DOI: 10.17117/na.2015.08.081

Поступила (Received): 11.08.2015

<http://ucom.ru/doc/na.2015.08.081.pdf>

Блюм М.А., Сычев В.А. Анализ операционного риска банковской информационной системы

Blum M.A., Sychev V.A.
**An analysis of the operational risk of the banking
information system**

*Данная статья посвящена операционного риска
банковской информационной системы.*

*Проанализированы определения операционного
риска в экономической литературе. Выделены
категории операционных рисков, а также виды
рисков, возникающих в операционных системах.*

*Представлена диаграмма анализа рисков
банковской информационной системы*

Ключевые слова: операционный риск, банковская
информационная система

*This article focuses on the operational risk of the
banking information system. Analyzed the definition
of operational risk in the economic literature. Scroll
to the category of operational risks, as well as the
types of risks that arise in operating systems. A
diagram of the risk analysis of the banking
information system*

Key words: operational risk, banking information
system

Блюм Марина Анатольевна

*Кандидат педагогических наук, доцент,
заведующая кафедрой*

*Тамбовский государственный технический
университет*

г. Тамбов, ул. Советская, 106

Blum Marina Anatolevna

*Candidate of Pedagogic Sciences, Associate
Professor, Head of Department*

Tambov state technical university

Tambov, Sovetskaya st., 106

Сычев Владислав Андреевич

Магистрант

*Тамбовский государственный технический
университет*

г. Тамбов, ул. Советская, 106

Sychev Vladislav Andreevich

Master

Tambov state technical university

Tambov, Sovetskaya st., 106

Операционный риск в банковской сфере стал объектом пристального внимания относительно недавно. Как самостоятельное направление, управление банковскими рисками, было выделено еще в конце 1990-х.

Затем серьезное внимание стало уделяться методам оценки и управления рыночными рисками. Далее появился интерес к кредитным рискам. К концу 90-х годов компании и надзорные органы все больше стали интересоваться рисками, «отличающимися от рыночных и кредитных». Их и называли операционными.

В экономической литературе не сложилось однозначного подхода к определению операционного риска, вследствие чего существуют различные

трактовки сущности данного вида риска. Одно из последних и распространенных определений диктует, что операционный риск – это риск возникновения убытков в результате недостатков или ошибок в ходе осуществления внутренних процессов, допущенных со стороны сотрудников, функционирования информационных систем и технологий, а также вследствие внешних событий.

Банки выделяют следующие категории операционных рисков:

- Информационный риск
- Риск персонала
- Риск внешних источников воздействия на внутренние процессы и технологии банка

Примерами могут служить:

- технологические неудачи;
- неадекватное хранение документов и записей;
- неграмотное управление, недостаток надзора, надежности и контроля;
- ошибки в финансовых моделях и отчетах;
- попытки скрыть потери или добиться личной выгоды (мошенническая торговля);
- мошенничество третьих сторон.

Рассмотрим одну из категорий, связанную с информационными рисками.

Информационный риск, который включает в себя:

- технологический риск сбоев оборудования (банкоматы, компьютерное и телекоммуникационное оборудование и пр.);
- технологический риск сбоев программного обеспечения и информационных технологий (информационная банковская система);

С точки зрения информационных технологий банковская информационная система (БИС) дает много возможностей, а именно – обеспечивает банку ведение кредитных продуктов, корреспондентских отношений, налогового учета, учета материальных ценностей и расчета заработной платы, подготовку обязательной отчетности в соответствии с требованиями Центрального Банка, предоставляет необходимые инструменты для анализа банковской деятельности. Использование БИС в банках позволяет сократить время и улучшить качество обслуживания клиентов.

Но при наличии информационной банковской системы необходимо помнить, что кроме повышения оперативности и удобства обслуживания клиентов мы получаем и риск. Риск сбоя работы системы, что может парализовать работу всей банковской системы и как следствие невозможность обслуживания клиентов до момента устранения неполадок, что может привести к долгому времени обслуживания клиентов, а следовательно, к неудовлетворенности клиентов, потери числа потребителей банковских услуг и продуктов.

В организации необходимо создать группу, которая несет ответственность за разработку, внедрение и поддержание системы анализа рисков в рабочем состоянии. Эта группа должна выявить и оценить все виды опасностей, включая атаки хакеров, человеческий фактор и возможные опасные факторы, которые могут присутствовать в процессах оказания банковских услуг.

Таблица 1. Тяжесть последствий отказа

Степень тяжести	События отказа	Время, необходимое для устранения причин отказа, ч
4	Выход из строя БИС, отдельных модулей и элементов её функционала	8
4	Отказы и сбои в работе автоматизированных систем	8
3	Сбои в работе каналов связи	2
3	Замена блока и/или переустановка ПО	2
2	Поломка оборудования (компьютеры, терминалы самообслуживания клиентов, другое оборудование)	0,5
2	Вызов администратора или программиста для устранения сбоя АБС	0,5
1	Перезагрузка системы из-за ошибок работника или пользователя	0,25

ДИАГРАММА АНАЛИЗА РИСКОВ

Рис. 2. Диаграмма анализа рисков

ОПАСНЫЕ ФАКТОРЫ ПО СТЕПЕНИ ТЯЖЕСТИ

Ст	Виды опасных факторов	Ст	Виды опасных факторов
4	Несанкционированное использование информационных систем	2	Отказы и сбои в работе автоматизированных систем
3	Преднамеренное искажение (сокрытие/раскрытие) важной информации, повлекшее денежные убытки	1	Сбои в работе каналов связи
3	Внедрение вредоносного программного обеспечения	1	Поломка оборудования (компьютеры, терминалы самообслуживания клиентов, другое оборудование)
4	Незаконное проникновение в информационные системы, в том числе посредством интернет (хакерские атаки)	1	Незапланированное отключение электроэнергии
4	Причинение ущерба информационным системам	2	Отсутствие (несовершенство) системы защиты или порядка контроля доступа к информации
4	Кража информации, повлекшая денежные потери	2	Неправильная организация информационных потоков внутри банка
2	Связанное с недостаточностью систем неправомерное раскрытие конфиденциальной информации и нарушение банковской тайны	2	Невыполнение обязательств перед банком поставщиками, провайдерами
3	Ущерб материальным ценностям (в данном случае информационным системам)	1	Ошибки при вводе и обработке данных по операциям и сделкам
2	Ущерб информационным системам от актов терроризма, вандализма	1	Ошибки (моделей и) систем
2	Выход из строя информационных банковской системы, отдельных модулей и элементов её функционала		

Рис. 1. Диаграмма анализа рисков

По каждому потенциальному фактору группа должна провести анализ риска с учетом вероятности появления фактора и значимости его последствий и составить перечень причин, по которым риск превращает допустимый уровень. А далее необходимо определить и документировать предупреждающие действия, которые устраняют риски или снижают их до допустимого уровня.

В случае информационных систем существуют следующие виды рисков:

- риски, вызванные утечкой информации и использование ее с целью навредить организации;
- риски технических сбоев работы автоматизированной системы каналов передачи информации;
- риски уменьшения количества потребителей банковских продуктов и услуг в результате неудовлетворенности клиентов качеством и долгого времени обслуживания;
- риски потери деловой репутации;
- информационные, операционные и стратегические риски.

Оценка тяжести последствий и вероятности возникновения отказа.

Градацию тяжести последствий представим в виде таблицы (см. табл. 1).

Используя некоторые данные из банка, можно представить диаграмму анализа рисков (см. рис. 1).

Можно сделать вывод, что опасными факторами являются: внедрение вредоносного программного обеспечения, отказ и сбой аппаратуры, замыкание электросети и незапланированное отключение электроэнергии, приводящие к низкой скорости клиентского обслуживания, увеличению жалоб потребителей, потери деловой репутации банка.

Список используемых источников:

1. Вальравен К.Д. Управление рисками в коммерческом банке.
2. Кузнецова Н.В. Управление рисками. Владивосток: ТИДОТ ДВГУ, 2004.
3. Пономарев С.В., Мищенко С.В., Белобрагин В.Я., Самородов В.А., Герасимов Б.И., Трофимов А.В., Пахомова С.А., Пономарева О.С. Управление качеством продукции: инструменты и методы менеджмента качества. М.: РИА Стандарты и качество, 2004.
4. Иода Е.В., Мешкова Л.Л., Болотина Е.Н. Классификация банковских рисков и их оптимизация. Тамбов: Изд-во ТГТУ, 2002.
5. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. М.: Стандартинформ, 2013.
6. ГОСТ Р ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные требования безопасности. М.: Стандартинформ, 2014.
7. ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Компоненты доверия к безопасности. М.: Стандартинформ, 2014.