УДК 658.14

***А.А. Пчелин***

# *О РИСКАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНОЙ ОРГАНИЗАЦИИ (БАНКА)*

*На основе междисциплинарного анализа сформирован перечень рисков информационной безопасности кредитной организации, который может быть использован для построения моделей угроз для различных банков. Модели угроз лежат в основе методик количественной оценки эффективности систем информационной безопасности, оценки влияния мер информационной безопасности на эффективность деятельности кредитных организаций. Показана научно-практическая значимость разработки методологии количественной оценки роли и значения систем информационной безопасности. Раскрыты содержание и сущность объективно существующей корреляционной связи между эффективностью деятельности банка и принимаемыми в нем мерами информационной безопасности. Обращено внимание на то, что объективная оценка рисков позволяет не только системно выстроить в банке работу по обеспечению информационной безопасности, но и привлечь внимание руководства банка к этой проблеме, поскольку создание эффективных систем информационной безопасности в современных условиях требует не только финансовых инвестиций, но и соответствующей поддержки со стороны учредителей банка, руководителей исполнительных органов, советов директоров.*

*Ключевые слова: информационная безопасность, банковская деятельность, эффективность, показатели эффективности, угрозы и риски, финансовая устойчивость, экспертные оценки, финансовые показатели, целевые ориентиры, ключевые показатели эффективности.*

В современных условиях развития РФ ключевое значение приобретают проблемы экономической безопасности. При этом устойчивость национальной экономической системы в значительной мере базируется на устойчивости банковской системы и обеспечении ее безопасности, в том числе в информационной сфере [1, 2]. Последние события, связанные с реализацией санкционной политики рядом западных стран в отношении РФ, отчетливо показали уязвимость российской банковской системы, опирающейся, в основном, на иностранную организационную и технологическую ИТ инфраструктуру. Прежде всего, это касается электронных платежных систем Visa и Master card, а также систем денежных переводов, таких как Swift. В этой связи важное значение имеет вопрос создания отечественных ИТ-систем, устойчивых к рискам информационной безопасности (ИБ). Защиту кредитных организаций от подобного рода рисков обеспечивают системы информационной безопасности (СИБ).

## Необходимость количественной оценки эффективности мер информационной безопасности. Этапы создания методики оценки эффективности систем информационной безопасности

Большинство специалистов банковской сферы признают важность наличия в кредитной организации СИБ, поскольку риски ИБ могут существенно затруднить деятельность банка. В то же время остается дискуссионным вопрос о конкретном облике систем, его составе и программном обеспечении, поскольку стоимость СИБ может достигать до 20% стоимости

всей информационной банковской системы [3]. Таким образом, создание СИБ требует значительных финансовых вложений, необходимость которых должна быть соответствующим образом обоснована.

В настоящее время подобный инструментарий аргументирования у специалистов ИБ российских банков практически отсутствует. Формирование бюджетов подразделений ИБ и построение СИБ осуществляется, в большинстве случаев, без глубокой научной проработки. Как правило, определяющими являются финансовые возможности банка, авторитет руководителей службы безопасности, положительный опыт использования тех или иных СИБ, а также промоутерские усилия компаний, продвигающих СИБ на рынке. Несмотря на широкое освещение проблемы ИБ в научной литературе вопрос количественной оценки влияния мер ИБ на эффективность деятельности банков не нашел освещения.

Перед практическим созданием банковской СИБ необходимо оценить эффективность ее будущей деятельности по критерию «эффективность – стоимость», поскольку архитектура, техническое оснащение, программное обеспечение, а также стоимость СИБ регионального банка и банка федерального значение, будут существенным образом отличаться. В этой связи важным является создание методики оценки эффективности СИБ [4]. Основные этапы создания подобной методики представлены на рис. 1.

В совокупности, эти этапы составляют алгоритм, в котором на каждом этапе необходимо производить оценку рисков ИБ. По оценке специалистов, затраты на создание подсистем оценки рисков составляют наиболее значительную часть в структуре расходов на создание всей СИБ [5].

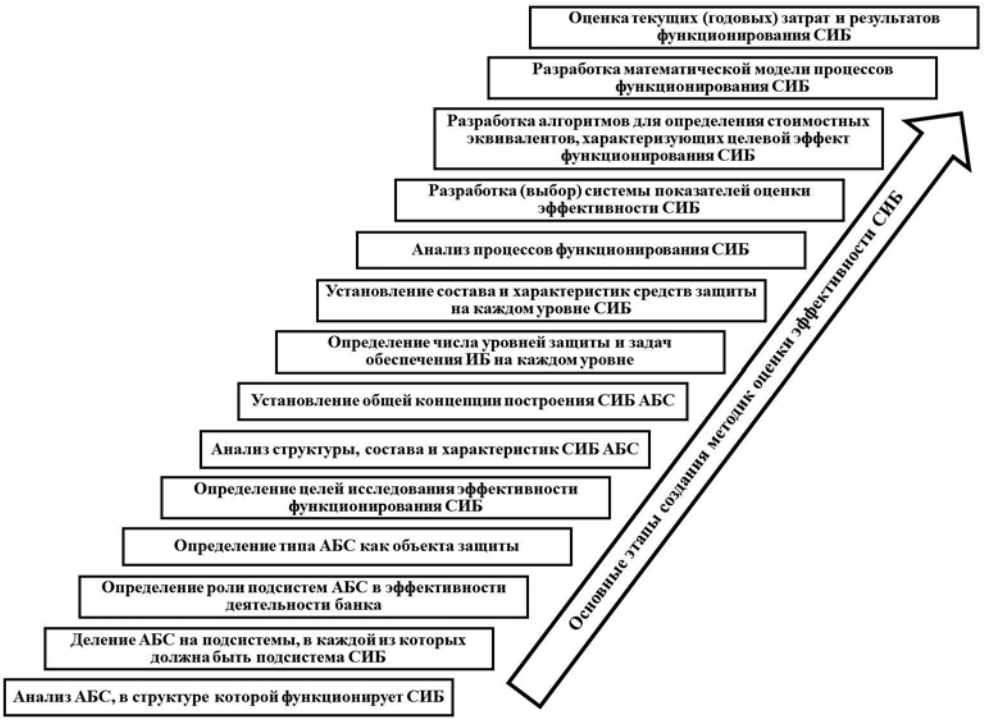


***Рис. 1. Основные этапы создания методик оценки эффективности СИБ***

**Основные проблемы оценки рисков информационной безопасности в банковской сфере**

Анализ рисков ИБ предусматривает необходимость исследования требований ряда международных и российских нормативных документов, разработанных различными ведомствами и организациями, такими как Международная организация по стандартизации, Федеральное агентство по стандартизации (Росстандарт), Федеральное агентство безопасности (ФСБ России), Федеральная служба по техническому и экспертному контролю (ФСТЭК России) и других.

Анализ рисков должен опираться также на отраслевые стандарты (ГОСТ) и документы Банка России, такие как ГОСТ 28147-89 «Система обработки информации. Защита криптографическая», ГОСТ-Р 50922-2006. «Защита информации», Стандарт Банка России «Методика оценки соответствия ИБ организаций банковской системы РФ требованиям СТО БР ИББС-1.0-2010», Приказ ЦБ РФ «О вводе в действие «Основных направлений политики ИБ ЦБ РФ» № ОД-103 от 06.03.2006, Письмо ЦБ РФ «О типичных банковских рисках» № 70-Т от 23.06.2004 и др.

Поскольку каждая организация имеет различные предметы ведения (стандарты, безопасность, внешнеэкономическая деятельность, банковская деятельность) правомерно утверждать, что подобный анализ носит характер междисциплинарного исследования.

Для того, чтобы методика количественной оценки влияния мер ИБ на экономическую эффективность банка была практически реализуемой, необходимо сформировать ограниченный перечень рисков, с которыми будут работать эксперты, поскольку в целом, банковской системе противостоит более 300 уязвимостей ИБ [6]. Безусловно, использование полного перечня рисков серьезно затруднит практическую работу, поэтому при формировании перечня рисков необходимо провести их ранжирование и соответствующую систематизацию для того чтобы сократить их количество при сохранении принципиальных положений, зафиксированных в нормативных документах.

Традиционный взгляд на ИБ включает в себя три «краеугольных камня»: конфиденциальность, целостность и доступность, известные также как «модель CIA» (Confidentiality-Integrity-Availability). В соответствии с международным стандартом «Сертификация по ISO 27001. Информационная безопасность» основные риски ИБ направлены на затруднение доступности, целостности, конфиденциальности информации [7].

Конфиденциальность – защита от несанкционированного ознакомления, является одним из наиболее проработанных аспектов ИБ, регламентируемым законами, нормативными актами, опытом соответствующих служб. Современные аппаратно-программные продукты позволяют закрыть большинство каналов утечки информации.

Целостность – актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения, подразделяется на статическую (неизменность информационных объектов) и динамическую (выполнение сложных действий, транзакций).

Доступность – возможность за приемлемое время получить требуемую информационную услугу. Информационные системы создаются для получения определенных информационных услуг.

Кроме того, для практической реализации политики ИБ целесообразно выделить такие группы рисков, как организационные риски, связанные с отработкой соответствующих документов, и репутационные (имиджевые)


***Рис. 2. Формирования перечня рисков информационной безопасности***

риски, связанные с нанесением ущерба деловой репутации и имиджу банка.

При формировании обобщенного перечня рисков необходимо учитывать также нормативные документы, в которых классификация рисков производится по другим основаниям. По существу, требуемый перечень формируется на базе междисциплианарного анализа четырех групп различных международных и российских нормативных документов, разработанных различными ведомствами (рис. 2).

**Междисциплинарный анализ рисков информационной безопасности**

В соответствии с Методикой ЦБ РФ по оценке рисков нарушения ИБ (РС БР ИББС-2.2-2009) [8], выделятся 7 групп, насчитывающих 40 рисков ИБ, которые зависят от различных причин (источников) возникновения.

Классификация указанных рисков приведена в табл. 1.

При формировании перечня рисков ИБ необходимо также учитывать факторы, способствующие возникновению рисков и влияющие на уровень защиты информации (ГОСТ-Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию») [9], которые делятся на классы: объективные и субъективные, внутренние и внешние.

Классификация основных факторов, влияющих на уровень защиты информации, и их содержание приведены в табл. 2.

В ходе решения задач по обеспечению ИБ особое значение придается обеспечению безопасности персональных данных (ПД), которые в соответствии с Федеральным законом «О персональных данных» [10] подразделяются на четыре категории: 1 – ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, ин-

Таблица 1

| № п.п. | Риски, их основное содержание |
|---|---|
| 1 | *Группа рисков, связанных с форс-мажорными ситуациями* |
| | Пожары, природные и техногенные катастрофы, чрезвычайные ситуации и стихийные бедствия и др. Всего 8 рисков. |
| 2 | *Группа рисков, связанных с деятельностью злоумышленников* |
| | Терроризм, шпионаж, обман, социальный инжиниринг. Всего 4 риска. |
| 3 | *Группа рисков, связанных с деятельностью контрагентов* |
| | Ошибки при проектировании, разработке и обслуживании СИБ. Всего 5 рисков. |
| 4 | *Группа рисков, связанных с отказами программных и технических средств* |
| | Повреждения технических средств, выходы из строя систем криптографической защиты, сбои и отказы программного обеспечения. Всего 6 рисков. |
| 5 | *Группа рисков, связанных с деятельностью внутренних нарушителей ИБ* |
| | Недобросовестность (халатность, ошибки) персонала, хищения информационных ресурсов, использование вредоносных программ и др. Всего 8 рисков. |
| 6 | *Группа рисков, связанных с деятельностью внешних нарушителей ИБ* |
| | Внешние проникновения, несанкционированный доступ к техническим средствам и информационным ресурсам и др. Всего 6 рисков. |
| 7 | *Группа рисков, исходящих от надзорных и регулирующих органов* |
| | Несоответствие внутренних документов действующему законодательству, несогласованность требований надзорных и регулирующих органов, зафиксированных в различных нормативных документах. Всего 2 риска. |

Таблица 2

| № п.п. | Факторы и их содержание |
|---|---|
| 1 | *Внутренние факторы* |
| | Каналы связи, излучения, наводки, аварии, отказы технических средств и программного обеспечения. Всего 9 факторов. |
| 2 | *Внешние факторы* |
| | Техногенные и природные катаклизмы. Всего 2 фактора. |
| 3 | *Субъективные факторы (внутренние)* |
| | Разглашение информации, использование незащищенных технических средств, нарушение правил хранения и обработки информации, использование нелицензионного программного обеспечения и др. Всего 29 факторов. |
| 4 | *Субъективные факторы (внешние)* |
| | Доступ к защищаемой информации с применением технических средств, использование возможностей (дефектов) программного обеспечения, криминальные проявления и др. Всего 25 факторов. |

тимной жизни; 2 – ПД, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию; 3 – ПД, позволяющие идентифицировать субъекта ПД; 4 – обезличенные или общедоступные ПД. Согласно Отраслевой частной модели угроз безопасности ПД (Рекомендации ЦБ РФ РС БР ИББС-2.4-2010), эти риски классифицируются по направлениям (объектам) воздействия. Классификация рисков нарушения безопасности ПД и их содержание приведены в табл. 3.

Таблица 3

| № пп | Категории персональных данных. Субъекты рисков ИБ. Уровень воздействия – Объекты воздействия – Типы рисков |
|---|---|
| **Персональные данные категорий 1, 2** | |
| 1 | *Компьютерные злоумышленники, осуществляющие деструктивное воздействие* |
| | Сетевой уровень, операционные системы, системы управления базами данных, прикладные программы доступа и обработки. Всего 4 типа рисков. |
| 2 | *Поставщики программно-технических средств и услуг* |
| | Уровень операционных систем, систем управления базами данных, банковские технологические приложения и сервисы. Всего 3 типа рисков. |
| 3 | *Сотрудники, действующие в рамках предоставленных полномочий* |
| | Физический уровень, сетевой уровень, приложения и сервисы, системы управления базами данных, программы доступа и обработки. Всего 6 типов рисков. |
| 4 | *Сотрудники, действующие вне рамок предоставленных полномочий* |
| | Уровень операционных систем, системы управления базами данных, банковские технологически приложения и сервисы, программы доступа. Всего 4 типа рисков. |
| **Персональные данные категории 3** | |
| 5 | *Компьютерные злоумышленники, осуществляющие деструктивное воздействие, сотрудники, действующие в рамках полномочий* |
| | Сетевой уровень, сетевые приложения и сервисы, операционные системы, системы управления базами данных, физический уровень. Всего 8 типов рисков. |
| 6 | *Сотрудники, действующие вне рамок предоставленных полномочий* |
| | Уровень операционных систем, системы управления базами данных, банковские технологические приложения и сервисы. Всего 3 типа рисков. |
| **Персональные данные категории 4** | |
| 7 | *Компьютерные злоумышленники, осуществляющие деструктивное воздействие* |
| | Операционные системы, системы управления базами данных. Всего 2 типа рисков. |
| 8 | *Сотрудники, действующие в рамках предоставленных полномочий* |
| | Операционные системы, системы управления базами данных, банковские технологические приложения и сервисы. Всего 3 типа рисков. |
| 9 | *Сотрудники, действующие вне рамок предоставленных полномочий* |
| | Операционные системы, системы управления базами данных, прикладные программы доступа и обработки. Всего 3 типа рисков. |

**Формирование обобщенного перечня рисков информационной безопасности кредитных организаций**

Междисциплинарный анализ причин возникновения, субъектов рисков, факторов, влияющих на уровень защиты ИБ, а также материалов по проблемам ИБ позволил сформировать обобщенный перечень основных рисков информационной безопасности, состоящий из 50 рисков. Обобщенный перечень рисков информационной безопасности типовой кредитной организации представлен в табл. 4.

**Заключение**

На основе междисциплинарного анализа разработан перечень, состоящий из 50 рисков ИБ, который воз-

Таблица 4.

| № пп | Группы рисков и их содержание |
|---|---|
| **1. Организационные риски** | |
| 1 | 1.1. Ошибки персонала, низкая квалификация. |
| 2 | 1.2. Нанесение умышленного вреда нелояльными сотрудниками. |
| 3 | 1.3. Злоумышленные действия администратора сетей. |
| 4 | 1.4. Совмещение обязанностей администратора ИС и администратора ИБ. |
| 5 | 1.5. Отсутствие средств сигнализации при возникновении нештатных ситуаций. |
| 6 | 1.6. Отсутствие регламента действий сотрудников ИБ в случае возникновения нештатной ситуации. |
| 7 | 1.7. Отсутствие систем видеонаблюдения за ключевыми узлами информационных систем, контроля доступа в рабочие помещения. |
| 8 | 1.8. Бесконтрольное использование и списание носителей информации. |
| 9 | 1.9. Злоумышленные действия при сервисном обслуживании. |
| 10 | 1.10. Бесконтрольное использование Интернета. |
| **2. Репутационные (имиджевые) риски** | |
| 11 | 2.1. Распространение во внешней среде информации экономического характера, угрожающей репутации банка |
| 12 | 2.2. Упоминание банка в контексте экстремизма, отмывания финансовых средств, киберугроз и кибертерроризма. |
| 13 | 2.3. Использование несертифицированных и нелицензионных продуктов. |
| 14 | 2.4. Возможность внешнего проникновения в Intranet системы банка. |
| **3. Риски конфиденциальности** | |
| 15 | 3.1. Несанкционированный доступ к данным в ИС и ПК. |
| 16 | 3.2. Отсутствие четких регламентов работы с персональным данными. |
| 17 | 3.3. Утечка служебной информации по различным каналам. |
| 18 | 3.4. Продолжительное сохранение окна авторизации при бездействии или в случае выхода сотрудника из помещения. |
| 19 | 3.5. Возможность удаленного съема информации с внешних позиций. |
| 20 | 3.6. Возможность бесконтрольного съема информации с внутренних позиций. |
| 21 | 3.7. Принятие в эксплуатацию непротестированных СКЗИ. |
| 22 | 3.8. Несанкционированный доступ к паролям и ключам. |
| 23 | 3.9. Несоблюдение конфиденциальности паролей. |
| 24 | 3.10. Несанкционированное использование системы электронных платежей, дистанционного банковского обслуживания (ДБО). |
| 25 | 3.11. Нарушения порядка хранения и передачи паролей. |
| 26 | 3.12. Недостоверная идентификация пользователей ИС. |
| 27 | 3.13. Виртуальные кражи и подлоги с использованием персональных данных. |
| 28 | 3.14. Перехват данных различными способами. |
| 29 | 3.15. Фактические кражи и хищения технических средств (телефоны, ноутбуки, флеш-накопители, коммуникаторы и др.). |
| 30 | 3.16. Отсутствие процедур мониторинга и анализа всех выполненных операций. |
| 31 | 3.17. Отсутствие в системах ДБО защитных мер, обеспечивающие невозможность отказа от авторства проводимых операций и транзакций (например, ЭЦП). |
| 32 | 3.18. Отсутствие механизмов регистрации несанкционированного допуска к информации для идентификации, авторизации клиентов и сотрудников банка. |

| | |
|---|---|
| 33 | 3.19. Дефицит организационных процедур, позволяющих проводить внутренние служебные разбирательства по фактам нарушений рисков конфиденциальности. |
| **4. Риски целостности** | |
| 34 | 4.1. Обычный выход из строя технических средств (среднестатистический). |
| 35 | 4.2. Выход из строя технических средств вследствие форс-мажорных обстоятельств. |
| 36 | 4.3. Сбои программного управления. |
| 37 | 4.4. Потеря или недоступность важных данных. |
| 38 | 4.5. Использование неполной или искаженной информации. |
| 39 | 4.6. Проникновение в информационные системы вредоносных кодов. |
| 40 | 4.7. Изменение конфигурации средств и систем обработки информации. |
| 41 | 4.8. Возникновение окон уязвимости в защите информационных систем, связанное с использованием «заплат» в защищенном ПО. |
| 42 | 4.9. Нарушения порядка копирования (резервирования) информации. |
| 43 | 4.10. Программные атаки на возможности процессоров и оперативной памяти. |
| 44 | 4.11. Совмещение обязанностей разработчика и пользователя ПО. |
| **5. Риски доступности** | |
| 45 | 5.1. Неправомочная скрытая продолжительная эксплуатация информационно-вычислительных ресурсов. |
| 46 | 5.2. DDoS-атаки на АБС и компьютеры сотрудников банка. |
| 47 | 5.3. Несанкционированный удаленный доступ к ИС и ПК. |
| 48 | 5.4. Незащищенный удаленный доступ (санкционированный) к ИС и ПК. |
| 49 | 5.5. Незащищенность электронной почты. |
| 50 | 5.6. СПАМ-угрозы. |

можно использовать в практической деятельности банка, поскольку нейтрализация (ликвидация, минимизация) рисков ИБ составляет сущность и содержание процесса обеспечения ИБ банка. На базе предложенного перечня могут быть также построены модели угроз, на основании которых осуществляется постановка задач на создание СИБ. Кроме того, перечень конкретных рисков может использоваться в ходе оценки влияния принимаемых мер ИБ на эффективность деятельности банка.

## *СПИСОК ЛИТЕРАТУРЫ*


1. *Федеральный* закон «О безопасности» № 390-ФЗ от 28.12.2010.

2. *Федеральный* закон «О банках и банковской деятельности» № 395-1 от 02.12.1990.

3. *Петенко С.А., Терехова Е.М.* Оценка затрат на защиту информации // Защита информации. – 2004. – № 1.

4. *Гусева Н.Н.* Исследование и разработка методико-математического аппарата оценки экономической эффективности функционирования системы обеспечения безопасности корпоративной информационной сети. Дисс. на соискание ученой степени канд. экономич. наук. – М.: МЭСИ, 2002. – 137 с.

5. *Горохов Д.Е.* Методика формирования рационального состава комплекса средств защиты информации на основе априорной оценки риска. Дисс. на соискание ученой степени канд. технич. наук. – Орел: Академия ФСО РФ, 2010.

6. *Конев И.* Практическая оценка информационных рисков. Директор ИС. 15.09.2007. http://www.osp.ru/cio/2007/09/4370713 10

7. *Сертификация* по ISO 27001. Перевод. Информационная безопасность. http://dorlov.blogspot.ru/2011/06/iso-27001.html 11

8. *Рекомендации* в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы РФ. Методика оценки рисков нарушения информационной безопасности» РС БР ИББС-2.2-2009 (приняты и введе-

ны в действие Распоряжением ЦБ РФ от 11.11.2009 № Р-1190).

9. *ГОСТ-Р 51275-99.* Защита информации. Объект информатизации. Факторы, воздействующие на информацию.

10. *Федеральный закон* «О персональных данных» № 152-ФЗ (в ред. от 04.06.2011) от 27.07.2006. ГИАБ

## *КОРОТКО ОБ АВТОРЕ*

*Пчелин Алексей Александрович* – начальник отдела, ОАО «Акционерный банк «Балтика»; соискатель кафедры, Московский государственный индустриальный университет, e-mail: aapchelin@yandex.ru.

UDC 658.14

**RISKS FOR INFORMATION SECURITY OF FINANCIAL ESTABLISHMENT (BANK)**

*Pchelin A.A.*, Head of Department, Baltica Bank JSC;
Applicant of Chair, Moscow State Industrial University, Moscow, Russia, e-mail: aapchelin@yandex.ru.

*Based on the cross-disciplinary analysis, the risks for the information security of a financial establishment are identified to be used in modeling hazards for different banks. The hazard models are the basis of quantitative evaluation procedures for information security efficiency and assessment of influence of information security measures on a financial establishment performance. The article highlights the scientific and practical importance of the quantitative evaluation procedure and the information security systems. The content and essence of entitative correlation between performance and information security of a bank are exposed. It is emphasized that objective assessment of risks allows a comprehensive approach to information security and, furthermore, attention of senior management, which is important as the efficient information security implementation in the up-to-date conditions requires both financial investment and appropriate support by bank promoters, management of executive departments and board of directors.*

*Key words: information security, banking, efficiency, measures of efficiency, hazards and risks, financial stability, expert appraisements, finance indexation, targets, key performance indicators.*

**REFERENCES**

1. *Federal'nyi zakon «O bezopasnosti» no 390-FZ ot 28.12.2010* (Federal Law on Safety no 390-FZ from 28.12.2010).

2. *Federal'nyi zakon «O bankakh i bankovskoi deyatel'nosti» no 395-1 ot 02.12.1990*. (Federal Law on Banks and Banking Activity no 395-1 from 02.12.1990).

3. Petenko S.A., Terekhova E.M. *Zashchita informatsii*. 2004, no 1.

4. Guseva N.N. *Issledovanie i razrabotka metodiko-matematicheskogo apparata otsenki ekonomicheskoi effektivnosti funktsionirovaniya sistemy obespecheniya bezopasnosti korporativnoi informatsionnoi seti* (Исследование и разработка методико-математического аппарата оценки экономической эффективности функционирования системы обеспечения безопасности корпоративной информационной сети), Candidate's thesis, Moscow, MESI, 2002, 137 p.

5. Gorokhov D.E. *Metodika formirovaniya ratsional'nogo sostava kompleksa sredstv zashchity informatsii na osnove apriornoi otsenki riska* (Procedure of making a well-disposed range of information security measures based on prior estimate of risk), Candidate's thesis, Orel, Akademiya FSO RF, 2010.

6. Konev I. *Direktor IS,* 15.09.2007, available at: http://www.osp.ru/cio/2007/09/4370713 10

7. *Sertifikatsiya po ISO 27001. Perevod. Informatsionnaya bezopasnost'*, available at: http://dorlov.blogspot.ru/2011/06/iso-27001.html 11

8. *Rekomendatsii v oblasti standartizatsii Banka Rossii «Obespechenie informatsionnoi bezopasnosti organizatsii bankovskoi sistemy RF.* Metodika otsenki riskov narusheniya informatsionnoi bezopasnosti» RS BR IBBS-2.2-2009 (prinyaty i vvedeny v deistvie Rasporyazheniem TsB RF ot 11.11.2009 № R-1190).

9. *Zashchita informatsii. Ob"ekt informatizatsii. Faktory, vozdeistvuyushchie na informatsiyu. GOST R 51275-99* (Information security. Informatization object. Information factor. State Standart *R* 51275-99.

10. *Federal'nyi zakon «O personal'nykh dannykh» no 152-FZ (v red. ot 04.06.2011) ot 27.07.2006* (Federal Law on Private Information no 152-*FZ* (as amended on 04.06.2011) from 27.07.2006).