Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, управления и природопользования
кафедра финансов

УТВЕРЖДАЮ
Заведующий кафедрой

_____ И.С. Ферова
подпись
« _____» _____ 2018 г.

ДИПЛОМНАЯ РАБОТА

специальность 38.05.01 «Экономическая безопасность»

АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КРЕДИТНОЙ ОРГАНИЗАЦИИ

Научный
руководитель _____ Старший преподаватель Е.В.Шкарпетина
подпись, дата должность, ученая степень

Выпускник _____ А.С.Матвеев
подпись, дата

Рецензент _____ начальник отделения ОЭБиПК МУ МВД РФ «Красноярское»_____ Д.Г.Поздняков
подпись, дата должность, ученая степень

Нормоконтролер _____ Е.В.Шкарпетина
подпись, дата

Красноярск 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Сегодня анализу рисков информационной безопасности уделяется все больше внимания. Этому есть несколько основных причин: безостановочный рост использования информационных технологий в процессе деятельности практически любой современной организации, увеличение ценности информации, обрабатывающейся и генерирующейся в процессе работы компании, а также интеграция различных информационных продуктов с целью покрытия всех нужд фирмы.

Особого внимания относительно рисков информационной безопасности заслуживает банковская сфера, так как стоимость информации в компаниях, работающих в данной области, ещё выше за счёт превалирования персональных данных клиентов, обладание которыми даёт возможность получить несанкционированный доступ к финансовым ресурсам. Кроме того, существует такое понятие, как банковская тайна, суть которого заключается в обязанности каждого банка (или иной кредитной организации) защищать сведения о вкладах и счетах своих клиентов и корреспондентов, банковских операциях по счетам и сделках в интересах клиента, а также сведения клиентов, разглашение которых может нарушить право последних на неприкосновенность частной жизни (ФЗ "О банках и банковской деятельности").Таким образом, информация, задействованная в работе коммерческих банков, нуждается в особой защите от потери ее свойств, а именно конфиденциальности, целостности и доступности. В частности, особое внимание должно уделяться поиску уязвимостей в системе защиты информации, анализу и оценке рисков информационной безопасности [1].

Однако на данный момент не существует стандартизированной методики анализа и оценки рисков информационной безопасности для кредитных организаций, обязательной для применения банками России. Все разработанные и активно использующиеся методики являются довольно общими для организаций, работающих в различных секторах экономики, они

не учитывают особенностей банковского законодательства и специфики деятельности кредитных организаций. Тем не менее, существует методика анализа и оценки рисков ИБ в организациях банковской системы РФ, разработанная в 2009 году Банком России, однако она носит лишь рекомендательный характер.

Цель данной работы: анализ и оценка рисков информационной безопасности на примере АО "Газпромбанк". Предложение мер по снижению рисков информационной безопасности, на основе полученных результатов.

Для достижения цели необходимо выполнить следующие задачи:

- Рассмотреть характеристику элементов экономической безопасности организации, их назначение и сущность
- Выделить основные методы анализа и оценки информационной безопасности
- Подобрать метод анализа, подходящий к банковскому сектору
- Создать таблицу вводных данных организации.

Предметом исследования в данной работе являются риски информационной безопасности и уязвимости исследуемой системы на примере кредитной организации АО "Газпромбанк"..

Объект исследования – ресурс "рабочая станция сотрудника". По данному ресурсу выделено три уязвимости, которые будут оценены на предмет критичности реализации угрозы и вероятности реализации угрозы, а также будут использованы в дальнейшем анализе рисков информационной безопасности.

В дипломной работе используются следующие нормативные документы: Федеральный закон от 02.12.1990 N 395-1 (ред. от 01.05.2017) "О банках и банковской деятельности", стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации, рекомендации Банка России в области стандартизации "Обеспечение информационной безопасности организаций банковской системы Российской Федерации". Рассматриваются труды российских авторов, методики анализа и оценки рисков информационной безопасности следующих

компаний: Symantec Lifecycle Security, Microsoft, CRAMM, FRAP, RiskWatch, ГРИФ.

Работа состоит из трех глав. В первой главе рассматривается теоретическая основа экономической безопасности организации, а также всех ее составляющих. Во второй главе приведены актуальные методы анализа рисков информационной безопасности, представлена теория расчета рисков информационной безопасности на примере кредитной организации. Третья глава включает в себя: общую характеристику кредитной организации АО "Газпромбанк"., расчет и анализ рисков информационной безопасности данного банка, разработка мер по снижению рисков, основываясь на полученных данных.

1 Теоретические аспекты экономической безопасности организации

1.1 Понятие экономической безопасности и ее структурых элементов

Под «безопасностью» в широком смысле слова понимается свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. При определении понятия «экономическая безопасность» рассматривались различные подходы к трактовке этой проблемы, опубликованные в отечественной литературе, основными из которых являются следующие:

1. Экономическая безопасность рассматривается, в первую очередь как проблема защиты информационных данных, которые обеспечиваются в форме двухуровневой системы. Первый уровень представляет защиту секретов службой безопасности организации, а второй — предусматривает создание психологической атмосферы «бдительности и ответственности» сотрудников организации посредством координаторов, назначаемых из лиц среднего руководящего звена и пользующихся авторитетом среди сотрудников организации. Хранение информационных данных является одной из важнейших частей экономической безопасности организации, следует отметить, что сведение проблемы экономической безопасности организации только к защите коммерческой тайны представляет собой слишком упрощенный вариант решения такой проблемы и не учитывает всего спектра влияния внешней среды как основного источника опасностей для деятельности организации [14].

2. Формирование рыночных отношений, изменение функций государства в управлении предприятий позволили рассматривать проблему экономической безопасности организации намного шире — как возможность обеспечения его устойчивости в разнообразных, в том числе и в неблагоприятных условиях, которые складываются во внешней среде, вне зависимости от характера ее влияния на деятельность организации, масштаба и характера внутренних измене-

ний. Так, экономическая безопасность организации определена как «защищенность его деятельности от отрицательных влияний внешней среды, а также как способность быстро устранить разно вариантные угрозы или приспособиться к существующим условиям, которые не сказываются отрицательно на его деятельности» [27].

По существу данное трактование отождествляет понятия экономической безопасности с понятием адаптации к текущим условиям, и тем самым теряется видение перспектив его развития.

3. Автор А.В. Иванов в своей работе трактует понятие экономической безопасности следующим образом: «Экономическая безопасность - количественная и качественная характеристика свойств фирмы, отражающая способность самовыживания и развития в условиях возникновения внешней и внутренней угрозы. Экономическая безопасность организации определяется совокупностью факторов, отражающих независимость, устойчивость, возможности роста, обеспечения экономических интересов и т. д.» [21]. При таком рассмотрении создается мнение, что предприятие и угрозы его деятельности являются разрозненными явлениями, не связанными между собой по своей природе. Реально же угрозы возникают в той же среде, в которой функционирует и само предприятие.

4. В рамках подхода к экономической безопасности организации как состоянию, определяемому влиянием внешней среды, следует отметить ресурсно-функциональный подход. Автор этого подхода Е. А. Олейников рассматривает экономическую безопасность организации как: «экономическая безопасность организации - состояние наиболее эффективного использования корпоративных ресурсов для предотвращения угроз и обеспечения стабильного функционирования организации в настоящее время и в будущем. В данном подходе в качестве основных направлений экономической безопасности организации различают семь функциональных составляющих: интеллектуально-кадровую, финансовую, технико-технологическую, политико-правовую, экологическую, информационную и силовую. Изучение сущности ресурсно-функционального подхо-

да к пониманию экономической безопасности организации позволяет отметить его основное достоинство — всеобъемлющий, комплексный характер, поскольку в рамках этого подхода исследуются важнейшие факторы, влияющие на состояние функциональной составляющей экономической безопасности организации, изучаются основные процессы, влияющие на ее обеспечение, проводится анализ распределения и использования ресурсов организации, рассматриваются экономические индикаторы, отражающие уровень обеспечения функциональной составляющей экономической безопасности организации, и разрабатываются меры по обеспечению максимально высокого уровня функциональной составляющей экономической безопасности организации» [28].

5. Отдельно следует сказать о подходах к экономической безопасности организации, которые можно назвать узкофункциональными, т. е. рассматриваемые с позиции отдельного аспекта его деятельности.

В этом подходе в качестве основной функции управления, направленной на обеспечение экономической безопасности, признается учет, поскольку именно учет создает информационные условия для эффективного использования ресурсов, предотвращения угроз и финансовой безопасности организации.

Однако, отсутствие возможности объединить узкофункциональные направления, снижают результативность данного подхода.

Анализ рассмотренных подходов к проблеме экономической безопасности организации позволяет сделать следующие выводы:

- экономическая безопасность организации складывается из нескольких функциональных составляющих, которые для каждой конкретной организации могут иметь различные приоритеты в зависимости от характера существующих угроз.

- основным фактором, определяющим состояние экономической безопасности является обладание предприятием устойчивыми конкурентными преимуществами. Эти преимущества должны соответствовать стратегическим целям организации и обеспечивать экономическую состоятельность организации.

- экономическая состоятельность является отражением отношений между хозяйствующими субъектами, позволяющими им эффективно существовать в бизнесе и адаптироваться к условиям внешней среды (признаки рыночной состоятельности), оптимально использовать производственный потенциал (признаки по показателям производственной состоятельности), обеспечивать сбалансированность внешнего и внутреннего равновесия (признаки финансовой состоятельности).

На основании сделанных выводов можно сформулировать наиболее общее определение: экономическая безопасность организации - это наличие конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического потенциалов и организационной структуры организации его стратегическим целям и задачам. Данное определение подчеркивает тот факт, что экономическая безопасность находится на стыке экономики и безопасности организации.

Исходя из данного выше определения, следует выделить основные функциональные блоки системы экономической безопасности организации, обеспечивающие максимальное соответствие менеджмента организации и его ресурсного потенциала:

-финансовая составляющая;

-информационная составляющая;

-технико-технологическая составляющая;

-кадровая составляющая;

-правовая составляющая.

Автор Т.А. Полякова пишет о финансовой составляющей следующее: «Финансовая составляющая экономической безопасности организации может быть определена как совокупность работ по обеспечению максимально высокого уровня, наиболее эффективной структуры капитала организации, повышению качества планирования и осуществления финансово-хозяйственной деятельности организации по всем направлениям стратегического, оперативного планирования и управления технологическим, интеллектуальным и кадровым

потенциалом организации, ее основным капиталом и оборотными активами с целью максимизации прибыли и повышения рентабельности бизнеса» [30]. Также автор отмечает: «Финансовая безопасность организации определяется как состояние наиболее эффективного использования корпоративных ресурсов организации, выраженное в наилучших значениях финансовых показателей прибыльности и рентабельности бизнеса, качества управления и использования основных и оборотных средств, структуры его капитала, нормы дивидендных выплат по ценным бумагам организации, а также курсовой стоимости его ценных бумаг как синтетического индикатора текущего финансово-хозяйственного положения организации и перспектив его технологического и финансового развития, процесс обеспечения финансовой составляющей экономической безопасности организации необходимо рассматривать как процесс предотвращения всесторонних ущербов от негативных воздействий на экономическую безопасность организации по различным аспектам ее финансово-хозяйственной деятельности» [30].

Негативные воздействия, угрожающие ущербом финансовой составляющей экономической безопасности организации подразделяют на два типа воздействий:

- группы внешних и внутренних негативных воздействий, движущей силой и основной причиной возникновения которых являются осознанные вредоносные действия людей или предприятий, либо некачественная работа сотрудников организации или ее партнеров;
- группы негативных воздействий, причиной которых являются обстоятельства непреодолимой силы или сходные с ними по своей сущности и источникам возникновения обстоятельства политического, макроэкономического характера, экономические, национальные, религиозные и другие проблемы, причинами которых стали те или иные стечения обстоятельств, не связанных напрямую с деятельностью данной организации и не вызванные действиями людей или организациими, так или иначе связанных с работой организации [9].

Информационная составляющая. Важной составляющей экономической безопасности организации является информация. Информация, касающаяся всех сторон деятельности организации, является в настоящее время наиболее ценным и дорогостоящим из ресурсов организации. Информация об изменении политической, социальной, экономической ситуации, научно-техническая информация, новое в методах организации и управления предприятием позволяют ему адекватно реагировать на любые изменения внешней среды, эффективно планировать и осуществлять свою хозяйственную деятельность. Наиболее актуальным в настоящее время является высказывание У.Черчилля: «Кто владеет информацией – тот владеет миром». Это на самом деле именно так. В условиях нестабильности экономической конъюнктуры возникает острая необходимость в том, чтобы знать, какая финансовая ситуация на мировых рынках сложится завтра. Организация, владеющая такого рода информацией, сможет правильно спланировать свое дальнейшее развитие, повысить устойчивость к уже предвиденным, заранее обозначенным неблагоприятным факторам. С большой осторожностью нужно подходить к защите информации. Риск потери конфиденциальной информации для компаний существенно возрастает в период финансового кризиса. Планируя переход в конкурирующую компанию, сотрудники умышленно или непреднамеренно забирают с собой данные о внутренних процедурах, условиях договоров и клиентах. В текущих рыночных условиях, когда компании могут столкнуться с необходимостью снижения расходов посредством сокращения штата, повышается риск, что сотрудники будут стремиться воспользоваться этим «преимуществом», пытаясь найти работу при сложившихся обстоятельствах.

Технико-технологическая составляющая. Каждое предприятие характеризуется набором технологий материального или интеллектуального производства, которые используются в работе. Качество этих технологий и их соответствие новейшим мировым стандартам кардинальным образом влияют на эффективность деятельности организации и на перспективы его дальнейшего развития, а следовательно, и на обеспечение экономической безопасности. Основ-

ная сущность технико-технологической составляющей заключается в том, насколько уровень используемых на данном предприятии технологий соответствует лучшим мировым образцам. В настоящий момент, когда организации начинают экономить буквально на всем, покупка новых технологий, модернизация производства, качественное усовершенствование отдельных составляющих откладывается на неопределенный срок. Вместе с тем, хотелось бы еще раз отметить, что высокотехнологичное оборудование, интеллектуальные технологии – важные факторы для достижения эффективного производства.

Кадровая составляющая. Кадры организации - одна из основных составляющих экономической безопасности организации. Группа менеджеров, обладающих достаточной квалификацией и профессионализмом, способна реорганизовать убыточное предприятие и, наоборот, не грамотное управление, ненадлежащее исполнение обязанностей, отсутствие дисциплины с большой долей вероятности приведут прибыльное предприятие к банкротству. Обеспечение кадровой безопасности включает в себя следующие элементы: работу по планированию, подбору и управлению сотрудников организации, предотвращению и предупреждению угроз негативных воздействий на экономическую безопасность организации за счет недостаточной квалификации сотрудников организации, исключению предпосылок к появлению неблагонадежных сотрудников.

Правовая составляющая. Значение правовой составляющей экономической безопасности организации состоит в эффективном и всестороннем правовом обеспечении деятельности организации, четком соблюдении предприятием и его сотрудниками всех правовых норм действующего законодательства при оптимизации затрат корпоративных ресурсов на достижение этих целей. Внешние воздействия на правовую составляющую экономической безопасности организации – это изменение норм действующего законодательства [17].

Данная структура функциональных составляющих соответствует структуре механизма обеспечения экономической безопасности организации и затрагивает все функциональные области деятельности организации: инновационную, ресурсную, инвестиционную, маркетинговую, их цели должны корре-

спондироваться со стратегическими интересами организации в рассматриваемой функциональной области деятельности, а показатели, характеризующие цели стратегии, должны соответствовать количественной оценке стратегических интересов организации. Установление такого соответствия является очень важным, поскольку именно с его помощью обеспечивается единство методической базы организации управления предприятием.

Для каждой современной организации, компании или организации одной из самых главных задач является именно обеспечение информационной безопасности. Когда предприятие стабильно защищает свою информационную систему, оно создает надежную и безопасную среду для своей деятельности. Повреждение, утечка, неимение и кража информации — это всегда убытки для каждой компании. Например, могут появиться убытки от плохой репутации компании, от отсутствия клиентов, от затрат на возобновление стабильной работы или от потери важной информации, которой располагала данная компания.

1.2 Характеристика и сущность информационной составляющей экономической безопасности организации

В настоящее время информация очень часто рассматривается как наиболее ценный ресурс. Это неудивительно, так как в современном компьютеризированном мире наиболее эффективные конкурентные преимущества фирма может получить в основном за счет обладания уникальной информацией, будь то новейшие технологические разработки, необходимые для успеха на развивающемся рынке мобильных устройств, или данные о предпочтениях интернет-пользователей, имеющие огромную ценность для эффективной целевой рекламы. Кроме того, информация ограниченного доступа (например, персональные данные клиентов) всегда представляла ценность для её обладателей и вызывала интерес со стороны злоумышленников.

Ещё одной причиной актуальности проблемы обеспечения информационной безопасности является повсеместное использования автоматизированных средств хранения, передачи и обработки информации.

Именно поэтому информационной безопасности в последнее время уделяется все больше внимания: высший менеджмент предприятий различных сфер деятельности готов тратить все больше сил и средств на создание и развитие системы защиты информации, а также системы менеджмента ИБ. Стоит заметить, что формирование режима информационной безопасности является комплексной задачей и осуществляется на трёх уровнях: законодательно-правовом, административном (организационном) и программно-техническом, поэтому для достижения поставленной цели требуется большое количество материальных и человеческих ресурсов [19].

Для того чтобы не возникло искажений в восприятии и интерпретации тех или иных понятий, используемых в данной работе, введем определения наиболее часто встречающихся из них:

"Информационная безопасность (ИБ) – сохранение конфиденциальности, целостности и доступности информации; кроме того, другие свойства, такие как аутентичность, учетность, неотказуемость и надежность, также могут охватываться".

"Доступность – характеристика, определяющая доступность и используемость по запросу со стороны авторизованного логического объекта".

"Конфиденциальность – характеристика, определяющая, что информация не может быть доступной и раскрытой не авторизованным индивидуумом, логическим объектом или процессом".

"Целостность – свойство сохранения правильности и полноты активов".

"Система информационной безопасности (СИБ) – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение".

"Риск информационной безопасности – это потенциальная возможность понести убытки из-за нарушения безопасности информационной системы" [2].

Риск можно охарактеризовать следующими параметрами:

- угроза, возможной реализацией которой вызван данный риск;
- ресурс, в отношении которого может быть реализована данная угроза;
- уязвимость, через которую может быть реализована данная угроза в отношении данного ресурса.

"Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему. Лица, преднамеренно реализующие угрозы, являются злоумышленниками."

Уязвимость – это так называемое "слабое место" в системе защиты информации, которое является основанием для возникновения угрозы со стороны злоумышленников.

Активы – все, что представляет ценность для данной организации. Существует актив информационный (данные и другая ценная информация, хранящаяся в цифровой форме: транзакции, платежи, и т.д.), аппаратный (например, серверы и имущество), программный и т.д.

"Информационный актив – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации БС РФ; находящаяся в распоряжении организации БС РФ и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме"[3].

Как известно, анализ и оценка рисков ИБ проводится для получения следующей информации:

- какие риски информационной безопасности существуют в организации;
- какова вероятность их реализации;
- какой ущерб будет нанесен в результате их реализации;
- какие риски компания может принять (на основе критериев принятия риска);
- какие средства защиты являются наиболее адекватными для борьбы с той или иной уязвимостью в СИБ;
- какой объем денежных средств должен быть в резерве на случай возникновения инцидента информационной безопасности и т.д. [23]

Существует несколько стандартов, в которых описываются требования к построению систем менеджмента информационной безопасности. Это такие документы, как ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО/МЭК 17799. В обоих из них содержится информация о правилах и порядке проведения анализа и оценки рисков информационной безопасности. Так, по ГОСТ Р ИСО/МЭК 27001 порядок работы с рисками следующий [2].

1. "Идентификация рисков:

- идентифицировать активы, относящиеся к области применения СМИБ, и определить собственников этих активов;
- идентифицировать угрозы этим активам;
- идентифицировать уязвимости, которые могут быть использованы этими угрозами;
- идентифицировать возможные воздействия, которые могут привести к утрате конфиденциальности, целостности и доступности активов.

2. Анализ и оценка риска:

- оценить ущерб бизнесу, который может быть нанесен в результате нарушения безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов;
- оценить реальную вероятность возникновения такого нарушения безопасности в свете превалирующих угроз и уязвимостей, воздействия на соответствующие активы, а также применяемые меры контроля;
- оценить уровни рисков;
- определить, является ли риск приемлемым или требуется обработка риска с использованием определенных критериев".

Очевидно, что данные рекомендации – это примерный и очень общий план действий по управлению рисками информационной безопасности, не позволяющий, следуя ему, эффективно оценить риски ИБ в крупной компании. Так как государственных стандартов недостаточно, широкое применение приобретают методики, разрабатываемые частными компаниями, такие как Lifecycle Security или методика Microsoft [2].

В процессе выбора, какому банку доверить свои финансы и операции над ними, человек оценивает различные варианты кредитных организаций по нескольким основным критериям: надежность, скорость обслуживания, удобство предоставляемых сервисов, выгодность условий предлагаемых продуктов и т.д. При этом считается, что надежность банка, подразумевающая снижение рисков, как финансовых, так и риска утечки персональных данных, является одним из основных критериев при выборе финансового партнера для большинства потенциальных клиентов.

Как было сказано ранее, банковское законодательство, а именно Федеральный Закон "О банках и банковской деятельности", обязывает все кредитные организации Российской Федерации "защищать сведения о вкладах и счетах своих клиентов и корреспондентов, банковских операциях по счетам и сделках в интересах клиента, а также сведения клиентов, разглашение которых может нарушить право последних на неприкосновенность частной жизни"[1].

Из вышесказанного следует, что банкам необходимо поддерживать систему информационной безопасности на должном уровне, достаточном для того, чтобы не только гарантировать сохранение банковской тайны, но и оставаться привлекательными для потенциальных клиентов за счет повышенной заботы о предотвращении разглашения персональных данных своих вкладчиков и заемщиков так же, как и о надежности их финансовых вложений.

Крайне важным документом, дающим рекомендации по построению системы менеджмента информационной безопасности на предприятиях банковского сектора Российской Федерации, является стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения". Первая версия стандарта была опубликована на сайте Центрального Банка еще в 2010 году.

В нем отмечается, что основными целями стандартизации по обеспечению ИБ организаций банковской системы РФ являются развитие и укрепление БС РФ, повышение к ней доверия, поддержание стабильности

кредитных организаций, достижение адекватности мер защиты реальным угрозам ИБ, а также предотвращение и (или) снижение ущерба от инцидентов ИБ. Для достижения поставленных целей необходимо установление единых требований и повышение эффективности мероприятий по обеспечению и поддержанию ИБ организаций банковской сферы РФ [25].

Данный стандарт определяет требования к выбору/коррекции подхода к оценке рисков нарушения ИБ, проведению оценки рисков нарушения ИБ и к разработке планов обработки рисков нарушения ИБ. В частности, устанавливается необходимость принятия на предприятии методики оценки рисков нарушения ИБ, определения критериев принятия рисков нарушения ИБ и уровня допустимого риска нарушения ИБ, а также перечисляются некоторые общие и при этом обязательные характеристики используемой методики.

Из теории о рисках информационной безопасности нам известно, что существует четыре варианта их обработки:

- перенос риска на сторонние организации (например, страхование риска);
- уход от риска (например, в результате отказа от деятельности, выполнение которой приводит к появлению риска);
- осознанное принятие риска;
- формирование требований по обеспечению ИБ, снижающих риск нарушения ИБ до допустимого уровня, и формирование планов по их реализации [7].

Вышеупомянутый стандарт законодательно закрепляет данные меры, а также определяет некоторые дополнительные условия разработки планов обработки рисков ИБ.

В 2009 году Центральным Банком Российской Федерации была разработана методика оценки рисков нарушения информационной безопасности для организаций банковской системы РФ. Данный документ учитывает особенности структуры и деятельности кредитных организаций и является хорошим вариантом методики анализа и оценки рисков ИБ для кредитных организаций, однако носит лишь рекомендательный характер. Он включает в себя не только конкретный алгоритм качественной и

количественной оценки, но и описание общего подхода к анализу рисков нарушения информационной безопасности банка. Кроме того, в приложениях можно найти рекомендуемый перечень классов, основных источников угроз ИБ и их описание, а также примерные формы документов, используемых в процессе анализа и оценки рисков ИБ.

Создание и функционирование любой организации представляет собой процесс инвестирования финансовых ресурсов на долгосрочной основе с целью извлечения прибыли. Процесс управления активами (имущественным потенциалом) также направлен на возрастание прибыли и характеризуется понятием операционно-финансового рычага, для которого характерна взаимосвязь экономических показателей: выручки, расходов производственного и финансового характера и чистой прибыли. Оптимальность этой связи обеспечивает запас финансовой прочности и является фактором экономической безопасности организации.

Бизнес-процесс организации связан с операционной деятельностью, бухгалтерским учетом, управлением финансами и кадрами, существенная роль в которых принадлежит информационным технологиям (совокупность вычислительных и информационных систем, средств связи, программ и т. п.), позволяющим решить эту задачу оптимальным способом, но требующим материальных и временных затрат на ее внедрение. Таким образом бизнес-процесс организации зависит от работоспособности информационной системы, а для потребителя безопасность внедряемых информационных технологий — это проблема, связанная с обеспечением их правильного и бесперебойного функционирования [10].

Информационная система организации, как правило, охватывает все сферы его деятельности: административную, производственную, финансовую, выступает как связующее звено при выработке стратегии бизнеса и качества управления предприятием и персоналом. В ней содержатся сведения, касающиеся планов, состояния материальных и финансовых потоков, договорной деятельности, данные финансового и управленческого учета. Такого рода коммер-

ческая информация носит сугубо конфиденциальный характер, а ее утрата может оказаться критичной для работы всей организации, поэтому организация работы пользователей с содержащейся в системе информацией требует специальных мер защиты, обеспечивающих конфиденциальность, целостность и доступность данных.

Цель информационной безопасности — выявить возможные угрозы безопасности информации, определить их последствия и возможный ущерб, обеспечить необходимые меры и средства защиты, и оценить их эффективность.

Поскольку анализ всей информационной инфраструктуры далеко не всегда оправдан с экономической точки зрения, целесообразно сосредоточиться на наиболее важных, одновременно выявляя не только сами угрозы, вероятность из осуществления, размер потенциального ущерба, но и их источники [5].

Зяброва Н.П. в своей работе выделяет следующие основные функции информационно-аналитического подразделения организации: «Сбор всех видов информации, имеющей отношение к деятельности данной организации: Информация по товарным, технологическим, трудовым, финансовым и другим рынкам, на которых работает данная организация или ситуация на которых может иметь отношение к деятельности в будущем, с конкретизацией по направлениям деятельности организации; Научно-техническая информация, анализ которой позволяет выделить направления повышения эффективности деятельности организации; Информация по политическим событиям и тенденциям макроэкономического развития мировой и национальных экономик. Анализ полученной информации включает в себя: Систематизацию и классификацию получаемой информации. Данные процессы можно выделить как основополагающие для эффективного функционирования информационно-аналитических подразделений; Постоянную аналитическую деятельность; непрерывный процесс обработки и анализа получаемой информации придает потоку информации свойства исходного материала для статического, логического, сравнительного и ситуационного анализа; Всесторонний характер аналитических процессов в организации. Прогнозирование тенденций развития научного и технологического

процесса в сферах технологической деятельности организации, экономических и политических процессов в стране и за рубежом, имеющих отношение к данному бизнесу, а также показателей, которых необходимо достичь организации во всех областях своей деятельности. Оценка уровня экономической безопасности организации по всем ее составляющим и в целом, выработка рекомендаций по повышению уровня экономической безопасности. Прочие виды деятельности по обеспечению информационной составляющей экономической безопасности организации: Деятельность службы по связям с общественностью, в обязанности которой входит доведение до сведения общества информации о деятельности данной организации. Работа по созданию благоприятного имиджа организации в глазах общественного мнения и распространение выгодной организации информации среди конкурентов и партнеров по рынку является важной сферой деятельности; Защита от несанкционированного доступа к конфиденциальной информации организации (защита от промышленного шпионажа)» [20].

При этом все более очевидной становится зависимость общего уровня экономической безопасности организации от ее информационной составляющей. Практика показывает, что любая целенаправленная недружественная акция, направленная против интересов хозяйствующего субъекта, начинается со сбора информации: даже мелкие хищения обычно предваряет изучение лицом с преступными замыслами возможности противоправных действий, и уж конечно без соответствующего информационного обеспечения не мыслимы такие деструктивные проявления как увод активов организации или рейдерские захваты.

Ухудшение таких параметров информации (информационных ресурсов), как конфиденциальность, целостность, доступность, достоверность и др., может привести к весьма негативным последствиям: сбоям в функционировании систем управления технологическими процессами и других критических систем; к разглашению сведений, составляющих коммерческую тайну и другие виды тайн; к нарушению достоверности финансовой документации; к несанкциони-

рованному доступу к персональным данным физических лиц и т.д. Результатом перечисленного могут стать: разрыв (или ухудшение) деловых отношений с партнерами; срыв переговоров, потеря выгодных контрактов; невыполнение договорных обязательств; необходимость проведения дополнительных рыночных исследований; отказ от решений, ставших неэффективными из-за огласки информации, и, как следствие, финансовые потери, связанные с новыми разработками; потеря возможности запатентовать результат научно-технической деятельности или продать лицензию; снижение цен или объемов реализации; ущерб авторитету или деловой репутации фирмы; более жесткие условия получения кредитов; трудности в снабжении и приобретении оборудования и т.д. В определенных ситуациях пренебрежение вопросами защиты информации может, как уже отмечалось, привести и к полной потере бизнеса.

Действующее российское законодательство содержит базовые правовые нормы, позволяющие реализовать корпоративные системы защиты информации.

Так, Федеральным законом от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» установлено: «Обладатель информации, наряду с прочим, если иное не предусмотрено федеральными законами, вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа, а также защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами»[1]. Ст. 16 указанного закона определено: «Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации»[1].

Одним из важнейших видов деятельности по обеспечению информационной безопасности организации является выявление, оценка и предотвращение угроз информационным системам и информационным ресурсам. Указанные угрозы можно условно разделить на четыре основные группы:

программные - внедрение «вирусов», аппаратных и программных закладок; уничтожение и модификация данных в информационных системах;

технические, в т.ч. радиоэлектронные, - перехват информации в линиях связи; радиоэлектронное подавление сигнала в линиях связи и системах управления;

физические - уничтожение средств обработки и носителей информации;

режимные - нарушение регламентов информационного обмена; незаконные сбор и использование информации; несанкционированный доступ к информационным ресурсам; незаконное копирование данных в информационных системах; хищение носителей, а также аппаратных или программных парольных ключей; дезинформация, сокрытие или искажение информации; хищение информации из баз данных.

Вопрос анализа угроз и рисков является определяющим при построении эффективной системы защиты информации. Однако, по оценкам специалистов, лишь не более 7 % компаний используют собственные ("углубленные") методики анализа рисков, которые позволяют выполнять количественный анализ и оптимизацию подсистемы информационной безопасности.

Самыми популяризированными угрозами информационной безопасности являются хакерские атаки, вирусные эпидемии и спам. Как правило, если функции обеспечения информационной безопасности организации фактически возлагаются на системных и прикладных администраторов ИТ подразделений, именно на борьбу с негативными явлениями такого рода они и ориентируют руководство.

В то же время, действия внутренних нарушителей, такие как халатность сотрудников, кражи информационных ресурсов и ИТ оборудования, финансовое и иные виды мошенничества с использованием корпоративных информационных систем и ресурсов и т.д., гораздо реже становятся предметом внима-

ния при решении проблем информационной безопасности в случае, если они рассматриваются в отрыве от общих задач обеспечения экономической безопасности организации. Результаты исследований показывают, что большинство компаний не предпринимают достаточных мер по защите от действий инсайдеров. Например, только 1 % опрошенных Infowatch компаний внедряет средства по защите от утечки информации. Эти данные подтверждаются и компанией КРОК на основе проведения аудита систем информационной безопасности.

В современном представлении ролевых функций службы информационной безопасности можно выделить четыре направления:

- разработка методологии и методик анализа угроз, оценки уровня информационной безопасности организации и корпоративных стандартов системы ее обеспечения;
- организация и осуществление конкретных видов деятельности по защите информации;
- эксплуатация технических средств защиты информации;
- аудит и контроль функционирования системы информационной безопасности организации [22].

Учитывая междисциплинарный характер вопросов, входящих в блок информационной безопасности, некоторые из перечисленных функций могут исполняться только совместно с другими структурными подразделениями организации (подразделениями ИТ, службой по работе с персоналом, юридической, хозяйственной службой и т.д.).

Из различных организационных схем функционирования подразделений, отвечающих за информационную безопасность организации (функции такого подразделения возлагаются на системных и прикладных администраторов; указанное подразделение находится в структуре ИТ службы, службы экономической безопасности организации, или же является самостоятельной структурной единицей компании, подчиняющейся высшему руководству), наиболее предпочтительным представляется вариант, при котором подразделение информаци-

онной безопасности входит в состав службы экономической безопасности организации. Именно в этом случае создаются наилучшие возможности решения проблем информационной безопасности в контексте общих задач безопасности бизнеса [8].

Резюмируя, отметим, что в современных условиях информационная безопасность является неотъемлемой составляющей системы экономической безопасности хозяйствующего субъекта. В свою очередь, надежное обеспечение экономической безопасности является непременным условием перехода на модель устойчивого развития не только отдельной организации, но и национальной экономики в целом.

2 Основные подходы к анализу и оценке информационной составляющей экономической безопасности кредитной организации

2.1 Обзор методик анализа и оценки рисков информационной безопасности

Процесс анализа и оценки рисков является одним из ключевых этапов наиболее известных методик построения систем защиты информации, таких как Symantec Lifecycle Security и методика компании Microsoft. Кроме того, существуют специализированные методики и программные продукты для анализа и оценки рисков, такие как CRAMM, FRAP, RiskWatch, ГРИФ и др. Опишем наиболее известные из них, чтобы получить правильное представление об особенностях каждой из методик для последующего выбора наиболее подходящей для применения в компаниях банковской сферы.

Symantec Lifecycle Security – это модель, описывающая такой способ организации системы информационной безопасности предприятия, который позволяет системно решать задачи, связанные с защитой информации, и предоставляет возможность адекватно оценить результат применения технических и организационных средств и мер защиты информации (Петренко, 2009). Данная методика включает в себя семь основных компонентов:

1. политики безопасности, стандарты, процедуры и метрики;
2. анализ рисков;
3. стратегический план построения системы защиты;
4. выбор и внедрение решений;
5. обучение персонала;
6. мониторинг защиты;
7. разработка методов реагирования в случае инцидентов и восстановление.

Так как в данной работе рассматривается проблема анализа и оценки рисков информационной безопасности, сосредоточим свое внимание на этом этапе жизненного цикла СИБ. Ниже представлены ключевые моменты процесса анализа рисков модели Symantec Lifecycle Security.

1. Подробное документирование компьютерной системы предприятия с акцентом на описание критически важных для деятельности предприятия приложений.
2. Определение степени зависимости нормального функционирования организации от исправности отдельных частей компьютерной сети, конкретных узлов, от безопасности хранимых и обрабатываемых данных.
3. Поиск уязвимых мест компьютерной системы предприятия.
4. Поиск угроз, которые могут быть реализованы в отношении выявленных уязвимых мест.
5. Поиск и оценка рисков, связанных с использованием компьютерной системы предприятия.

Еще одним широко известным способом построения комплексной системы защиты информации на предприятии является методика, разработанная компанией Microsoft. Она включает в себя модель управления рисками информационной безопасности компании. Весь цикл управления рисками можно разделить на четыре основных стадии.

1. Оценка рисков.

- Планирование сбора данных, обсуждение ключевых условий успешной реализации и подготовка рекомендаций.
- Сбор данных о рисках и его документирование.
- Определение значимости рисков. Описание последовательности действий по качественной и количественной оценке рисков.

2. Поддержка принятия решений.

- Определение функциональных требований.
- Выбор подходящих элементов контроля.

- Проверка предложенных элементов контроля на соответствие функциональным требованиям.
- Оценка снижения рисков.
- Оценка прямых и косвенных затрат, связанных с внедрением элементов контроля.
- Определение наиболее экономически эффективного решения по нейтрализации риска путем анализа выгод и затрат.

3. Реализация контроля. Развертывание и использование элементов контроля, снижающих риск для ИБ организации.

- Поиск целостного подхода.
- Организация многоуровневой защиты.

4. Оценка эффективности программы. Анализ эффективности процесса управления рисками, проверка выбранных элементов контроля на соответствие необходимому уровню защиты.

- Разработка системы показателей рисков.
- Оценка эффективности программы управления рисками и выявление возможностей её улучшения.

Остановимся подробнее на первой стадии. Следует отметить, что этапы качественной оценки рисков обычно примерно одинаковы: выявление рисков ИБ, определение вероятности возникновения каждого из них, определение стоимости активов, которые пострадают от реализации конкретного риска, а также распределение описанных рисков на группы в зависимости от ранее оговоренных критериев значительности риска, а также возможности его принятия. Так и в данной методике на начальном этапе рискам присваиваются значения в соответствии со шкалой: "высокий" (красная область), "существенный" (жёлтая область), "умеренный" (синяя область) и "незначительный" (зеленая область). После этого, при необходимости выявленных наиболее существенных рисков и подсчета финансовых показателей, проводится количественная оценка.

Для проведения эффективной оценки требуется собрать самые актуальные данные об активах организации, угрозах безопасности, уязвимостях, текущей среде контроля и предлагаемых элементах контроля. Далее проводится сложный и многоступенчатый процесс анализа и оценки рисков, в результате которого владельцы бизнеса получают информацию не только о существующих рисках, вероятностях их реализации, уровнях влияния на деятельность компании, но и оценку ожидаемого годового ущерба (ALE).

Здесь также стоит упомянуть о существовании средства оценки безопасности "Microsoft Security Assessment Tool (MSAT)", который представляет собой бесплатное программное обеспечение, позволяющее "оценить уязвимости в ИТ-средах, предоставить список расставленных по приоритетам проблем и список рекомендаций по минимизации этих угроз".

Процесс анализа информационной сети на наличие в ней уязвимостей осуществляется с помощью ответов более чем на 200 вопросов, "охватывающих инфраструктуру, приложения, операции и персонал". Первая серия вопросов предназначена для определения бизнес-модели компании, на основе полученных ответов средство создает "профиль бизнес-риска (BRP)". По результатам ответа на вторую серию вопросов составляется список защитных мер, внедренных компанией с течением времени. В совокупности эти меры безопасности "образуют уровни защиты, предоставляя большую защищенность от угроз безопасности и конкретных уязвимостей". Сумма уровней, образующих "комбинированную систему глубокой защиты", называется "индексом глубокой защиты (DiDI)". После этого BRP и DiDI сравниваются между собой для измерения распределения угроз по областям анализа — инфраструктуре, приложениям, операциям и людям.

Данная оценка предназначена для использования в организациях среднего размера, "содержащих от 50 до 1500 настольных систем". В результате её использования менеджмент компании получает общую информацию о состоянии системы защиты информации предприятия, охватывая большинство "областей потенциального риска", но описываемое

средство не предусмотрено для предоставления "глубокого анализа конкретных технологий или процессов".

Методика "CCTA Risk Analysis and Management Method (CRAMM)" – одна из первых методик анализа рисков в сфере информационной безопасности. В основе метода CRAMM лежит комплексный подход, сочетающий процедуры количественной и качественной оценки рисков.

Исследование информационной безопасности системы с помощью CRAMM может проводиться двумя способами, преследующими две качественно разные цели: обеспечение базового уровня ИБ и проведение полного анализа рисков. От того, какая задача стоит перед специалистами по оценке рисков, зависит количество проводимых этапов работы. Перечислим все возможности данной методики, делая акцент на обстоятельствах применения той или иной процедуры анализа.

Первая стадия является подготовительной и обязательной при постановке любой из двух возможных целей исследования информационной безопасности системы. Во время данного этапа формально определяются границы рассматриваемой информационной системы, ее основные функции, категории пользователей и персонала, принимающего участие в исследовании.

На второй стадии проводится анализ всего, что касается выявления и определения ценности ресурсов рассматриваемой системы: проводится идентификация физических, программных и информационных ресурсов, находящихся внутри границ системы, а затем производится распределение их на заранее выделенные классы. В результате заказчик имеет хорошее представление о состоянии системы и может принять решение о необходимости проведения полного анализа рисков. При условии, что обеспечения базового уровня ИБ клиенту не достаточно, строится модель информационной системы с позиции ИБ, которая позволит выделить наиболее критичные элементы.

На третьей стадии, которая проводится только в том случае, если необходимо проведение полного анализа рисков, рассматривается все, что

относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. На данном этапе оценивается влияние определенных групп ресурсов на работоспособность пользовательских сервисов, определяется текущий уровень угроз и уязвимостей, вычисляются уровни рисков, и проводится анализ результатов. В итоге заказчик получает идентифицированные и оцененные уровни рисков ИБ для исследуемой системы.

На четвертой стадии для каждой группы ресурсов и каждого из 36 типов угроз программное обеспечение CRAMM составляет список вопросов, предполагающих однозначный ответ. Как и в случае с методикой компании Microsoft, в CRAMM проводится качественная оценка риска путем отнесения уровней угроз к той или иной категории в зависимости от полученных ответов. Всего в данной методике есть пять категорий уровней угроз: "очень высокий", "высокий", "средний", "низкий" и "очень низкий". В свою очередь, уровень уязвимости ресурса оценивается, в зависимости от ответов, как "высокий", "средний" и "низкий". На основе данной информации, а также размеров ожидаемых финансовых потерь, рассчитываются уровни рисков по шкале от 1 до 7, объединенные в матрице оценки риска (рис.1).

Threat	Very Low	Very Low	Very Low	Low	Low	Low	Medium	Medium	Medium	High	High	High	Very High	Very High	Very High
Vuln.	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High	Low	Medium	High
Asset Value															
1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	3
2	1	1	2	1	2	2	2	3	3	2	3	3	3	3	4
3	1	2	2	2	2	3	2	3	3	3	3	4	3	4	4
4	2	2	3	2	3	3	3	3	4	3	4	4	4	4	5
5	2	3	3	3	3	4	3	4	4	4	4	5	4	5	5
6	3	3	4	3	4	4	4	4	5	4	5	5	5	5	6
7	3	4	4	4	4	5	4	5	5	5	5	6	5	6	6
8	4	4	5	4	5	5	5	5	6	5	6	6	6	6	7
9	4	5	5	5	5	6	5	6	6	6	6	7	7	7	7
10	5	5	6	5	6	6	6	6	6	6	7	7	7	7	7

Рисунок 1 - Матрица оценки риска в методике CRAMM

Здесь следует отметить, что метод CRAMM по праву может быть отнесен к методикам, использующим как качественный, так и количественный подходы к анализу рисков информационной безопасности, так как в процессе

проведения оценки учитывается уровень ожидаемых финансовых потерь от реализации риска, а результаты предоставляются в баллах по шкале от 1 до 7. Этот факт значительно повышает рейтинг методики CRAMM в глазах специалистов в данной предметной области.

На последней стадии исследования, носящей название "Управление рисками", производится выбор адекватных элементов контроля: программное обеспечение CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням, из которых выбирается оптимальный вариант системы безопасности, удовлетворяющий требованиям заказчика.

Методика "Facilitated Risk Analysis Process (FRAP)" – это модель построения системы защиты информации, включающая в себя качественный анализ рисков. Разберем именно эту, интересующую нас, составляющую методики. Ниже приведены основные этапы оценки рисков.

1. На первом этапе, с опорой на данные опросов, техническую документацию, автоматизированный анализ сетей, составляется список находящихся в зоне риска активов.
2. Идентификация угроз. При составлении списка угроз могут использоваться различные подходы:

- Конвенциональный метод. В этом случае, эксперты составляют перечни (checklists) потенциальных угроз, из которых впоследствии выбираются наиболее актуальные для данной системы;
- Статистический. Здесь проводится анализ статистики происшествий, связанных с информационной безопасностью данной ИС и подобных ей, и оценивается их средняя частота, после чего производится оценка точек риска;
- "Мозговой штурм", проводимый сотрудниками компании. Отличие от первого метода в том, что он проводится без привлечения внешних экспертов.

3. После составления списка потенциальных угроз производится сбор статистики по каждому случаю возникновения риска: частоте той или иной ситуации, а также по уровню претерпеваемого ущерба. Опираясь на эти

значения, эксперты оценивают уровень угрозы по обоим параметрам: вероятности возникновения угрозы (High Probability, Medium Probability and Low Probability) и ущерба от нее (High Impact, Medium Impact and Low Impact). Далее, в соответствии с правилом, задаваемым матрицей рисков (рис.4), определяется оценка уровня риска:

- уровень A – направленные на элиминацию угрозы меры (например, внедрение СЗИ) должны быть предприняты немедленно и в обязательном порядке;
- уровень B – необходимо предпринять меры, направленные на снижение риска;
- уровень C – необходим мониторинг ситуации;
- уровень D – никаких действий в данный момент предпринимать не требуется.

4. После того как угрозы были идентифицированы и относительные риски оценены, следует составить план действий, позволяющий устранить риск или уменьшить его до приемлемого уровня.
5. По окончании оценки рисков результаты должны быть подробно документированы и переведены в стандартизованный формат. Эти данные могут быть использованы при планировании дальнейших процедур в области обеспечения безопасности, бюджета, выделяемого на эти процедуры, и т.д.

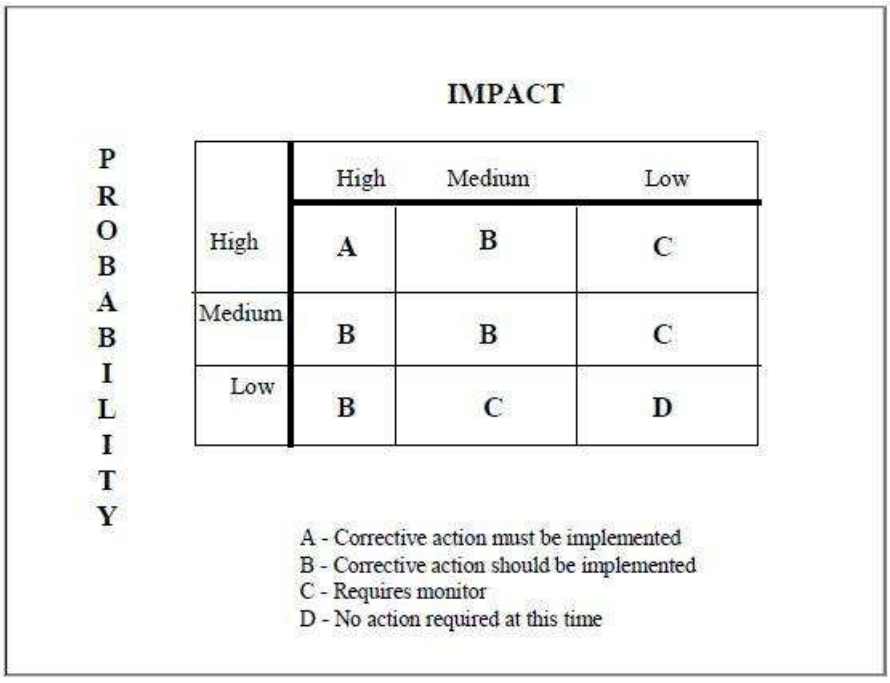

Рисунок 2 - Матрица рисков FRAP

Risk Advisor – это программный продукт, разработанный компанией MethodWare, в котором реализована методика, позволяющая задать модель информационной системы с позиции информационной безопасности, идентифицировать риски, угрозы, потери в результате инцидентов. Можно выделить пять основных этапов работы:

Описание контекста. В первую очередь необходимо создать общую схему внешних и внутренних информационных контактов организации. Эта модель строится в нескольких измерениях и задается следующими параметрами: стратегическим, организационным, бизнес-целями, управлением рисками, критериями. Картина общего контекста с точки зрения стратегии описывает сильные и слабые стороны организации в плане внешних контактов. Здесь производится классификация угроз связанных с отношениями с партнерами, оцениваются риски, сопряженные с различными вариантами развития внешних связей организации. Описание контекста в организационном измерении включает в себя картину отношений внутри организации, стратегию развития и внутреннюю политику. Схема управления рисками включает в себя концепцию информационной безопасности. Наконец, в контексте бизнес-целей и критериев оценки, описываются, как следует из названия, ключевые бизнес-цели и качественные и количественные критерии, с опорой на которые производится управление рисками.

Описание рисков. Для того чтобы облегчить и стандартизировать процесс принятия решений, связанных с управлением рисками, данные по ним необходимо стандартизировать. В разных моделях используются разные шаблоны для формализации имеющейся информации. В описываемой нами методике задается матрица рисков, в которой учитываются не только собственные параметры этих рисков, но и информация об их связях с остальными элементами общей системы. Следует отметить, что риски оцениваются здесь по качественной, а не количественной шкале и делятся всего

на две категории: приемлемые и, соответственно, неприемлемые. После этой оценки производится выбор контрмер и анализ стоимости и эффективности выбранных средств защиты.

Описание угроз. Прежде всего, составляется общий список угроз. Затем они классифицируются по качественной шкале, описываются взаимосвязи между различными угрозами и связи типа "угроза - риск".

Описание потерь. На этом этапе описываются события, связанные с инцидентами информационной безопасности, после чего оцениваются риски, вызванные этими событиями.

Анализ результатов. После построения модели, формируется детальный отчет (состоящий более чем из 100 разделов). Агрегированные описания представляются потребителю в виде графа рисков.

Компания RiskWatch, также как и Microsoft, разработала собственную методику анализа и оценки рисков, которая реализуется в ряде их программных средств. В методе RiskWatch в качестве критериев для оценки и управления рисками используются ожидаемые годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI). Методика RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. Процесс анализа рисков состоит из четырех этапов.

На первом этапе, являющемся, по сути, подготовительным, определяется предмет исследования: дается описание типа организации, состава исследуемой системы, базовых требований в области информационной безопасности и т.д. Программное обеспечение RiskWatch предлагает широкий выбор всевозможных категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты, из которых аналитик выбирает только те, что реально присутствуют в исследуемой системе. Кроме того, есть возможность добавления новых элементов и корректировка уже существующих описаний.

На втором этапе производится более детальное описание системы (какие ресурсы в ней присутствуют, какие типы потерь могут иметь место при

реализации риска и какие классы инцидентов можно выделить путём сопоставления категории потерь и категории ресурсов). Есть два варианта ввода данных: вручную или путём импорта из отчетов, сгенерированных в процессе анализа компьютерной сети на наличие в ней уязвимостей. Для выявления возможных слабых мест системы используется опросник, в котором предлагается ответить более чем на 600 вопросов, связанных с категориями ресурсов. В связи с тем, что компании из разных сфер деятельности имеют свои исключительные особенности, а также учитывая быстро развивающийся рынок информационных технологий, кажется очень разумным и удобным наличие возможности корректировки вопросов и исключение/добавление новых. Далее определяется частота реализации каждой из присутствующих в системе угроз, уровень уязвимости и ценность ресурсов. На основе данной информации рассчитывается эффективность использования тех или иных элементов контроля информационной безопасности.

На третьем этапе производится количественная оценка риска. Первым делом определяется взаимосвязь между ресурсами, потерями, угрозами и уязвимостями, определенными в процессе проведения первых двух этапов работы. Далее для каждого риска рассчитывается математическое ожидание потерь за год по следующей формуле:

$$m = p * v \tag{1.1}$$

где p - частота возникновения угрозы в течение года,
v - стоимость ресурса, который подвергается угрозе.

Например, если выведение сервера из строя на один час обойдется компании в $100000, а вероятность совершения DDoS-атаки в течение года равна 0.01, то ожидаемые потери составят $1000. Кроме того моделируются сценарии "что если…", в которых аналогичные ситуации рассматриваются с учетом внедрения средств защиты. Путём сравнения ожидаемых потерь при

условии использования элементов контроля и без них можно оценить, насколько эффективным будет внедрение тех или иных защитных мер.

На последнем этапе генерируются отчёты разных видов: краткие итоги, полные и краткие отчеты об элементах, описанных на стадиях 1 и 2, отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз, отчет об угрозах и мерах противодействия, отчет о результатах аудита безопасности [26].

Таким образом, рассматриваемое средство позволяет не только оценить риски, которые на данный момент существуют у предприятия, но и выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия. Кроме того, описываемое программное обеспечение может являться удобной основой для разработки собственного, максимально подходящего для предприятий конкретного типа (например, кредитных организаций), средства анализа и оценки рисков информационной безопасности.

ГРИФ – российское комплексное средство анализа и управления рисками информационной системы организации, разработанное компанией Digital Security. Принцип работы данного программного обеспечения основан на двух концептуально разных подходах к оценке рисков информационной безопасности, получивших названия "модель информационных потоков" и "модель угроз и уязвимостей". Рассмотрим каждый из алгоритмов по отдельности.

Модель информационных потоков характеризуется тем, что в основе алгоритма анализа и оценки рисков лежит построение модели информационной системы организации. Расчет значений рисков базируется на информации о средствах защиты ресурсов с ценной информацией, взаимосвязях ресурсов между собой, влиянии прав доступа групп пользователей и организационных мерах противодействия.

На первом этапе необходимо подготовить полное описание архитектуры исследуемой сети, включающее информацию о ценных ресурсах, их взаимосвязях, группах пользователей, средствах защиты информации и др. Исходя из введенных данных, можно построить полную модель информационной системы компании, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Перейдем к непосредственному описанию алгоритма. Оценка риска производится отдельно по каждой связи "группа пользователей – информация" по трем типам угроз: конфиденциальность, целостность и доступность (при этом для первых двух типов результат рассчитывается в процентах, а для последнего – в часах простоя). Ущерб от реализации разных видов угроз тоже задается отдельно, т.к. оценить комплексные потери не всегда возможно. Ключевыми критериями, от которых зависит вероятность реализации той или иной угрозы, являются виды (локальный и/или удаленный) и права (чтение, запись, удаление) доступа пользователей к ресурсам, наличие доступа в Интернет, количество человек в группе, использование антивирусного ПО, криптографических средств защиты (особенно значимо для дистанционного доступа) и т.д. На этом же этапе определяются средства защиты информации и рассчитываются коэффициенты локальной защищенности информации на ресурсе, удаленной защищенности информации на ресурсе и локальной защищенности рабочего места группы пользователей. Минимальный коэффициент отражает реальный уровень защиты ресурса, т.к. указывает на наиболее уязвимое место в информационной системе. Для того чтобы получить итоговую вероятность реализации угрозы, полученный показатель необходимо умножить на базовую вероятность реализации угрозы ИБ, которая рассчитывается на основе метода экспертных оценок.

На последнем этапе значение полученной итоговой вероятности умножается на величину ущерба от реализации угрозы и рассчитывается риск угрозы информационной безопасности для связи "вид информации - группа пользователей". Алгоритм расчета величины риска по угрозе отказ в

обслуживании имеет незначительные отличия, связанные, в основном, с единицами измерения.

Система также позволяет задавать контрмеры, эффективность внедрения которых можно оценить по формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}} \quad (1.2)$$

где E - эффективность внедрения контрмеры,

R_{old} – риск без учета контрмеры,

R_{new} – риск с учетом контрмеры.

В результате работы алгоритма заказчик получает следующую информацию.

- Риск реализации по трем базовым угрозам для вида информации.
- Риск реализации по трем базовым угрозам для ресурса.
- Риск реализации суммарно по всем угрозам для ресурса.
- Риск реализации по трем базовым угрозам для информационной системы.
- Риск реализации по всем угрозам для информационной системы.
- Риск реализации по всем угрозам для информационной системы после задания контрмер.
- Эффективность контрмеры.
- Эффективность комплекса контрмер.

Модель анализа угроз и уязвимостей описывает ещё один подход к анализу и оценке рисков информационной безопасности. В качестве входной информации выступает перечень ресурсов, содержащих ценную информацию, описание угроз, воздействующих на каждый ресурс, и уязвимостей, через которые возможна реализация вышеупомянутых угроз. Для каждого из видов исходных данных (кроме уязвимостей) указывается степень критичности. Также вводится вероятность реализации той или иной угрозы.

Алгоритм может работать в двух режимах: рассчитывая вероятность реализации одной базовой угрозы или распределяя оценки по трём базовым типам угроз. Перечислим этапы метода в общем виде для обоих режимов.

1. Рассчитывается уровень угрозы по конкретной уязвимости на основе критичности и вероятности реализации угрозы через данную уязвимость.
2. Уровень угрозы по всем уязвимостям рассчитывается путем суммирования уровней угроз через конкретные уязвимости.
3. Рассчитывается общий уровень угроз по ресурсу.
4. Рассчитывается риск по ресурсу.
5. Рассчитывается риск по информационной системе.

Алгоритм анализа и оценки рисков ГРИФ – это образец методики, которая учитывает особенности структуры компании заказчика, используя два разных подхода к расчету величин рисков. Каждый из этих двух методов может быть более эффективен в случае с одной фирмой и менее эффективен в ситуации с другой. Таким образом, методика ГРИФ исключает возможность использования неподходящего алгоритма расчета уровня риска, гарантируя достижения оптимального результата [26].

2.2 Метод расчета и анализ рисков информационной безопасности в кредитной организации

Очевидно, что среди описанных в данной работе методик нет идеального варианта для кредитных организаций, так как ни одна компания-разработчик не ставила своей целью создание алгоритма анализа и оценки рисков ИБ для предприятий какой-либо конкретной сферы. Наоборот, более логичным является разработка универсального средства для решения проблем информационной безопасности предприятия, которое позволило бы получить максимальную выгоду от его продажи как можно большему числу фирм-клиентов. Тем не менее, большинство из того, что со временем появляется на рынке в качестве нового продукта, базируется на достижениях прошлых лет (не

считая инновационных продуктов и технологий). Поэтому в данной работе создание рекомендаций по анализу и оценке рисков ИБ для предприятий банковской сферы будет производиться с учетом и на основе уже существующих алгоритмов и стандартов.

Для того чтобы определить, какая из методик анализа и оценки рисков является наилучшей для применения в качестве основы при разработке нового алгоритма, эффективного для применения в банках, необходимо провести сравнительный анализ доступных вариантов по различным критериям. При выборе показателей, на которые стоит обратить внимание при сравнении, следует учесть все возможные особенности кредитных организаций, чтобы разработанная методика покрывала нужды таких компаний. Основные особенности организаций банковской сферы:

- Банковская тайна.
- Необходимость отказоустойчивости сервисов, так как простой в несколько минут может привести банк к банкротству.
- Огромный объем персональных данных (необходимый, к примеру, для выдачи кредита), требующий особой защиты.
- Мишень для большого числа мошенников, стремящихся получить несанкционированный доступ к чужим денежным средствам.
- Сильная конкуренция на рынке и, как следствие, повышенная вероятность кибер-атак с целью получения конкурентного преимущества.
- Сложная система дистанционного обслуживания клиентов (банкоматы, интернет-банк и т.д.).
- Зависимость от Банка России.

На основе данной информации были выделены критерии сравнения методик, по которым можно будет выбрать наиболее подходящий вариант для дальнейшей разработки рекомендаций для банковской сферы.

Таблица 1 - Сравнение основных методик анализа и оценки рисков ИБ

Критерии сравнения	Lifecycle Security	MSAD	CRAMM	FRAP	Risk Advisor	RiskWatch	ГРИФ
Способы измерения величин рисков							
Качественная оценка	+	+	+	+	+	+	+
Количественная оценка	-	+	+	-	-	+	+
Подход к анализу и оценке рисков							
Модель информационных потоков	+	+	+	-	+	+	+
Модель анализа угроз и уязвимостей	+	-	+	+	-	+	+
Использование элементов риска							
Материальные активы	+	+	+	+	+	+	+
Нематериальные активы	+	+	+	+	+	+	+
Ценность активов	+	+	+	+	+	+	+
Угрозы	+	+	+	+	+	+	+
Уязвимости	+	+	+	+	+	+	+
Средства защиты	-	+	+	+	+	+	+
Потенциальный ущерб	+	+	+	+	+	+	+
Вероятность реализации угроз	+	+	+	+	+	+	+
Расчет финансовых показателей							
Расчет возврата инвестиций (ROI)	-	-	-	-	-	+	+
Расчет ожидаемых годовых потерь (ALE)	-	-	-	-	-	+	-
Дополнительные характеристики							
Акцент на расчете величины риска по угрозе "отказ в обслуживании"	-	-	-	-	-	-	+
Соответствие СТО БР ИББС-1.0-2014	-	-	+	+	-	+	+
Соответствие РС БР ИББС-2.2-2009	-	-	-	-	-	-	-

Можно предположить, что в связи со сложностью структуры информационной системы банка, большим объемом персональных данных клиентов, финансовым характером деятельности, предполагающим еще большую вероятность понести убытки, а также необходимостью бесперебойной работы сервисов, банки обязаны уделять исключительно особое внимание предмету информационной безопасности и, в частности, анализу рисков ИБ.

Таким образом, следует сосредоточить внимание на тех методиках, которые предоставляют максимальные возможности для комплексного анализа и оценки рисков ИБ, таких как CRAMM, ГРИФ и RiskWatch. На основе этих трёх методик будет проводиться разработка рекомендаций для организаций банковской сферы [12].

Перечислим основные характеристики, которыми должна обладать комплексная методика для банковского сектора:

1. Соответствие стандарту Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации": "Общие положения" СТО БР ИББС-1.0-2014.
2. Использование заранее составленных библиотек классов ресурсов, угроз, уязвимостей, потерь, групп пользователей, характерных для предприятий банковского сектора.
3. Возможность изменения и дополнения вышеописанных библиотек для обеспечения большей гибкости, разрабатываемого средства.
4. Использование как качественной, так и количественной методики расчета величин рисков.
5. Применение метода информационных потоков и метода анализа угроз и уязвимостей.
6. Акцент на расчет величин рисков по угрозе "отказ в обслуживании".
7. Акцент на расчет величин рисков по угрозе "несанкционированный доступ".
8. Предложение краткосрочных, среднесрочных и долгосрочных планов по усовершенствованию СЗИ.
9. Возможность расчета эффективности применения тех или иных контрмер.
10. Расчет таких финансовых показателей, как ROI, ALE, затраты на контрмеры.
11. Генерация нескольких видов отчетов (для менеджеров разного уровня).

Далее перечислим характеристики, которыми должна обладать методика, чтобы соответствовать стандарту Банка России СТО БР ИББС-1.0-2014.

Во-первых, в процессе анализа должен рассматриваться вариант принятия риска на основе информации о "критериях принятия рисков нарушения ИБ и уровне допустимого риска нарушения ИБ", определенных внутри организации.

Во-вторых, методикой должен устанавливаться способ и порядок процедур качественной и/или количественной оценки риска, основанной на определении степени возможности реализации угроз ИБ выявленными и/или предполагаемыми источниками угроз ИБ, зафиксированными в моделях угроз и нарушителя, и степени тяжести последствий от потери свойств ИБ.

В-третьих, по каждому из рисков нарушения ИБ, который является недопустимым, должен быть определен план, устанавливающий один из возможных способов его обработки: перенос риска на сторонние организации, уход от риска, осознанное принятие риска, формирование требований по обеспечению ИБ, снижающих риск нарушения ИБ до допустимого уровня, и формирование планов по их реализации. Планы обработки рисков нарушения ИБ должны содержать последовательность и сроки реализации и внедрения организационных, технических и иных мер защиты.

В-четвертых, на подготовительной стадии методики в организации должны быть определены следующие роли:

- связанные с деятельностью по определению/коррекции методики оценки рисков нарушения ИБ/подхода к оценке рисков нарушения ИБ;
- по оценке рисков нарушения ИБ;
- по разработке планов обработки рисков нарушения ИБ.

Также должны быть назначены ответственные за выполнение указанных ролей.

Теперь, когда нам известны особенности будущей методики, приступим к её пошаговому описанию. Так как целью данной работы не является разработка программного обеспечения для анализа и оценки рисков, то мы ограничимся составлением теоретических рекомендаций и описанием алгоритмов, которые впоследствии могут быть использованы в качестве основы для создания ПО.

Первый этап – подготовительный. Здесь определяются критерии принятия риска, границы исследуемой системы, назначаются роли

(ответственные за ту или иную часть общего процесса), из заранее составленных библиотек классов ресурсов, угроз, уязвимостей, потерь, групп пользователей выбираются те, что реально присутствуют в банке и, при необходимости, добавляются новые (или корректируются уже присутствующие в списках). В качестве базы классов основных источников угроз ИБ можно взять предлагаемый в рекомендациях по стандартизации Банка России перечень источников угроз с описаниями.

Второй этап – более подробное описание исследуемой системы. Необходимо указать все присутствующие в ИС ресурсы, хранящуюся на них информацию; провести сканирование системы на наличие уязвимостей, на основе полученных данных зафиксировать все возможные угрозы; определить количественные показатели всех вышеперечисленных элементов анализа: ценность информации, величина возможного ущерба по трем типам угроз (конфиденциальности, целостности и доступности), уровень уязвимости, базовую вероятность возникновения угрозы, критичность реализации угрозы. На этом же шаге указываем взаимосвязи между ресурсами, связи типа "ресурс – угроза", "уязвимость – угроза", "вид информации – группа пользователей" и другие. Это необходимо для возможности применения разных моделей оценки риска: на основе информационных потоков (подходит для оценки рисков ИБ, возникающих в процессе предоставления дистанционных банковских сервисов) и с помощью анализа угроз и уязвимостей (является эффективным инструментом в большинстве случаев).

Третий этап – оценка рисков. Рассмотрим процесс оценки рисков ИБ методом анализа угроз и уязвимостей. Сначала уровень риска определяется качественным методом, а затем рассчитывается количественная величина.

За основу качественного метода оценки риска можно взять алгоритм, использующийся в методике CRAMM, так как он предполагает распределение уровней рисков по шкале от 1 до 7, что позволяет применять более гибкий подход к определению тех категорий рисков, которые должны быть оценены

количественным методом. В качестве входных данных здесь используются три основных показателя.

1. Уровень угрозы ("очень высокий", "высокий", "средний", "низкий" и "очень низкий").
2. Уровень уязвимости ресурса ("высокий", "средний", "низкий").
3. Размер ожидаемых финансовых потерь (по шкале от 1 до 10).

Количественный метод мы позаимствуем из алгоритма методики ГРИФ, так как в случае с банковской сферой является крайне удобным разделение оценок по типам угроз с акцентами на ситуациях "отказ в доступе" и "нарушение конфиденциальности информации". Коротко опишем его основные моменты, обращая внимание на способ вычисления величины риска (для примера рассмотрим угрозу конфиденциальности):

1. Рассчитываем уровень угрозы по конкретной уязвимости:

$$\mathrm{Th_c} = \frac{\mathrm{ER_c}}{100} \times \frac{\mathrm{P(V)_c}}{100} \qquad (2.1)$$

где $\mathrm{ER_c}$ - критичность реализации угрозы конфиденциальности в %;

$\mathrm{P(V)_c}$ - вероятность реализации угрозы конфиденциальности через данную уязвимость в %.

Получаем значение уровня угрозы по уязвимости в интервале от 0 до 1.

2. Рассчитываем уровень угрозы по всем уязвимостям:

$$\mathrm{CTh_c} = 1 - \prod_{\mathrm{j=1}}^{\mathrm{n}} (1 - \mathrm{Th_{c,j}}) \qquad (2.2)$$

где $\mathrm{Th_c}$ - уровень угрозы конфиденциальность по уязвимости.

Получаем значение уровня угрозы по всем уязвимостям в интервале от 0 до 1.

3. Рассчитываем общий уровень угроз по ресурсу:

$$\mathrm{CThR_c} = 1 - \prod_{\mathrm{j=1}}^{\mathrm{n}} (1 - \mathrm{CTh_{c,j}}) \qquad (2.3)$$

где $\mathrm{CTh_c}$ - уровень угрозы конфиденциальность по всем уязвимостям.

Получаем значение общего уровня угрозы в интервале от 0 до 1.

4. Рассчитывается риск по ресурсу:

$$\mathrm{R_c} = \mathrm{CThR_c} \times \mathrm{D_c}\ , \tag{2.4}$$

$$\mathrm{R_\sum} = \left(1 - \left(\left(1 - \frac{\mathrm{R_c}}{100}\right) \times \left(1 - \frac{\mathrm{R_i}}{100}\right) \times \left(1 - \frac{\mathrm{R_a}}{100}\right)\right)\right) \times 100 \tag{2.5}$$

где $\mathrm{D_c}$ - критичность ресурса по угрозе конфиденциальность. Задается в деньгах или уровнях;

$\mathrm{CThR_c}$ - общий уровень угроз конфиденциальность;

$\mathrm{R_\sum}$ - суммарный риск по трем угрозам.

Получаем значение риска по ресурсу в уровнях (заданных пользователем) или деньгах.

5. Рассчитываем риск по информационной системе:

5.1. Для режима работы в деньгах:

$$\mathrm{CR_c} = \sum_{\mathrm{j=1}}^{\mathrm{n}} \mathrm{R_{c,j}}\ , \tag{2.6}$$

$$\mathrm{CR_\sum} = \mathrm{CR_c} + \mathrm{CR_i} + \mathrm{CR_a} \tag{2.7}$$

где $\mathrm{CR_c}$ - риск по системе по угрозам конфиденциальность;

$\mathrm{CR_\sum}$ - риск по системе суммарно по трем видам угроз.

5.2. Для режима работы в уровнях:

$$\mathrm{CR_c} = \left(1 - \prod_{\mathrm{j=1}}^{\mathrm{n}} \left(1 - \frac{\mathrm{R_{c,j}}}{100}\right)\right) \times 100 \tag{2.8}$$

$$CR_{\sum} = \left(1 - \left(\left(1 - \frac{CR_c}{100}\right) \times \left(1 - \frac{CR_i}{100}\right) \times \left(1 - \frac{CR_a}{100}\right)\right)\right) \times 100 \quad (2.9)$$

где CR_c - риск по системе по угрозам конфиденциальность;

$CR_{\sum}$ - риск по системе суммарно по трем видам угроз.

Приведем входные параметры качественного и количественного методов к общим обозначениям. Показатель ER, означающий критичность реализации угрозы, соответствует определению уровня угрозы из качественного метода оценки, P(V), означающий вероятность реализации угрозы, соответствует определению уровня уязвимости ресурса, а D, означающий критичность ресурса, соответствует размеру ожидаемых финансовых потерь (Таб.2).

Таблица 2 - Соответствие входных переменных из качественного и количественного методов оценки рисков ИБ

Количественная оценка			Качественная оценка	
Обозначение	Описание	Единицы измерения	Описание	Шкалы
ER	Критичность реализации угрозы	%	Уровень угрозы	"очень высокий", "высокий", "средний", "низкий", "очень низкий"
P(V)	Вероятность реализации угрозы	%	Уровень уязвимости ресурса	"высокий", "средний", "низкий"
D	Критичность ресурса	От 1 до 10	Размер ожидаемых финансовых потерь	От 1 до 10

Применение метода анализа информационных потоков будет эффективным в случае оценки рисков в системе дистанционного обслуживания клиентов банка. Алгоритм, разработанный компанией Digital Security и описанный выше в данной главе, также подходит для использования в организациях банковской сферы. Рассмотрим отдельно оценку рисков по угрозе "отказ в обслуживании" (рассчитывается время простоя ресурса) [26].

- Определяем базовое время простоя для информации.

- Рассчитываем коэффициент защищенности информации для определенной группы пользователей. Здесь учитываются такие показатели, как права доступа группы пользователей к данной информации, средства резервирования, наличие антивирусного программного обеспечения.
- Рассчитываем время простоя информации с учетом средств защиты информации и времени простоя сетевого оборудования (часы в год).
- Время простоя для информации T_{inf}, учитывая все группы пользователей, имеющих к ней доступ, вычисляется по следующей формуле:

$$T_{inf} = \left(1 - \prod_{i=1}^{n} \left(1 - \frac{T_{ug,n}}{T_{max}}\right)\right) \times T_{max} \quad (2.10)$$

где T_{max} - максимальное критичное время простоя;
$T_{ug,n}$ - время простоя для связи "информация - группа пользователей".
- Перемножив итоговое время простоя и ущерб от реализации угрозы, получим риск реализации угрозы "отказ в обслуживании" для связи "информация - группа пользователей".

Процесс оценки рисков должен предусматривать анализ эффективности внедрения конкретных средств защиты (как и в методе ГРИФ).

Четвёртый этап – составление краткосрочных, среднесрочных и долгосрочных планов обработки рисков и усовершенствования СЗИ.

Пятый этап – генерация отчётов. На этом шаге также рассчитываются финансовые показатели: ROI, ALE, затраты на реализацию планов обработки рисков [24].

Глава 3 Мероприятия по снижению рисков информационной составляющей экономической безопасности на примере кредитной организации АО "Газпромбанк"

3.1 Характеристика: анализ и оценка кредитной организации АО "Газпромбанк"

Теперь, когда на основе наиболее активно использующихся методик анализа и оценки рисков информационной безопасности, а также стандартов и рекомендаций ЦБ, выбрана наиболее подходящая методика для предприятий банковского сектора, необходимо провести её апробацию на конкретном банке.

Для данной работы в качестве рассматриваемой компании был выбран Газпромбанк - коммерческий банк газовой промышленности «Газпромбанк» был создан в июле 1990 года, в августе 1996 года его организационно-правовая форма была приведена в соответствие с действующим законодательством и определена как «общество с ограниченной ответственностью». 13 ноября 2001 года коммерческий банк газовой промышленности «Газпромбанк» (Общество с ограниченной ответственностью) был преобразован в Акционерный банк газовой промышленности «Газпромбанк» (Закрытое акционерное общество), 31 августа 2007 года Акционерный банк газовой промышленности «Газпромбанк» (Закрытое акционерное общество) изменил тип акционерного общества и наименование на «Газпромбанк» (Открытое акционерное общество)

Газпромбанк – один из крупнейших универсальных финансовых институтов России, предоставляющий широкий спектр банковских, финансовых, инвестиционных продуктов и услуг корпоративным и частным клиентам, финансовым институтам, институциональным и частным инвесторам. Банк входит в

тройку крупнейших банков России по всем основным показателям и занимает третье место в списке банков Центральной и Восточной Европы по размеру собственного капитала.

Банк обслуживает ключевые отрасли российской экономики: газовую, нефтяную, атомную, химическую и нефтехимическую, черную и цветную металлургию, электроэнергетику, машиностроение и металлообработку, транспорт, строительство, связь, агропромышленный комплекс, торговлю и другие отрасли.

Розничный бизнес также является стратегически важным направлением деятельности Банка, и его масштабы последовательно увеличиваются. Частным клиентам предлагается полный набор услуг: кредитные программы, депозиты, расчетные операции, электронные банковские карты и др.

Газпромбанк занимает сильные позиции на отечественном и международном финансовых рынках, являясь одним из российских лидеров по организации и андеррайтингу выпусков корпоративных облигаций, управлению активами, в сфере частного банковского обслуживания, корпоративного финансирования и других областях инвестиционного банкинга.

В числе клиентов Газпромбанка – около 4 миллионов физических и порядка 45 тысяч юридических лиц.

В настоящее время Газпромбанк владеет шестью дочерними и зависимыми банками в России, Белоруссии, Швейцарии и Люксембурге, имеет представительства в Астане (Казахстан), Пекине (Китай), Улан-Баторе (Монголия) и Нью-Дели (Индия).

В России региональная сеть Газпромбанка представлена 24 филиалами, расположенными от Калининграда до Южно-Сахалинска. Общее число офисов, предоставляющих высококачественные банковские услуги, превышает 350.

Газпромбанк является членом Российского национального комитета Международной торговой палаты. Банк занимает 3-е место в рейтинге Интерфакс-100 по объему активов по результатам 2016 года.

Направления деятельности Газпромбанка:

- Кредитование предприятий газовой отрасли и расширение кредитования других секторов российской экономики
- Активная деятельность на рынке ценных бумаг и валютном рынке
- Депозитарные услуги для акционеров ОАО Газпрома и держателей других ценных бумаг
- Выпуск и обслуживание расчетных и кредитных банковских карт
- Проектное финансирование
- Андеррайтинг и корпоративные финансы
- Универсальный банк для корпоративных клиентов
- Лидирующие позиции в области международных и внутренних расчетов.

Филиал Газпромбанка в г. Красноярске зарегистрирован 25 января 2006 года.

На сегодняшний день клиентами Филиала в г. Красноярске являются крупнейшие региональные предприятия нефтяной и газовой отрасли, атомной промышленности, энергетики, связи, цветной металлургии, строительного комплекса и др. Приоритетным направлением в работе Газпромбанка является обслуживание предприятий реального сектора экономики, а также частных клиентов и акционеров ОАО «Газпром».

Сегодня Филиал занимает прочные позиции на рынке банковских услуг г. Красноярска по всем показателям. В настоящее время филиал Банка - ГПБ (ОАО) в Красноярске – это универсальный банк международного уровня, отвечающий современным требованиям и предлагающий юридическим и физическим лицам полный спектр банковских услуг.

Высокое качество обслуживания клиентов способствует стабильному развитию клиентской базы филиала.

Залогом успешной деятельности и гарантией дальнейшего развития филиала являются надежность, стабильность и качество предоставляемых услуг, индивидуальный подход к каждому Клиенту и высокий профессиональный уровень сотрудников филиала, что позволяет гибко реагировать на запросы Клиентов. Мы проводим индивидуальную тарифную политику и можем пред-

ложить Вам и Вашему предприятию оптимальные схемы совершения финансовых операций.

Основными направлениями деятельности филиала являются:

- расчетно-кассовое обслуживание юридических и физических лиц;
- кредитование юридических и физических лиц;
- прием вкладов населения;
- выпуск и обслуживание банковских карт;
- валютные операции с юридическими и физическими лицами;
- операции с ценными бумагами.

В связи с тем, что анализ и оценка рисков информационной безопасности должна проводиться экспертами в данной области при участии менеджеров всех уровней, а также требует наличия информации обо всех активах компании и уязвимостях ее системы информационной безопасности, для меня не представляется возможным проведение комплексного анализа рисков ИБ в Газпромбанке. Однако в процессе преддипломной практики, которая проходила в вышеупомянутой организации, была возможность ознакомиться с организационной структурой банка, некоторыми используемыми программными продуктами (SAS Enterprise Guide, Lotus Notes, MyClient), информацией, к которой можно получить доступ через эти приложения, способами взаимодействия между подразделениями и отдельными сотрудниками, политикой информационной безопасности и прочими характеристиками и особенностями работы данного банка.

Кроме того, мной были замечены некоторые интересные особенности обеспечения информационной безопасности рабочего места сотрудника: ограниченный доступ в Интернет, невозможность использования незарегистрированных внешних носителей информации, при отключении от компьютера периферийных устройств ввода информации невозможность подключения тех же самых устройств без выхода из системы с последующим повторным подключением. Эта информация позволит выявить или наоборот

исключить возможность наличия уязвимостей в определенных местах системы информационной безопасности банка.

Комплексный анализ и оценка рисков даже небольшой части информационной системы банка по разработанным методикам – это крайне сложная и ответственная задача. В данной работе будет проведена проверка логичности полученного алгоритма на примере АО "Газпромбанк", а также качественной и количественной оценкой риска от реализации двух угроз, связанных с получением доступа к ресурсу. При расчете будем использовать метод анализа угроз и уязвимостей.

Первый этап – подготовительный.

1. Определяем критерии принятия риска.

Риск является допустимым, если на этапе качественной оценки риска ему будет присвоена оценка 1 или 2 по шкале от 1 до 7.

2. Определяем границы исследуемой системы.

В связи с тем, что мы ограничены в информации обо всей ИС банка, рассмотрим в качестве исследуемой системы рабочее место сотрудника банка кредитного отдела.

3. Назначаем роли:

- ответственный за коррекцию методики оценки рисков в случае обнаружения её недостаточной эффективности;
- ответственный за нарушение подхода к оценке рисков;
- ответственный за оценку рисков нарушения ИБ;
- ответственный за разработку планов обработки рисков нарушения ИБ.

4. Выбираем актуальные для нас классы ресурсов, угроз, уязвимостей, потерь и группы пользователей.

- Ресурсы: аппаратные, программные.
- Угрозы по источникам: связанные с ЧС, с внутренними/внешними нарушителями ИБ, с техническими сбоями и др.
- Уязвимости: по недостатку технических, организационных, физических средств ЗИ.

- Потери: конфиденциальности, целостности и доступности.
- Группы пользователей: сотрудники компании.

Второй этап – более подробное описание исследуемой системы. В силу того, что мы ограничиваем исследуемую ИС до рабочего места сотрудника, выделим самые значительные ресурсы и наиболее ценную информацию в них (Таб.3).

Таблица 3 - Самые ценные ресурсы исследуемой системы

Класс ресурса	Ресурс	Информация	Критичность ресурса, D
Аппаратный	Рабочая станция	Финансовая отчетность	$D_c = 10$
		Конфиденциальная информация о работе отдела	$D_a = 2$
		Персональные данные клиентов	$D_i = 5$
		Инф. о счетах	
		Инф. о транзакциях	
		Корпоративная электронная почта	
Программный	SAS Enterprise Guide	Персональные данные клиентов	$D_c = 10$
			$D_a = 3$
			$D_i = 4$
		Инф. о счетах	
		Инф. о транзакциях	
	Lotus Notes	Корпоративная электронная почта	$D_c = 10$
			$D_a = 7$
			$D_i = 4$
	MyClient	Персональные данные клиентов	$D_c = 10$
			$D_a = 9$
		Финансовая отчетность	$D_i = 7$

Далее составим перечень угроз и уязвимостей, через которые могут быть реализованы данные угрозы (Таб.4). Экспертами в области информационной безопасности должен быть составлен список вопросов, в результате ответов на которые будут получены оценки критичности ресурсов, критичности

реализации угроз и вероятности реализации угроз. Мы назначим данные величины сами.

Выделим две угрозы по ресурсу "Рабочая станция", одна из которых реализуется с помощью двух уязвимостей. Для каждой угрозы рассчитаем показатели конфиденциальности, целостности и доступности ресурса.

Таблица 4 - Угрозы безопасности и уязвимости исследуемой системы

Угроза	Уязвимость	Критичность реализации угрозы, ER	Вероятность реализации угрозы, P(V)
Халатность сотрудника: покинул рабочее место без выхода из системы. Результат: открыт доступ к информации	Автоматический выход из системы происходит только через 10 минут бездействия пользователя	$ER_c = 70\%$	$P(V)_c = 4\%$
		$ER_a = 10\%$	$P(V)_a = 1\%$
		$ER_i = 50\%$	$P(V)_i = 1\%$
Получение обслуживающим персоналом логина и пароля сотрудника Результат: открыт доступ к информации	Недостатки организационных мер защиты: сотрудник хранит логин и пароль под клавиатурой	$ER_c = 70\%$	$P(V)_c = 2\%$
		$ER_a = 10\%$	$P(V)_a = 1\%$
		$ER_i = 50\%$	$P(V)_i = 1\%$
	Недостатки организационных мер защиты: обслуживающий персонал работает в то же время, когда и основные сотрудники – есть возможность подсмотреть логин и пароль при вводе	$ER_c = 70\%$	$P(V)_c = 1\%$
		$ER_a = 10\%$	$P(V)_a = 1\%$
		$ER_i = 50\%$	$P(V)_i = 1\%$

Третий этап – оценка рисков.

Определяем уровень риска качественным методом:

1. Переводим показатели ER и P(V) из процентов в качественные показатели следующим образом (Таб.5):

Таблица 5 - Перевод показателей из количественных в качественные величины

ER		P(V)	
0 – 20%	"очень низкий"	0 – 33%	"низкий"
21 – 40%	"низкий"		
		34 – 66%	"средний"

41 – 60%	"средний"		
61 – 80%	"высокий"	67 – 100%	"высокий"
81 – 100%	"очень высокий"		

2. По матрице оценки рисков методики CRAMM (Рис.3) смотрим, какому уровню соответствует риск реализации угрозы через определенную уязвимость. Результат качественной оценки показан в таблице 6.

Таблица 6 - Результат качественной оценки рисков.

Угроза	Уязвимость	Критичность реализации угрозы, ER	Вероятность реализации угрозы, P(V)	Качественная оценка
Халатность сотрудника: покинул рабочее место без выхода из системы. Результат: открыт доступ к информации	Автоматический выход из системы происходит только через 10 минут бездействия пользователя	$\mathbf{ER_c}$ - "высокий"	$\mathbf{P(V)_c}$ - "низкий"	6
		$\mathbf{ER_a}$ - "очень низкий"	$\mathbf{P(V)_a}$ - "низкий"	5
		$\mathbf{ER_i}$ - "средний"	$\mathbf{P(V)_i}$ - "низкий"	6
Получение обслуживающим персоналом логина и пароля сотрудника Результат: открыт доступ к информации	Недостатки организационных мер защиты: сотрудник хранит логин и пароль под клавиатурой	$\mathbf{ER_c}$ - "высокий"	$\mathbf{P(V)_c}$ - "низкий"	6
		$\mathbf{ER_a}$ - "очень низкий"	$\mathbf{P(V)_a}$ - "низкий"	5
		$\mathbf{ER_i}$ - "средний"	$\mathbf{P(V)_i}$ - "низкий"	6
	Недостатки организационных мер защиты: обслуживающий персонал работает в то же время, когда и основные сотрудники – есть возможность подсмотреть логин и пароль при вводе	$\mathbf{ER_c}$ - "высокий"	$\mathbf{P(V)_c}$ - "низкий"	6
		$\mathbf{ER_a}$ - "очень низкий"	$\mathbf{P(V)_a}$ - "низкий"	5
		$\mathbf{ER_i}$ - "средний"	$\mathbf{P(V)_i}$ - "низкий"	6

В результате качественной оценки получаем, что ни один риск не является приемлемым, а значит необходимо проведение количественной оценки. Для удобства обозначим первую угрозу Th_1, а вторую Th_2, при этом $\mathrm{Th}_{2,1}$ будет означать реализацию второй угрозы через первую уязвимость, а

$\mathrm{Th}_{2,1_c}$ – реализацию второй угрозы через первую уязвимость с нарушением свойства конфиденциальности ресурса.

Определяем уровень риска количественным методом:

1. Рассчитываем уровень угрозы по конкретной уязвимости:

$$\mathrm{Th}_c = \frac{\mathrm{ER}_c}{100} \times \frac{\mathrm{P(V)}_c}{100} \quad (3.1)$$

$$\mathrm{Th}_{1_c} = \frac{70}{100} \times \frac{4}{100} = 0{,}028$$

$$\mathrm{Th}_{1_a} = \frac{10}{100} \times \frac{1}{100} = 0{,}001$$

$$\mathrm{Th}_{1_i} = \frac{50}{100} \times \frac{1}{100} = 0{,}005$$

$$\mathrm{Th}_{2,1_c} = \frac{70}{100} \times \frac{2}{100} = 0{,}014$$

$$\mathrm{Th}_{2,1_a} = \frac{10}{100} \times \frac{1}{100} = 0{,}001$$

$$\mathrm{Th}_{2,1_i} = \frac{50}{100} \times \frac{1}{100} = 0{,}005$$

$$\mathrm{Th}_{2,2_c} = \frac{70}{100} \times \frac{1}{100} = 0{,}007$$

$$\mathrm{Th}_{2,2_a} = \frac{10}{100} \times \frac{1}{100} = 0{,}001$$

$$\mathrm{Th}_{2,2_i} = \frac{50}{100} \times \frac{1}{100} = 0{,}005$$

где ER - критичность реализации угрозы (указывается в %);

P(V) - вероятность реализации угрозы через данную уязвимостьт(указывается в %).

Получаем значения уровня угрозы по уязвимости в интервале от 0 до 1.

2. Рассчитываем уровень угрозы по всем уязвимостям (для первой угрозы данный показатель уже рассчитан, так как она может быть реализована только через одну уязвимость):

$$\mathrm{CTh}_c = 1 - \prod_{j=1}^{n}(1 - \mathrm{Th}_{c,j}) \quad (3.2)$$

$$\mathrm{Th}_{2_c} = 1 - (1 - 0{,}014) \times (1 - 0{,}007) = 0{,}021$$

$$\mathrm{Th}_{2_a} = 1 - (1 - 0{,}001) \times (1 - 0{,}001) = 0{,}002$$

$$\mathrm{Th}_{2_i} = 1 - (1 - 0{,}005) \times (1 - 0{,}005) = 0{,}01$$

где Th c , i , a - уровень угрозы конфиденциальность, целостность или доступность по уязвимости.

Значения уровня угрозы по всем уязвимостям получим в интервале от 0 до 1.

3. Рассчитываем общий уровень угроз по ресурсу:

$$\mathrm{CThR_c} = 1 - \prod_{j=1}^{n}(1 - \mathrm{CTh_{c,j}}) \qquad (3.3)$$

$$\mathrm{CThR_c} = 1 - (1 - 0{,}028) \times (1 - 0{,}021) = 0{,}048$$

$$\mathrm{CThR_a} = 1 - (1 - 0{,}001) \times (1 - 0{,}002) = 0{,}003$$

$$\mathrm{CThR_i} = 1 - (1 - 0{,}005) \times (1 - 0{,}01) = 0{,}015$$

где CTh c , I , a - уровень угрозы конфиденциальность, целостность или доступность по всем угрозам.

Значение общего уровня угрозы получим в интервале от 0 до 1.

4.Рассчитывается риск по ресурсу:

$$\mathrm{R_c} = \mathrm{CThR_c} \times \mathrm{D_c}\ , \qquad (3.4)$$

$$\mathrm{R_i} = \mathrm{CThR_i} \times \mathrm{D_i}\ ,$$

$$\mathrm{R_a} = \mathrm{CThR_a} \times \mathrm{D_a}\ ,$$

$$\mathrm{R_\Sigma} = \left(1 - \left(\left(1 - \frac{\mathrm{R_c}}{100}\right) \times \left(1 - \frac{\mathrm{R_i}}{100}\right) \times \left(1 - \frac{\mathrm{R_a}}{100}\right)\right)\right) \times 100 \qquad (3.5)$$

$$\mathrm{R_c} = 0{,}048 \times 10 = 0{,}48$$

$$\mathrm{R_a} = 0{,}003 \times 2 = 0{,}006$$

$$\mathrm{R_i} = 0{,}015 \times 5 = 0{,}075$$

$$\mathrm{R_\Sigma} = \left(1 - \left(\left(1 - \frac{0{,}48}{100}\right) \times \left(1 - \frac{0{,}075}{100}\right) \times \left(1 - \frac{0{,}006}{100}\right)\right)\right) \times 100 = 0{,}56$$

D c , i , a - критичность ресурса по угрозе конфиденциальность, целостность или доступность. Задается в деньгах или уровнях;

CThR c , i , a - общий уровень угроз конфиденциальность, целостность или доступность по ресурсу;

$R_{\sum}$ - суммарный риск по трем угрозам.

Таким образом, получим значение риска по ресурсу в уровнях (заданных пользователем) или деньгах.

3.2 Мероприятия по снижению рисков информационной безопасности банка

Проведя анализ по ресурсу "Рабочая станция", были получены следующие результаты:

$\mathrm{CThR_c} = 0{,}048$

$\mathrm{CThR_a} = 0{,}003$

$\mathrm{CThR_i} = 0{,}015$

CThR c , i , a - общий уровень угроз конфиденциальность, целостность или доступность по ресурсу. Рассчитывается в интервале от 0 до 1.

$R_c = 0{,}48$

$R_a = 0{,}006$

$R_i = 0{,}075$

R – риск по ресурсу.

$R_{\sum} = 0{,}56$

$R_{\sum}$ - суммарный риск по трем угрозам, рассчитывается в уровнях, заданных пользователем. В нашем случае это интервал от 0 до 10.

Проанализировав вышеуказанные показатели, следует сделать следующие выводы: общий уровень угроз целостности и доступности по ресурсу очень низкий. Самый высокий показатель общего уровня угроз –

показатель конфиденциальности. Это объясняется критичностью реализации угрозы выбранного ресурса. Однако, используя некоторые рекомендательные действия, возможно снизить данный показатель. Суммарный риск всех показателей по ресурсу – низкий.

В работе были определены 3 уязвимости ресурса:

- автоматический выход из системы происходит только через 10 минут бездействия пользователя;
- недостатки организационных мер защиты: сотрудник хранит логин и пароль под клавиатурой;
- недостатки организационных мер защиты: обслуживающий персонал работает в то же время, когда и основные сотрудники – есть возможность подсмотреть логин и пароль при вводе.

Рекомендации по снижению уровня угроз, относительно заявленных уязвимостей:

- уменьшение времени автоматического выхода из системы при бездействии
- многофакторная аутентификация. Например, пароль и карта, или пароль и отпечаток пальца.
- Установка дополнительно защитного программного обеспечения (vipnet и др.)
- возможность быстрого отзыва прав, то есть минимизация ущерба за счёт быстрого выяснения и пресечения несанкционированных действий.
- любые изменения в позиции сотрудника, влекущие изменения в его правах, должны как можно быстрее отражаться на его реальных правах в компьютерной системе

Для доказательства своей личности пользователь использует один или несколько аутентификаторов. Наиболее известный аутентификатор - это пароль. Также, это может быть карта доступа, отпечаток пальца и многое другое. Всего в отрасли ИБ активно используется более двадцати видов аутентификаторов. Одним из важных элементов усиления системы аутентификации является так называемая многофакторная аутентификация, позволяющая значительно снизить вероятность успешного прохождения аутентификации посторонним ли-

цом. Многофакторной аутентификацией является одновременное использование аутентификаторов из разных, групп аутентификаторов:

- то, что пользователь знает (например, пароль, пин-код)
- то, чем пользователь владеет (например, банковская карта, карта доступа)
- то, что является неотъемлемой характеристикой пользователя (например, отпечаток пальца)
- то, где пользователь находится (используя, например, данные из СКУД)

Многофакторная аутентификация (например: пароль и карта, или пароль и отпечаток пальца) - увеличивает для злоумышленника сложность прохождения процедуры аутентификации, так как необходимо провести атаку на разнородные системы аутентификации.

Сокращение количества аутентификаторов, которые необходимо знать/обладать пользователю - снижает риск компрометации аутентификаторов. Например, пользователь может запомнить один пароль, или следить за сохранностью одной карты доступа. Если паролей много, то пользователь будет просто вынужден куда-то их записать, тем самым увеличивая вероятность их компрометации.

Упрощение процедуры аутентификации для пользователя. Достигается с помощью SSO. Также, например, приложить палец к сканеру проще, чем ввести пароль. Кроме того, пароль надо ещё помнить, а карту доступа хранить. Упрощает для пользователя следование политикам безопасности. Снижает вероятность их нарушения.

Использование этих инструментов и практик, в значительной степени снижают возможность несанкционированного доступа и несанкционированных действий при использовании информационных систем, тем самым повышают общий уровень информационной безопасности кредитной организации [5].

ЗАКЛЮЧЕНИЕ

На современном этапе развития мы наблюдаем стремительно растущую роль информационной сферы в жизни общества. Становясь системообразующим фактором, информационная среда всё активнее оказывает воздействие на безопасность как политическую и оборонную, так и личную, экономическую и пр.

Понятие «информационная безопасность» сформировалось, когда люди стали пользоваться средствами информационных коммуникаций. На современном этапе сохранность конфиденциальности получаемой и передаваемой информации – это жизненно важный аспект.

Первостепенной целью информационной безопасности является обеспечение конфиденциальности. Утечка информации может привести к необратимым последствиям – миллионным убыткам вследствие коммерческого преступления.

Информационные технологии дают возможность применять приёмы, позволяющие воспроизводить интеллектуальную деятельность человека. По мере того, как развивается научно-технический прогресс, многократно увеличивается роль информационных технологий. Обеспечение информационной безопасности занимает важное место в работе всех государственных институтов.

В первой части данной работы были рассмотрены теоретические аспекты экономической безопасности, информационной безопасности, дана характеристика элементам экономической безопасности организации.

Следует выделить наиболее общее определение экономической безопасности организации — это наличие конкурентных преимуществ, обусловленных соответствием финансового, информационного, кадрового, технико-технологического потенциалов и организационной структуры организации его стратегическим целям и задачам. Данное определение подчеркивает тот факт, что экономическая безопасность находится на стыке экономики и безопасности организации.

Исходя из данного выше определения, рассмотрены основные функциональные блоки системы экономической безопасности организации, обеспечивающие максимальное соответствие менеджмента организации и его ресурсного потенциала:

-финансовая составляющая;

-информационная составляющая;

-технико-технологическая составляющая;

-кадровая составляющая;

-правовая составляющая.

Во второй главе представлены основные подходы к анализу и оценке информационной безопасности организации. Произведен обзор методик, подходящих для анализа кредитных организаций. Были рассмотрены следующие специализированные методики и программные продукты для анализа и оценки рисков: CRAMM, FRAP, RiskWatch, ГРИФ.

В таблице 1 была представлена сравнительная характеристика вышеописанных методик, на основании которой подобрана наиболее подходящая методика оценки и анализа кредитной организации. Детально описан метод расчета и анализа рисков информационной безопасности кредитной организации.

В заключительной части представлена общая характеристика кредитной организации АО "Газпромбанк". Для оценки и анализа информационной

безопасности был взят ресурс "Рабочая станция сотрудника", необходимые для расчета данные представлены в таблицах 3 и 4. Произведены расчеты, в результате которых получены следующие данные:

- общий уровень угроз конфиденциальности $\mathrm{CThR_c} = 0{,}048$
- общий уровень угроз целостности $\mathrm{CThR_i} = 0{,}015$
- общий уровень угроз доступности $\mathrm{CThR_a} = 0{,}003$

Показатели рассчитываются в интервале от 0 до 1, чем ближе значение показателя к 0, тем ниже уровень угроз. Исходя из результатов, сделан вывод: общий уровень угроз целостности и доступности по ресурсу очень низкий. Самый высокий показатель общего уровня угроз – показатель конфиденциальности. Это объясняется критичностью реализации угрозы выбранного ресурса. Однако, используя рекомендательные действия, возможно снизить данный показатель.

Также рассчитан суммарный риск по трем угрозам ресурса "Рабочая станция сотрудника" - $\mathrm{R_{\sum}} = 0{,}56$

$\mathrm{R_{\sum}}$ - суммарный риск по трем угрозам, рассчитывается в уровнях, заданных пользователем. В нашем случае это интервал от 0 до 10. Чем ближе к 0 данное значение, тем ниже риск. Значение показателя низкое, можно утверждать, что защита от несанкционированного доступа является достаточно надежной.

В заключении третьей главы представлены меры по снижению рисков информационной безопасности банка, использование которых приведет к снижению риска несанкционированного доступа, следовательно, повысится общий уровень информационной безопасности кредитной организации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Федеральный закон от 02.12.1990 N 395-1 (ред. от 01.05.2017) "О банках и банковской деятельности"

2 Стандарт Банка России ормационной безопасности организаций банковской кой Федерации": "Общие положения" СТО БР ИБ -2014] // Сайт Банка России www.cbr.ru.

3 Рекомендации Банка Р ндартизации "Обеспечение информационной безоп ий банковской системы Российской Федерации енки рисков нарушения информационной безопас -2.2-2009 [от 01-01-2010] // Сайт Банка России www.c

4 Аникеева К.А. Перспекти ий в банковском деле / К.А. Аникеева, А.В. Золотарю лютное регулирование и валютный контроль. – 2014.

5 Баранова Е.К, Бабаш А.В нная безопасность и защита информации. Москва: ИЦ [

Сегодня налог составляет совокупность сборов, пошлин и других выплат, удерживаемых в соответствии с определенными правилами. Собранные средства направляются на обеспечение государственности и социально-экономическое развитие. Наряду с этим, налоги играют важную роль в регулировании деятельности предприятий и организаций, в улучшении уровня жизни населения. Налоги есть главный источник финансовых ресурсов, который централизует государство, чтобы обеспечить

6 Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Серия 3: Образовательные ресурсы и технологии. 2015 № 1 (9). С. 73–79.

7 Баранова Е.К., Бабаш А.В. Практикум по моделированию систем защиты информации: учебное пособие. – М.:РИОР:ИНФРА-М, 2014.

8 Баранова Е.К., Чернова М. Сравнительный анализ программного инструментария для анализа и оценки рисков информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 160–168.

9 Баранова Е.К., Зубровский Г.Б. Управление инцидентами информационной безопасности. Проблемы информационной безопасности / Труды I Международной научно- практической конференции «Проблемы информационной безопасности» Гурзуф, Крымский федеральный университет им. В. И. Вернадского, 26–28 февраля 2015 г. С.27–33.

10 Башлыков М. Актуальные вопросы информационной безопасности // Финансовая газета (Региональный выпуск). 2006. № 4. С.14.

11 Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. (Гриф УМО по дополнительному профессиональному образованию). № 2. Изд.3, перераб. и доп. М.: Книжный дом «ЛЕНАНД», 2014. — 248 с.

12 Варлатай С. К. Аппаратно-программные средства и методы защиты информации / С. К. Варалтай. – Владивосток : ДВПИ, 2007. – 318 с.

13 Васильев В.И. Интеллектуальные системы защиты информации. учеб. пособие. М.: Машиностроение, 2013 г. – с. 172

14 Волков Я. Системы обеспечения информационной безопасности как часть корпоративной культуры современной организации // Финансовая газета. 2006. № 34. С. 15.

15 Гайдар Е.В. BI-технологии предотвращают мошенничество в банковской сфере / Е.В. Гайдар, А.В. Золотарюк, Е.С. Худеньких // Валютное регулирование и валютный контроль. – 2015. – №5. – С. 63–66.

16 Генкин А., Суворова Е. Электронные платежи: будущее наступает сегодня. М.: Альпина Паблишер, 2011. 284 с.

17 Голов А. Построение эффективной системы информационной безопасности // Фин. газ. 2006. № 8. С. 4-6.

18 Достов В.Л., Шуст П.М., Валинурова А.А., Пухов А.В. Электронные финансы. Мифы и реальность. М.: КноРус, 2012. 232 с.

19 Золотарюк А.В. Информационные технологии банковского бизнеса // Валютное регулирование и валютный контроль. – 2014. – №8. – С. 56–57

20 Зяброва Н. П. Концепция постановки управленческого учета в банковском секторе / Н. П. Зяброва // Научный журнал КубГАУ. – 2013. – № 87. –С.1-11.

21 Иванов А.В., Шлыков В. В. Экономическая безопасность предприятия. М., 1995. 265 с.

22 Исамидинов А. Н. Защита коммерческой тайны в сфере трудовых отношений. № 11. М.: Книжный дом «ЛИБРОКОМ», 2014. — 120 с.

23 Ковалев Д., Сухорукова Т. Экономическая безопасность предприятия // Экономика Украины. 1998. № 10. С. 48–51.

24 Коржов В. Современные DDoS-атаки. URL: http://www.osp.ru/lan/2014/09/13042710/

25 Леньков А.Н. Потенциальные угрозы экономической безопасности коммерческого банка и объекты ее защиты // Известия Санкт - Петербургского государственного электротехнического университета ЛЭТИ. - 2013. - № 7. - С. 125 – 126.

26 Макаренко С.И., Чукляев И.И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. № 1(2). 2014. С. 13-21.

27 Мельников, В. П. Информационная безопасность и защита информации / В. П. Мельников. – М. : Издат. центр «Академия», 2008. – 336 с.

28 Основные направления развития финансового рынка Российской Федерации на период 2016-2018 год [Электронный ресурс]. URL: http: www.cbr.ru https:/ /finmarkets/files/development/onrfr_2017-18.pdf.

29 Петренко С.А. (2009). Анализ рисков в области защиты информации. Санкт-Петербург.

30 Полякова Т.А. Организационное и правовое обеспечение информационной безопасности: Учебник и практикум. – М.: Юрайт, 2017. – С. 54 – 56.

31 Портал информационной безопасности [Электронный ресурс]. - Режим доступа: www.content -security.ru.

32 Ревенков П.В., Бердюгин А.А. Дистанционное банковское обслуживание: Интернет создает нового клиента и дополнительные риски // Финансы и кредит, (2014), №7, С. 30-39

33 Ревенков П.В. Дистанционное банковское облуживание: актуальные направления регулирования // Банковское дело. 2012. № 9. С. 57-62.

34 Сергин А. М. Банковский надзор и устойчивость кредитных организаций: проблемы действующей системы / А. М. Сергин // Вестник Омского университета. Серия «Экономика». – 2015. – № 2. – С.55-65.

35 Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2008. 320 с.

36 Скобелев А. Рэнкинг российских интернет-банков 2014 // Банковские технологии. 2014. № 4. С.54-58.

37 Смольянинова Е.Н., Духанина Н.А., Дашидондокова А.Ц. Проблемы безопасности расчётов пластиковыми картами // Фундаментальные исследования. 2015. № 2-22. С. 4969-4973

38 Соляной В.Н., Сухотерин А.И. Взаимодействие человека, техники и природы: проблема информационной безопасности. Научный журнал (КИУЭС) Вопросы региональной экономики. УДК 007.51 №5 (05) Королев. ФТА. - 2010.

39 Чистов Д.В. Проектирование информационных систем: Учебник и практикум / Д.В. Чистов, П.П. Мельников, А.В. Золотарюк, Н.Б. Ничепорук; под ред. проф. Д.В. Чистова. – М.: Юрайт, 2015.

40 Шишкин В.В., Юрков Н.К., Мусин Н.Ж. Методика обеспечения информационной безопасности // Надежность и качество сложных систем. 2013. № 4. С. 9-13.

41 Ярочкин В. И. Безопасность информационных систем. М., 1996. 197 с.

42 Ярочкин В. И. Система безопасности фирмы. М., 1997. 185 с.

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт экономики, управления и природопользования
кафедра финансов

УТВЕРЖДАЮ
Заведующий кафедрой
_____ И.С. Ферова
подпись
«_8_» июня 2018 г.

ДИПЛОМНАЯ РАБОТА

специальность 38.05.01 «Экономическая безопасность»

АНАЛИЗ И ОЦЕНКА ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ НА ПРИМЕРЕ КРЕДИТНОЙ ОРГАНИЗАЦИИ

Научный руководитель	_____ подпись, дата	старший преподаватель должность, ученая степень	Е.В.Шкарпетина инициалы, фамилия
Консультант	_____ подпись, дата	д-р. юр.наук, профессор должность, ученая степень	Н.Н.Цуканов инициалы, фамилия
Выпускник	_____ подпись, дата		А.С.Матвеев инициалы, фамилия
Рецензент	_____ подпись, дата	начальник отделения ОЭБиПК МУ МВД должность, ученая степень	Д.Г.Поздняков инициалы, фамилия
Нормоконтролер	13.06.18г. подпись, дата		Е.В.Шкарпетина инициалы, фамилия

Красноярск 2018