленческие) средства подразумевают создание надёжной и безопасной системы управления IT-рисками (разделение ответственности за обеспечение безопасности IT-активов, управление мероприятиями по оценке и снижению рисков, обеспечение правильной подготовки пользователей IT-систем, создание механизмов реагирования в экстренных ситуациях и т. п.);
- технические средства заключаются в использовании автоматизированных механизмов контроля безопасности IT-активов (например, использование криптографической защиты информации, защищённых каналов связи, программных методов аутентификации и авторизации, антивирусной защиты);
- технологические (операционные) средства помогают обеспечить и контролировать непрерывность функционирования IT-активов банка (например, контроль физического доступа к оборудованию, архивирование и резервное копирование информации, защита от пожаров, обеспечение бесперебойного энергоснабжения и т. п.).

Все эти средства довольно подробно описаны в Стандарте ИБ, причём там указаны и инструменты, наиболее подходящие для различных процессов, поэтому мы не будем останавливаться на их описании. Подчеркнём важную особенность Стандарта ИБ, который делает акцент на корпоративном управлении и корпоративной этике как важном элементе соблюдения политики информационной безопасности. Установленные стандарты корпоративного управления, основанные на лучших практиках, очень существенны в решении проблемы инсайдеров, которые рассматриваются

как основные источники угроз и уязвимостей информационной безопасности. Предотвращение конфликтов интересов, разделение полномочий и ролей, недопущение наделения суперполномочиями, контроль над обращением конфиденциальной информации — все эти организационные средства, значимые для любых видов операционного риска, приобретают исключительное значение для IT-рисков ввиду их взаимосвязи практически со всеми бизнес-процессами банка.

Как правило, ограничение риска для каждой единицы субпортфеля рисков может достигаться применением разных средств, поэтому необходимо проанализировать альтернативные варианты средств контроля, предложенные техническими специалистами, чтобы выбрать наиболее эффективные. Сравнение средств контроля может проводиться по множеству параметров, наиболее значимыми из которых являются стоимость средства контроля и планируемая выгода от его внедрения, определяемая как величина, на которую средство контроля позволит снизить оценку риска в денежном выражении. Существенной особенностью IT-рисков, о которой следует помнить при выработке мер минимизации, является то, что внедрение средств защиты IT-активов, как правило, привносит новые уязвимости и соответственно новые риски. Поэтому, помимо стоимостной оценки первичных рисков и средств контроля, нужно провести анализ вновь возникающих уязвимостей, дать риску стоимостную оценку, а затем в комплексе оценивать, стоит ли применять данный метод минимизации.

Новые риски возникают не только при ограничении IT-риска, но и при передаче его путём аутсорсинга. Возрастающие объёмы функций, которые западные финансовые институты передают в аутсорсинг, заставили Базельский комитет[3] обратить пристальное внимание на эту проблему. Понятно, что передача какой-то функции на аутсорсинг редко служит цели только минимизации IT-риска, но обычно включает и эту цель. Например, у европейских банков на первых двух местах находятся мотивы, связанные со снижением совокупной стоимости владения данной функцией и доступ к новым технологиям. Базельский комитет указывает, что наряду с выгодами, которые приобретаются при передаче функций на аутсорсинг, следует эффективно управлять возникающими при этом рисками. Укажем некоторые из них, связанные с IT-сферой. К группе стратегических рисков, например, относится риск того, что финансовый институт не обладает достаточным опытом и знаниями, чтобы осуществлять адекватный надзор за сервис-провайдером. Возможные технологические сбои, мошенничество и ошибки, отказ от обслуживания, нарушение конфиденциальности — вот не полный список угроз, которые следует, по мнению Базеля, рассматривать в связи с аутсорсингом.

Особенности IT-рисков требуют, чтобы защитные меры осуществлялись непрерывно, регулярно проверялись на адекватность угрозам, связанные с применением мер снижения риски учитывались в профиле риска банка. Актуализация информации о факторах риска, оценка риска и обновление (разработка) комплекса мероприятий по его минимизации должны проводиться с определённой периодичностью, зафиксированной во внутренних документах банка. Мониторинг уровня IT-риска, например, по ключевым показателям риска разумнее поручать специалистом, которые не являются сотрудниками информационно-технологических служб банка, поскольку они смогут обеспечить объективную оценку и анализ. Лучшие практики свидетельствуют, что ключевыми факторами успеха в процессе реализации программы снижения рисков является поддержка высшего руководства банка, наличие документально оформленных процедур всех этапов управления IT-рисками, чёткое распределение ответственности за внедрение каждого средства контроля, тестирование внедряемых и уже внедрённых контрольных инструментов.

## Планирование на случай непредвиденных обстоятельств

Мы обошли в предыдущих разделах вопрос о минимизации последствий реализации риска. Этот вопрос особенно важен в отношении рисков, которые нельзя устранить, ограничить или передать, но они представляют чрезвычайную опасность для банка. Поскольку внедрение большинства средств контроля не позволяет свести риск к абсолютному нулю, а для отдельных единиц портфеля рисков их применение невозможно, определённая часть IT-риска, сохраняющаяся после принятия мер по снижению, принимается банком. Эту часть принято обозначать термином «остаточный риск», который является разностью между всем присущим банку IT-риском и его контролируемой частью. Таким образом, вероятность и величина потерь от реализации факторов остаточного риска не контролируется банком, а значит, банк не защищён от его возможных проявлений. Такого рода чрезвычайные риски выявляются посредством процедур стресс-тестирования, которые основываются, как правило, на экспертных знаниях специалистов банка (либо привлечённых экспертов, консультантов). Некоторые банковские специалисты, занимающиеся вопросами риск-менеджмента, рассматривают анализ чувствительности и стресс-тестирование как аналогичные процедуры. Однако процедура анализа чувствительности не позволяет учесть ни одновременное действие нескольких факторов риска, ни чрезвычайно сильные отклонения, ни взаимоусиление факторов и последствий, а также широкое распространение последствий реализации даже одного фактора. Поскольку очень редкие, но несущие высокие потенциальные потери события даже в рамках отрасли происходят нечасто, провести количественное моделирование из-за недостатка данных затруднительно. Уровень надёжности качественного анализа напрямую будет зависеть от знаний и опыта экспертов.

Устранить или существенно снизить такие чрезвычайные риски нельзя, но можно минимизировать их последствия с тем, чтобы даже в этих чрезвычайных условиях банк продолжить обслуживание клиентов, быстро восстановил нормальный режим работы. Это делается путём разработки плана действий на случай

[3] Outsourcing in Financial Services, Basel, Switzerland, February 2005.

непредвиденных обстоятельств (contingency plan). При этом план действий в области IT должен быть составной частью комплексного общебанковского плана обеспечения непрерывности деятельности, поскольку в стрессовых ситуациях одновременно проявляются многие виды банковских рисков, такие как стратегический риск, риск ликвидности, репутационный риск, прочие категории операционного риска.

План действий на случай непредвиденных обстоятельств в области IT, чтобы быть эффективным, должен как минимум содержать следующие разделы:

- политика банка в области планирования действий в кризисных ситуациях в сфере IT, в которой формализованно выражаются цели и задачи плана и определяется общий порядок функционирования банка в кризисных ситуациях: структура управления и разделения полномочий и ответственности (которая может отличаться от «штатной» управленческой структуры), порядок выделения необходимых финансовых и людских ресурсов и т. д. В этом разделе также определяется порядок перехода банка в кризисный режим работы и обратно, регламентируются общие подходы к соответствующему обучению персонала, тестированию плана и его периодическому обновлению;
- описание состава кризисных ситуаций (сценариев), для борьбы с возможными последствиями которых был разработан план;
- описание принятых в банке превентивных мер, направленных на снижение или минимизацию величины последствий каждого типа кризисных ситуаций (например, резервное копирование данных, средства пожаротушения, обеспечение бесперебойного электропитания и т. п.). Превентивные меры никак не влияют на вероятность реализации негативного события (например, отключения электричества в городской сети), но направлены на подавление причиняемого ими ущерба (источник бесперебойного питания позволяет предотвратить потерю данных);
- состав задач, которые необходимо решить в случае возникновения каждой конкретной кризисной ситуации, если, несмотря на превентивные меры, возникновение этой ситуации нанесло или может нанести значительный ущерб («что нужно сделать»);
- описание процедур и регламентация порядка действий персонала, направленных на решение стоящих в этой кризисной ситуации задач («как нужно действовать»). Действия персонала в кризисной ситуации должны быть расписаны «по ролям», т. е. в соответствии с должностными обязанностями и соответствующими компетенциями каждого сотрудника.

Как свидетельствуют лучшие практики[4], при разработке плана следует особое внимание уделить процедурным вопросам, связанным с распределением ответственности, определением оптимальной последовательности решения задач. Применительно к IT эти задачи, как правило, заключаются в восстановлении нормального функционирования различных информационных систем, оборудования, восстановлении целостности и доступности ключевых данных. Эта специфика IT-рисков существенно облегчает расстановку приоритетов в задачах плана — последовательность выполнения задач определяется сравнительной критичностью элементов IT-инфраструктуры, функционирование которых нарушено. При этом порядок действий персонала разумно разбивать на три этапа:

- этап инициации, выполнение которого начинается сразу после возникновения неблагоприятного события. На этом этапе производится оценка причинённого ущерба, потенциала дальнейшего негативного развития ситуации, и принимается решение о начале выполнения мероприятий, предусмотренных планом;
- восстановительный этап предусматривает выполнение прописанных в плане работ, направленных на восстановление нормальной работы IT-среды банка;
- этап финализации предусматривает выполнение заключительных работ, таких как восстановление всей информации с резервных носителей, тестирование восстановленных систем, информирование служащих о возврате к обычному порядку работы.

Поскольку наступление кризисных ситуаций практически невозможно прогнозировать, план действий в случае непредвиденных обстоятельств должен быть готов к использованию каждый день. Это предусматривает периодический пересмотр и обновление плана (на предмет актуальности информации о структуре IT-среды и организационной структуры банка, полноты состава рассматриваемых рисков и т. д.), а также его тестирование (проведение «учебных тревог»). Важную роль играет обучение персонала — каждый сотрудник должен знать порядок своих действий в кризисной ситуации и местоположение всех необходимых ресурсов.

* * *

В заключение ещё раз хотелось бы подчеркнуть, что управление информационной безопасностью кредитной организации, особенно в части идентификации, оценки и мониторинга IT-риска, следует проводить в рамках управления операционными рисками. Учитывая, что Россия намерена уже в 2009 году присоединиться к соглашению Базель II по капиталу, согласно которому банки должны соблюдать требования к достаточности собственных средств с учётом как кредитных и рыночных рисков, так и операционных рисков, времени осталось не так уж и много. А с точки зрения минимизации IT-риска внедрение Стандарта ИБ, который сейчас имеет рекомендательный характер, позволит улучшить контрольную среду банка, снизив таким образом долю невыявленного риска и остаточного риска. Соответственно снизятся затраты банка на ожидаемые потери, а также требования к капиталу под операционный риск. Что касается достаточности капитала, которая в условиях растущего рынка становится больным вопросом для многих, особенно крупных и средних банков, не позволяя им расти далее с достигнутыми темпами, вопрос заключается ещё и в том, разрешит ли российский регулятор рассчитывать требования к регуляторному капиталу на основе продвинутых подходов или остановится на уровне стандартизованного подхода. ■

[4] High-level Principles for Business Continuity, Basel, Switzerland, August 2006.