

АНАЛИЗ И КАЧЕСТВЕННАЯ ОЦЕНКА ОПЕРАЦИОННЫХ РИСКОВ КРЕДИТНЫХ ОРГАНИЗАЦИЙ: РИСКИ ИНФОРМАЦИОННЫХ СИСТЕМ

В настоящей статье понятие информационной безопасности кредитной организации рассматривается как неотъемлемая часть системы управления операционным риском. Под информационными рисками (IT-риски) понимаются риски возникновения потерь в результате воздействия людей и внешних событий на информационные системы, а также риски сбоев и неадекватной работы информационных систем. Рассмотрены основные аспекты анализа, оценки и снижения IT-рисков, методы идентификации, качественной оценки и классификации IT-рисков в терминах Базель II. Предложены методы построения карты информационной инфраструктуры потоков данных внутри кредитной организации, и продемонстрированы на пример построения информационных потоков в инвестиционном бизнес-процессе.

Введение

Одним из основных видов рисков кредитных организаций является операционный риск (далее - ОР), обусловленный неопределенностью состояния и функционирования их внутренней и внешней среды. Потери от наступления событий ОР могут быть приводить к существенным прямым и косвенным убыткам, разорениям компаний и даже гибели людей.

Громкие банкротства последних лет (1991г. Bank of Credit and Commerce International (BCCI) – потери более 10 млрд. долларов США, 1993г. Metallgesellschaft Refining and Marketing – потери более 1.4 млрд. долларов США, 1995г. Barrings Bank - потери более 1.3 млрд. долларов США; 1996г. Daiwa Bank – потери более 1.1 млрд. долларов США и др.), причиной которых стали ошибки организации системы управления ОР, свидетельствуют о масштабности и недостаточной проработанности вопросов оценки, предупреждения и минимизации потерь от наступления событий, относящихся к ОР.

В 2006г. международным комитетом по надзору за банковскими органами было опубликовано «Новое соглашение об оценке достаточного капитала» (известное как Базель II), содержащее описание базовых принципов и требований к построению системы управления ОР в кредитных организациях. Предложенная система подходов позволяет кредитным организациям постепенно переходить от более простых методов к более сложным и чувствительным по мере того, как улучшается их система управления рисками и растут ресурсы. В настоящей работе подробно будет рассмотрен один из методов,

¹ Автор выражает признательность профессору, к.т.н. Мастяевой И.Н. за помощь в подготовке статьи.

предлагаемых Базель II, а именно «сценарный анализ» для качественной оценки рисков информационных систем.

Оценка операционного риска

В соответствии с рекомендациями Базель II кредитные организации могут проводить оценку ОР с использованием трех следующих подходов:

- § количественный анализ распределения фактических убытков;
- § балльно-весовой метод;
- § сценарный анализ.

Количественная оценка ОР требует построения экономико-математической модели измерения, прогнозирования и оценки совокупного распределения величины ОР кредитной организации. Важнейшим источником информации, необходимой для реализации данного подхода, являются исторические данные о произошедших (в т.ч. в других организациях) событиях и убытках, связанных с ОР.

Сущность балльно-весового метода заключается в оценке ОР в сопоставлении с мерами по его минимизации. На основе экспертного анализа выбираются информативные для целей управления ОР индикаторы риска и определяется их относительная значимость (весовые коэффициенты). Затем выбранные показатели сводятся в таблицы (оценочные карты) и оцениваются с использованием различных шкал. Полученные результаты обрабатываются с учетом весовых коэффициентов и сопоставляются в разрезе направлений деятельности кредитной организации, отдельных видов банковских операций и других сделок.

В рамках сценарного анализа на основе экспертного анализа для каждого из направлений деятельности кредитной организации, отдельных видов операций и других сделок определяются возможные сценарии возникновения событий или обстоятельств, приводящих к операционным убыткам, и разрабатывается модель распределения частоты возникновения и размеров убытков, которая затем используется для оценки ОР.

Смешанный подход, сценарный анализ

Общая слабость, которой страдают все методы, основанные на информации об уже понесенных операционных потерях, заключается в их неспособности оценивать риск тех потерь, которые еще не происходили. Учет такого рода событий исключительно важен при оценке риска, поскольку они обычно имеют значительную величину и способны привести к приостановке деятельности кредитной организации. Выявлению таких событий служит метод сценарного анализа, который позволяет путем анализа "Что будет, если?.." в связке с данными о случаях реализации катастрофических событий оценить, каким чрезвычайным потерям может подвергаться кредитная организация в будущем.

Первым шагом в реализации сценарного моделирования является выделение множества тех событий, по которым недостаточно данных, и объединение их в сценарные классы в соответствии с классификацией категорий ОР. Под сценарием понимается случай реализации ОР и вся цепочка последствий его реализации, которая отслеживается по всем единицам портфеля ОР. На основании множества сценариев оцениваются параметры распределений тех потерь, собственной накопленной статистики о которых оказывается недостаточно. Кроме того, данный подход применяется для моделирования редких, но существенных событий, составляющих «тяжелые хвосты» распределений операционных потерь. К таким событиям в первую очередь относятся информационные и телекоммуникационные сбои, аварийные отключения питания, сбои в работе программного обеспечения и серверов и т.п. (далее - ИТ-риски). Количественно оценивать последствия реализации таких рисков крайне тяжело и далеко не всегда возможно. Основной проблемой является недостаточное количество статистических данных о реализации событий такого рода. Именно поэтому в рамках продвинутых подходов к оценке ОР (Advanced Measurement Approach –АМА [9]) количественные методы оценки ОР рекомендуется дополнять качественными показателями, такими как ключевые показатели риска (КРИ), процедуры анкетирования подразделений (self-assessment) и сценарное моделирование. Остановимся более подробно на некоторых аспектах построения системы качественной оценки ИТ-рисков кредитных организаций.

Информационные риски

При построении системы качественной оценки ИТ-рисков первым этапом является идентификация ИТ-рисков. На этом этапе осуществляется 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. В таком случае необходимо установить приоритеты и рассматривать в первую очередь совокупность наиболее важных информационных активов. При этом целесообразно создать карту информационной инфраструктуры кредитной организации, определить, какие объекты ИТ-инфраструктуры выбраны для анализа рисков, а какие остались за его рамками. Карту следует поддерживать в актуальном состоянии, чтобы при изменении ИТ-инфраструктуры или более глубоком анализе рисков легко можно было оценить, какие объекты нуждаются в рассмотрении. Карта информационной инфраструктуры создается в рамках инвентаризации ИТ-активов кредитной организации.

Инвентаризация ИТ-активов

Поясним вначале, что мы будем понимать под ИТ-активами кредитной организации. Это, во-первых, информационные активы, т.е. нематериальные активы, к которым относятся различные виды банковской информации (платежная, аналитическая и пр.), программное обеспечение, рассматриваемое вне его носителя (аппаратных средств), технологические активы (в т.ч. материальные активы, аппаратные средства ЭВМ, локальные вычислительные сети и пр.). При идентификации ИТ-активов, следует учитывать поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как, например, репутация. Выбранные технологии и технологические активы - зона прямого воздействия факторов ИТ-рисков.

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



Рис.1

Банк России в Стандарте ИБ [3] 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.

Каждый из элементов ИТ-активов должен описываться группой параметров, из которых можно выделить параметры, общие для всех описываемых элементов ИТ, 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 счете миссии банка;
- чувствительность элемента, под которой понимается необходимый уровень защиты ИТ-актива (высокой чувствительностью обладают, например, данные, связанные с конкурентными стратегиями и преимуществами банка, клиентская информация).

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 сети с указанием внешних каналов связи (например, Интернет), аппаратных компонентов сетевой инфраструктуры, уровня защищенности отдельных внешних и внутренних каналов (шифрование и др.), установленных средств контроля сетевой безопасности (сетевые экраны, системы обнаружения проникновения и т.п.). Описание информации и ее носителей должно проводиться взаимосвязанно, 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 кредитной организации, а также входящих и исходящих потоков. Модельный пример построения информационных потоков в бизнес-процессе Investment Banking рассмотрен ниже (рис. 3).

Планирование, проведение и документирование результатов инвентаризации ИТ-инфраструктуры кредитной организации 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 шкалы для оценки значимости и чувствительности элементов ИТ-активов. Значимость и чувствительность каждого должны оцениваться по заранее подготовленной формализованной шкале, чтобы каждая из категорий одинаково понималась всеми опрашиваемыми экспертами и обеспечивалась перекрестная сравнимость полученных оценок. Например, методика CRAMM, которую приводит Банк России в качестве практики применения Стандарта ИБ [3], 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.

Выявление угроз

На следующем этапе необходимо выявить угрозы ИТ-активам кредитной организации, т.е. факторы риска, способные повлечь операционные убытки. При классификации ИТ-рисков возникает проблема согласования взглядов сотрудников информационных подразделений, которые занимаются вопросами информационной безопасности, и риск-менеджеров, которым необходимо оценивать капитал под ОР и проводить самооценку мониторинг показателей ОР в рамках кредитной организации. Классификация ИТ-рисков должна быть единой, полной и непротиворечивой, и задача ее создания с точки зрения методологии ложится на риск-менеджеров. Конечно, каждый банк может ввести свою классификацию ИТ-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 ОР, ИТ-риски следует классифицировать по следующим категориям:

	Категория РС	Описание
1	Внутреннее мошенничество	<i>несанкционированное использование информационных систем, преднамеренное искажение (сокрытие/раскрытие) важной информации;</i>
2	Внешнее мошенничество	<i>незаконное проникновение в информационные системы, в т.ч. посредством сети Интернет, причинение ущерба информационным системам, кража информации;</i>
3	Трудовые отношения	<i>нарушения банком или служащими банка трудового законодательства, норм безопасности рабочих мест (в данном случае – техники безопасности и правил эксплуатации ИТ-систем);</i>
4	Материальные активы	<i>повреждение или утрата основных средств (в данном случае - информационных систем) по причинам стихийного или случайного характера (в т.ч. результате актов терроризма, стихийных бедствий, пожара);</i>
5	Нарушение деятельности или функционирования систем	<i>выход из строя информационной банковской системы, отдельных модулей и элементов ее функционала, отказы и сбои в работе автоматизированных систем, сбои в работе каналов связи, поломка оборудования и т.п.;</i>

6	Ошибки организации деятельности и исполнения операций	<i>ненадлежащая организация деятельности, ошибки управления и исполнения (в т.ч. в результате неадекватной организации внутренних процессов и процедур, отсутствия (несовершенства) системы защиты и порядка доступа к информации, неправильной организации информационных потоков внутри банка, ошибок при вводе и обработке данных по операциям и сделкам и т.п.).</i>
---	---	--

Основываясь на классификации факторов риска, необходимо далее для каждого из принятых в рассмотрение элементов ИТ-активов выявить потенциальные рисковые события, которые могут на нем реализоваться. Хорошей практикой является разработка моделей угроз и нарушителей информационной безопасности для банка. Стандарт ИБ - Банк России [3] 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 подчеркивается, что такая модель должна обладать прогностической силой. Подход "угроза - уязвимость" (модель угроз и нарушителей в терминологии Банка России), являющийся на Западе стандартом при оценке ИТ-рисков, предполагает сопоставление каждому элементу ИТ-активов определенных источников угроз (факторов риска), которые могут нанести 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, которые могут 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.

Целостность отражает необходимость защиты информации от несанкционированного изменения и утраты. Целостность нарушается при неразрешенных 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 привести к ошибкам в расчетах, реализации мошеннических действий, принятию неверных решений менеджментом банка.

Доступность - это обеспечение получения требуемой информационной услуги (информации) в нужное время. Информационные системы внедряются для предоставления определенных информационных услуг внутренним пользователям (персоналу) и внешним пользователям (клиентам, партнерам). Ес-

ли предоставить эти услуги в приемлемый срок невозможно, это влечет за собой потери, начиная от снижения операционной эффективности и вплоть до оттока клиентов, связанного с риском потери деловой репутации.

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

Выявление уязвимостей

Термин "уязвимость" характеризует отсутствие или слабость (недостаток) предохранительных мер, позволяющих снизить риск. К ним могут относиться процедуры обеспечения безопасности ИТ-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 тяжелые последствия от реализации риска - величина потерь. Например, отсутствие антивирусной защиты увеличивает как частоту рискованных 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.

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 ИТ-инфраструктурой и для контроля ИТ-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 кредитной организации.

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 определенной угрозе, должно считаться уязвимостью, даже если вероятность реализации угрозы достаточно мала, поскольку ущерб (величина потерь) от данной угрозы может быть весьма существенным.

Формирование предложений по устранению недостатков

Последним этапом качественной оценки ИТ- рисков является формирования перечня мер и предложений по устранению недостатков и минимизации возможных убытков. Поскольку подразделение риск-менеджмента может выступать исключительно как иницилирующее подразделение в этом вопросе, то на данном этапе необходимо ясно и доступно изложить и визуализировать полученные результаты качественной оценки, вынести на рассмотрение руководству кредитной организации предложения по устранению выявленных недостатков ИТ-систем.

Широко применяемым способом представления информации о рисках систем и процессов является построение карты рисков. Ниже приведен пример построения карты рисков для модельного примера бизнес-процесса Investment Banking. По горизонтальной шкале рассмотрены возможные (наиболее реалистичные) угрозы, по вертикальной – основные этапы бизнес-процесса. Заполнение ячеек карты происходит как на основании накопленной статистики (внешней и собственной) так и на основании экспертных оценок. Как было упомянуто ранее, количественно оценивать ИТ-риски систем банка удастся далеко не всегда, и для построения адекватных моделей риск-менеджеры применяют как статистическое (историческое) моделирование, так и экспертное (сценарное) оценивание.

По результатам оценивания уязвимостей в том или ином узле, на карту рисков наносится соответствующий цвет – чем темнее ячейка, тем критичнее и опаснее является рассматриваемая угроза. Таким образом, механизм применения карты рисков совместно с регулярным ее мониторингом позволяет своевременно выявлять слабые звенья в цепочках бизнес-процессов и своевременно информировать руководство банка о возможных проблемах в будущем.

Пример качественной оценки бизнес-процесса (Investment Banking)

В заключение продемонстрируем предложенную выше схему построения качественной оценки рисков ИТ-систем на модельном примере бизнес-процесса Investment Banking.

1. Идентификация IT-рисков, построение карты IT-инфраструктуры банка.

Инвестор обращается к менеджеру банка с просьбой совершить инвестиционную операцию (купить актив). Клиентский менеджер получает электронный запрос на проведение операции, проверяет его подлинность и заносит в специализированную программу. Через внутрибанковскую сеть данный запрос поступает в депозитарий банка. В депозитарии запрос проходит проверку на корректность (остаток по счету не должен быть меньше заранее оговоренной маржи, банк должен иметь возможность проводить запрашиваемые операции с данным видом активов) и затем данный запрос в случае подтверждения передается через внешнюю сеть на биржу. На бирже запрос проходит аналогичный контроль и далее по вышеуказанной схеме через внешнюю, внутреннюю сеть, депозитарий и клиентского менеджера информация о проведенной/не проведенной сделке обрабатывается в депозитарии банка и затем поступает обратно к инвестору.

На рис. 3 продемонстрирована схема такого взаимодействия. Красным цветом обозначены потоки информации во внутрибанковской сети, синим - по внешним каналам.

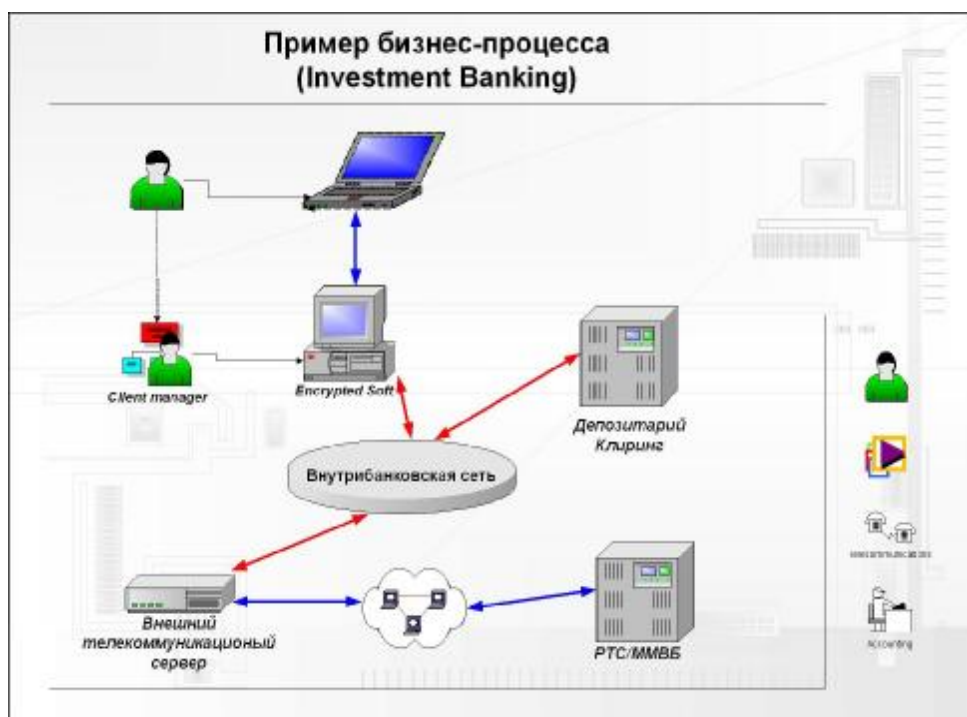


Рис. 2



Рис. 3

2. Выявление угроз.

На втором этапе, на основании экспертных заключений и исторических данных о произошедших внешних и внутренних событиях составляется перечень основных угроз: внешнее мошенничество, внутреннее мошенничество, сбои на этапе клиринга (нарушение деятельности и функционирования систем), сбои на этапе контроля операции (ошибки организации деятельности), внешние события и т.п.

3. Выявление уязвимостей.

На третьем этапе происходит выявление уязвимостей в каждом узле бизнес-процесса. Рассматриваются такие сценарии как мошенничество инвестора, мошенничество клиентского менеджера, сбои в работе внутрибанковской сети и программного обеспечения, внешние сбои при анализе и передачи информации, сбои на этапе клиринга и т.д.

После этого производится оценка значимости выявленных уязвимостей, ранжируется и заносится на карту рисков (рис.3 - карта рисков для примера Investment Banking).

4. Формирование предложений по устранению недостатков.

На заключительном этапе производится оценка адекватности модели, стресс-тестирование, определяется необходимая частота проведения мониторинга показателей модели. На основании данных модели формируются предложения по устранению недостатков и выносятся на рассмотрение руководству банка. В частности, для модельного примера Investment Banking критическими (см. рис. 2) оказались сбои во внутренней сети на этапе клиринга и

сбои во внешней сети на этапе внешней обработки, получения и подтверждения информации. В качестве предложений по устранению недостатков здесь могут быть рассмотрены возможности доработки программного обеспечения, проведение дополнительно ручного или автоматического контроля осуществляемых операций, согласование с биржей механизмов дополнительных подтверждений осуществляемых расчетов и т.д. Кроме того, необходимо обратить внимание на ячейки карты рисков, выделенные красным цветом. Эти уязвимости пока не критичны для банка, тем не менее, остаются актуальными и в любой момент могут явиться причиной операционных убытков.

Заключение

Необходимость создания резервов под операционный риск или включение операционного риска в расчет норматива достаточности собственного капитала (Н1) может стать для российских коммерческих банков реальностью уже в 2009 году, так как это отражает стратегию развития банковского сектора и курс Банка России на внедрение риск-ориентированных подходов к оценке финансовых организаций.

К этому времени у кредитных организаций должна существовать внедренная и эффективно функционирующая система управления ОР. В этой связи в настоящее время тема ОР развивается очень активно, многие российские банки включают ОР в приоритетные направления стратегии развития ближайших лет. Предложенные Базелем подходы к управлению ОР образуют гибкую систему, построенную по принципу «от простого к сложному», и задают направление для исследования и развития системы управления ОР в кредитных организациях.

Для некоторых типов ОР количественные методы оценки применены быть не могут. Для контроля и управления такими видами рисков необходимо применение качественных подходов к оценке ОР. В работе рассмотрены основные существующие на сегодняшний день методики качественной оценки ОР: ключевые показатели риска и контроля, сценарный анализ, построение карты рисков. Подробно рассмотрены этапы реализации системы качественной оценки ИТ-рисков и продемонстрированы на модельном примере Investment Banking.

В настоящее время контроль и управление ИТ-рисками является одним из приоритетнейших направлений операционного риск-менеджмента. В этой связи, внедрение системы качественной оценки ОР (в т.ч. ИТ-рисков) в дополнение к количественным методам расчета капитала на покрытие ОР, а также применение механизмов страхования, дает возможность кредитным организациям более эффективно управлять и контролировать величину ОР, позволит к моменту вступления в силу требований ЦБР выстроить у себя сбалансированную и наиболее адекватную собственным направлениям бизнеса систему управления ОР.

Список использованной литературы:

1. Васильев Ф.П. *Методы оптимизации*. – Факториал Пресс, 2002.
2. Информация ЦБР от 04.08.2004г. «О новом соглашении по оценке достаточности капитала Базельского комитета по надзору и перспективах его реализации в России».
3. *Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения* - (СТО БР ИББС-1.0-2006) // Вестник Банка России, 2006. №6(876).
4. Зинкевич В., Штатов Д. *Информационные риски: анализ и качественная оценка* // Бухгалтерия и банки, №1 2007г.
5. Яковлев Б.В., Грудовая В.И., Головки И.М. *Разработка методики качественного и количественного анализа операционных рисков* // Национальный технический университет Украины «Киевский политехнический институт», Киев 2006г.
6. Письмо ЦБР №76-Т от 24.05.2005 г. «Об организации управления операционными рисками в кредитных организациях».
7. Указание ЦБР №1379-У от 16.01.2004г. (с изменениями от 10.07.2007г.) «Об оценке финансовой устойчивости банка в целях признания её достаточной для участия в системе страхования вкладов».
8. Basel Committee on Banking Supervision, Operational Risk Consultative Document, Supporting document to the New Basel Capital Accord. – January 2001.
9. International Convergence of Capital Measurement and Capital Standards: a Revised Framework, Comprehensive Version // Basel Committee on Banking Supervision, Basel: June 2006.
10. G. Mignola, R. Ugocioni. *Sources of Uncertainty in Modelling Operational Risk Losses*. // Torino, Italy, 2006.
11. Официальные сайты профессиональных ассоциаций риск-менеджеров: www.orx.org, www.hedjing.ru, www.garp.com, www.primacentral.org.