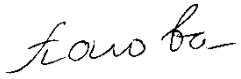
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

На правах рукописи



Попова Елена Владимировна

Методы и алгоритмы обоснования системы защиты информации по критерию конкурентоспособности предприятия

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени

кандидата технических наук

Научный руководитель:

д. т. н., профессор

Молдовян А. А.

Санкт-Петербург – 2017

Содержание

Введение

Актуальность темы диссертационной работы. Проблемы информационной безопасности (ИБ) предприятия актуализируются вовлечением информационных технологий в бизнес-процессы, возрастанием ценности информации по сравнению с другими ресурсами, наличием безбарьерного интернет-пространства, высокотехнологичными, целевыми действиями нарушителей ИБ.

Информация является интеллектуальным активом предприятия, который необходимо защищать. Часть информационных ресурсов компании могут быть уникальными нематериальными ресурсами, которые трудно воспроизвести, сымитировать и заменить.

Для повышения состояния защищённости предприятия от угроз нарушения ИБ необходимо выбрать оптимальный вариант системы защиты информации (СЗИ). Обеспечение ИБ предприятия даёт преимущество по отношению к другим предприятиям в данной отрасли. Необходимо выбрать наилучший вариант СЗИ для малого предприятия из N сформированных, при котором конкурентоспособность предприятия будет максимальной.

Таким образом, решение проблем выбора наилучшего варианта СЗИ для повышения состояния защищённости предприятия от угроз нарушения ИБ по критерию конкурентоспособности предприятия является актуальным и соответствует современной научной проблематике.

Степень разработанности темы исследования. Проблеме обеспечения ИБ за счёт построения обоснованного варианта СЗИ посвящены работы Грибунина В.Г., Малюка А.А., Петрова В.А., Пискарева А.С., Шеина А.В., Зегжды Д.П., Герасименко В.А., Грушо А.А., Щербакова А.Ю., Девянина П.Н., Романец Ю.В., Тимофеева П.А., Шаньгина В.Ф., а также зарубежных авторов К. Лендвера, Р. Сандху, М. Бишопа и других. Однако в известных работах выбор СЗИ по критерию конкурентоспособности предприятия не рассматривался. Вопросам

анализа эффективности СЗИ посвятили труды такие российские и зарубежные авторы как Домарёв С.В., Маслова Н.А., Суханов А.В., Peltier, Thomas R., Behnia A., Rashid R.A. и Chaudhry J.A. В работах этих авторов не использовалась неполная, неточная и нечисловая информация (*ннн*-информация), целесообразность учета которой указана в работах Хованова Н.В.

Объектом исследования являются СЗИ предприятия.

Предметом исследования являются критерии, нечёткие модели и методы выбора варианта СЗИ для предприятия.

Основной **целью** работы является обоснование выбора наилучшего варианта СЗИ по критерию конкурентоспособности предприятия и повышение состояния его защищённости от угроз нарушения ИБ.

В соответствии с поставленной целью решены следующие **задачи**:

1) Анализ источников проблематики исследования и постановка задачи.

2) Разработка алгоритма генерации допустимых вариантов системы защиты информации.

3) Разработка метода оптимизации вариантов защиты.

4) Разработка алгоритма обработки нечётких входных данных.

5) Разработка метода обоснования СЗИ по критерию конкурентоспособности предприятия.

6) Экспериментальная оценка предложенных методов и алгоритмов и сравнение их с существующими аналогами.

Методы исследования. Поставленные задачи решены на основе применения теории принятия решений, теории защиты информации, теории графов, методов дискретной математики, системного анализа, экспертного анализа.

Основные результаты, выносимые на защиту:

1) алгоритм генерации допустимых вариантов системы защиты информации;

2) метод оптимизации вариантов защиты;

3) алгоритм обработки нечётких входных данных;

4) метод обоснования СЗИ по критерию конкурентоспособности предприятия и алгоритм оценки эффективности СЗИ.

Научная новизна работы. Научная новизна полученных результатов обусловлено следующим:

1) полученный в диссертации метод обоснования СЗИ по критерию конкурентоспособности предприятия отличается от известных тем, что учитывает значения предложенных показателей конкурентоспособности и использует их для принятия решений;

2) разработанный алгоритм генерации допустимых вариантов системы защиты информации, в отличие от известных, учитывает стоимость и совместимость средств защиты информации;

3) разработанный алгоритм обработки нечётких входных данных отличается от известных тем, что в нем впервые используется в качестве входных данных опорные точки функции принадлежности коэффициента изменения конкурентоспособности.

4) полученный метод оптимизации вариантов защиты и алгоритм оценки эффективности СЗИ, в отличие от известных, учитывают коэффициент изменения конкурентоспособности.

Достоверность полученных результатов обеспечивается научной обоснованностью приводимых расчётов, корректностью используемых математических выражений; подтверждается сверкой теоретических положений с полученными в ходе внедрения на двух предприятиях реальными значениями; широкой апробацией результатов диссертационной работы на научно-технических конференциях мирового и всероссийского уровня.

Практическая значимость определяется возможностью использования для выбора наилучшего варианта СЗИ для конкретных условий функционирования предприятия.

Результаты внедрения. Результаты диссертационной работы успешно опробованы на двух малых предприятиях г. Санкт-Петербурга (ЗАО «КОНТО», ООО «Лесной Двор») и внедрены в учебный процесс «Смольного института РАО».

Апробация результатов исследования. Результаты, полученные в ходе исследования, докладывались и обсуждались на ряде конференций, в том числе на II Международной научно – практической конференции «Инновационные процессы в сфере сервиса: проблемы и перспективы» (2010); II Всероссийской научной конференции «Научное творчество XXI века» с международным участием (2010); конференции «Актуальные проблемы современной науки и образования» (2010); Всероссийской научно – практической конференции «Проблемы развития предпринимательства» (2010); V межвузовской научно – практической конференции студентов, магистрантов и аспирантов «Социально – экономические аспекты сервиса: современное состояние и перспективы развития» (2011); III Международной научно-практической конференции «Инновационные технологии в сервисе» ITS (2012); конференции «Региональная информатика (РИ-2012)», конференции "Информационная безопасность регионов России (ИБРР-2013)", конференции «Региональная информатика (РИ-2016)».

Публикации. По теме диссертации опубликовано 17 работ, в том числе 4 статьи в изданиях, рекомендованных ВАК.

Структура диссертации. Диссертационная работа состоит из введения, четырёх глав, заключения, списка источников литературы и приложений. Общий объем диссертационного исследования составляет 155 страниц машинописного текста, включая 18 таблиц, 27 рисунков и 5 приложений. Библиографический список содержит 166 наименований.

Краткое содержание работы. В первой главе исследованы вопросы наиболее используемых в настоящее время методов выбора и создания СЗИ на предприятиях. Рассмотрены существующие методики расчёта эффективности

работы СЗИ. Сформулирована техническая задача, которая заключается в том, что необходимо найти целесообразный способ (средство) защиты информационных ресурсов, при котором конкурентоспособность предприятия будет максимальная. Во второй главе получен алгоритм генерации допустимых вариантов системы защиты информации и представлен метод оптимизации вариантов защиты. В третьей главе получен алгоритм обработки нечётких входных данных и представлен метод обоснования СЗИ по критерию конкурентоспособности. В четвертой главе показаны результаты внедрения разработанных методов и алгоритмов в хозяйственную деятельность двух малых предприятий, сравниваются реальные и теоретические результаты.

Глава 1 Анализ научных источников по проблематике исследования и постановка задачи

1.1 Этапы создания СЗИ

Цель данной главы – исследовать вопросы наиболее используемых в настоящее время методов выбора и создания СЗИ на предприятиях, а также формирования службы информационной безопасности (СИБ) предприятия. Познакомиться с существующими методиками расчёта эффективности работы СЗИ. Изучить роль информационной безопасности в обеспечении конкурентоспособности предприятия. Сформулировать постановку технической задачи.

Построение СЗИ – это комплексный поэтапный процесс, который начинается с определения цели СЗИ и переходит в поддержание работоспособности реализованного варианта СЗИ. Первым шагом при построении системы защиты информации должно стать понимание необходимости такой защиты. Помимо крупных и средних предприятий, в поле зрения злоумышленников всё больше попадают и малые предприятия. «Создатели вредоносных программ давно обратили внимание, что не на всех малых предприятиях уделяют информационной безопасности должное внимание. Вместо того, чтобы взламывать систему крупной компании, можно украсть данные из нескольких малых предприятий и остаться при этом незамеченными [30]. Специально созданные программы сканируют компьютеры в незащищённых системах, поставляя злоумышленникам полученные данные.

Для сохранения конкурентных преимуществ предприятиям нужно охранять свои базы данных [115], обрабатывать новую информацию и уделять нужное внимание информационной безопасности» [90].

Создание СЗИ включает начальный этап определения объектов, подлежащих защите. Согласно ГОСТ РФ 50922-2006 «система защиты информации: Совокупность органов и (или) исполнителей, используемой ими

техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации» [16]. «При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется: … принятие решения о необходимости создания системы защиты информации информационной системы, а также определение целей и задач защиты информации в информационной системе…» [131].

Построение СЗИ – это комплексный поэтапный процесс, начинающийся с определения цели СЗИ. Целью является достижение состояния защищённости предприятия от угроз нарушения ИБ с опорой на количественные значения конкурентоспособности, в которые входят показатели целостности, доступности, конфиденциальности информации.

«Организационные и технические меры защиты информации, реализуются в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе» [131]. При принятии решения о защите информации на предприятии, нужно определить объекты защиты.

Определение информации дается в законе № 149 - ФЗ от 27.07.2006 «Об информации, информатизации и защите информации» в статье 2: «информация - сведения (сообщения, данные) независимо от формы их представления» [38]. Понятие очень объемное, и возникает вопрос, нуждаются ли в защите все сведения. В этом же законе «Об информации, информатизации и защите информации» говорится, что все сведения являются открытыми и общедоступными, за исключением информации, отнесенной к категории ограниченного доступа, которая и нуждается в защите.

«К информации с ограниченным доступом относятся: государственная тайна и конфиденциальная информация» [38]. Под государственной тайной, в соответствии с Законом РФ № 5485-1 от 21.07.1993 «О государственной тайне»,

следует понимать: «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контр-разведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации» [39]. При этом в соответствии со «степенью тяжести ущерба, который может быть нанесен безопасности Российской Федерации вследствие распространения указанных сведений, государственная тайна имеет три степени секретности: «особой важности», «совершенно секретно» и «секретно» [39].

Конфиденциальность информации в соответствии с определением, данным в статье 2 №149 - ФЗ «Об информации, информатизации и защите информации», трактуется, как требование не передавать информацию третьим лицам без согласия ее обладателя. В указе Президента РФ от 06.03.1997 № 188 (ред. от 23.09.2005) «Об утверждении Перечня сведений конфиденциального характера» перечислены сведения, носящие конфиденциальный характер [127]. Персональные данные относятся к конфиденциальной информации. В законе от 27.07.2006 № 152-ФЗ «О персональных данных» говорится, что «персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [41].

Ещё одним видом конфиденциальной информации наряду с персональными данными [114] является информация, которую можно отнести к коммерческой тайне. В законе № 98-ФЗ от 29 июля 2004 года «О коммерческой тайне» к ней относят информацию, которая имеет «действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам. Право объявлять информацию коммерческой, и на определение перечня и состава такой информации принадлежит лицу, владеющему этой информацией» [40].

Таким образом, можно говорить о том, что «защите подлежит любая информация, неправомерное обращение с которой может нанести ущерб ее обладателю» [38]. При этом, защита информации является не только правом, но и обязанностью [35,72,142].

Предприятия, на которых не создан специальный административно-правовой режим (режим секретности), как правило, не работают со сведениями, составляющими государственную тайну. Необходимо акцентировать внимание на информации, зашита которой определяется Законодательством РФ, и её потеря может негативно отразиться на работе предприятия [34]. Очевидно, что универсальный перечень такой информации составить сложно, но можно выделить, общие сведения, нуждающиеся в защите. [88,52,124]

Перечень сведений, подлежащие защите, формируют в зависимости от целей и задач бизнес-процессов конкретного предприятия. К ним относятся:

- договоры и контракты, как уже заключенные, так и находящиеся в разработке, причем последние, очевидно нуждаются в большей защите, так как конкуренты, зная предлагаемые условия, могут составить более выгодное предложение, исключив предприятие из конкурентной борьбы за заказ;
- сведения о товарах и услугах, предоставляемых компанией;
- финансовые документы;
- состояние материальных запасов, резервов;
- сведения о поставщиках;
- персональные данные, как работников предприятия, так и клиентов, не зависимо от того, контактировали они в прошлом, продолжают сотрудничество в настоящем или предположительно являются потенциальными клиентами компании в будущем.

В данном вопросе возможна технологическая помощь со стороны внешних аудиторов, которые квалифицированно отберут информацию, нуждающуюся в защите [110,97]. Но если у предприятия нет средств на привлечение сторонних специалистов, данный вопрос может быть решен самостоятельно. Возможно создание комиссии из специалистов, которые составляют список сведений, подлежащих защите.

После этого, выбранную информацию следует ранжировать, то есть присвоить ей определенный гриф секретности [4,120,66]. Такими грифами «для

государственных предприятий, могут быть: «открытая информация», «для служебного пользования», «секретно», «совершенно секретно», «особой важности»» [39]. В частных компаниях указанные грифы не могут быть использованы, но градация может быть разработана на основе аналогичных словосочетаний.

Возникает вопрос, что положить в основу градационного деления информации. Критерием может служить денежная оценка возможного ущерба, которую можно получить с использованием метода экспертных оценок. Этот метод предполагает опрос группы экспертов, причём в роли экспертов могут выступать те же сотрудники, которые составляли предварительный перечень защищаемой информации.

«Сначала информация делится на общедоступную и ограниченного доступа на рисунке 1.1. Из информации ограниченного доступа выделяют информацию, составляющую государственную тайну и конфиденциальную.

Если предприятие негосударственное, выбранную информацию можно ранжировать по стоимости информационного ресурса» [101].

Общедоступная информация свободно циркулирует в информационных потоках предприятия. Остальная информация подлежит защите в обязательном порядке. Информация, составляющая государственную тайну и персональные данные, прописана в соответствующих законах [39, 41].

Для составления данного перечня следует собрать экспертную комиссию из специалистов, занятых информационными технологиями. Одновременно с этим, этой же экспертной комиссией проводится оценка этих сведений с учётом основных типов угроз нарушения: конфиденциальности, целостности, доступности информации.

Рисунок 1.1 – Градация информации, циркулирующей на предприятии

Рассмотрим метод определения стоимости информации. Согласно международному стандарту по информационной безопасности ISO 27001 [164] стоимость информационного ресурса определяет его владелец. В 1977 году в докладе перед Конгрессом и Президентом США впервые было заявлено, что «информация не является больше бесплатным общественным благом» [161].

Стоимость информации не определена ни в одном российском законе. Стоимость информации в государственных организациях можно определить косвенным путём по грифам секретности. Чем секретнее информация, тем, очевидно, выше её стоимость. Но грифы секретности присваивать информации в коммерческой организации запрещено. Частное лицо или коммерческие структуры должны сами определять стоимость информации. Для начала, рассмотрим элементы, составляющие стоимость: Рыночная стоимость информации (РС); Возможные дополнительные потери (ВП); Недополученная прибыль (НП).

Таким образом, стоимость информации (СИ) можно определить как сумму следующих элементов (1.1).

$$СИ = РС + ВП + НП \quad (1.1)$$

Точно оценить все три слагаемых чрезвычайно сложно. Оценки будут приблизительными, но возможно распределение информации на классы и выявление самого значимого класса для предприятия.

Для оценки стоимости информационного ресурса при нарушении конфиденциальности информации можно использовать следующие составляющие: ущерб от раскрытия конфиденциальных сведений; снижение стоимости акций компании; потеря клиентов; уменьшение контрактов; средства, затраченные на восстановление положительного имиджа компании; средства, затраченные на восстановление связей с клиентами и поставщиками [130].

Для оценки стоимости ресурса при нарушении целостности информации следует оперировать такими понятиями как время восстановления целостности ресурса, время повторного ввода потерянной информации.

Для оценки стоимости ресурса при нарушении доступности информации оценивают упущенную выгоду, время простоя.

После оценки стоимости каждого информационного ресурса подлежащего защите по всем трем направлениям, целесообразно присвоить ему итоговый класс. Ранжирование по классам производится в зависимости от стоимостной величины: низкий; средний; высокий. Наименование классов и диапазоны совокупной стоимости выбираются каждой организацией самостоятельно.

После этого издаётся документ «Перечень сведений подлежащих защите» в форме приказа по предприятию. Затем можно переходить к анализу рисков.

1.2 Анализ рисков и угроз информационной безопасности

После определения информации, защита которой необходима, следует провести анализ возможных угроз и каналов утечки информации [51,31,46]. Не

все потенциальные угрозы могут быть реализованы в отношении защищаемой информации, нужно определить угрозы, вероятность реализации которых достаточно большая для конкретного предприятия. На этом же этапе следует оценить вероятные потери от реализации этих угроз.

Поэтому не менее важным для создания системы защиты информации является этап анализа рисков [11]. На данном этапе используются полученные ранее результаты, а именно, перечень сведений, подлежащих защите и их ценность.

В качестве основы для проведения анализа можно использовать Британский стандарт BS7799 и, принятый на его основе, международный стандарт ISO 17799, а также Германский стандарт BSI. Британский стандарт дает лишь общие рекомендации и принципы, в то время как Германский стандарт рассматривает различные элементы информационной системы (ИС). Можно использовать наши стандарты - ГОСТ ИСО/МЭК 17799 и ГОСТ ИСО/МЭК 27001 [21], являющиеся техническими переводами версий международных стандартов серии ISO 27000.

В них говорится, что «риск (information security risk) – это возможность того, что данная угроза будет использовать уязвимости актива или группы активов и, тем самым, нанесет вред организации. Угроза - это любое событие, которое потенциально может нарушить правила информационной безопасности» [21]. Например, угрозами информационной безопасности могут быть раскрытие, модификация или разрушение информации [56].

Процесс анализа рисков можно начинать с характеристик системы, то есть со сбора данных о самой ИС. Должны быть получены сведения об используемом в ИС аппаратном и программном обеспечении, внутренних и внешних связях ИС, данные о функциональных требованиях ИС, топологии сети, информационных потоках компании. Для получения этих данных можно использовать анкетирование, опросы, просмотр документации, автоматические средства.

Анализ информационных рисков – это комплекс мероприятий, направленный на выявление угроз, оценку вероятности их реализации и возможного ущерба. Идентификация угроз начинается с классификации угроз. Классификация угроз осуществляется по следующим признакам:

• по виду защищаемой информации;

• по видам возможных источников угроз безопасности;

• по типу информационной системы (ИС), на которую направлены угрозы;

• по способу реализации угроз безопасности;

• по виду несанкционированных действий;

• по используемой уязвимости;

• по объекту воздействия» [132].

Составить конечный список потенциальных угроз, появляющихся на всех предприятиях, достаточно сложно и нецелесообразно, так как они многочисленны, специфичны и не стационарны. Для каждого предприятия подготавливается свой конкретный список возможных угроз. Составить полный список угроз достаточно сложно [62], так как они разнообразны и динамичны. Один из вариантов списка предложен в Приложение 1.

Реализация угроз возможна при наличии уязвимостей в информационной системе (ИС) [75]. «Уязвимость – это недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, которым (которая) может быть использована для реализации угроз безопасности информации» [17]. Потенциально уязвимыми являются буквально все основные элементы ИС: рабочие станции, серверы, сетевые устройства, каналы связи [86,63,113]. «В список уязвимостей для предприятия включают: уязвимости программного обеспечения (ПО), уязвимости системного ПО, уязвимости прикладного ПО. Можно пользоваться единой базой данных Common Vulnerabilities and Exposures» [101].

Возможно применение следующих методов идентификации уязвимостей ИС: использование сведений об уязвимостях, распространяемых

производителями; периодическое тестирование системы, используя утилиты для автоматического поиска уязвимостей или тесты на проникновение; анкетирование. В результате составляется список уязвимостей, которые могут быть использованы потенциальными источниками угроз.

Для определения вероятности реализации угроз существуют различные методы. Если накоплены сведения о зафиксированных инцидентах за определённый период, например, предыдущий год [76], можно построить линию тренда, дополняя её прогнозным участком. Также можно воспользоваться сценарным анализом, в рамках которого изучаются причины происхождения нарушений ИБ, следствия этих нарушений и итоговая составляющая этих событий для деятельности предприятия. Результаты анализа оцениваются экспертами, итерационным или совещательным методами.

Величина ущерба и вероятности не обязательно должны быть выражены в количественных показателях, так как возможно использование методов сценарного анализа и интервального прогнозирования. Риски ранжируют по вероятности реализации и по величине ущерба для предприятия.

Таким образом, методики оценки рисков могут быть качественными и количественными. Качественный анализ более быстрый и простой. Нет необходимости присваивать денежную стоимость активу, вычислять частоту появления угрозы и точный размер ущерба. Задача качественной оценки — распределение факторов риска по группам, выявление самых серьезных угроз.

Существует несколько моделей качественного анализа [157]. Варианты различаются лишь количеством градаций риска. Одна из самых распространенных моделей — трехступенчатая. Каждый фактор оценивается по шкале "низкий — средний — высокий". «Приложение к стандарту ГОСТ ИСО/МЭК 27001 содержит единственный пример, который также можно отнести к качественному методу оценки. Данный пример использует трех и пятибалльные оценочные шкалы:

1. Оцениваются уровни стоимости идентифицированного ресурса по пятибалльной шкале: «незначительный», «низкий», «средний», «высокий», «очень высокий».

2. Оцениваются уровни вероятности угрозы по трехбалльной шкале: «низкий», «средний», «высокий».

3. Оцениваются уровни вероятности уязвимости: «низкий», «средний», «высокий».

4. По заданной таблице рассчитываются уровни риска.

5. Проводится ранжирование инцидентов по уровню риска» [21].

Качественный и количественный методы имеют как положительные, так и отрицательные стороны. Качественная модель используется в тех случаях, когда дополнительная точность не требуется, предприятие быстро развивается, многие параметры быстро меняются, и значения рисков изменяются теми же темпами. Он позволяет ранжировать риски по определенным критериям, существенным для данного предприятия, выявлять вопросы, требующие немедленного решения. Недостатком этого метода является то, что не приводятся точные измерительные показатели, которые могли бы быть использованы в расчётных исследованиях.

«Количественная оценка риска (risk estimation) – это процесс присвоения значений вероятности и последствий риска» [22], то есть перемножаются вероятности осуществления угрозы за определенный промежуток времени, например за год, и стоимость потерь от реализации угроз. Результаты количественного анализа более наглядные, точные, эффективнее используются для бизнес-планирования. Недостатком этого метода является то, что он требует больше времени, более затратен и, хоть и в меньшей степени, но опирается на субъективные показатели.

Можно выделить общие негативные черты, присущие обоим методам:

1. Большая погрешность вычислений. Невозможно добиться высокой точности при оперировании вероятностью или величиной ущерба. Но она не всегда и требуется. Например, можно оценить частоту появления события с большой погрешностью, при этом, достаточно знать, что значение частоты входит в рамки приемлемых значений. При расчёте эффективного уровня затрат на защиту, также не нужна излишняя точность, так как достаточно знать, что потери не превышают допустимые.

2. Быстрое устаревание. Оценка риска не может быть актуальна длительное время. При изменении параметров системы нужно проводить новую оценку.

Таким образом, проанализировав риски реализации угроз для предприятия, можно переходить к следующему этапу.

1.3 Модель нарушителя информационной безопасности

После анализа рисков необходимо спрогнозировать вероятных нарушителей. Под нарушителем подразумевается лицо, обеспечивающее реализацию угроз информационной безопасности. Предварительно обрисовав облик нарушителя для конкретного предприятия, составив модель нарушителя, можно соответственно реагировать на возможные угрозы и выбрать необходимые средства защиты.

Человеческий фактор является основным при исследовании нарушений информационной безопасности. Движение, обработка, хранение, использование информации невозможно без людей, но, в то же время, они могут быть первопричиной нарушений, «слабым звеном» в налаженной системе информационной безопасности. Модель нарушителя — описание потенциальных нарушителей правил разграничения доступа. В модель нарушителя должны входить:

- классы нарушителей;

- поставленные ими цели;
- оснащенность и квалификация;
- разработанные сценарии поведения.

При составлении модели нарушителей делят на:

- внешних нарушителей;
- внутренних нарушителей.

Количество инцидентов, совершаемых при участии внутренних нарушителей может доходить до 80%. В связи с этим, даже малое предприятие, не подключённое к Интернету, должно озаботиться проблемами информационной безопасности. Необходимо проработать мотивы и обстоятельства, толкающие людей на совершение злонамеренных действий, чтобы предотвратить нарушения или принять соответствующие контрмеры. К внутренним нарушителям можно отнести:

- обслуживающий персонал;
- программистов;
- технический персонал;
- сотрудников бизнес подразделений;
- руководителей предприятия.

К внешним нарушителям относятся люди, которые могут находиться в помещениях с определённым оборудованием только под контролем сотрудников предприятия. К ним относятся:

- клиенты;
- посетители;
- поставщики;
- посторонние, нарушающие режим предприятия;
- посторонние, находящиеся за пределами предприятия;

При использовании модели нарушителя для анализа соответствующих угроз информационной безопасности нужно помнить о возможном существовании связи между внутренними и внешними нарушителями.

Следует оценить уровень информированности потенциального нарушителя о защищаемой системе (ЗС) и возможность влияния на ЗС. Также необходимо определить, где может находиться нарушитель во время совершения несанкционированных действий, имеет ли он непосредственно физический доступ к автоматизированным рабочим местам (АРМ), к средствам защиты (СЗ) информации, или атака будет организована дистанционно.

Немаловажным является время возможного совершения несанкционированных действий, например, в рабочее или в нерабочее время, а также длительность организуемой атаки.

Но в особую категорию нужно выделить модель нарушителя – конкурента. Действия конкурентов могут быть как завуалированными, так и провокационно открытыми. Цели варьируются от блокирования функционирования информационной системы конкурента, подрыва имиджа до деструктивных действий, направленных на неконтролируемое возрастание ущерба, разорение, банкротство.

1.4 Методы снижения рисков и вероятности реализации угроз

После того как риск проанализирован, и выбрана модель нарушителя, можно переходить к обработке «риска (risk treatment), то есть к выбору, реализации мер и средств по минимизации риска. Эффективность обработки риска зависит от предыдущих результатов оценки риска. Но обработка риска может не обеспечить приемлемый уровень остаточного риска» [23]. То есть потребуется еще одна итерация оценки риска с небольшими изменениями критериев оценки, за которой последует процедура обработки риска. В обработку риска входят следующие понятия: уменьшение риска; передача риска; принятие риска; отказ от риска.

Уменьшение или снижение риска (risk reduction) – меры, принимаемые для снижения вероятности реализации угрозы или негативных последствий,

связанных с риском, или того и другого. Если оценённый риск не соответствует критериям безопасности, его величину пытаются уменьшить различными способами. Вероятность снижают устранением причин появления риска. Величину ущерба можно снизить ещё на предварительных разработках, а также увеличением мероприятий по усилению защищённости объекта (внедрение межсетевого экрана, проведение обучения сотрудников и т.д.).

Необходимо отслеживать возможность появления новых рисков при изменении параметров объекта [9]. Возможно слияние рисков, если этот процесс способствует улучшению обработки. Процесс снижения риска должен проходить до достижения уровня, утверждённого как приемлемый для данного предприятия.

Передача или перенос риска (risk transfer) происходит, когда риск полностью или частично переадресуется сторонней организации. Риск, оставшийся после risk reduction, может подвергнуться дальнейшей модификации, «перенесён» в другую компанию, которая взяла на себя соответствующие обязательства. Такими компаниями могут выступать субподрядчики или страховые компании. Страховка покрывает финансовые последствия ущерба. Договор субподряда обязывает партнёра проводить мониторинг информационной системы компании, осуществлять действия по прекращению атаки до достижения определённого уровня ущерба.

Но перенос риска не означает полного его обнуления. Возможны модификации остаточных рисков, возникновение новых. Поэтому может понадобиться дополнительная обработка риска. Следует помнить, что при переносе риска, возможно, перенести ответственность за менеджмент риска, но не за имиджевые потери. Клиенты идентифицируют неблагоприятное влияние ущерба с самим предприятием, и этим могут воспользоваться конкуренты.

Аннулирование или предотвращение риска (risk avoidance) - решение не принимать участия в действиях, сопряженных с риском, или принятие мер по недопущению ситуации, связанной с риском. Предприятие может отказаться от

деятельности, которая вызывает неприемлемый риск, если это возможно. Если расходы на обработку риска превышают выгоду от этой деятельности, возможен полный отказ от планируемых мероприятий. Например, возможно запрещение использование сотрудниками беспроводной связи, вместо того, чтобы бороться с множеством рисков, связанных с этими технологиями. Но нужно понимать, что компании, разрешающие сотрудникам и клиентам пользоваться беспроводной связью, будут более привлекательными для клиентов и получат преимущество в конкурентной борьбе.

Принятие или сохранение риска (risk retention) - принятие бремени потерь от конкретного риска. Если стоимость контрмер превосходит финансовые потери при реализации угрозы, а отказ от конкретных мероприятий невозможен, приходится мириться с вероятными последствиями. Перед этим необходимо разработать критерии принятия риска, которые зависят от целей предприятия, применяемых технологий, финансовых возможностей. Если уровень риска соответствует разработанным критериям принятия риска, то риск может быть сохранен.

Риск может быть зафиксирован как приемлемый на данном этапе, но в дальнейшем возможны мероприятия по его снижению до более низкого уровня. Возможно также принятие риска, если он связан с кратковременной деятельностью. При принятии риска необходимо предвидеть возможность возрастания инцидентов безопасности, потенциальные убытки, и неоднозначную реакцию клиентов на возможные инциденты.

Решение о наиболее приемлемом варианте обработки риска или комбинации вариантов может быть принято с помощью экспертного анализа. После обработки риска остаточные значения подвергаются анализу, и принимается решение о продолжении или завершении обработки. Анализируя затраты на обработку, потенциальные выгоды от выполнения вариантов обработки, осуществляя рентабельные действия, риск принимается и считается допустимым.

Процедуры обработки риска, также как и процедуры оценки риска обычно выполняются итеративно. Итеративный подход увеличивает глубину и детализацию процесса обработки риска при каждой последующей итерации. На определённом этапе итерационных процессов «общий риск (total risk) - это риск, перед лицом которого стоит компания, не внедрившая никаких защитных мер» [23], переходит в остаточный (residual risk). Снизить риск до нуля невозможно. Систем или сред, защищенных на 100%, не существует, но возможно понижение риска до остаточного, который зафиксирован как приемлемый для данного промежутка времени.

1.5 Определение требований к системе защиты информации

Следующим этапом является формулирование требований к системе. «Формирование требований к защите информации, содержащейся в информационной системе, осуществляется обладателем информации (заказчиком)» [131].

Система защиты информации не должна мешать работе предприятия, она активирует все бизнес-процессы, её создание экономически оправданно, но при этом она защищает информационные ресурсы предприятия от различных угроз.

Одним из важнейших требований к системе является её адаптируемость к изменениям технологических схем, условий функционирования предприятия, стратегического вектора развития и изменения законодательства. Остальные требования делятся на:

- организационные (создание контролируемой зоны, определение порядка информационного взаимодействия);
- технические (шифрование данных, разграничение прав доступа к ресурсам);
- экономические (минимум затрат, использование серийных оптимальных средств защиты);

- эргономические (удобство для пользователей);
- функциональные (обеспечение решения задач, поставленных перед СЗИ).

Фундаментом решения задачи построения системы защиты информации должны быть следующие результаты:

- оптимальная архитектура системы защиты;
- соответствие технологии обработки информации уровню ее защиты;
- оперативная замена вышедших из строя технических средств.

Основным требованием к системе защиты информации является защищенность от несанкционированного доступа к информации (НСД). Для решения этой проблемы необходимо обеспечить:

- поддержку непротиворечивых, однозначно определённых правил разграничения доступа;
- учёт и регистрацию событий, имеющих отношение к защищённости информации;
- стабильную работу программных продуктов (ПП), поддерживающих систему разграничения доступа.

При этом лица, наделённые соответствующими правами, взаимодействующие с объектами, соответствующими их учётной записи, будут наделяться различными полномочиями: для чтения, записи, создания или уничтожения информации [133].

Домарев в работе «Безопасность информационных технологий. Методология создания систем защиты» предлагает «выделить следующие группы требований к системе защиты информации: общие требования; организационные требования; конкретные требования к подсистемам защиты, техническому и программному обеспечению, документированию, способам, методам и средствам защиты.

Общие требования включают в себя идентификацию пользователей, программ, основных процессов и процедур» [32]. Ограничение доступа к информации, достигается путем:

- иерархической классификации информационных ресурсов (ИР);
- ограничений доступа к ИР;
- определение программ и процедур, доступных для каждого пользователя.

Таким образом, СЗИ должна гарантировать фиксацию идентификации, аутентификации [105], авторизации. Организационные требования к СЗИ предусматривают реализацию следующих процедур:

- осуществление контроля изменений в программном обеспечении (ПО);
- фиксирование протокола о доступе к системе;
- профилактику социальной инженерии.

В общем случае Домарев предлагает условно разделить СЗИ на «подсистемы:

- управления доступом к ресурсам;
- регистрации и учета действий пользователей;
- криптографическую;
- обеспечения целостности информационных ресурсов и конфигурации ИС» [32].

Для каждой из подсистем определяются требования. Например, «подсистема управления доступом должна обеспечивать идентификацию, аутентификацию, контроль над доступом пользователей; контроль над потоками информации; очистку освобождаемых областей оперативной памяти и внешних накопителей [144].

Подсистема регистрации учета выполняет регистрацию и учет многих процессов, проходящих в ИС; регистрацию изменения полномочий доступа; оповещение о попытках нарушения защиты» [32].

Криптографическая подсистема отвечает за шифрование конфиденциальной информации; выдачу ключей; использование аттестованных криптографических средств [45].

Подсистема обеспечения целостности отвечает за контроль целостности; резервное копирование; тестирование ИС; отслеживание и борьбу с распространением вирусов; реагирование на проблемы с персональной авторизацией; контроль над использованием только лицензионного ПО.

На основе анализа сформулированных требований генерируются основные функциональные задачи, которые должна решать СЗИ для конкретного предприятия. Итоговым результатом построения СЗИ является не только решение целевых задач, но и стабилизация бизнес-процессов предприятия за счёт снижения отрицательных воздействий использования уязвимостей злоумышленниками, и устранения негативного эффекта реализации методов недобросовестной конкуренции. После формулирования требований к будущей СЗИ, можно приступать к выбору дополнительных средств защиты.

1.6 Выбор средств защиты информации

Под средством защиты информации понимается совокупность технического, инженерного, электронного, оптического и другого оборудования, которое используются для обеспечения информационной безопасности. Средства защиты информации делятся на:

- физические (инженерные средства и сооружения, затрудняющие физический доступ к материальным носителям информации);
- аппаратные или технические (механические, электрические, электронные устройства, предназначенные для защиты информации);
- программные (программы, разработанные для защиты информации);

- криптографические (технические и программные средства шифрования данных);
- комбинированные (генерация аппаратных, программных средств и криптографических методов защиты информации).

Физические средства защищают работников, материальные объекты, информацию от противоправных действий способами, аналогичными способам, использовавшимися при защите материальных ценностей. Это замки, дополнительные стены, решетки, сигнализация.

Технические средства - это различные механические, электромеханические, электронные устройства, разработанные физико-техническими специалистами, которые решают задачи защиты информации. Например, генераторы шума, блокираторы сотовой связи, сканирующие радиоприемники, устройства, следящие за потенциальными путями утечки информации.

Программные средства – это «объекты, состоящие из программ, процедур, правил, а также, если предусмотрено, сопутствующих им документации и данных, относящихся к функционированию системы обработки информации» [15]. Некоторые из них могут быть объединены с программным обеспечением. К ним относятся:

- средства архивации данных;
- антивирусы;
- средства идентификации и аутентификации;
- средства управления доступом;
- средства для протоколирования и аудита.

Например, «межсетевой экран (МЭ) – это система межсетевой защиты, позволяющая разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую» [113]. Происходит фильтрация информации из одной системы в другую на основе заданных правил.

Средства криптографической защиты используют при передаче информации по каналам связи. Они обеспечивают приемлемую защиту передаваемой информации от несанкционированного доступа (НСД) и защиту информации от изменения (использование цифровой подписи, имитовставок).

К комбинированным средствам относятся программно-аппаратные средства, объединённые в одном устройстве. Они выполняют те же функции, что аппаратные и программные средства, настроенные на синхронную работу. Например, скремблеры, шифраторы, электронные идентификаторы.

Выбрать необходимые средства защиты можно исходя из выявленных угроз и уязвимостей, приоритетных задач предприятия и финансовых возможностей. При выборе средства защиты важно оценить его стоимость и стоимость его использования; известные уязвимости; требования для установки обновлений; зависимости от других продуктов; взаимодействие с существующей инфраструктурой.

Для этого необходимо ответить на следующие вопросы:

- насколько средство защиты необходимо для снижения риска;
- сколько и какие пользователи будут их использовать;
- публикуются ли уязвимости в общих базах данных;
- имеются ли зависимости от других продуктов;
- как часто регистрируются отказы, и помогают ли корректирующие действия.

После приобретения средств защиты, их необходимо внедрить в ИС. Внедрение включает в себя не только инсталляцию, но и настройку. Некоторые продукты поставляются с отключенными функциями безопасности или наоборот настроенными на максимальный уровень защиты, что может оказаться чрезмерным [78].

После внедрения, проводят повторный анализ рисков, и рассчитывают новые характеристики системы. Приобретение и настройка средств защиты требует написания скорректированных политик, правил и приказов.

С течением времени необходимо производить переоценку защищенности ИС. Переоценку рекомендуется осуществлять при изменениях функции цели, появлении новых угроз, а также периодически, например, раз в год. Повторная оценка может базироваться на предыдущих результатах, что позволит выявить динамику, подтвердить правильность выбранных действий, сократить требуемые для проведения оценки ресурсы.

Усилив систему защиты информации дополнительными средствами защиты, предприниматели могут рассчитывать не только на увеличение защитных свойств системы, но и на усиление защищённости информационных ресурсов по сравнению с информационными ресурсами конкурентов [94]. Последним этапом проводится тестирование СЗИ.

1.6.1 Тестирование систем защиты информации

После формирования СЗИ, необходимо убедиться в том, что она выполняет возложенные на нее задачи, провести тестирование. Реальное использование продукта также является тестированием. Тестирование разделяется на несколько видов:

- теоретическое (теоретический анализ особенностей функционирования продукта в условиях локальных и удалённых атак);
- практическое;
- полномасштабное (на этапе между разработкой и внедрением в режиме, близком к реальному);
- стресс–тест (работа в режиме максимальной нагрузки);
- дружеский взлом (собственными специалистами или привлечёнными экспертами).

Тестирование можно проводить, ограничиваясь организационными мерами, например, имитация несанкционированной аутентификации, доступ к файлу с грифом, использование дополнительного софта. Целью тестирования может

быть как проверка работоспособности, так и поиск не выявленных уязвимостей. Для первого случая достаточно типовых сценариев – неправильные пароли, доступ к сетевым сервисам, а для второго – использование сертифицированного сканера. Сканер определяет степень защищённости от внешних атак, то есть проверяются межсетевой экран, proxy-сервер, маршрутизатор.

При проведении тестирования возможно обращение к документам Гостехкомиссии России, в которых прописаны требования к СЗИ, требования служат основой при аттестационных и сертификационных испытаниях. Ниже представлены методы, рекомендуемые в документе «Типовая методика испытаний объектов информатики по требованиям безопасности информации» Гостехкомиссии России [24].

Применяются следующие методы проверок и испытаний:

- экспертный метод;
- оценка защищенности информации в ИС по выбранным критериям;
- проверка отдельных составляющих защиты информации с помощью тестирующих средств;
- попытки «преодоления» систем защиты информации.

Экспертный метод предусматривает сверку состояния объекта с требованиями по безопасности информации, которые изложены в актах, сертификатах, лицензиях, предписаниях на эксплуатацию. В этих документах перечислены необходимые меры по защите информации.

Оценка защищенности информации по выбранным критериям проводятся для каналов утечки, которые потенциально могут быть связаны с техническими средствами разведки.

Проверка отдельных составляющих защиты информации для средств ИС (технических или программных) проводится по установленному графику аттестационной комиссии. Тестирующие средства, применяемые в процессе испытаний технических или программных средств должны быть

сертифицированные. При их отсутствии возможна разработка и сертификация необходимых тестирующих средств в процессе аттестационных испытаний.

Испытания попыткой «преодоления» системы защиты осуществляются известными методами несанкционированного доступа к информации, несмотря на наличие применяемых мер и средств защиты.

Существуют следующие испытания конкретных подсистем защиты информации:

1) Подсистема управления доступом. Если при проверке идентификации предъявленный идентификатор не известен системе, то средства интерфейса должны прекращать процесс предоставления доступа. При проверке аутентификации оценивается вероятность подбора субъектом аутентификации секретного признака или устройства за период взаимодействия. При проверке контроля доступа проверяется корректность работы механизмов доступа, соответствия их правилам доступа.

2) Подсистема регистрации и учета. Проверяют охват регистрацией происходящих событий на всех этапах технологического процесса. Вовлечены ли в этот процесс все защищаемые носители информации. Как производится проверка вариантов очистки задействованных частей оперативной памяти.

3) Криптографическая подсистема. Производится проверка генерации ключей, попытка использования одинаковых ключей для разных субъектов доступа.

4) Подсистема обеспечения целостности. Проверяются варианты контроля целостности по имитовставкам или хешированным значениям. Проверяются возможности неразрешённого ввода программ в операционную систему (ОС).

Документы по тестированию прорабатываются для каждой подсистемы СЗИ, и после тестирования формируется отчёт, в котором указывается обнаруженные ошибки и рекомендации по их устранению.

1.6.2 Создание службы информационной безопасности предприятия

В приказе Федеральной службы по техническому и экспертному контролю говорится, что «для обеспечения защиты информации, содержащейся в информационной системе, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации» [131].

На предприятии формируется самостоятельное подразделение, которое занимается проблемами информационной безопасности - служба информационной безопасности (СИБ). Прописывается политика информационной безопасности, согласованная с бизнес-процессами предприятия.

«СИБ проводит регистрацию событий и инцидент-менеджмент, контроль целостности, антивирусного программного обеспечения, политик, управление уязвимостями, анализ трафика. Необходимо выбирать наилучший вариант СЗИ для повышения состояния защищённости предприятия, используя критерий обеспечения конкурентоспособности предприятия» [101].

Служба информационной безопасности (Service of info security) – это самостоятельное подразделение, которое занимается решением проблем информационной безопасности. Структура и численность службы информационной безопасности предприятия зависит от размера предприятия, сферы его деятельности, места предприятия на рынке товаров и услуг, наличия на предприятии материальных ценностей, объёма информации, активности конкурентов. Поэтому рекомендовать универсальную структуру службы информационной безопасности невозможно.

Прежде всего, нужно определить, место службы информационной безопасности в структуре предприятия, способы взаимодействия с другими подразделениями, подчинённость руководителя службы безопасности.

Перед службой информационной безопасности могут стоять разные задачи. Она может провести анализ ситуации, разработать модель угроз и принять решение о необходимости приобретения средств защиты, а дальнейшее

администрирование поводится в рамках работы подразделения информационных технологий. При другом подходе, приобретение средств защиты согласуется с IT-проблемами и реализацией бизнес-задач предприятия, а внедрение и сопровождение системы защиты проводит служба информационной безопасности.

Нужно определить, как соотносятся права специалистов службы и специалистов других подразделений, например, администратора системы. Также необходимо ответить на вопросы: «Насколько процесс согласования решений распределён по руководителям различных рангов, растянут во времени, и насколько лица, с которыми идёт согласование, компетентны в данных вопросах?».

Служба информационной безопасности уникальна для каждого предприятия. Например, для малых предприятий, которые не располагают большими ресурсами, состав службы информационной безопасности ограничивается 1-5 сотрудниками. Если предприятие не может нанять квалифицированных специалистов по информационной безопасности, можно ограничиться имеющимися сотрудниками, которые занимаются вопросами информационных технологий. Они наделяются дополнительными полномочиями, возможно, проходят переподготовку и получают прибавку к зарплате.

«Международный стандарт ISO/IEC 13335-1: 2004 Information technology — Security techniques — Management of information and communications technology security рекомендует подчинять службу информационной безопасности непосредственно высшему руководству компании» [165]. Руководитель службы информационной безопасности подчиняется напрямую генеральному директору компании, при этом оперативно решаются вопросы при возникновении чрезвычайных ситуаций, нет необходимости в промежуточных согласованиях, и отпадают проблемы компетентности в точках согласования.

СЗИ строится или модернизируется, согласуясь с общей стратегией развития предприятия, и служба информационной безопасности поддерживает работу этой системы. Она является органом управления СЗИ.

При этом руководитель службы информационной безопасности имеет полный контроль над ИС. Руководители подразделений информационных технологий также напрямую подчиняются руководству компании. Таким образом, удаётся избежать возможных конфликтов между различными подразделениями компании, и более эффективно решать вопросы информационной безопасности. Схема управления и координации действий представлена на рисунке 1.2.

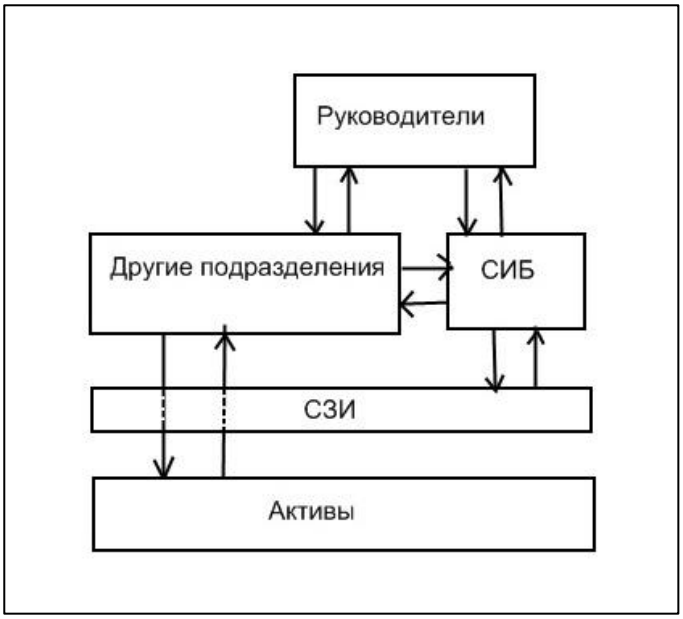


Рисунок 1.2– Схема взаимодействия СИБ со всеми структурами предприятия

Служба информационной безопасности, подчиняясь руководству, взаимодействует с другими подразделениями. Другие подразделения взаимодействуют с нематериальными активами через СЗИ [98]. Служба информационной безопасности обеспечивает защиту активов от угроз посредством СЗИ. Именно служба информационной безопасности инициирует итерационный пересчёт остаточного риска [99], очередное тестирование, пересчёт характеристик системы. Проблеме обеспечения ИБ за счёт построения

обоснованного варианта СЗИ посвящена книга В. Г. Грибунина, В. В. Чудовского «Комплексная система защиты информации на предприятии». В ней описывается создание «комплексной системы защиты информации (КСЗИ), главная цель которой является обеспечение непрерывности бизнеса. Рассматривается защита информации по техническим каналам и защита информации от несанкционированного доступа» [26].

В работе Г. Е. Шепитько, А. А. Локтева, Г. Н. Гудова система защиты описывается «моделью защиты, в которую входят множество угроз безопасности, ресурсов защищённой системы, механизмов безопасности, наборы уязвимых мест и барьеров. СЗИ строится с учётом следующих принципов: комплексность; эшелонирование; равнопрочность рубежей; разумная достаточность; непрерывность» [140].

В книге Н. В. Гришиной «Организация комплексной системы защиты информации» описывается «комплексный подход построения системы, который включает изучение объекта внедряемой системы, оценку угроз безопасности объекта, анализ средств, которыми оперируют при построении системы, оценку экономической целесообразности. Главная цель создания СЗИ – её надёжность. Надёжность защиты информации прямо пропорциональна системности» [27].

Аверченков В. И., Рытов М. Ю. описывают системы защиты информации разных стран [1]. Малюк А. А., Павизин С. В. и Погожин Н. С. предлагают ввести понятие «функции защиты. Защищённость информации определяется вероятностями осуществления функций защиты. СЗИ является функционально независимой подсистемой автоматизированной системы (АС), важнейшим требованием к которой является адаптируемость» [64].

Петрова В.А., Пискарева А.С., Шеина А.В. рассматривают принципы защиты информации и модели СЗИ [89]. Зегжда Д.П. [44] описывает модели безопасности и выделяет угрозы раскрытия и целостности. Малюк А. А. в работе «Информационная безопасность: концептуальные и методологические основы защиты информации» пишет, что «архитектура СЗИ должна быть аналогична

архитектуре защищаемой ИС и рассматривается в функциональном, организационном и структурном аспектах» [65].

СЗИ классифицируются по активности реагирования на НСД. Грушо А. А. приводит пример «гарантированно защищённой системы обработки информации. Формулируются теоремы о невозможности утечки и о выполнении политики безопасности» [28]. Щербаков А. Ю. описывает методологию создания защищённых компьютерных систем [90]. Девянин П. Н. в работе «Модели безопасности компьютерных систем» вводит аксиому, в которой говорится, что «все вопросы безопасности информации описываются доступами субъектов к объектам» [29]. Вводится схема классификации математических моделей безопасности компьютерных систем.

Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. описывают этапы построения системы защиты автоматизированной системы обработки информации (АСОИ) и меры обеспечения безопасности компьютерных систем [113]. Carl E. Landwehr (К. Лендвер) приводит следующие модели: «High Water Mark Model, Access Matrix Model, Bell and LaPadula Model» [154]. Ravi S. Sandhu (Р. Сандху) описывает семейство моделей «Role Based Access Control (RBAC)» [148]. Matt Bishop (М. Бишоп) уделяет внимание безопасности систем голосования; конфиденциальности, анонимности, доступности информации; инсайдерским атакам; использованию Model Checking [155].

Но во всех этих работах выбор СЗИ по критерию конкурентоспособности предприятия не рассматривается.

1.7 Оценка эффективности работы СЗИ

СЗИ является сложным многосвязным объектом, оценить эффективность работы которого важно для подтверждения правильности выбора варианта СЗИ для данного предприятия. Существует ряд работ, посвящённых этой проблеме.

В соответствии с приказом ФСТЭК России от 18 февраля 2013 г. N 21, «оценка эффективности реализованных в рамках системы защиты персональных

данных мер по обеспечению безопасности персональных данных может проводиться организацией самостоятельно или с привлечением юридических лиц, имеющих соответствующую лицензию. При этом форма оценки эффективности, а также содержание и форма итоговых документов не установлены» [129, 82].

Критериями оценки работы СЗИ может служить категории пригодности и оптимальности. Пригодность оценивается выполнением требований, прописанных к данной системе, оптимальность достигается при принятии одной из характеристик экстремального значения [43]. Сложнее ситуация, когда характеристик несколько, и по каждой необходимо достижение экстремального значения. Тогда приходится прибегать к сложным методам, которые получают интегрированные сводные показатели.

Выбор критерия происходит после изучения целей СЗИ. «Под эффективностью функционирования СЗИ понимают степень соответствия результатов защиты информации поставленной цели» [16]. Количественная оценка эффективности важна для сравнительных характеристик работы СЗИ.

С. В. Домарёв предлагает использовать системный подход при расчёте эффективности СЗИ [33]. При изучении СЗИ кажется логичным использование системного подхода, который предполагает восприятие объекта как системы, работающей в некотором поле. Системный подход изучает целостность объекта, его внутреннюю структуру, связи с внешними факторами. При этом предполагается анализ общих элементов, переходящий к частным. Оценочные составляющие СЗИ разрабатываются по трём векторам: «основы», «направления», «этапы».

Каждый вектор состоит из четырёх, пяти и семи элементов соответственно. При их перемножении возникает матрица из 140 вопросов, на которые необходимо ответить. Ответы являются требованиями к СЗИ. Оценить эффективность работы СЗИ можно на основе готовых программных продуктов, оптимизирующую систему с заданными требованиями. Данный подход помогает

максимально фиксировать связи между элементами защиты, но при этом не учитывается стохастическая природа событий и явлений, которые возникают в процессе защиты информации.

Если относится к выделениям средств на информационную безопасность только как к затратам, можно снизить затраты и получить освобождение средств. Но в перспективе это отдалит компанию от решения стратегических задач, связанных с повышением адаптивности к рынку, обеспечением конкурентоспособности, так как информационная безопасность влияет на эти процессы.

Поэтому многие компании относятся к вложениям в информационную безопасность как к инвестициям. В связи с этим, можно ожидать конкретные результаты от построения СЗИ, окупаемость инвестиций и возможность оценки их эффективности. Основным экономическим эффектом, на который рассчитывает предприятие, создавая СЗИ, является уменьшение ущерба при реализации угроз информационной безопасности.

Для оценки эффективности работы СЗИ можно рассчитать эффективность вложений в информационную безопасность. Существуют способы вычисления отдачи на инвестиционный капитал (Return of Investments – ROI). ROI – это отношение экономического эффекта, получаемое от проекта к затратам на реализацию этого проекта в процентах. Полученное значение нужно сравнить с эталонным проектом, то есть со средним по всем показателям в данном сегменте [68].

Динамические показатели эффективности вложений основаны на методе дисконтированных потоков денежных средств. Цель затрат в увеличении прихода финансовой составляющей, и уменьшение ущерба. Величину чистого дисконтного дохода рассчитывают по следующей формуле (1.2):

$$\text{ЧДД} = Э_u = \sum_{t=0}^{T}(P_t - З_t)\frac{1}{(1+E)^t}\ , \qquad (1.2)$$

где $Э_и$ – интегральный эффект, T – горизонт расчёта, P_t – результаты, достигаемые на момент времени t, $З_t$ – затраты за это время, E – норма дисконта, которая равна норме дохода на капитал, соответствующая запросам инвестора, $\frac{1}{(1+E)}$ – коэффициент приведения. При значении ЧДД больше нуля, инвестиции эффективны. Недостатком этого метода является то, что эффективность инвестиций и эффективность работы СЗИ не тождественны, результаты не могут соответствовать норме дохода на капитал.

Ещё один способ подсчёта эффективности СЗИ опирается на подсчёт величины остаточного риска. Эффективность работы СЗИ зависит от величины остаточного риска. Причём, чем он меньше, тем лучше. Этим же способом считают эффективность контрмеры, вычисляя остаточный риск (1.3):

$$\Delta R = R_2 - R_1, \qquad (1.3)$$

где R_2 – величина остаточного риска до реализации контрмеры, R_1 – величина остаточного риска после реализации контрмеры. Эффективность контрмеры, учитывающей затраты считается так (1.4):

$$Э_к = \frac{\Delta R}{C_k}, \qquad (1.4)$$

где $С_к$ – затраты на контрмеры. Чем больше $Э_к$, тем более эффективны контрмеры. При этом могут решаться оптимизационные задачи по критерию $Э_к$ при фиксированном значении остаточных рисков. Либо можно минимизировать остаточные риски при заданных затратах при осуществлении контрмер.

Для подсчёта количественных значений остаточного риска, как и обычного необходимо знать вероятность реализации угрозы, что затруднительно для проектируемой СЗИ и получения прогнозных значений. Поэтому в некоторых методах угрозы, уязвимости расписывают в виде таблиц и формируют итоговую таблицу, в которой вероятность представлена

перебором значений. Например, метод CRAMM, разработанный для анализа рисков проводит идентификацию рисков, выбор контрмер для эффективной работы СЗИ. Недостатками метода являются работа с уже созданными ИС, а не проектируемыми, большая стоимость лицензий [147, 145].

Вероятность часто заменяется частотными значениями [158] при анализе риска. Для получения частоты возникновения угрозы нужна большая статистическая выборка, и данные должны удовлетворять требованиям повторяемости и статистической однородности для адекватности получаемых выводов.

Поиск эффективности может привести к задачам, соответствующим системам нелинейных уравнений. Находят максимальный эффект от нейтрализации угроз с помощью средств безопасности, сводя уравнение к задаче булева линейного программирования. Для решения используется алгоритм Балаша, решающий задачу целочисленного программирования. Недостатком метода является существование тупиковых точек, и в случае полного перебора сложность метода составляет $O(n2^n)$ операций, где n – число переменных [67].

Иерархический метод подсчёта эффективности СЗИ учитывает разделение механизмов защиты по иерархическим уровням, и разницу в возможностях влияния на объекты защиты в зависимости от иерархических структур СЗИ [123]. Рассматриваются следующие уровни: аппаратный, BIOS, ОС, сетевой, СУБД, функционального ПО. Формируется матрица рейтингов стойкости, в которой столбцы соответствуют числу иерархических уровней, а строки - числу механизмов защиты. Число угроз для более высоких иерархических уровней СЗИ будет уменьшаться, так как они столкнутся с механизмами защиты на предыдущих уровнях.

Формируют вектор с координатами вероятности нейтрализации угроз в зависимости от иерархических уровней СЗИ. После поэлементного перемножения строк матрицы рейтингов стойкости на вектор покоординатных

вероятностей получают матрицу защищенности. Сумма элементов матрицы защищённости и даст рейтинг защищённости всей системы. Можно использовать рейтинг защищённости в качестве целевой функции для оптимизации структуризации механизмов защиты. К недостаткам данного метода можно отнести отсутствие величины ущерба в конечных формулах, частоты появления атак.

Применяется также информационно-энтропийный метод. Высчитываются значения информационных энтропий подсистем (1.4). Энтропию всей системы считают как свёртку функций. При линейной зависимости результата вычислений, система считается эффективной.

$$\psi(t) = (\int_0^t s_n\,(t-\tau) \dots \left(\int_0^t s_3 \left(\int_0^t s_1\,(\tau) s_2(t-\tau) d\tau\right) d\tau \dots\right) d\tau, \qquad (1.5)$$

где $s_n, \dots, s_1$ – значения энтропий различных подсистем.

Недостатками этого метода являются необходимость принятия пороговых значений для оценивания результатов вычислений или составление эталонных образов [57], что затруднительно в связи с ограниченностью и неполнотой результатов эксперимента [125].

Во всех рассмотренных работах не рассматривается стохастическая природа событий и явлений, которые возникают в процессе защиты информации.

Если система защиты информации не будет искусственно дополняться к уже имеющейся системе управления, а будет внедрена в структуру управления как элемент, руководимый службой информационной безопасности, и корригирующий с основными бизнес-процессами компании, то это приведёт к повышению эффективности работы СЗИ. Взаимодействуя с бизнес-процессами, СЗИ увеличивает свою эффективность благодаря эффективному бизнесу. Необходимо выбрать оптимальный вариант СЗИ по критерию, характеризующий бизнес-процессы как эффективные. Например, в качестве критерия предлагается взять обеспечение конкурентоспособности предприятия.

1.8 Информация как значимый ресурс усиления конкурентоспособности предприятия

Для повышения информационной безопасности предприятия будем внедрять наилучший вариант СЗИ, выбранный по критерию обеспечения конкурентоспособности предприятия. Следовательно, необходимо изучить конкурентоспособность предприятия.

1.8.1 Подходы к изучению приоритетных направлений развития фирм и конкурентных стратегий.

Подходы к изучению приоритетных направлений развития фирм и конкурентных стратегий претерпевают значительные изменения во второй половине двадцатого века. В 60-70 гг. прошлого столетия возникает «школа планирования» [126]. Успех фирмы ассоциируется с её аналитическими возможностями, навыками в разработке и реализации стратегий, при этом преобладает долговременное планирование.

В 70-80 гг. стала доминировать «школа позиционирования». Происходит перенос акцента с фирмы на её внешнее окружение. Менеджеры начинают мыслить в терминах конкурентных стратегий, анализируя отрасль, в которой действуют поставщики, конкуренты, товары–заменители, новички в отрасли, потребители. Для успеха фирме необходимо позиционировать себя в отрасли так, чтобы воздействовать на эти пять сил.

Начиная с 90 гг. происходит возврат на обновлённой интеллектуальной основе к внутренним возможностям фирмы, появляется «ресурсная школа». В связи с этим особую роль приобретают уникальные ресурсы компании, которые невозможно или чрезвычайно дорого сымитировать, а также заменить какими–либо другими ресурсами. Эти ресурсы способны приносить в течение длительного времени ренту, которая позволяет компании сохранять устойчивые конкурентные преимущества на рынке. Базовой характеристикой таких ресурсов

является их нематериальный характер, доходы от их использования фирма может превращать в своё конкурентное преимущество.

Возрастает роль нематериальных активов в формировании потенциала конкурентоспособности. Это знания, умения, репутация, бренды, взаимоотношения с потребителями, атмосфера доверия и сотрудничества. [121].

Нематериальная сущность ключевых ресурсов организаций является залогом специфичности активов, которые могут использоваться только внутри компании. Поэтому понижается возможность имитации и воспроизведения своих ключевых ресурсов конкурентами» [90].

1.8.2 Конкурентоспособность предприятия

Количественное измерение конкурентоспособности товара и услуги позволит управлять её уровнем, и является основой для измерения конкурентоспособности предприятия.

Конкурентоспособность товаров и услуг – это их способность выдержать конкуренцию со стороны аналогичных товаров и услуг других производителей. А конкуренция – это соперничество на каком-либо поприще между отдельными субъектами [37]. Таким образом, конкурентоспособность товара и услуг – это «способность удовлетворять требованиям конкретного потребителя в определённый период времени по показателям качества и его затратам на приобретение и эксплуатацию данной продукции» [55]. Это возможность реализации товара или услуги на конкретном рынке в конкретный период.

«Конкурентоспособность в общем смысле – это способность конкурировать, то есть бороться и противостоять чему – либо. Уровень конкурентоспособности определяет степень превосходства одного объекта над другим. Поэтому из большого разнообразия определений конкурентоспособности предприятия можно выбрать определение, данное экономистами В. Грибовым, В. Грузиновым в работе «Конкурентоспособность предприятия» [25], которые рассматривают

понятие конкурентоспособности как преимущество по отношению к другим предприятиям данной отрасли внутри страны и за ее пределами» [90].

«Конкурентоспособность предприятия является относительной характеристикой, которая выражает отличия данного предприятия от предприятий-конкурентов по способности удовлетворения своими товарами и услугами потребностей людей. Конкурентоспособность не является внутренним качеством фирмы, она может быть оценена только в рамках группы фирм, относящихся к одной отрасли, либо фирм, выпускающих аналогичные товары и услуги. Конкурентоспособность предприятия характеризует возможности и динамику его приспособления к условиям рыночной конкуренции» [90].

«Основная хозяйственная задача любой фирмы, производящей товары и услуги, - создать условия для своего устойчивого функционирования и добиваться максимального удовлетворения потребностей конкретных потребителей [159]. Задача компании заключается в обеспечении потребителей более высокой по сравнению с конкурентами ценностью, в развитии долгосрочных взаимоотношений с покупателями. Для сохранения конкурентоспособности необходима гибкость, адаптивность, быстрота реакции на изменения запросов клиентов» [93].

Конкурентоспособность предприятия характеризует величину и эффективность использования всех ресурсов предприятия, и, в частности, таких важных составляющих как информация, интеллектуальный капитал, персональные данные [47].

«Предприятие получает дополнительное конкурентное преимущество и выгодно выделяется на фоне остальных конкурентов. Кроме того, согласно закону ФЗ-152 «О персональных данных» ст.17 п. 2 [41] субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и компенсацию морального вреда в судебном порядке. То есть разглашение приватных сведений может привести к судебным искам,

юридическим издержкам, ухудшению репутации компании и падению её конкурентоспособности» [90].

Конкурентоспособность малых предприятий обусловлена единством права собственности и управления предприятием, ключевой ролью руководителя в деятельности предприятия, и отсутствием огромного административного аппарата, который часто тормозит развитие предприятия. За принимаемые решения предприниматели несут высокий уровень ответственности, так как риски могут носить фатальный характер. При этом малым предприятиям характерна способность к переменам, внедрение новшеств, потенциально востребованных спросом, доступных бюджету предприятия.

Согласно Федеральному закону Российской Федерации от 24 июля 2007 г. N 209-ФЗ "О развитии малого и среднего предпринимательства в Российской Федерации", который был принят Государственной Думой 6 июля 2007 года к субъектам малого и среднего предпринимательства относятся: внесенные в единый государственный реестр юридических лиц потребительские кооперативы и коммерческие организации (за исключением государственных и муниципальных унитарных предприятий), а также физические лица, внесенные в единый государственный реестр индивидуальных предпринимателей и осуществляющие предпринимательскую деятельность без образования юридического лица (далее - индивидуальные предприниматели), крестьянские (фермерские) хозяйства. Они должны соответствовать следующим условиям:

- для юридических лиц суммарная доля участия Российской Федерации, субъектов Российской Федерации, муниципальных образований, иностранных юридических лиц, иностранных граждан, общественных и религиозных организаций (объединений), благотворительных и иных фондов в уставном (складочном) капитале (паевом фонде) указанных юридических лиц не должна превышать двадцать пять процентов (за исключением активов акционерных инвестиционных фондов и закрытых паевых инвестиционных фондов), доля участия, принадлежащая одному или нескольким юридическим лицам, не

являющимся субъектами малого и среднего предпринимательства, не должна превышать сорок девять процентов;

- средняя численность работников за предшествующий календарный год не должна превышать следующие предельные значения средней численности работников для каждой категории субъектов малого предпринимательства - до ста человек включительно для малых предприятий;
- выручка от реализации товаров (работ, услуг) без учета налога на добавленную стоимость или балансовая стоимость активов (остаточная стоимость основных средств и нематериальных активов) за предшествующий календарный год не должна превышать предельные значения, установленные Правительством Российской Федерации для каждой категории субъектов малого и среднего предпринимательства.

Согласно постановлению Правительства Российской Федерации от 4 апреля 2016 г. № 265 установлены предельные значения выручки от реализации товаров (работ, услуг) за предшествующий год без учёта налога на добавленную стоимость для субъектов малого предпринимательства — 800 млн. рублей.

По данным Федеральной службы государственной статистики на первый квартал 2017 года число малых предприятий (без микропредприятий) составило 256722 единиц [80].

Акцентируя внимание на нематериальных активах, малые предприятия сталкиваются с возникающими вопросами информационной безопасности [103].

1.8.3 Информационная безопасность предприятия.

«Оценивая нематериальные активы как потенциал динамического конкурентного преимущества, предприятия особое внимание уделяют интеллектуальному капиталу. Конкуренты могут копировать оборудование, продукцию, но воспроизвести информацию и интеллектуальный капитал при

проведении политики информационной безопасности значительно сложнее» [90].

Согласно Федеральному закону от 4 июля 1996 года 85-ФЗ «Об участии в международном информационном обмене», «информационная безопасность – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства» [134]. В Федеральном законе от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и защите информации", в статье 18 говорится, что «защита информации заключается в принятии правовых, организационных и технических (программно-технических) мер в целях:

1) обеспечения целостности и сохранности информации, недопущения ее несанкционированного изменения или уничтожения;

2) соблюдения конфиденциальности информации ограниченного доступа;

3) реализации права на доступ к информации;

4) недопущения несанкционированного воздействия на средства обработки и передачи информации» [38].

Таким образом, наиболее подходящее определение записано в ГОСТе 28806–90: «Безопасность информации (данных): Состояние защищённости информации, при котором обеспечены её (их) конфиденциальность, доступность и целостность» [15].

Использование на предприятиях информационных технологий является основой получения конкурентных преимуществ [102], но при этом обостряет вопросы информационной безопасности. По данным Росстата (данные обновлены в 2016 г.) доля предприятий, использовавших персональные компьютеры в профессиональной деятельности в 2014 г. составляет 88,7 % и представлена на рисунке 1.3.

Рисунок 1.3– Распределение организаций по удельному весу численности работников, использовавших персональные компьютеры на конец года; в процентах от общего числа обследованных организаций

Двадцать один процент от общего числа обследованных компаний приходится на предприятия, с удельным весом работников от 10 до 29 человек, использующих персональные компьютеры, и тридцать девять процентов на предприятия, с удельным весом работников от 70 до 100 человек, использующих персональные компьютеры [80].

Затраты предприятий на приобретение вычислительной техники и программных средств с 2012 по 2014 гг. превосходят одну треть в процентах к итогу от всех затрат на информационные и коммуникационные технологии (ИКТ) и представлены на **Ошибка! Источник ссылки не найден.**4 [63].

Использование персональных компьютеров, и затраты на информационно-коммуникационные технологии (ИКТ) не гарантируют эффективной борьбы с нарушениями информационной безопасности без комплексного подхода к решению этой проблемы [100]. Аналитическая компания Ponemon Institute по заказу Hewlett Packard Enterprise Security провела исследование кибер-преступности в России в 2014 году [83].

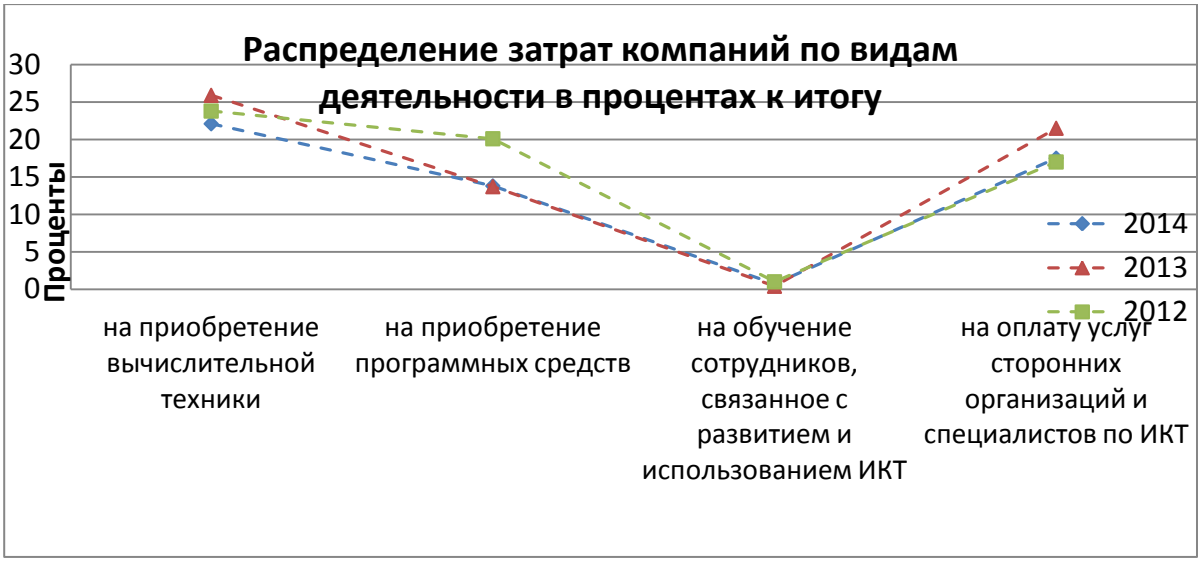


Рисунок 1.4– Затраты организаций на информационные и коммуникационные технологии по видам деятельности

Исследователи из Ponemon Institute проанализировали статистику последствий кибер-атак на российские предприятия и выявили четыре основные группы последствий игнорирования информационной безопасности на предприятиях. На рисунке 1.5 видно, что сорок семь процентов приходится на подрыв деятельности предприятия, двадцать два процента от общего числа последствий составляют потерю доходов, девятнадцать процентов - потеря данных, и девять процентов - повреждение оборудования.

Почти половина последствий кибер-атак приводит к невозможности функционирования предприятия в прежнем режиме.

В 2015 году произошёл рост числа таргетированных атак на корпоративные ресурсы, маскировка целевых атак под массовые, использование технологий «Watering Hole». По данным сайта www.securitylab.ru [84], более 50% кибер-атак в 2015 году не были технически сложными. Использование уязвимостей «zero day» зафиксировано менее чем в 20% атак. Следовательно, примерно в 80% случаев у компаний была возможность противостоять угрозам при условии обеспечения информационной безопасности. «Количество преступлений, совершаемых хакерами в России, с 2013 по 2016 год увеличилось в шесть

раз» [54].

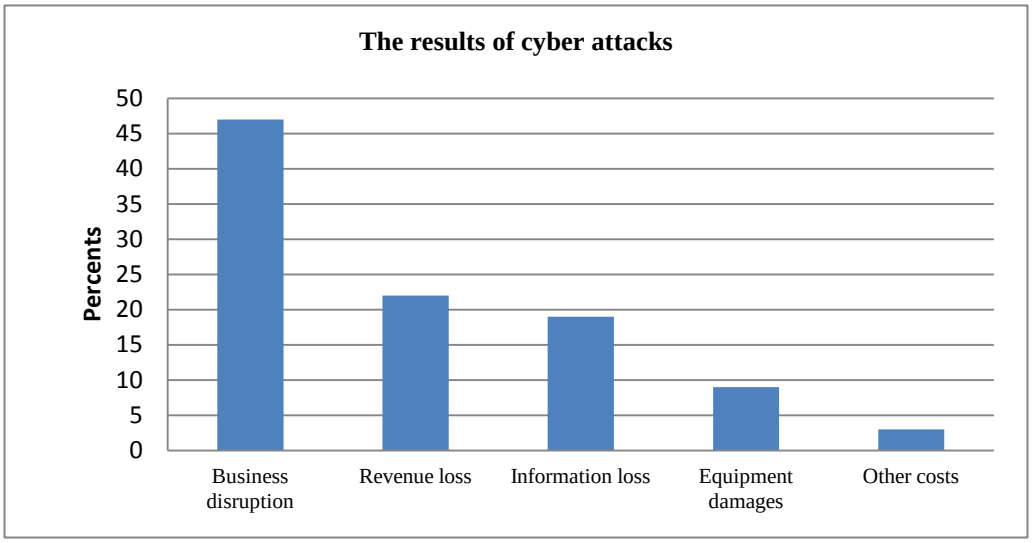


Рисунок 1.5– Последствия кибер-атак

Интерактивное восприятие сигналов рынка и взаимодействие с клиентами даёт возможность получения информации о потребительских предпочтениях, выделения приоритетных клиентов и дифференцированного взаимодействия с ними, формирования информационной клиентской базы. Самая доступная в настоящее время информационная технология – Интернет играет значительную роль в организации бизнеса предприятий.

Именно через Интернет происходит удалённое общение с потребителями, поставщиками, подбор кадров, получение консультационных услуг, ведение электронного бизнеса, взаимодействие с налоговыми и контролирующими органами посредством технологии цифровой подписи [105]. Издержки резко снижаются благодаря более эффективному управлению материальными запасами, затратами, спросом, практики предложения индивидуальных цен и рекламы [3].

Созданные Web–сайты компании помогают наиболее дёшево, быстро и эффективно охватить целевые рынки. Привлекаются новые клиенты, создаётся клиентская база данных, в которой отражена жизненная ценность клиентов, причины ухода бывших клиентов, психологические, географические, гендерные

и возрастные особенности клиентов. Активная позиция потребителя реализуется через круглосуточную доступность взаимодействия с компанией [5], возможность получения необходимого объёма информации о предоставляемых товарах и услугах [49].

Присутствие фирмы в Интернете способствует повышению имиджа торговой марки компании» [90], продвижению товаров и услуг фирмы, добавлению нового канала распространения услуг [48], улучшению сервисного обслуживания текущих и потенциальных потребителей. Но все эти плюсы обращаются в минусы при нарушении информационной безопасности [155].

Значимая для предприятия информация должна быть защищена путём внедрения наилучшего варианта СЗИ, критерием выбора которого является обеспечение конкурентоспособности предприятия.

1.9 Формулировка технической задачи диссертационного исследования

Малые предприятия, не обладающие большими материальными ресурсами, не имеющие возможности привлечения в свой штат высококлассных специалистов по ИБ, нуждаются в защите от угроз ИБ. Специфика бизнеса малых предприятий заключается в малой устойчивости от стрессовых ситуаций, связанных с реализацией атак на ИР предприятия, с потерей информации, составляющей коммерческую тайну, репутационными потерями при разглашении конфиденциальной информации. Повышение конкуренто-способности предприятия возможно только при обеспечении ИБ.

Для обеспечения ИБ предприятия сначала изучают бизнес-процессы предприятия, существующие ИС предприятия, уровень защиты ИР. Выбирают N возможных комбинаций средств защиты, которые будут в дальнейшем являться основой для построения СЗИ.

Техническая задача заключается в следующем: необходимо найти целесообразный способ (средство) защиты ИР, при котором конкурентоспособность предприятия будет максимальной.

Выводы по главе 1

В данной главе были исследованы вопросы наиболее используемых в настоящее время методов выбора и создания СЗИ на предприятиях; формирования службы информационной безопасности предприятия; методики расчёта эффективности работы СЗИ; обоснована роль информационной безопасности в повышении конкурентоспособности предприятия, сформулирована техническая задача.

Таким образом, цель, поставленная в начале главы 1, выполнена.

Глава 2 Метод оптимизации вариантов защиты информации

2.1 Алгоритм генерации допустимых вариантов системы защиты информации

Цель данной главы – получение алгоритма генерации допустимых вариантов системы защиты информации и метода оптимизации вариантов защиты; вывод количественной формулы влияния обеспечения ИБ на конкурентоспособность предприятия.

Необходимо сгенерировать N вариантов средств ЗИ для малого предприятия, удовлетворяющих наложенным ограничениям. Выбираем основные типовые средства ЗИ r_{ij} (средство защиты информации от несанкционированного доступа (СЗИ НСД), межсетевые экраны (МЭ), антивирусы), их количество обозначаем k. Определяем количество существующих средств каждого типа и обозначаем его n_k. Поместим средство каждого типа r_{ij} в определённый столбец таблицы (таблица 2.1). Прописываем их свойства и характеристики.

Свойство стоимость $C(r_{ij})$ однозначно определяется у каждого элемента таблицы. Свойство совместимости $\varphi(r_{ij})\epsilon\{0,1\}$ может принимать значение 0 или 1 у одного и того же элемента таблицы в зависимости от объекта сравнения. Прописываем значение свойства совместимости для каждой пары элементов таблицы.

В качестве характеристики можно выбрать сертификаты (присваивается 0, если его нет).

Таблица 2.1– Средства защиты информации, участвующие в генерации вариантов

R1	*R2*	…	*Rк*
r_{11}	r_{12}	…	r_{1k}
r_{21}	r_{22}	…	r_{2k}
r_{31}	r_{32}	…	r_{3k}
…	…	…	…
$r_{n_1 1}$	$r_{n_2 2}$	…	$r_{n_k k}$

где $n_1, n_2, \dots, n_k$ – количество элементов в каждом столбце.

Выбираем по одному элементу из каждого столбца. Выбор элементов отражает ориентированный граф, представленный на рисунке 2.1.

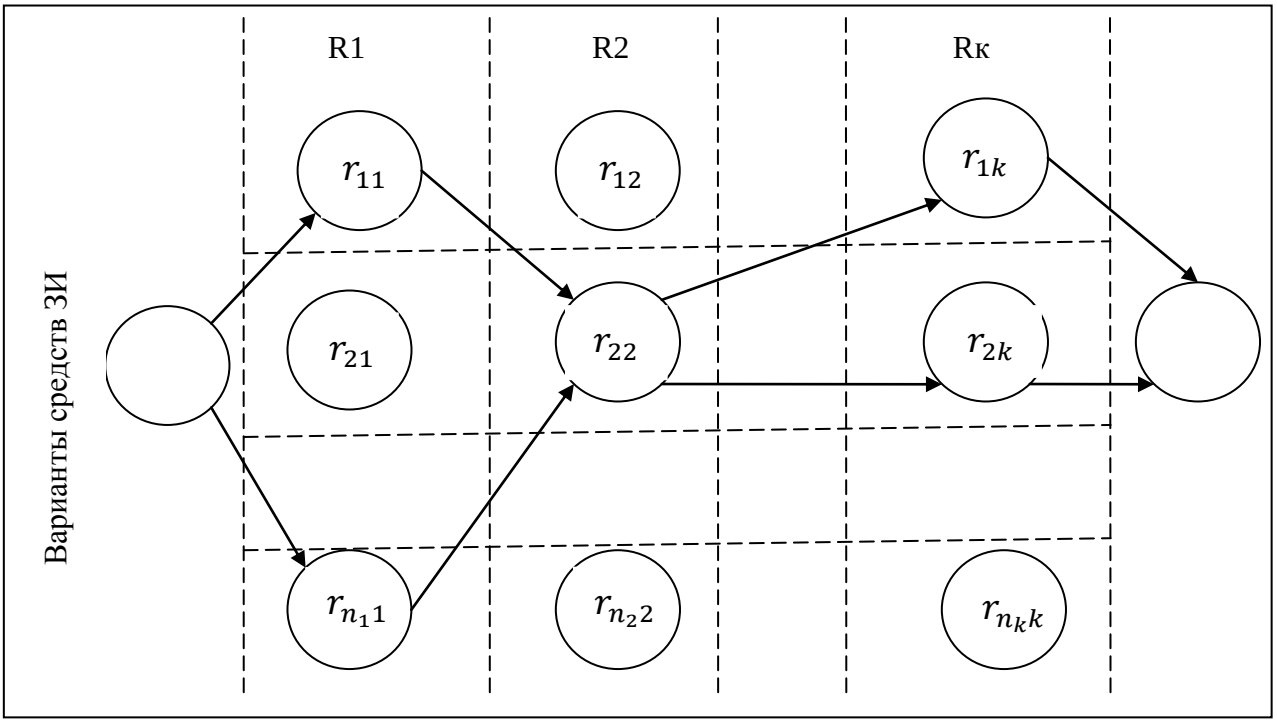


Рисунок 2.1– Ориентированный граф генерации вариантов средств ЗИ

Маршрут является простой цепью, так как у него не должно быть повторяющихся рёбер и вершин. Всего таких комбинаций $n_1 \cdot n_2 \cdot \dots \cdot n_k$. Необходимо отбросить часть комбинаций. Ограничения значительно сокращают число комбинаций.

Так как малые предприятия не располагают большими ресурсами, существует ограничение на расходы, связанные с приобретением средств защиты (2.1).

$$\sum_{j=1}^{k} C(r_{ij}) \leq C^{d}, \tag{2.1}$$

где C^{d}-допустимые расходы на приобретение средств защиты.

Можно сразу отбросить те средства, стоимость которых превышает C^{d}.

Дополнительное ограничение накладывается на совместимость средств защиты. Совместимость средств защиты означает возможность совместного использования без потери функциональных возможностей этих средств.

При совместимости со всеми вершинами графа уже пройденного пути, следующей вершине (средству защиты) присваивается коэффициент $\varphi = 1$. При обратной ситуации — $\varphi = 0$. При благоприятном исходе, когда все выбранные средства будут совместимыми сумма строго равна k (2.2).

$$\begin{cases} \sum_{j=1}^{k} \varphi(r_{ij}) = k \\ \varphi(r_{ij}) \epsilon \{0,1\} \end{cases} \tag{2.2}$$

Для формирования алгоритма генерации допустимых вариантов системы защиты информации, мы будем применять метод ветвей и границ, который заключается в последовательном разбиении множества допустимых решений. На каждом шаге метода элементы таблицы будут подвергаться анализу – удовлетворяют выбранные элементы наложенным ограничениям или нет.

Мы прокладываем ориентированный маршрут с условием выбора только одной вершины из каждого столбца таблицы. Алгоритм заключается в следующих действиях:

1. Средству из первого столбца присваивается 1.
2. Так как сумма коэффициентов совместимости должна равняться k, во втором столбце мы выбираем только совместимые средства. Одновременно проверяем первое ограничение. Если оно не выполнено, данная ветвь больше не продлевается, образуя тупиковый маршрут.

3. Выбираем в следующем столбце средства, совместимые с предыдущими средствами, расположенными на данной ветке, и проверяем выполнение первого ограничения.
4. Если маршрут проложен по всем столбцам и условия ограничений выполнены, то данный вариант системы защиты информации считается допустимым.

Получается сетевая структура, которая значительно сокращает число вариантов.

Сгенерировав N комбинаций средств защиты информации для данного предприятия, можно приступать к выбору оптимального варианта СЗИ на основе средств ЗИ из N отобранных вариантов.

2.2 Коэффициент изменения конкурентоспособности

При проектировании СЗИ приходится сталкиваться с высокой степенью неопределённости некоторых параметров функционирования, что затрудняет анализ её эффективности и выбор оптимального варианта.

Оптимальным принимается решение, которое в предполагаемых условиях наилучшим образом удовлетворяет задачам целевого функционирования. В конечном итоге оптимальность решения достигается за счет наиболее рационального распределения ресурсов, которые выделены на построение СЗИ.

В процессе создания «оптимальной СЗИ возникает задача сравнения характеристик исследуемых объектов. Трудность заключается в возникновении неопределенности стохастического характера, например, возникновения невыявленного противодействия; недостаточной изученности некоторых процессов функционирования уникальной СЗИ, спроектированной для конкретного предприятия; неполного понимания последствий нарушения информационной безопасности в проектируемой системе.

Решение задач анализа и синтеза СЗИ усложняется необходимостью учета большого числа параметров СЗИ» [92], синтеза количественных и качественных

показателей, дефицитом информации, трудностью получения исходных данных, особенно на ранних этапах проектирования СЗИ.

Указанные особенности затрудняют применение традиционных методов математической статистики, теории вероятности и классических методов оптимизации моделей при решении прикладных задач анализа и синтеза СЗИ.

При выборе оптимального варианта СЗИ из предложенных альтернатив, приходится пользоваться несколькими критериями. При нахождении экстремальных значений методом моделирования часто оптимизация производится по одному критерию, а другие фиксируются и принимаются в качестве ограничений. Приходится субъективно выбирать доминирующий критерий, упрощать задачу, искажая условия, оценивать ограничения.

При многокритериальном оценивании сложных объектов возникает проблема сравнения объектов в целом, так как по разным критериям рейтинги объектов с большой вероятностью получаются разными, и появляются трудности в градации объектов. Возникает необходимость вычисления сводной оценки, которая с одной стороны объединила бы информацию обо всех характеристиках объекта, а с другой позволила бы сравнивать объекты, присваивая им количественный рейтинг.

При принятии решения выбирается оптимизационный вариант в соответствии с неединственной целевой функцией. Алгоритм построения сводной оценки при принятии решения следующий:

- фиксируются критерии, по которым оцениваются объекты;
- выбираются весовые коэффициенты, определяющие рейтинг выбранных критериев;
- оцениваются объекты по выбранным критериям;
- строится общая оценка многокритериальных характеристик объектов;
- по полученным оценкам объекты подвергаются градации, и выбирается объект, более подходящий поставленной задаче.

Мы сгенерировали *N* комбинаций средств ЗИ, на основе которых строится СЗИ для конкретного предприятия. Эти системы оцениваются по нескольким критериям, причём рейтинги по каждому критерию не совпадают. Например, «необходимо построить СЗИ, которая имеет оптимизационные значения по защите предприятия от угроз нарушения доступности, целостности и конфиденциальности информации. В качестве обоснования выбора оптимизационного варианта СЗИ предлагается количественное значение конкурентоспособности предприятия.

Пусть $\boldsymbol{x} = (x_1, \dots, x_m)$ – вектор исходных характеристик исследуемой системы. За $Э_{\text{уИБ}}$ обозначим условный эффект (2.3), равный разности ущербов до внедрения СЗИ и после.

$$Э_{\text{уИБ}} = У_{\text{до}} - У_{\text{пос}}, \tag{2.3}$$

где $У_{\text{до}}$ - величина ущерба в денежном выражении до внедрения СЗИ;

$У_{\text{пос}}$ - величина ущерба в денежном выражении после внедрения СЗИ. Вынесем $У_{\text{до}}$ за скобку и представим ущербы как перемножение числа инцидентов на средневзвешенные величины. «Пусть $n_{\text{пос}}$ и $n_{\text{до}}$ - число инцидентов после и до внедрения СЗИ соответственно, а $\overline{У_{\text{до}}}$, $\overline{У_{\text{пос}}}$ - средневзвешенные величины ущерба до и после внедрения СЗИ» [92].

В числителе $n_{\text{пос}}$ представим как $n_{\text{до}}$ на коэффициент снижения количества нарушений $к_1$, $\overline{У_{\text{пос}}}$ представим как $\overline{У_{\text{до}}}$, умноженный на коэффициент уменьшения тяжести нарушений $к_2$» [92]. После сокращений у нас останется в качестве вычитаемого произведение коэффициентов $к_1 к_2$, которые будут составлять коэффициент изменения конкурентоспособности (коэффициент уменьшения ущерба) $\rho(\boldsymbol{x})$ (2.4).

$$Э_{\text{уИБ}}(\boldsymbol{x}) = У_{\text{до}} - У_{\text{пос}} = У_{\text{до}}\left(1 - \frac{У_{\text{пос}}}{У_{\text{до}}}\right) = У_{\text{до}}\left(1 - \frac{n_{\text{пос}}\overline{У_{\text{пос}}}}{n_{\text{до}}\overline{У_{\text{до}}}}\right) \tag{2.4}$$

$$Э_{\text{уИБ}}(\boldsymbol{x}) = У_{\text{до}}\left(1 - \frac{n_{\text{до}} к_1(\boldsymbol{x}) к_2(\boldsymbol{x})\overline{У_{\text{до}}}}{n_{\text{до}}\overline{У_{\text{до}}}}\right) = У_{\text{до}}\big(1 - к_1(\boldsymbol{x}) к_2(\boldsymbol{x})\big)$$

$$\left(к_1(\boldsymbol{x})к_2(\boldsymbol{x}) = \rho(\boldsymbol{x})\right), \quad \rho, к_1, к_2 \, \epsilon[0,1],$$

«где $к_1, к_2$ - коэффициент снижения количества нарушений и коэффициент уменьшения тяжести нарушений после внедрения СЗИ соответственно» [92].

Условный эффект $Э_{уИБ}(\boldsymbol{x})$ (2.4) равен денежной оценке ущерба предприятию, умноженную на единицу минус коэффициент изменения конкурентоспособности $\rho(\boldsymbol{x})$ «в результате обеспечения информационной безопасности (2.6).

$$Э_{уИБ}(\boldsymbol{x}) = У_{до} \times \left(1 - \rho(\boldsymbol{x})\right), \quad \rho\epsilon[0,1] \, , \tag{2.5}$$

Для увеличения условного эффекта, нужно выбрать минимальное значение коэффициента изменения конкурентоспособности» [92].

Получив теоретическое значение коэффициента изменения конкурентоспособности (таблица 2.2) с помощью многокритериального метода (ММРСП),

Таблица 2.2 – Получение реальных и теоретических значений коэффициента изменения конкурентоспособности и условного эффекта

Реальные значения	**Теоретические значения**
$\rho(\boldsymbol{x}) = к_1(\boldsymbol{x})к_2(\boldsymbol{x}) = \frac{У_{пос}}{У_{до}}$	$\rho(\boldsymbol{x})$ из ММРСП
$Э_{уИБ}(\boldsymbol{x}) = У_{до} - У_{пос}$	$Э_{уИБ}(\boldsymbol{x}) = У_{до}(1 - \rho(\boldsymbol{x}))$

основываясь на эвристической информации экспертов, можно перейти к получению реальных значений ущерба от лиц, ответственных за ИБ предприятия, после внедрения СЗИ и верифицированию теоретические значения.

2.3 Выбор способа многокритериальной оптимизации

Методы многокритериальной оптимизации более полно отражают задачи,

ставящиеся перед реальными многосвязными системами, которыми являются системы защиты информации (СЗИ). Перед лицом, принимающим решение, появляется проблема выбора наиболее подходящего метода многокритериальной оптимизации, и, как следствие, принятие допущений, условностей, границ теоретических аналогов реальных объектов. Ставится задача выбора оптимального варианта СЗИ, который спроектирован для конкретного предприятия. Оптимизация проводится по нескольким критериям: равнозначным, независимым, наиболее полно отражающим объекты выбора.

Рассмотрим различные способы выбора оптимизационного варианта. На основе проведённого анализа выберем метод, соответствующий поставленной задаче и имеющий минимальные недостатки.

При многокритериальном оценивании объектов применяется метод рейтингования [58]. Если в задаче ищутся минимальные значения, уменьшение значений характеристик соответствует увеличению степени привлекательности системы. Необходимо взвешивание отдельных показателей в свете значимости их рейтинговой оценки [71]. Нормированные взвешенные показатели складываются, и на основании полученной суммы происходит ранжирование объектов.

При построении траектории выбора наилучшего варианта есть соблазн сократить количество вариантов, например, до множества Парето, убрав заведомо худшие. Согласно принципу Эджворта-Парето [74], при многокритериальном выборе один вариант лучше другого, если по одному частному критерию он лучше другого, а по остальным не хуже. Сформированное множество Парето не больше первоначального количества вариантов, и задача нахождения наилучшего варианта, как кажется, упрощается. Но наилучшие решения могут лежать за пределами множества Парето, если не выполняются определённые условия использования принципа Эджворта-Парето, например, аксиома транзитивности, в которой говорится, что отношение предпочтения

должно быть транзитивным бинарным отношением.

Ещё один путь упрощения задачи – сокращение количества критериев. Метод главного критерия уменьшает множество критериев до одного [13]. Один критерий объявляется главным, по нему ищется экстремум, а остальные критерии формируют ограничения. Один из главных недостатков метода – это упрощение задачи, и допустимая область решения может оказаться пустым множеством.

Метод уступок [13] преодолевает возможные недостатки предыдущего метода. Критерии оцениваются по значимости и используются в порядке возрастания. Выбирается первый критерий и решается однокритериальная задача. Затем находят величину возможного отклонения. Не выходя за размеры фиксированных отклонений, итерационно находятся следующие экстремальные задачи. В конце используют последний критерий, и решается задача, аналогичная задаче с главным критерием. При достижении граничных условий решение может быть слабо эффективным.

Метод свёртки применяют при агрегировании всех критериев в скалярную величину, и на основании этой величины происходит оценивание объекта [12]. Свёртка имеет аддитивный или мультипликативный вид. Мультипликативная запись зависит от уменьшения значений отдельных критериев и может стремиться к нулю. При аддитивной свёртке уменьшение значений некоторых критериев компенсируется увеличением других, имеющих большую «весомость». Мультипликативную свёртку можно перевести в аддитивную, логарифмируя произведение.

Немаловажным этапом метода свёртки является задача выбора весовых коэффициентов, которая допускает различные решения. Метод логического анализа основан на прямом экспертном присвоении конкретных значений критериям. Эксперты присваивают значения критериям в диапазоне натурального ряда от единицы до величины количества критериев [110]. Весовые коэффициенты считаются как отношение суммы присвоенных значений

разными экспертами одному критерию к общей сумме по всем критериям и по всем экспертам. В случае разной компетентности экспертов, им присваиваются коэффициенты значимости экспертов, которые включаются в формулы. В этом методе важны не только коэффициенты значимости экспертов, но и достаточное количество экспертов.

Метод анализа иерархий [110] основан на построении матриц парных сравнений различных критериев. Матрица должна быть квадратная, обратно-симметричная и согласованная. Оценивается критерий натуральными числами от 1 до 9. Диагональные элементы после нормализации и образуют весовые коэффициенты. При построении первоначальной матрицы, если критерий менее важен его значение оценивается обратным числом. Таким образом, важный критерий с оценкой n и менее важный с оценкой $\frac{1}{n}$, симметрично расположенные относительно диагонали, отличаются в n^2 раз, где $n\epsilon\{1,\dots,9\}$, что является грубым приближением.

Формулы Фишберна [110] дают аналитическую запись весовых коэффициентов. Если критерии упорядочены в порядке убывания, то предлагается применить арифметическую или геометрическую убывающую прогрессию. Весовые коэффициенты, полученные с помощью простых формул, упрощают задачу, но, во-первых, не во всех задачах критерии подчинены отношению порядка, и, во-вторых, встаёт вопрос обоснования применения формул прогрессии.

К методу свёртки относится метод сводных показателей (МСП). Существует вектор исходных характеристик исследуемого объекта $\boldsymbol{x} = (x_1, \dots, x_m)$. $q_i(x_i)$ – нормированные отдельные показатели объекта. $\boldsymbol{w} = (w_1, \dots, w_m)$ - вектор весовых коэффициентов. $Q(q_1, \dots, q_m; \boldsymbol{w})$- сводный показатель исследуемого объекта. В методе рандомизированных сводных показателей (МРСП) неопределённость задания весовых коэффициентов компенсируется рандомизацией вектора весовых коэффициентов [137,150]. Весовые коэффициенты имеют совместное равномерное распределение на

области допустимых значений. Рандомизированный сводный показатель представляет собой случайную величину, у которой считается математическое ожидание $\bar{Q}^{(j)} = M\tilde{Q}^{(j)}$, стандартное отклонение $S^{(j)} = \sqrt{D\tilde{Q}^{(j)}}$ и достоверность доминирования $P\left(\{\tilde{Q}^{(m)} > \tilde{Q}^{(l)}\}\right) > \alpha$. Для увеличения точности и приближения вероятности доминирования к единице применяют дополнительную нечисловую, неполную и неточную информацию, то есть *ннн*-информацию (I).

Из перечисленных методов наиболее подходящим к решению задачи выбора наилучшего варианта СЗИ по независимым равнозначным критериям является метод свёртки с рандомизированными весовыми коэффициентами, то есть МРСП.

2.4 Различные модификации метода рандомизированных сводных показателей

МРСП подвергается изменениям при вариативном подборе задач. Одним из способов модификации МРСП является применение модели с иерархической системой критериев [70], где на каждом уровне решаются локальные задачи, а итоговые результаты объединены на верхнем уровне. На нулевом уровне строятся несколько сводных показателей, которые делят критерии на подзадачи. Сводные показатели следующего уровня формируются на основе показателей предыдущего уровня. Происходит декомпозиция сложной задачи на более простые подзадачи.

Недостатком данной модификации является потенциальная сложность разбивки на подзадачи. Используется принцип сильных и слабых связей. То есть связи между сводными показателями, формирующими показатель более высокого уровня должны быть сильнее, чем с другими показателями «своего» уровня. Также происходит увеличение дисперсии с переходом на следующий иерархический уровень. При формировании сводных показателей на всех иерархических уровнях для повышения точности оценок формируется экспертами дополнительная *ннн*-информация. Но эксперту психологически

трудно оценить сводные показатели на разных уровнях, имеющие сложные связи.

В другой работе [36] формируются два различных набора оценок объектов в определённые промежутки времени, сформированные двумя экспертными группами. Итоговые результаты (более высокий иерархический уровень) получают как усреднение предыдущих результатов. Для этого метода необходимо двойное количество экспертов с одинаковыми оценками компетентности, и расчёт допустимых границ согласованности действий экспертов как внутри группы, так и между группами.

Во всех работах, с описанием практических расчётов применения МРСП, в основе вычислений использовались точные данные об исследуемых объектах, полученные из печатных источников, котировок, электронных документов [58,137]. Количественные оценки разных свойств одного объекта затем подвергались линейному нормированию и подстановке в формулы метода. При исследовании СЗИ, спроектированной для конкретного предприятия точные данные, характеризующие её показатели по критериям, например, конфиденциальности, целостности, доступности информации невозможно найти в каких-либо источниках. Поэтому необходима модификация МРСП, подходящая для выбора наилучшего варианта СЗИ с учётом возможности использования точного результата в формулах количественной оценки конкурентоспособности предприятия.

Понятие конкурентоспособности предприятия не является однозначным и общепринятым. Миронов М. Г. считает, что «конкурентоспособность предприятия - это способность предприятия изготовлять и сбывать товар с большей конкурентоспособностью, чем у конкурента» [69]. Но конкурентоспособность предприятия определяется не только конкурентоспособностью продукции и услуг.

«Конкурентоспособность в общем смысле - это способность конкурировать, то есть бороться и противостоять чему-либо. Уровень конкурентоспособности

определяет степень превосходства одного объекта над другим. Поэтому из большого разнообразия определений конкурентоспособности предприятия можно выбрать определение, данное экономистами В. Грибовым, В. Грузиновым в работе «Конкурентоспособность предприятия» [25], где они рассматривают понятие конкурентоспособности как преимущество по отношению к другим предприятиям данной отрасли внутри страны и за ее пределами» [90].

Конкурентоспособность не является исключительным качеством одного предприятия, она оценивается среди группы «предприятий, относящихся к одной отрасли, либо предприятий, выпускающих аналогичные товары или услуги. Конкурентоспособность предприятия высчитывается по отношению к определённому рынку либо к конкретной группе потребителей» [90], относящихся к сегментированному участку рынка.

В современных рыночных отношениях конкуренция как движущая сила заставляет производителей постоянно искать новые пути повышения своей конкурентоспособности [138]. Задача любого предприятия не сводится сегодня только к удовлетворению потребностей покупателей, но и к предвосхищению будущих запросов и даже к их формированию. Качественно–ценовые характеристики товаров и услуг должны превосходить аналогичные у конкурентов, и клиенты могут получить большую ценность, необходимость которой они смогут осознать через некоторое время.

Способность опережать конкурента основывается на наделении товаров и услуг новыми потребительскими свойствами. Поэтому очень важна количественная оценка конкурентоспособности, которая поможет в дальнейшем формировать и управлять конкурентными преимуществами предприятия. «Количественная оценка уровня конкурентоспособности различных объектов представляет собой очень сложную задачу, так как в настоящее время нет единых международных стандартов по методике оценки конкурентоспособности объектов» [90].

У многих авторов в формуле расчёта конкурентоспособности перемножаются индексы конкурентоспособности товарной массы и относительной эффективности организации. Например, Моисеева Н. К. предложила следующую формулу (2.6) для оценки «конкурентоспособности производителя

$$K_{\text{п}} = J_{\text{т}} J_{\text{э}} \ , \qquad (2.6)$$

где $K_{\text{п}}$ - общий показатель конкурентоспособности по товарной массе;

$J_{\text{т}}$ - индекс конкурентоспособности по товарной массе;

$J_{\text{э}}$ - индекс относительной эффективности деятельности предприятия» [73].

Но индексы конкурентоспособности по товарной массе и относительной эффективности деятельности предприятия не являются независимыми величинами. Показатели эффективности зависят от объёма продаж и добавленной стоимости, которые в свою очередь пропорциональны конкурентоспособности товаров организации.

Шальминова А. С. для определения «интегрального показателя конкурентоспособности использует метод желательности и находит его как среднегеометрический взвешенный (2.7)

$$K = \sqrt[\alpha_1+\alpha_2+\alpha_3+\alpha_4+\alpha_5]{J_1 J_2 J_3 J_4 J_5} \ , \qquad (2.7)$$

где $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$- коэффициенты весомости показателей эффективности;

$J_1 J_2 J_3 J_4 J_5$ – частные показатели эффективности (эффективность производственной деятельности, финансового положения, эффективность продвижения товара, конкурентоспособность товара, эффективность инновационного проекта)» [139]. Но если один из частных показателей равен нулю, то и интегральный показатель становится равным нулю.

«Так как на предприятии создаются конкурентные преимущества товара, из которых далее формируются конкурентоспособности более высоких уровней, Р. А Фатхутдинов в работе «Управление конкурентоспособности организации» [128] рассчитывает уровень конкурентоспособности как средневзвешенную величину по показателям конкурентоспособности конкретных товаров на

конкретных рынках. Для интегральной оценки конкурентоспособности предприятия предлагается формула (2.8), учитывающая долю товара в объёме продаж и относительный вес рынков на которых они реализуются

$$K_{пред} = \sum_{i=1}^{n} a_i b_i K_i, \quad (2.8)$$

где a_i - доля товара (услуги) в объёме продаж за анализируемый период, доли единицы, $i = 1,2,3,\dots,n$, $\sum_{i=1}^{n} a_i = 1,0$; b_i – относительный вес рынка, на котором представлен товар организации.

Для промышленных развитых стран b_i рекомендуется принимать – 1,0; для остальных стран – 0,7; для внутреннего рынка – 0,5.

Доля i-го товара (услуги) организации в объёме продаж определяется отношением (2.9)

$$\mathrm{a}_i = \frac{V_i}{V}, \quad (2.9)$$

где V_i – объём продаж i-го товара (услуги) за анализируемый период в стоимостном выражении; V - общий объём продаж за анализируемый период.

K_i – уровень конкурентоспособности i – го товара или услуги» [90].

Во всех этих формулах вопросы влияния информационной безопасности на конкурентоспособность предприятия не рассматриваются.

Конкурентоспособность товара и услуги прямо пропорциональна качеству и обратно пропорциональна цене [42]. Полезный эффект и цена товара являются определяющими для клиента и основными составляющими конкурентоспособности товара. При сравнении данного предприятия с предприятиями–конкурентами можно использовать в качестве основы для сравнения базовые товары или услуги. Так как размерность эффективности определяется размерностями эффекта и затрат, а затраты выражены в денежном выражении, то денежная оценка эффекта также является предпочтительной.

«В работе И. Н. Рыбакова «Качество и конкурентоспособность продукции при рыночных отношениях» за показатель оценки качества продукции (полезный эффект) принята коммерческая оценка качества [118]. Показатель

конкурентоспособности продукции и услуг (2.10) выражается как отношение коммерческой оценки качества к полным затратам на её приобретение и использование

$$P = \frac{Q_k}{C+E}, \quad (2.10)$$

где C - покупная цена продукции, E - сопутствующие затраты на использование, а коммерческая оценка качества пропорциональна коэффициенту привидения и суммарному стоимостному эффекту $Q_k = \alpha F$» [104].

Первый множитель α является коэффициентом привидения, а F – суммарный стоимостный эффект (полезный эффект). Его составляющие имеют различный удельный вес, могут быть в той или иной степени представлены одновременно и для их общего количественного выражения следует использовать суммарный стоимостный эффект для потребителя при приобретении товара или услуги. «Величина суммарного стоимостного эффекта равна (2.14)

$$F = F_{\text{т}} + F_{\text{и}} + F_{\text{б}} + F_{\text{з}} + F_{\text{г}} + F_{\text{в}} + F_{\text{др}}, \quad (2.11)$$

где $F_{\text{т}}$ - стоимость продукции или услуг, вырабатываемые товаром за срок службы;

$F_{\text{и}}$ - стоимость информации, вырабатываемой товаром;

$F_{б}$ - стоимость интеллектуальных и эстетических благ, предоставляемых товаром;

$F_{\text{з}}$ - стоимость полезных для здоровья и окружающей среды эффектов, возникающих при использовании товара;

$F_{\text{г}}$ - стоимость гарантийных услуг, предоставляемых поставщиком товара;

$F_{\text{в}}$ - стоимость высвобождаемых товаров, которые могут быть реализованы благодаря новому товару;

$F_{др}$ - стоимость других полезных для потребителя результатов, имеющих денежное выражение, например, уменьшение издержек на страхование.

Таким образом, величина F отождествляется с потребительской стоимостью товара. Существует также ряд составляющих качества товара или услуги, не имеющих денежного выражения, к которым следует отнести: комфортное удовлетворение от удобства, стабильности, простоты обращения товара - $А_к$; престижное удовлетворения от новизны, оригинальности или уникальности товара - $А_{пр}$; эстетическое удовольствие от внешнего вида, запаха, упаковки товара - $A_э$; удовлетворение поставщиком, связанное с его имиджем [7], товарным знаком репутацией - $А_и$.

Эти составляющие выражаются коэффициентами, которые считаются по отношению к опорным значениям аналогичных составляющих для базовых товаров того же назначения, определяемых посредством экспертной оценки» [104]. Получаются коэффициенты (2.12)

$$\alpha_к = \frac{А_к}{А_к^б};\ \alpha_{пр} = \frac{А_{пр}}{А_{пр}^б};\ \alpha_э = \frac{A_э}{A_э^б};\ \alpha_и = \frac{А_и}{А_и^б}. \qquad (2.12)$$

Результирующий коэффициент привидения равен $\alpha = \alpha_к \alpha_{пр} \alpha_и \alpha_э$. Коммерческая оценка качества отражает все стороны удовлетворения запросов потребителя и особенности его восприятия. Уровень конкурентоспособности товара (2.16) на конкретном рынке вычисляется по формуле

$$K_i = \frac{P_i}{P_i^б}, \qquad (2.13)$$

где P_i - конкурентоспособность i-го товара;

$P_i^б$ – конкурентоспособность базового i-го товара.

Но в этой формуле не учитываются выгоды, которые получает клиент при повышении информационной безопасности предприятия [59]. Предоставление товаров и услуг становятся всё более персонифицированным. Происходит ориентация на личные потребности клиента. Предприятия стремятся повысить эффект полезности товара путём более полного удовлетворения специфических потребностей клиента.

Предоставление товаров и услуг непрерывно связано с накапливанием персонифицированной информации [61]. Создаются базы данных покупателей, потенциальных потребителей. Интерактивное взаимодействие с потребителями посредством электронной почты, через Web-сайты компании анализируется и влияет на настройки бизнес-процессов [135]. Покупая товар или услугу, потребитель фиксирует положительный или отрицательный опыт по приобретению, в том числе в связи с соблюдением политики информационной безопасности на предприятии.

При нарушении информационной безопасности, краже конфиденциальных данных, ухудшении имиджа компании, подаче судебных исков в связи с нарушением закона ФЗ – 152 «О персональных данных» [41] к компании со стороны клиентов, закрепляется негативный опыт взаимодействия с данной компанией, происходит неизбежный отток клиентов, и, в конечном итоге, понижение уровня конкурентоспособности компании.

Поэтому при обеспечении информационной безопасности, полезный эффект от приобретения товара увеличивается. Вероятность реализации злонамеренных действий снижается, а полезный эффект товара увеличивается на условный эффект, возникающий при обеспечении информационной безопасности. Показатель конкурентоспособности i-го товара определяется по формуле (2.14):

$$P_i = \frac{\alpha_i F_i + Э^i_{\text{уИБ}}}{C_i + E_i + Z_i}, \quad (2.14)$$

где $Э^i_{\text{уИБ}}$ - доля условного эффекта для каждого товара от $Э_{уИБ}$; $Э_{уИБ}$ - условный эффект (2.4), равный денежной оценке ущерба предприятию при игнорировании вопросов информационной безопасности, умноженную на разность единицы и коэффициента изменения конкурентоспособности в случае обеспечения информационной безопасности предприятия; Z_i - доля затрат для каждого товара от Z, а Z – затраты на реализацию СЗИ и службы информационной безопасности (СИБ).

Пусть $Э^{i}_{\text{уИБ}} = d_i Э_{\text{уИБ}}$ - доля условного эффекта для каждого товара или услуги. Тогда условный эффект равен сумме (2.15):

$$Э_{\text{уИБ}} = d_1 Э_{\text{уИБ}} + \cdots + d_n Э_{\text{уИБ}}. \qquad (2.15)$$

И $\forall\ i$ коэффициенты $d_i \geq 0$ и их сумма нормирована $d_1 + \cdots + d_n = 1$. $Z^i = d_i Z$ – доля затрат для каждой услуги. Тогда конкурентоспособность i – го товара подсчитывается по формуле (2.16):

$$K_i = \frac{P_i}{P_i^{б}} = \frac{\alpha_i F_i + Э^{i}_{\text{уИБ}}}{\alpha_i^{б} F_i^{б}} \times \frac{C_i^{б} + E_i^{б}}{C_i + E_i + Z_i}. \qquad (2.16)$$

Подставляя это выражение в формулу (2.8), получаем формулу конкурентоспособности предприятий (2.7) с учётом обеспечения информационной безопасности предприятия

$$К_{\text{пред}} = \sum_{i=1}^{n} a_i b_i \frac{\alpha_i F_i + Э^{i}_{\text{уИБ}}}{\alpha_i^{б} F_i^{б}} \times \frac{C_i^{б} + E_i^{б}}{C_i + E_i + Z_i}\,. \qquad (2.17)$$

Конкурентоспособность предприятия без учёта обеспечения информационной безопасности до внедрения СЗИ считается по формуле (2.18)

$$К^{\text{безИБ}}_{\text{пред}} = \sum_{i=1}^{n} a_i b_i \frac{\alpha_i F_i}{\alpha_i^{б} F_i^{б}} \times \frac{C_i^{б} + E_i^{б}}{C_i + E_i} = \sum_{i=1}^{n} \theta_i, \qquad (2.18)$$

где $\theta_i = a_i b_i \frac{\alpha_i F_i}{\alpha_i^{б} F_i^{б}} \times \frac{C_i^{б} + E_i^{б}}{C_i + E_i}$.

Тогда коэффициенты d_i считаются по формуле (2.19)

$$d_i = \frac{\theta_i}{К^{\text{безИБ}}_{\text{пред}}}\,. \qquad (2.19)$$

При равенстве коэффициентов d_i, доли затрат и условного эффекта можно считать по формулам (2.20)

$$Z_i = \frac{Z}{n}\,, \quad Э^{i}_{\text{уИБ}} = \frac{Э_{\text{уИБ}}}{n}, \qquad (2.20)$$

где n - количество производимых товаров или предоставляемых услуг на предприятии.

Полученная формула (2.20) вычисляет объективные количественные оценки, и даёт возможность использовать эту формулу в качестве критерия

выбора варианта СЗИ. Обеспечение конкурентоспособности предприятия достигается при максимальном значении условного эффекта, минимальном значении коэффициента изменения конкурентоспособности и является основой минимизации экстремальных значений в оптимизационной задаче.

2.5 Метод оптимизации вариантов зашиты

Перепишем оптимизационную задачу с учётом полученных формул (2.21).

$$\sum_{s=1}^{n} a_s b_s \frac{Q_s + Э_{уИБ}^{sj}(\boldsymbol{x}^{0j})}{Q_s^б} \times \frac{C_s^б + E_s^б}{\mathrm{C+E}+Z_s(\boldsymbol{x}^{0j})} = \max_{j\in\Omega}\left(\sum_{s=1}^{n} a_s b_s \frac{Q_s + Э_{уИБ}^{sj}(\boldsymbol{x}^{j})}{Q_s^б} \times \frac{C_s^б + E_s^б}{\mathrm{C+E}+Z_s(\boldsymbol{x}^{j})}\right) \tag{2.21}$$

$$\boldsymbol{x}^{0j} = Arg\max\left(\rho_i^j(x_i)\right), \qquad i = 1,\dots,m; \quad j = 1,\dots,k$$

$$\boldsymbol{x}^{0j} \epsilon X^d,$$

при ограничении

$$Z\left(\boldsymbol{x}^{oj}\right) \le Z^d$$

$$\sum_{j=1}^{k} C\left(r_{ij}\right) \le C^d,$$

$$\begin{cases} \sum_{j=1}^{k^c} \varphi\left(r_{ij}\right) = k^c \\ \varphi\left(r_{ij}\right)\epsilon\{0,1\} \end{cases}$$

$$h = \frac{1}{h_i}$$

$$P\left(\left\{\tilde{Q}^{(m)} > \tilde{Q}^{(l)}\right\}\right) > \alpha$$

где $\boldsymbol{x}^{\mathrm{o}}$ – аргумент максимизации; X^d – множество допустимых значений векторов числовых характеристик; Z^d – допустимые затраты для предприятия; P – достоверность доминирования,$\alpha \in [0,1]$ – параметр достоверности доминирования, h_i – шаг дискретизации ММРСП; $m, l = 1,\dots,k$; k^c – типы средств ЗИ; Ω- множество вариантов СЗИ. Из *N* альтернативных вариантов СЗИ выбирается наилучший вариант, который обеспечивает максимум конкурентоспособности предприятия.

Выводы по главе 2

В данной главе были получен алгоритм генерации допустимых вариантов системы защиты информации, метод оптимизации вариантов защиты; выведена количественная формула влияния обеспечения ИБ на конкурентоспособность предприятия.

Таким образом, цель, поставленная в начале главы 2, выполнена.

3 Метод обоснования СЗИ по критерию конкурентоспособности предприятия

3.1 Требования к экспертам

Цель данной главы – описать алгоритм обработки нечётких входных данных, получить метод оптимизации вариантов защиты.

Метод обоснования СЗИ по критерию конкурентоспособности предприятия опирается на модифицированный метод рандомизированных сводных показателей, который содержит нечёткую логическую модель с экспертными оценками. «Эксперт (от лат. expertus - опытный, знающий, сведущий) - специалист, дающий заключение при рассмотрении какого-нибудь вопроса»[77]. Эксперты должны:

- быть компетентными;
- быть опытными;
- иметь учёную степень;
- быть эрудированными в смежных областях;
- быть объективными [101].

В кодексе Российской Федерации об административных правонарушениях говорится, что «В качестве эксперта может быть привлечено любое не заинтересованное в исходе дела совершеннолетнее лицо, обладающее специальными познаниями в науке, технике, искусстве или ремесле, достаточными для проведения экспертизы и дачи экспертного заключения» [50].

Эксперты должны пройти инструктаж, определить степень согласованности действий. Эксперты получают шкалу измерений, объект измерений, узнают, какое значение показателей является наилучшим. При формировании экспертной группы проводятся предварительные измерения, рассчитывается ранг объекта. Коэффициент ранговой согласованности Кендалл-Смита определяется формулой (3.1)

$$W = \frac{12S}{n^2(m^3-m)}, \quad 0 \le W \le 1 \tag{3.1}$$

где S - сумма квадратов отклонений суммы рангов каждого объекта экспертизы от среднего арифметического рангов, n - число экспертов, m - число оцениваемых объектов. W стремится к 0 при несогласованности, и к 1 при обратной ситуации. Выводы экспертов должны быть инвариантны относительно допустимых преобразований шкал измерений» [101].

Например, три эксперта оценивают три показателя (таблица 3.1):

Таблица 3.1 – Данные для расчёта ранговой согласованности

	Показатель 1	Показатель 2	Показатель 3	Всего
Эксперт 1	1	3	1	
Эксперт 2	2	2	2	
Эксперт 3	3	2	1	
Сумма	6	7	4	17
Квадрат суммы	36	49	16	101

Тогда S рассчитывается с такими значениями показателей (3.2)

$$S = 101 - \frac{17^2}{3} = 4{,}67. \tag{3.2}$$

Коэффициент Кендалл-Смита равен (3.3)

$$W = \frac{12*4{,}67}{3^2(3^3-3)} = 0{,}26. \tag{3.3}$$

Коэффициент $W < 0{,}4$, следовательно, оценки данных экспертов слабо согласованы. Слабо согласованные оценки, при этом, могут иметь согласованные группы в выборке экспертов.

При подборе экспертов подсчитывают «коэффициент профессиональной перспективности K (3.4)

$$K = О_{уо}\left(1 + \frac{C}{4} + \frac{B}{18}\right), \tag{3.4}$$

где $О_{уо}$ - оценка уровня образования (0,60 для среднего образования; 0,75 для

среднетехнического; 1,00 для высшего);

C - стаж работы по специальности;

B – возраст» [79].

При большом расхождении величины K разных экспертов, могут учитываться весовые квалификационные коэффициенты экспертов, которые основываются на самооценке и взаимооценке. Весовые квалификационные коэффициенты L_i подсчитываются по формуле (3.5)

$$L_i = \frac{B_i}{\sum_{j=1}^{n} B_j} \text{ и } \sum_{i=1}^{n} L_i = 1 \quad (3.5)$$

где n – количество экспертов; B_i - баллы, присвоенные i-му эксперту. Баллы присваиваются по выбранным критериям, например, образование, стаж работы в исследуемой области, количество проведённых экспертиз, квалификация в смежных областях.

Немаловажным является вопрос количества экспертов. С одной стороны с ростом числа экспертов точность измерений возрастает. С другой стороны, для минимизации расходов и ограниченности выборки экспертов их число желательно минимизировать. В качестве компромисса можно взять такое количество экспертов n, при котором разница между рассеянием результатов оценок для n и $n+1$ экспертов не значительна.

Когда группа сформирована, эксперты проходят инструктаж по экономической деятельности предприятия, знакомятся с бизнес-процессами, защищаемыми информационными ресурсами. Затем выбираются методы работы экспертов. Можно использовать метод непосредственной оценки, метод Дельфи, метод парного сравнения; метод индивидуальной оценки.

«При использовании метода индивидуальной оценки, объект оценки получает определенное значение по оценочной шкале, а затем эти индивидуальные значения разных экспертов усредняются по Колмогорову или методу медиан» [101]. Средней величиной чисел X_i , $i = 1 \dots n$ по Коши является $\forall$ функция $f(X_1, \dots, X_n)$ такая, что её значение не меньше, чем

$min \quad X_i$ и не больше, чем $max\ X_i$.

Частным случаем средних величин по Коши являются средние величины по Колмогорову. Для чисел X_i , $i = 1 \ldots n$ средним по Колмогорову считается результат $G\{(F(X_1) + \cdots + F(X_n))/n\}$, где F - монотонная функция, а G – обратная функция к F. Если $F(x) = x$, то средним по Колмогорову является среднее арифметическое. Если $F(x) = 1/x$, то средним по Колмогорову является среднее гармоническое. Медиана и мода не могут быть средними по Колмогорову.

Метод медиан заключается в расположении объектов в ряд, согласно присвоенных рангов, в порядке не убывания. Если объектов нечётное число, то медианой является центральный ранг. При чётном числе объектов медиана вычисляется как среднее арифметическое центральных членов ряда. Метод медиан используют при оперировании порядковой шкалой.

Для ММРСП перечисленные методы усреднения не подходят, так как эксперты формируют опорные значения функции принадлежности нечётких чисел. Нечёткие множества дают возможность формализации величин, имеющих качественную основу.

Эксперт редко сразу получает точную оценку исследуемого объекта. Ему легче представлять информацию с помощью естественного языка и оперировать нечеткой принадлежностью конкретного значения к какому-либо множеству. Лингвистические оценки вносят в поступающую от эксперта информацию неопределённость в виде нечёткости. Вследствие этого целесообразно применение теории нечётких множеств и нечёткой логики [141].

Пусть $X = \{x\}$ – универсальное множество, то есть множество, которое при объединении с любым другим множеством равно самому себе. Под нечётким множеством (fuzzy set) [166] *A* понимается следующая совокупность (3.6)

$$A = \{(x, \mu_A(x)) | x \in X\}, \tag{3.6}$$

где $\mu_A(x)$ - функция принадлежности, характеризующая степень принадлежности элемента *x* нечёткому множеству *A*.

Если нечеткое множество A дискретно и определено на конечном универсальном множестве $X = \{x_1, x_2, \dots, x_n\}$, то его удобно обозначать следующим образом (3.7)

$$A = \frac{\mu_A(x_1)}{x_1} + \frac{\mu_A(x_2)}{x_2} + \cdots \frac{\mu_A(x_n)}{x_n} = \sum_{i=1}^{n} \frac{\mu_A(x_i)}{x_i}, \quad (3.7)$$

где $\frac{\mu_A(x_i)}{x_i}$ - пара «функция принадлежности/элемент», называемая синглтоном (singleton), а «+» - обозначает совокупность пар.

«Лингвистическое значение может быть задано множеством, содержащим числовые либо нечисловые элементы. Лингвистическим терм-множеством называется множество всех лингвистических значений, используемых для определения некоторой лингвистической переменной.

Нечёткое число – это нечёткое множество A, определённое на множестве действительных чисел R и его функция принадлежности нормальна и выпукла. Для представления как нечетких чисел, так и лингвистических значений используются нечеткие множества. Лингвистическое значение может быть задано множеством, содержащим числовые либо нечисловые элементы, то нечеткое число должно определяться только на множестве вещественных чисел» [138].

Количественные признаки описываются лингвистическими переменными, имеющие значения слов естественного или искусственного языка.

Для сравнения объектов необходимо выбрать шкалы, градации, единицы измерения.

3.2 Шкалы

«Шкала – это символьный ряд значений, отражающий диапазон значений измеряемой величины» [85]. Шкалы делятся на качественные: номинальные, порядковые, нечёткие; и количественные: абсолютные, нелинейные, шкалы интервалов, шкалы отношений (рисунок 3.1).

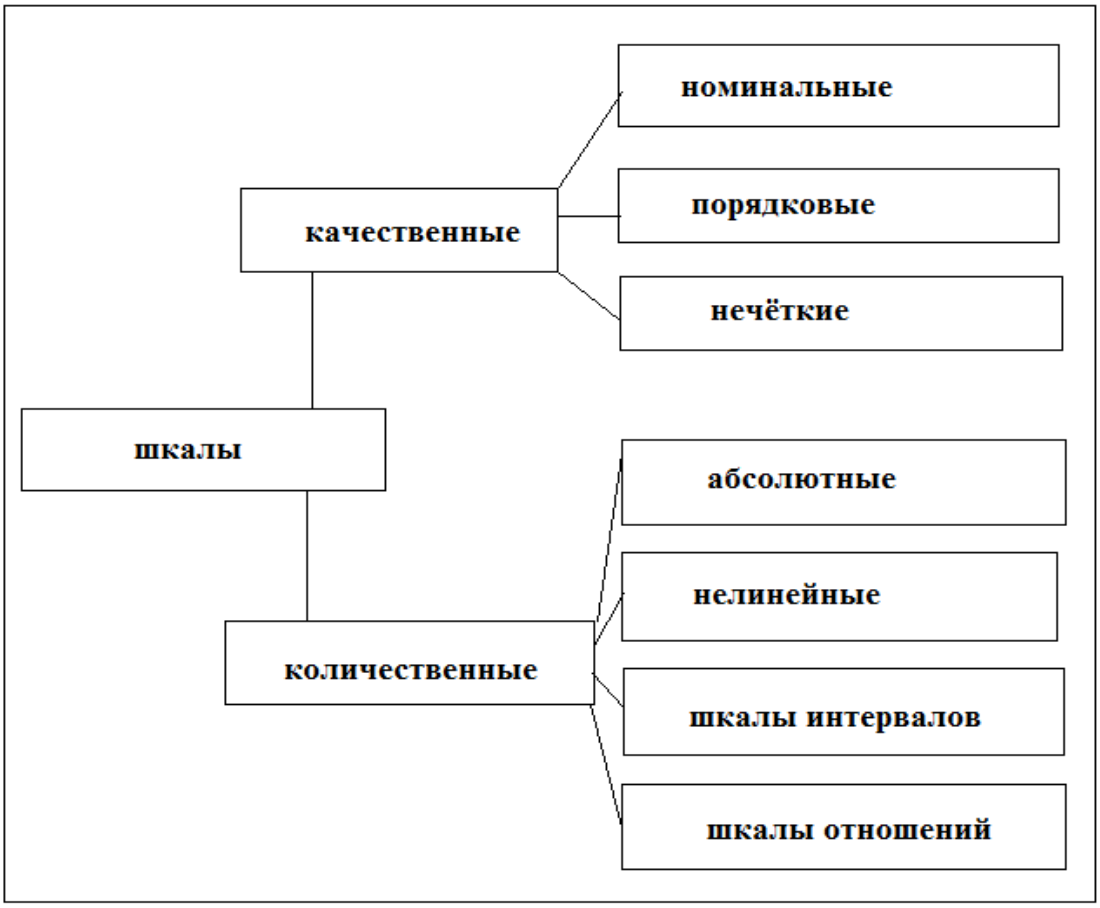


Рисунок 3.1– Виды шкал

Номинальные шкалы или шкалы измерений оперируют отношениями эквивалентности. В них нет точки отсчёта, единицы измерения, отношений «меньше» и «больше». Качественным значениям объекта измерений приписываются символы из определённого класса эквивалентности.

Порядковая шкала (ordinal scale) – это шкала, на которой числа нанесены для обозначения относительных позиций объектов, но не фиксируют различия между ними. Порядковая шкала не имеет нулевой точки и атрибутов интервальности.

Нечёткие или лингвистические шкалы содержат уровни, соответствующие значениям лингвистических переменных из терм-множества. Этим уровням соответствуют нечёткие множества принадлежности, заданные на универсальных множествах. Количественные признаки описываются лингвистическими переменными, имеющие значения слов естественного или искусственного языка, с функциями принадлежности нечёткого множества.

Шкалы интервалов (разностей) имеют единицы измерения, произвольно выбранное начало отсчёта, разделены на одинаковые интервалы.

Шкалы отношений содержат инвариантные точки отсчёта и единицы измерения, выбранные по соглашению.

Абсолютные шкалы имеют инвариантные точки отсчёта, единицы измерения и устанавливают однозначное соответствие между объектами и числами.

Линейными называют метрические шкалы. Нелинейные шкалы имеют непостоянные интервалы деления шкалы.

Используя нечёткие шкалы на начальном этапе измерения величин, сформированная группа экспертов поставляет эвристическую информацию, которая является входными данными в ММРСП, и выходные данные используются в методе обоснования СЗИ по критерию конкурентоспособности предприятия.

Для сравнения N вариантов выбранных объектов выбирается нечёткая шкала с уровнями, соответствующими значениям лингвистических переменных из терм-множества.

3.3 Модифицированный метод рандомизированных сводных показателей

В диссертационной работе предлагается следующая модификация МРСП, для решения задачи выбора наилучшего варианта СЗИ для конкретного предприятия:

1. Использование в качестве начального этапа нечёткой модели, основанной на нечёткой информации, предоставляемой экспертами.
2. Применение в ММРСП сначала нечёткой лингвистической шкалы, а затем абсолютной шкалы вместо порядковой шкалы, использовавшейся в МРСП.
3. В МРСП входные данные – точные значения характеристик исследуемых систем, на выходе – рейтинги для каждой системы. Входные данные в

ММРСП – опорные значения функции принадлежности, на выходе – значение коэффициента, оптимизированное по всем критериям для каждой системы.

1. Нечёткая информация даёт возможность применить методы нечёткого моделирования. Метод нечёткого моделирования, использующий экспертные знания, основан на ментальной модели, создаваемой экспертом на основе реальной системы. Ментальная модель продуцирует вербальную, в рамках которой эксперт выражает свои знания. Связь перечисленных моделей представлена на рисунке 3.2.

Рисунок 3.2 – Процесс построения начального этапа ММРСП

Эксперты формируют опорные значения функции принадлежности коэффициента изменения ущербов (коэффициента изменения конкурентоспособности), который равен отношению величины ущербов от нарушения информационной безопасности после и до внедрения СЗИ, - $u_k^{(ijl)}$ в опорных точках $k = 1, \dots, 4$, и для объектов $j = 1, \dots, k$, по критериям $i = 1, \dots, m$; всего экспертов $l = 1, \dots, n$. Формируется трапецеидальная функция

принадлежности $\mu_{A^l}(u^l)$ нечёткого числа (3.7):

$$\mu_{A^l}(u^l) = \begin{cases} 0, \ u^l \le u_1^l \\ \frac{u^l - u_1^l}{u_1^l - u_2^l}, u_1^l < u^l < u_2^l \\ 1, u_2^l \le u^l \le u_3^l \\ \frac{u^l - u_4^l}{u_3^l - u_4^l}, u_3^l < u^l < u_4^l \\ 0, \ u^l \ge u_4^l, \end{cases}, \tag{3.8}$$

где $u_1^l < u_2^l \le u_3^l < u_4^l$.

Для вывода выходной функции принадлежности используется принцип обобщения. Получается модель с нечёткими входами и нечётким выходом MISO, схема которой представлена на рисунке 3.3.

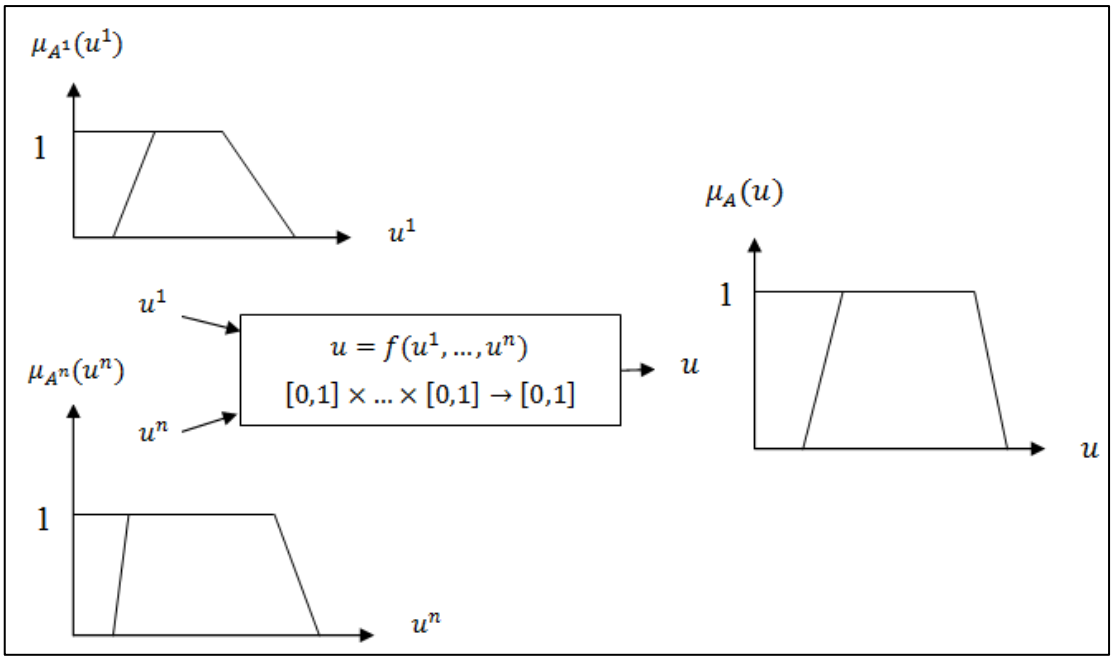


Рисунок 3.3 – MISO-система с нечёткими входами и нечётким выходом

На выходе получается функция нескольких переменных. Нечёткий вывод основывается на базе знаний, которую составляют обобщённые логические правила: ЕСЛИ $((u^1$ есть $A^1)$ И…И $(u^n$ есть $A^n))$ ТО $(u$ есть $A)$. Вектор U определён на декартовом произведении областей определения отдельных входных величин $U^1 \times \dots \times U^n$. Правила задают причинно-следственные отношения между нечёткими значениями входных и выходных величин.

Функция f отображает множество элементов областей определения входных величин на область значения выходной величины. $f: U^1 \times ... \times U^n \to U$. Принцип обобщения для функции нескольких переменных представляет собой задание функции принадлежности выходного значения системы (3.8).

$$\mu_A(u) = \bigvee_{u = f(u^1, \dots, u^n)} \left(\mu_{A^1}(u^1) \wedge \dots \wedge \mu_{A^n}(u^n)\right), \qquad (3.9)$$

$$\forall\ u^1, \dots, u^n, u\ \in R$$

где символ $\vee$ означает объединение множеств на основе операции max, $\wedge$ - означает объединение множеств на основе операции min.

Например, если на вход поступают два нечётких числа с функциями принадлежности $\mu_{A^1}(u^1)$ и $\mu_{A^2}(u^2)$, а функция f считает среднее значение, то метод получения выходной функции принадлежности приведён на рисунке 3.4.

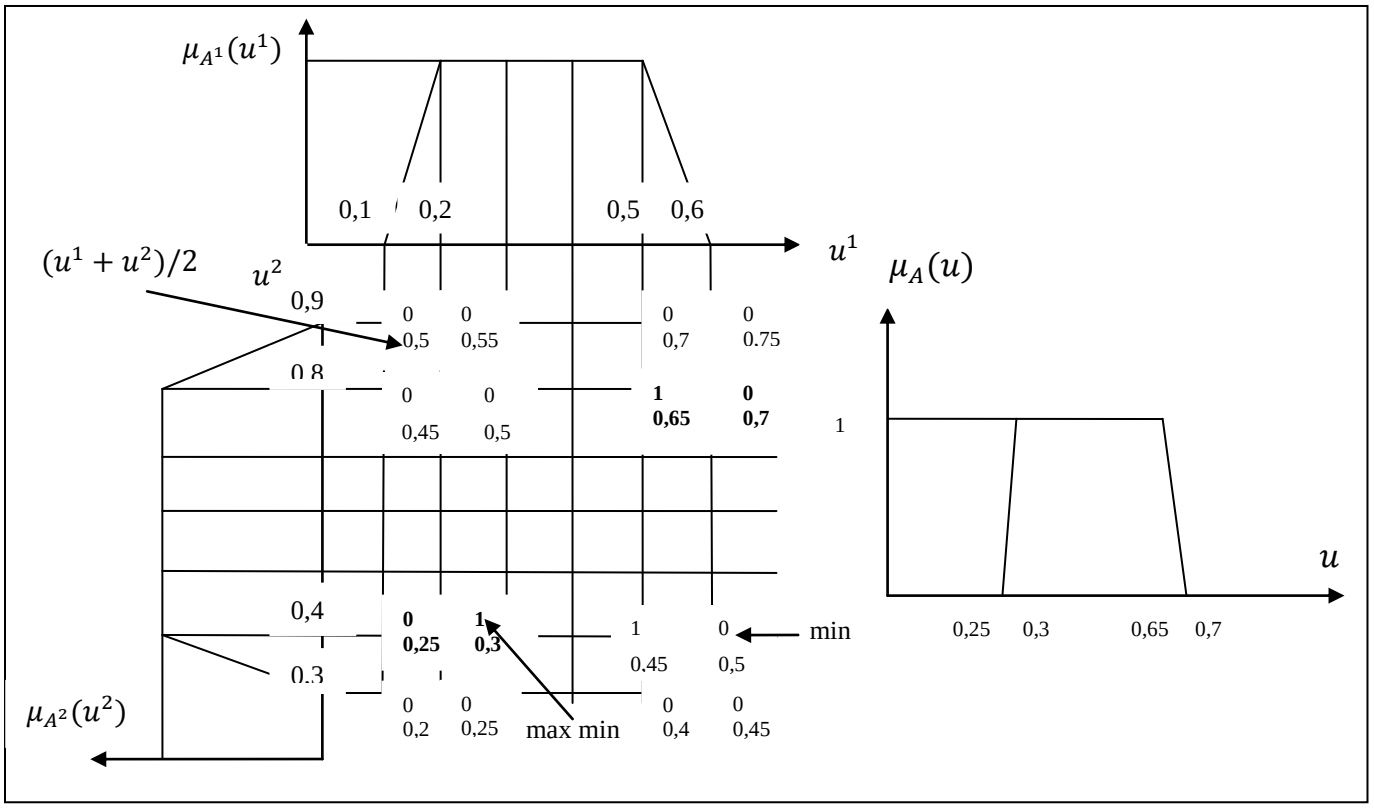


Рисунок 3.4 – Метод получения функции принадлежности нечёткого числа u, которая получена с использованием операторов max и min

Затем производится дефаззификация итоговой функции принадлежности.

Функция принадлежности трапецеидального нечёткого числа – это кусочно-

линейная функция, функция принадлежности которой представлена формулой 3.8. Дефаззификацию трапецеидального числа будем проводить по методу центра масс. Функция $L(u) = \frac{u-u_1}{u_2-u_1}$ называется левым скатом функции принадлежности, функция $R(u) = \frac{u-u_4}{u_3-u_4}$ называется правым скатом функции принадлежности, и изображены на рисунке 3.5.

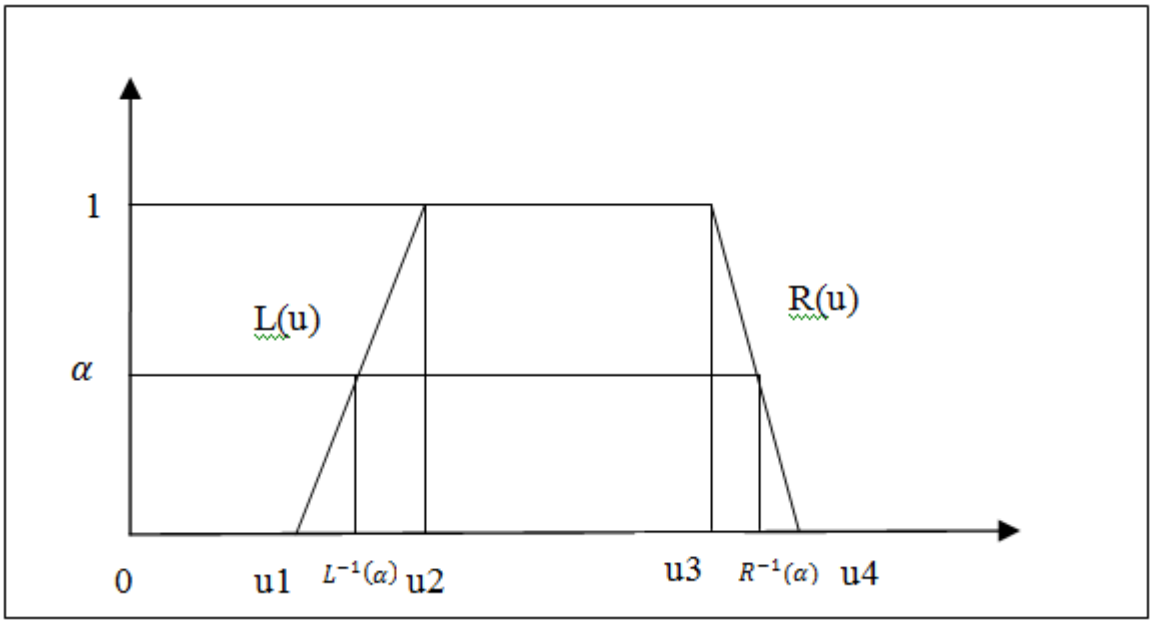


Рисунок 3.5 – Функция принадлежности трапецеидального (L-R type) нечёткого числа

Пусть функция $L^{-1}(\alpha)$ и $R^{-1}(\alpha)$ - обратные функции к функциям $L(u)$ и $R(u)$ соответственно. Градуированное среднее значение [160] α -уровневой величины трапецеидального числа равно (3.10)

$$\frac{(L^{-1}(\alpha)+R^{-1}(\alpha))\cdot\alpha}{2}. \quad (3.10)$$

Тогда интегральное представление градуированного среднего значения нечёткого числа А рассчитывают по формуле (3.10)

$$centr(A) = \frac{\int_0^1 \frac{(L^{-1}(\alpha)+R^{-1}(\alpha))\cdot\alpha}{2} d\alpha}{\int_0^1 \alpha d\alpha}, \quad (3.11)$$

где $0 \leq \alpha \leq 1$.

Подставляя значения обратных функций, получаем (3.12, 3.13)

$$centr(A) = \frac{\int_0^1 \frac{(u_1+(u_2-u_1)\cdot\alpha)+(u_4-(u_4-u_3)\cdot\alpha)}{2}\alpha d\alpha}{\int_0^1 \alpha d\alpha} \quad (3.12)$$

$$centr(A) = \frac{u_1+2u_2+2u_3+u_4}{6}, \quad (3.13)$$

В случае $u_2 = u_3$ получаем (3.14)

$$centr(A) = \frac{u_1+4u_2+u_4}{6}, \quad (3.14)$$

где $u_1, u_2, u_3, u_4 \in \mathcal{R}$.

Дефаззифицируя функцию принадлежности нечёткого числа, мы получаем чёткое центроидное значение для трапецеидального числа, которое подвергается дальнейшей обработке в методе (рисунок 3.6).

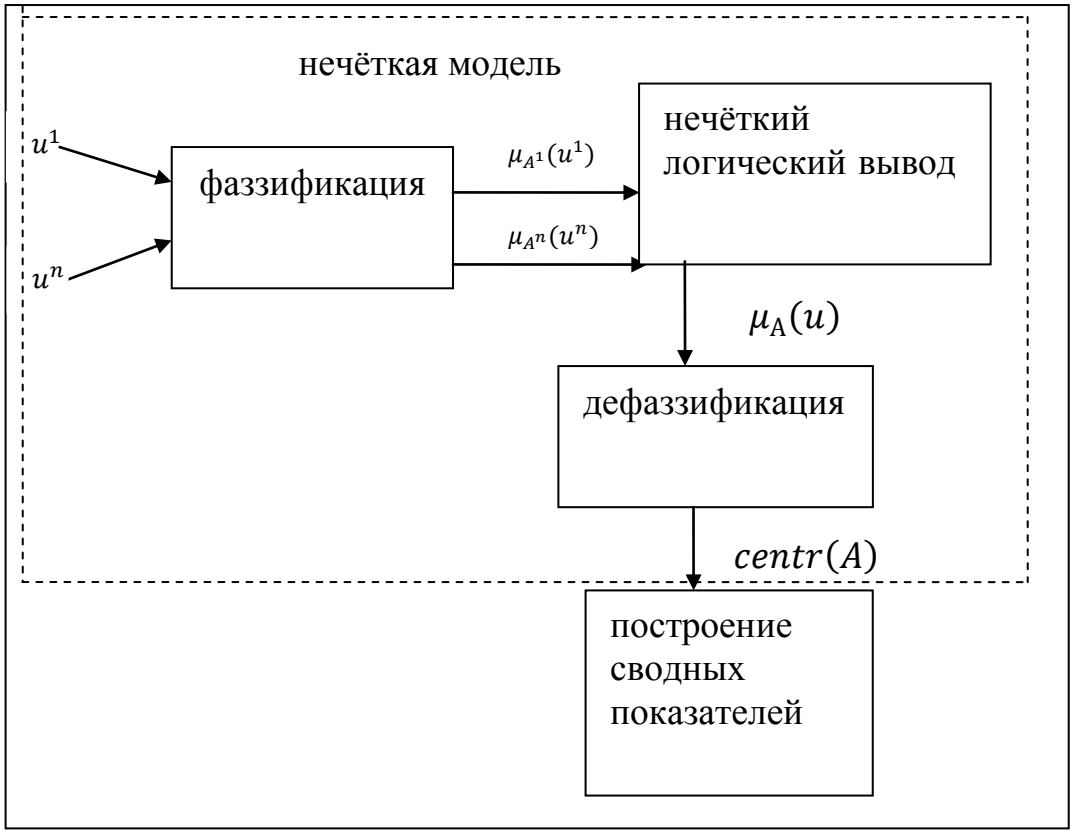


Рисунок 3.6– Структура нечёткой модели

На выходе нечёткой модели получаются чёткие значения.

2.В МРСП используется метод рейтингования. Сравниваемым объектам присваивается рейтинги, которые располагаются на шкале в определённом порядке. Но при этом нельзя получить степень выраженности характеристик, приписываемых объектам. Поэтому используются порядковые шкалы, в которых

отсутствуют атрибуты интервальности (3.15).

$$\forall\, x_1, x_2 \in R\ \{x_1 \le x_2\} \Leftrightarrow \{\varphi(x_1) \le \varphi(x_2)\}. \quad (3.15)$$

Порядковые шкалы определяются системой монотонных допустимых преобразований.

В ММРСП в нечёткой модели используются нечёткие шкалы. Термальные значения являются основой для формирования нечёткого числа. На следующих этапах сравниваемые величины располагаются на шкале с определёнными интервалами и началом отсчёта. Следовательно, необходимо использовать абсолютные шкалы. Абсолютная шкала определяется группой положительных пропорциональных преобразований и имеет однозначное определение единицы измерения (3.16).

$$\forall\, x_1, x_2 \in R\ \{x_1 = x_2\} \Leftrightarrow \{\varphi(x_1) = \varphi(x_2)\}. \quad (3.16)$$

С помощью абсолютных шкал можно ранжировать объекты, получать количественные значения.

3. В МРСП $\boldsymbol{x} = (x_1, \dots, x_m)$ - вектор исходных характеристик исследуемого объекта, имеющий точные значения. На выходе в МРСП получают математическое ожидание $\bar{Q}^{(j)} = M\tilde{Q}^{(j)}$ для каждой системы, которое является свёрткой оптимизации по нескольким критериям.

В ММРСП формируется эвристическая информация u_k^{ij} , где k – номер опорных точек , i - номер критериев, j - номер системы защиты информации от каждого эксперта.

4. На выходе в ММРСП получают количественные значения коэффициента для каждой системы, которые не только ранжирует системы защиты информации, но и могут использоваться в формулах.

3.5 Алгоритм обработки нечётких входных данных

Алгоритм обработки нечётких входных данных составляет последовательность следующих действий:

5. Генерируются несколько альтернативных вариантов комбинаций средств ЗИ для данного предприятия.
6. Подбираются эксперты, формируется экспертная группа, проводится инструктаж, происходит ознакомление с бизнес-процессами предприятия.
7. Вербальные экспертные оценки являются входными данными для нечёткой модели ММРСП.
8. Определяются опорные точки лингвистической переменной коэффициента изменения конкурентоспособности (пессимистичные верхние и нижние оценки, интервал наиболее ожидаемых значений).
9. Производится фаззификация входных значений, формирование трапецеидальных функций принадлежности.
10. Формируется набор продукционных правил типа «ЕСЛИ…ТО», отражающих взаимосвязи входных и выходных значений. Выбирается оператор для конъюнктивного условия в продукционных правилах.
11. Производится нахождение функции принадлежности выходного значения по принципу обобщения для функции нескольких переменных.
12. Дефаззифицируется результирующая функция принадлежности на выходе нечёткой модели, и результаты дефаззификации поступают на вход чёткой модели ММРСП.

Нечёткие данные после обработки поступают в чёткую часть гибридной модели

3.6 Метод обоснования системы защиты информации по критерию конкурентоспособности

Модифицированный метод начинается с нечёткой модели, так как в основе берётся нечёткая экспертная информация. «Фаззификация – это установка соответствия между численным значением входной переменной системы

нечеткого логического вывода и значением функции принадлежности лингвистической переменной» [119].

Эксперты используют нечёткую шкалу и формируют по четыре значения терм-множества коэффициента изменения конкурентоспособности u_l^{ij}, при $l = 1{,}4$ - пессимистичные оценки, при $l = 2{,}3$ - интервал наиболее ожидаемых значений для нескольких систем $j = 1, \dots, k$ и критериев $i = 1, \dots, m$ (доступность, целостность и конфиденциальность информации) (3.17).

$$u_k^{ij} = \begin{cases} \{u_1^{ij}(\alpha), u_4^{ij}(\alpha)\}, \alpha = 0 \\ \{u_2^{ij}(\alpha), u_3^{ij}(\alpha)\}, \alpha = 1 \end{cases}, \quad (3.17)$$

где α - уровень нечёткого множества A.

По принципу обобщения получается выходная функция принадлежности по конкретному критерию для каждой анализируемой системы.

Затем производится дефаззификация полученных оценок. «Дефаззификация в системах нечеткого вывода – это процесс перехода от функции принадлежности выходной лингвистической переменной к её четкому (числовому) значению» [119]. Если $\mu_A(u)$ гладкая, непрерывная функция, дефаззификации можно провести центроидным (3.18) методом:

$$P(A) = \frac{\int_{min\,u}^{max\,u} u\mu_A(u)du}{\int_{\min u}^{\max u} \mu_A(u)du} \quad (3.18)$$

Если $\mu_A(u)$ кусочно-непрерывная, трапецеидальная, то интегрирование происходит по –уровням (формула 3.13). Формируются значения в виде матрицы размером $i \times j$. На вход чёткой модели ММРСП поступают выходные значения нечёткой лингвистической модели коэффициента изменения конкурентоспособности ρ_i^j (3.19) по шкале каждого из критериев» [92].

$$centr(A)_i^j = \rho_i^j \quad (3.19)$$

При дефиците числовой информации, касающейся вектора весовых коэффициентов, в результате байесовской рандомизации неопределённости, отдельные показатели превращаются в соответствующие случайные величины.

Задача градационного построения объектов сводится к задаче выявления стохастического доминирования между соответствующими рандомизированными сводными показателями. Дефаззифицированные входные данные дают возможность получения теоретического значения коэффициента, на основе которого происходит ранжирование исследуемых систем.

На рисунке 3.7 изображёна блок-схема модифицированного метода рандомизированных сводных показателей. k оцениваемых объектов (СЗИ) оптимизируют по m критериям. Каждая отдельная координата $\rho_i^{(j)}$ является функцией одной исходной характеристики $x_i^{(j)}$: $\rho_i^{(j)}(x_i)\ j = 1, \dots, k;\ i = 1, \dots, m,$ причем минимальное значение является наиболее предпочтительным. Для этого выбираются нормирующие функции $q_i\left(\rho_i(x_i)\right),\ i = 1, \dots, m\ \ q \in [0,1]$. Так как возрастание коэффициента изменения конкурентоспособности приведёт к ухудшению ИБ предприятия, то q_i задаётся как монотонно убывающая функция.

Необходимо оценить объект для определения его места среди выбранного множества объектов по близости значений характеристик к экстремальным значениям [14]. Для этого нужно определить значимость каждого критерия по отношению к другим, которая задаётся вектором весовых коэффициентов $\boldsymbol{w} = (w_1, \dots, w_m),\ \ w_i \geq 0$. Каждая координата вектора определяет вклад критерия в сводную оценку исследования. Так как важно относительное значение координат вектора, вводится нормирование суммы $w_1 + \cdots + w_m = 1$, из которой следует нормирование самих весовых коэффициентов $0 \leq w_i \leq 1$, $i = 1, \dots, m$.

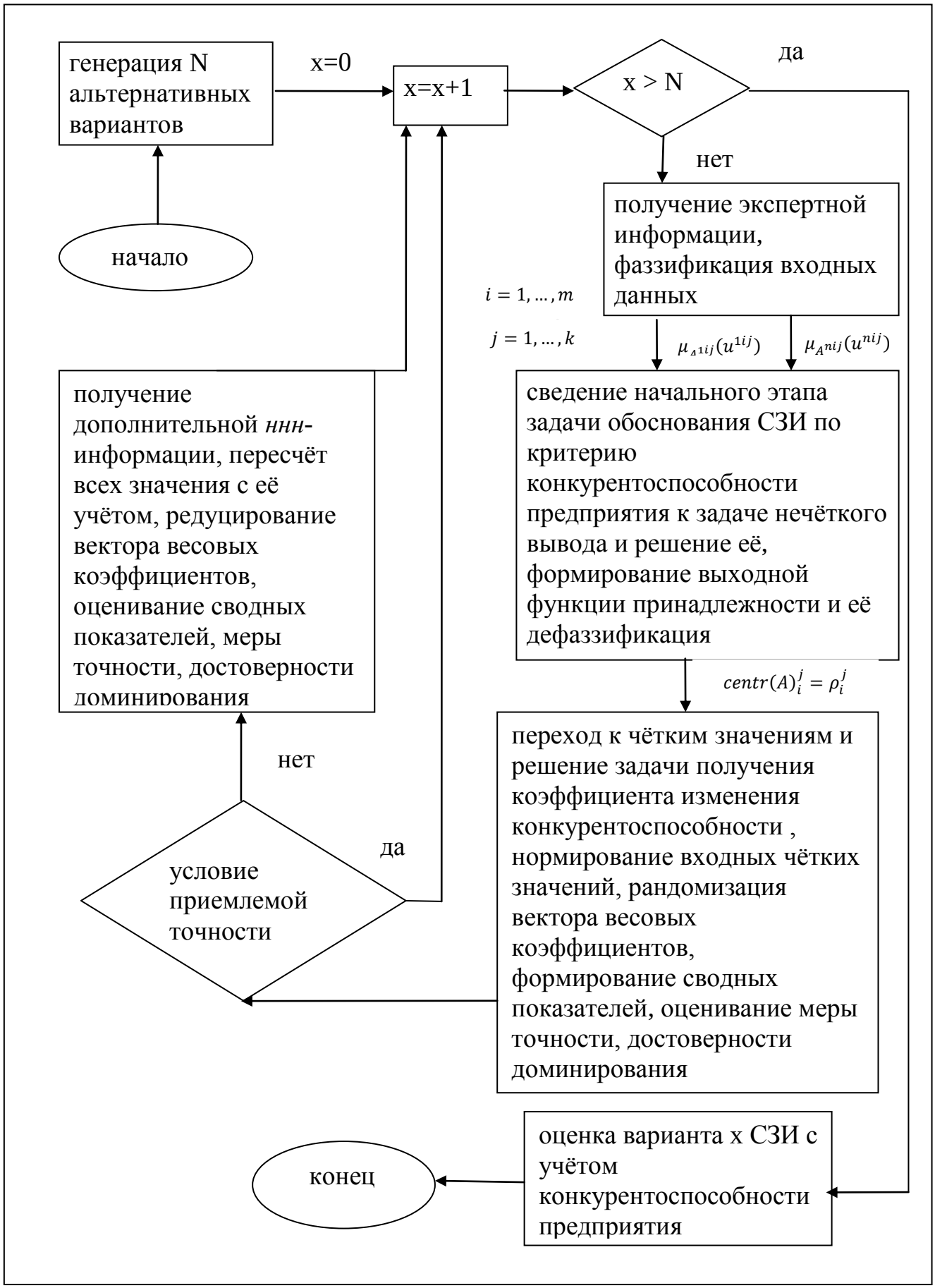


Рисунок 3.7– Блок-схема модифицированного метода рандомизированных сводных показателей

Строится синтезирующая функция $Q(q_1, \dots, q_m; \boldsymbol{w}) \in [0,1]$. В качестве синтезирующей функции берут аддитивную средневзвешенную величину (3.20)

$$Q^{(j)} = \sum_{i=1}^{m} q_i^j \, w_{i.} \quad (3.20)$$

Для задания дискретности модели вводится величина шага $h = \frac{1}{n}$, $n \in N$. (3.21)

$$w_i \epsilon \{0, \frac{1}{n}, \dots, \frac{n-1}{n}, 1\}. \quad (3.21)$$

h задаёт «размер множества допустимых векторов весовых коэффициентов (3.22)

$$N(m,n) = \frac{(n+m-1)!}{n!(m-1)!}. \quad (3.22)$$

Рандомизируя неопределённость выбора конкретного вектора весовых коэффициентов при помощи случайного индекса $\tilde{t} \in \{1, \dots, N(m,n)\}$, получаем (3.23)

$$\widetilde{\boldsymbol{w}} = (\widetilde{w}_1, \dots, \widetilde{w}_m) = \left(w_1^{(\tilde{t})}, \dots, w_m^{(\tilde{t})}\right), \quad (3.23)$$

где $\widetilde{\boldsymbol{w}}$ - вектор, элементы которого имеют равномерное распределение.

Вычисляется математическое ожидание и дисперсия рандомизированного вектора весовых коэффициентов (3.24):

$$\overline{w_i} = \frac{1}{N(m,n)} \sum_{i=1}^{N} w_i^j = \frac{1}{m}, \quad s_i = \sqrt{\frac{1}{N} \sum_{i=1}^{N} \left[w_i^j - \overline{w_i}\right]^2} \quad (3.24)$$

На этом шаге оценивают весовые коэффициенты и стандартные отклонения в условиях дефицита информации о сравнительной значимости отдельных критериев. Случайный вектор $\widetilde{\boldsymbol{w}}$ приводит к аддитивному рандомизированному сводному показателю» [92] (3.25):

$$\tilde{Q}^{(j)}(q, \widetilde{\boldsymbol{w}}) = \sum_{i=1}^{m} q_i^j \, \widetilde{w}_i \, . \quad (3.25)$$

Происходит свёртывание нескольких показателей, которые по отдельности характеризуют объект с определённой стороны, в сводный интегральный

показатель. В качестве простейшей детерминированной оценки рандомизированного сводного показателя используется математическое ожидание (3.26)

$$\bar{Q}^{(j)} = M\tilde{Q}^{(j)} \quad (3.26)$$

случайной величины, а мерой точности оценки $\bar{Q}^{(j)}$ служит стандартное отклонение (3.27) (корень из дисперсии)

$$S^{(j)} = \sqrt{D\tilde{Q}^{(j)}} \quad (3.27)$$

случайной величины. Достоверность доминирования рандомизированного сводного показателя $\tilde{Q}^{(m)}$ над $\tilde{Q}^{(l)}$ определяется по формуле (3.28)

$$P\left(\left\{\tilde{Q}^{(m)} > \tilde{Q}^{(l)}\right\}\right) > \alpha\,, \quad (3.28)$$

где $\alpha \in [0,1]$, $m, l = 1, \dots, k$.

Для объектов, описываемых векторами $\boldsymbol{\rho}^{(j)} = \left(\rho_1^{(j)}, \dots, \rho_m^{(j)}\right)$, $j = 1, \dots, k$, можно получить сводные оценки, меры точности этих оценок и меры достоверности попарного доминирования. Таким образом, получают итоговые значения, ранжирование объектов, оценку точности полученных величин, определение достоверности полученного ранжирования и выполнение условия приемлемой точности.

Например, в исследуемой системе можно выделить три отдельных показателя: конфиденциальность, целостность, доступность (m=3), относительная значимость которых измеряется весовыми коэффициентами w_1, w_2, w_3. Вследствие дискретности модели, весовые коэффициенты отсчитываются с шагом $h = \frac{1}{4}$ $n = 4$. Множество всех возможных векторов весовых коэффициентов $\boldsymbol{w}^{(t)} = (w_1^{(t)}, w_2^{(t)}, w_3^{(t)})$ равно $N(m, n) = 15$ элементам.

Пусть оцениваются три (k = 3) СЗИ, созданных для конкретного предприятия по выбранным показателям конфиденциальности, целостности и доступности. Им сопоставляются три вектора исходных характеристик $\rho^{(j)} =$

$\left(\rho_1^{(j)}, \rho_2^{(j)}, \rho_3^{(j)}\right)$, $j = 1,2,3$, которым соответствуют после процедуры линейного нормирования значения $q_i(\rho_i(x_i))$.

После подсчёта всех возможных значений $\tilde{Q}(q^{(j)}; w^{(t)})$, $t = 1, \dots, 15$, $j = 1,2,3$, сводного показателя трёх оцениваемых объектов, получают математические ожидания $\bar{Q}^{(j)}$, стандартные отклонения $S^{(j)}$ и вероятность доминирования $P(j, l)$. Затем выбирают максимальную оценку сводного показателя. Это даст возможность выбрать оптимальный вариант СЗИ. Затем проверяются условия приемлемой точности.

Если $\bar{Q}^{(j)} > \bar{Q}^{(j')}$ и $\bar{Q}^{(j)} - S^{(j)} > \bar{Q}^{(j')} + S^{(j')}$, то система j предпочтительнее системы j'.

Если $\exists\, j$: $\bar{Q}^{(j)} > \bar{Q}^{(j')}$ и $\bar{Q}^{(j)} - S^{(j)} \leq \bar{Q}^{(j')} + S^{(j')}$, то система j предпочтительнее системы j' с вероятностью доминирования $P(\{\tilde{Q}^{(j)} > \tilde{Q}^{(j')}\})$. При вероятности доминирования, близкой к 0,5 необходима дополнительная информация.

Все эти показатели получают при полном дефиците информации, касающейся весовых коэффициентов. Если вычислительные результаты не удовлетворяют условиям приемлемой точности, то прибегают к дополнительной нечисловой информацией, представленной экспертами в виде системы равенств или неравенств (3.29)

$$OI = \{w_1 < w_2; w_4 = w_5\}. \quad (3.29)$$

Такая информация называется ординальной.

Эксперты предоставляют неточную информацию, выраженную в виде системы (3.30)

$$II = \{a_i \leq w_i \leq b_i, i \in \{1, \dots, m\}\}. \quad (3.30)$$

Такая информация называется интервальной. Возможно и объединение этих множеств $OI \cup II = I$. «Тогда говорят о нечисловой, неполной и неточной информации, то есть *ннн*-информации. Учёт *ннн*-информации значительно

сокращает количество значений рандомизированного вектора весовых коэффициентов $\widetilde{w}(I)$» [92].

Вычисленное затем математическое ожидание $\bar{Q}^{(j)}(I)$, стандартные отклонения $S^{(j)}(I)$ и вероятность доминирования $P(j,l)(I)$ показывают, что «учёт *ннн*-информации повышает точность оценок весовых коэффициентов, сводных показателей, уменьшает стандартные отклонения и увеличивает достоверность ранжирования весовых коэффициентов, сводных показателей, так как вероятности доминирования увеличиваются» [92].

Таким образом, ММРСП учитывает *ннн*-информацию [8] для ранжирования сложных многопараметрических объектов, и повышения точности и достоверности доминирования рандомизированных оценок сводных показателей объектов в чёткой части гибридной модели. Происходит редукция задачи оценивания, сравнения и выбора сложных параметрических объектов к задаче оценивания, сравнения и выбора экстремальных оценок рандомизированных сводных показателей.

В случае большого набора параметров [53] и большого количества оцениваемых объектов, возможно применение созданной программы [10] «системы поддержки принятия решений (СППР) АСПИД-3W (анализ и синтез показателей при информационном дефиците)» [147] в чёткой модели ММРСП, которая избавляет от ручного подсчёта и увеличивает скорость получения результата. [151].

Благодаря ММРСП, мы получаем оптимальный вариант СЗИ и теоретическое значение коэффициента изменения конкурентоспособности. ММРСП используется в модели повышения ИБ.

Схема обоснования СЗИ по критерию конкурентоспособности предприятия представлена на рисунке 3.8.

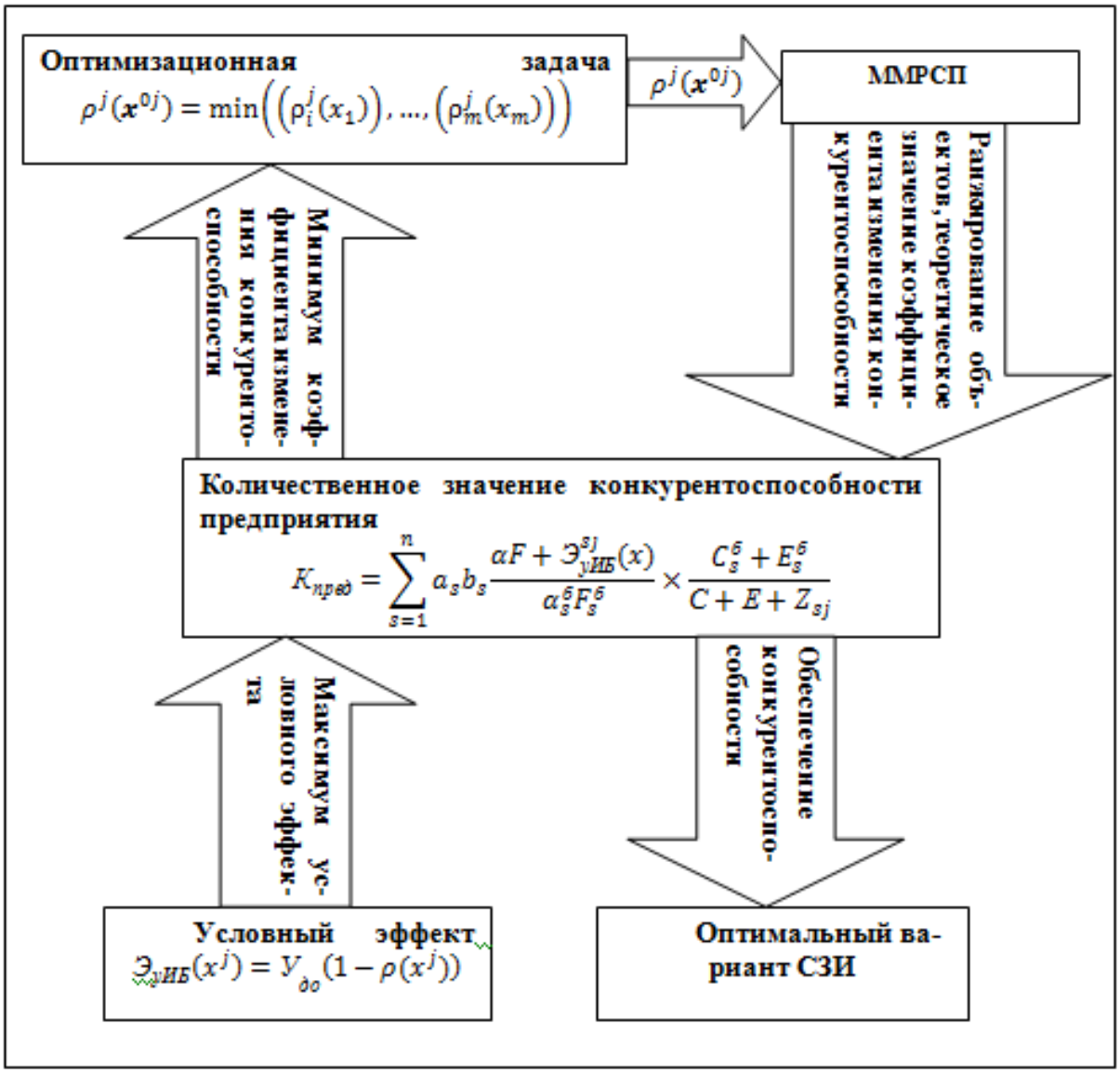


Рисунок 3.8 – Схема обоснования СЗИ по критерию конкурентоспособности

Для обеспечения состояния защищённости предприятия от угроз нарушения ИБ, выбирается наилучший вариант СЗИ по критерию конкурентоспособности. Максимальный условный эффект достигается путём решения оптимизационной задачи по нахождению минимума коэффициента изменения конкурентоспособности.

С помощью ММРСП решается многокритериальная задача, получается теоретическое значение коэффициента изменения конкурентоспособности, СЗИ ранжируется, и выбирается оптимизационный вариант с учётом обеспечения конкурентоспособности предприятия.

Сформулируем начальный этап последовательности действий метода обоснования СЗИ по критерию конкурентоспособности предприятия - алгоритм обработки нечётких входных данных.

3.7 Алгоритм оценки эффективности СЗИ

Способ оценки эффективности СЗИ. В соответствии с приказом ФСТЭК России от 18 февраля 2013 г. N 21, «оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных может проводиться организацией самостоятельно или с привлечением юридических лиц, имеющих соответствующую лицензию». «При этом форма оценки эффективности, а также форма и содержание документов, разрабатываемых по результатам (в процессе) оценки, не установлены» [82,81].

Эффективность СЗИ связана с эффективностью процессов, происходящих на предприятии. Взаимодействуя с КИС и со структурой рабочих процессов компании, СЗИ выдаёт синергетический эффект, взаимодействуя с эффективными бизнес-процессами, проявляющимися через показатели конкурентоспособности.

«Под эффективностью СЗИ понимается степень соответствия результатов защиты информации поставленной цели» [16]. Целью является повышение состояния защищённости предприятия от угроз нарушения ИБ с опорой на количественное значение конкурентоспособности, в которое входят показатели целостности, доступности, конфиденциальности информации. Следовательно, выбранный оптимизационный вариант СЗИ является эффективным.

Подсчёт экономической эффективности важен для предварительных расчётов и для обоснования выделяемых затрат для руководства предприятия. В этом случае эффективность СЗИ (3.31) «зависит от результатов и затрат, сбалансированных в приемлемой пропорции

$$Эф_{сзи} = \frac{результаты - затраты}{затраты}, \quad (3.31)$$

где $Эф_{сзи}$ - это экономическая эффективность СЗИ. При этом затраты не должны превышать Z^d (допустимые затраты).

Основным результатом при внедрении СЗИ является уменьшение ущерба в денежном выражении в случае реализации угроз ИБ. За результаты реализации конкретной СЗИ, используя критерий обеспечения конкурентоспособности предприятия, принимаем максимальное значение $Э_{уИБ}$ условного эффекта при усилении информационной безопасности» [106]. Максимальное значение $Э_{уИБ}$ достигается благодаря решению оптимизационной задачи, при нахождении минимального значения коэффициента изменения конкурентоспособности [106] по критериям конфиденциальности, целостности, доступности информации (рисунок 3.9).

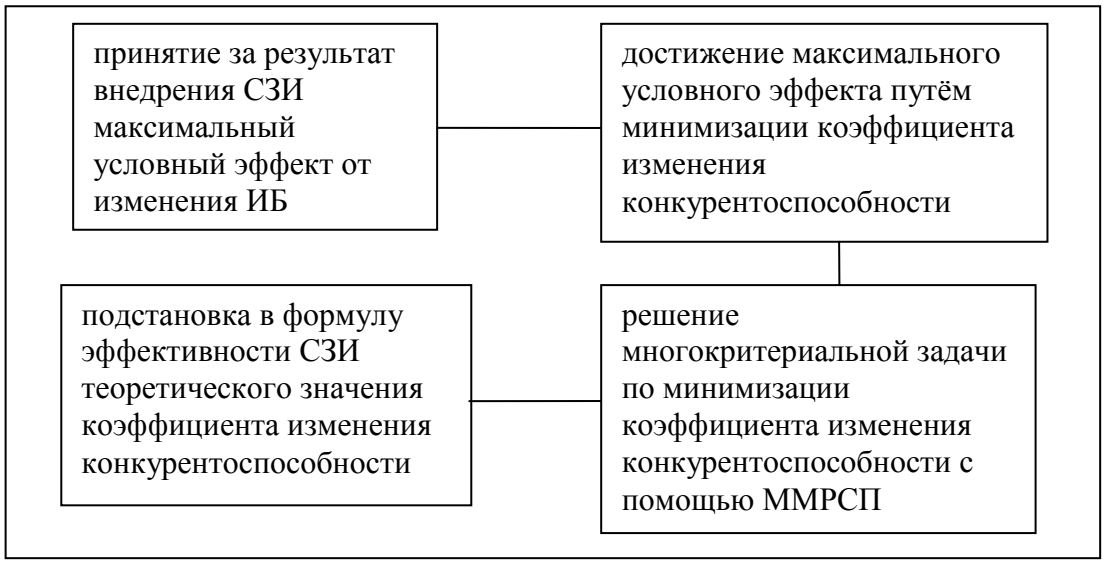


Рисунок 3.9– Схема алгоритма оценки экономической эффективности СЗИ

Алгоритм экономической эффективности отражают следующие формулы (3.32)

$$\rho(\boldsymbol{x}^0) = \min\left(\left(\rho_1(x_1)\right), \dots, \left(\rho_m(x_m)\right)\right), \qquad \rho \in [0,1]\ \boldsymbol{x}^0 = Arg\ min(\rho_i(x_i)),$$

$$i = 1, \dots, m \quad \boldsymbol{x}^0 \in X^d$$

$$Э_{сзи} = \frac{Y_{до}(1-\rho(x))-Z}{Z} = \frac{Y_{до}(1-\rho(x))}{Z} - 1 \quad (3.32)$$

при ограничении $Z(\boldsymbol{x}) \leq Z^d$, где Z – затраты на создание и поддержание работоспособности СЗИ.

Если величина эффективности больше нуля, то работа системы защиты информации считается эффективной.

Так как коэффициент изменения конкурентоспособности $\rho(x_i)$ является функцией характеристик СЗИ, которые зависят от затрат на создание СЗИ, то коэффициент изменения конкурентоспособности является зависимой переменной от затрат. Рассмотрим эластичность коэффициента изменения конкурентоспособности [106], то есть степень влияния аргумента коэффициента изменения конкурентоспособности на саму функцию.

Для этого подсчитаем коэффициент эластичности (coefficient of elasticity). Это безразмерная величина, которая показывает на сколько процентов изменится коэффициент изменения конкурентоспособности при изменении независимой переменной, то есть затрат на 1 % (3.33)

$$K_{\text{эл}} = \left|\frac{\Delta\rho \cdot Z}{\Delta Z \cdot \rho}\right|, \qquad (3.33)$$

где Z затраты на создание и поддержание работоспособности СЗИ.

При неэластичном коэффициенте $K_{\text{эл}} < 1$, скорость изменения затрат будет больше скорости изменения коэффициента изменения конкурентоспособности. То есть реакция на затраты слабая. При эластичном коэффициенте $K_{\text{эл}} > 1$, реагирование на изменения аргумента слишком большое, что не всегда приводит к желаемым результатам. Оптимальное воздействие аргумента при $K_{\text{эл}} = 1$.

При единичной эластичности коэффициент изменяется в той же пропорции, что и затраты. Так как для обеспечения эффективности СЗИ $\text{Э}_{\text{уИБ}} - Z \geq 0$, то в случае прямой пропорциональной зависимости $\rho = 1 - \frac{\text{Z}}{\text{У}_{\text{до}}}$, график которой представлен на рисунке 3.10.

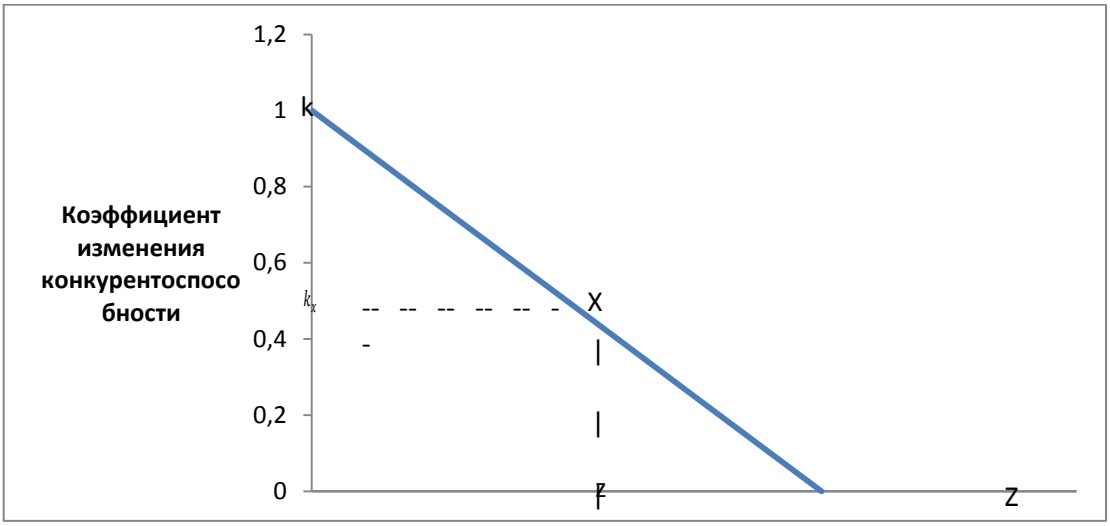


Рисунок 3.10 – График зависимости коэффициента изменения конкурентоспособности от затрат

Эластичность коэффициента изменения конкурентоспособности в точке X равна отношению $\frac{|k \cdot k_x|}{|k_x \cdot 0|}$, «где k_x - ордината точки X, k - точка пересечения графика с осью ординат, совпадающая с единицей. То есть эластичность $K_{эл} = \frac{|k \cdot k_x|}{|k_x \cdot 0|} = 1$ при $k_x = 0{,}5$. Таким образом, значение коэффициента изменения конкурентоспособности при единичной эластичности равно $\rho = 0{,}5$.

В случае криволинейной зависимости, находят отношение отрезков, образованных пересечением касательной к графику и осями координат и координат данной точки» [106]. Значение коэффициента изменения конкурентоспособности, полученное при единичной эластичности в случае пропорциональной зависимости от затрат, можно сравнить с расчётными результатами, после внедрения оптимальной СЗИ, выбранной по критерию обеспечения конкурентоспособности предприятия.

Формируя коэффициент изменения конкурентоспособности с помощью ММРСП, мы прибегаем к методу экспертных оценок.

Выводы по главе 3

В данной главе был описан алгоритм обработки нечётких входных данных, получен метод обоснования СЗИ по критерию конкурентоспособности предприятия.

Таким образом, цель, поставленная в начале главы 3, выполнена.

4 Внедрение метода обоснования системы защиты информации по критерию конкурентоспособности предприятия

4.1 Исследование систем защиты информации малых предприятий

Цель данной главы – внедрить разработанные методы и алгоритмы в хозяйственную деятельность малых предприятий Санкт-Петербурга и в учебном процессе «Смольного института Российской Академии Образования»; собрать и обработать данные по внедрению; верифицировать полученные теоретические значения.

В результате внедрения в хозяйственную деятельность двух малых предприятий Санкт-Петербурга (ЗАО «КОНТО», ООО «Лесной Двор») наилучших вариантов СЗИ, выбранных с учётом конкурентоспособности предприятия, были получены теоретические значения, которые затем верифицированы.

В Приложении 5 приводятся соответствующие акты о внедрении. Применялся разработанный алгоритм генерации допустимых вариантов системы защиты информации и метод обоснования СЗИ по критерию конкурентоспособности предприятия.

До этого никаких коллективных мер и средств (включая СЗИ) по обеспечению информационной безопасности на данных предприятиях не было.

СЗИ не может успешно эксплуатироваться без принятия ряда административно-управленческих мер. В структуре управления этими предприятиями появилось новое подразделение - служба информационной безопасности, включающая от 1 до 3 сотрудников. Их функции состоят в том, чтобы эксплуатировать коллективную СЗИ и интегрировать соответствующие меры по обеспечению информационной безопасности на предприятии в систему управления предприятием.

В 2014 г. происходило изучение предприятия, выбор оптимального варианта СЗИ, реализация СЗИ. В 2015 г. изучалась работа предприятия после

внедрения. В 2016 г. обобщались и систематизировались полученные результаты. Далее приведем конкретные данные (таблица 4.1) по этим предприятиям.

Таблица 4.1 – Краткие характеристики предприятий, участвовавших в эксперименте

	«КОНТО»	«Лесной Двор»
Сфера деятельности	Операции с ценными бумагами, операции на фондовом рынке	Обработка древесины, производство изделий из дерева, пропитка древесины
Количество сотрудников	8	48
Количество сотрудников, применяющих ИТ в своей проф. деятельности	5	17
Количество сотрудников службы ИБ	1	2
Количество компьютеров (АРМ + сервера)	6	19
ЛВС	да	да
Электронная почта	да	да
Интернет	да	да
Дополнительные особенности		Наличие распределенных филиалов

Учитывая краткие характеристики каждого предприятия и особенности, указанные в таблице, было произведено обследование предприятий. На предприятии «Лесной Двор» используется бесплатная почта, на предприятии «КОНТО» используется корпоративная электронная почта. Автоматизированные рабочие места (АРМы) и сервера объединены в локальную вычислительную сеть (ЛВС), есть выход в Интернет, поэтому были предложены следующие оптимальные варианты средств ЗИ.

Доступ компьютеров локальной сети в Интернет предложено проводить через прокси–сервер. Кроме кэширования, в прокси-сервере можно настроить квотирование трафика, ограничения для групп пользователей и создание

«чёрного» списка для url-адресов. Предложено развернуть Active Directory, как единую точку аутентификации для предприятия «Лесной двор».

Предприятию и «КОНТО» был установлен бесплатный прокси–сервер ES Proxy, а предприятию «Лесной двор» - Squid на сервер, предоставляющие доступ в Интернет для ЛВС. На прокси–сервер и все АРМы предприятий установили антивирусы и файерволы.

На предприятии «КОНТО» был установлен бесплатный антивирус для малых предприятий Microsoft Security Essentials и бесплатный файервол Comodo Firewall. На предприятии «Лесной Двор» был установлен бесплатный Comodo Antivirus and Firewall.

На всех предприятиях были установлены средства защиты информации от несанкционированного доступа (НСД) «Аура 1.2.4».

Предприятие «Лесной Двор» имеет четыре удаленных филиала, использует Интранет-технологии и архитектуру клиент-сервер. Поэтому для обеспечения информационной безопасности предприятия на каждый компьютер, который отвечает за связь с центральным офисом, был установлен бесплатный антивирус Ad-Aware Free Internet Security и бесплатные файерволы Comodo Firewall.

Во всех предприятиях были настроены учётные записи, разграничены привилегии, проведён инструктаж по работе с паролями, запрещено открывать вложенные письма в электронной почте. На предприятии «Лесной Двор» рекомендовано приобрести доменное имя на сервере хостинг провайдера для организации сайта и корпоративной почты. На всех предприятиях установлены бесплатные е-мейл-клиенты Thunderbird.

Во всех предприятиях были организованы службы ИБ, состоящие из 1- 2 сотрудников. Так как малые предприятия не могут себе позволить большие затраты, то на должности сотрудников службы ИБ были назначены люди, уже работающие с информационными технологиями (ИТ) компании, с наделением их дополнительными обязанностями и прибавкой к зарплате.

Данные действия позволили обеспечить положительные тенденции в обеспечении информационной безопасности всех предприятий, что подтверждают следующие исследования.

4.2 Оценивание ущербов от нарушения информационной безопасности до и после внедрения системы защиты информации

В каждом предприятии до и после внедрения СЗИ и службы ИБ были проведены анкетирования, сводные данные по которым приведены ниже [60]. Анкеты приведены в Приложении 2.

Используемые сокращения:

УЭП – доля в процентах участников эксперимента на данном предприятии от всех его сотрудников, применяющих ИТ, в своей профессиональной деятельности

УТП – процент уменьшения тяжелых последствий (по количеству нарушений ИБ) в 2015 г. по сравнению с 2014 г.

УЗП – процент уменьшения заметных последствий (по количеству нарушений ИБ) в 2015 г. по сравнению с 2014 г.

УНП – процент уменьшения незначительных последствий (по количеству нарушений ИБ) в 2015 г. по сравнению с 2014 г.

ПОС – доля в процентах сотрудников - участников эксперимента, положительно оценивающих влияние СЗИ и службы ИБ на свою работу;

ПОЦ – доля в процентах сотрудников - участников эксперимента положительно оценивающих влияние СЗИ и службы ИБ на работу компании в целом.

Результаты анкетирования ЗАО «КОНТО» приведены в таблице 4.2.

Таблица 4.2 – Результаты анкетирования ЗАО «КОНТО»

УЭП	УТП	УЗП	УНП	ПОС	ПОЦ
100,0	47,4	33,9	30,7	100,0	100,0

Достигнуты положительные результаты при внедрении СЗИ. Так произошло качественное изменение нарушений работы ИС, связанных с ИБ. Что более наглядно демонстрирует следующий график (рисунок 4.1).

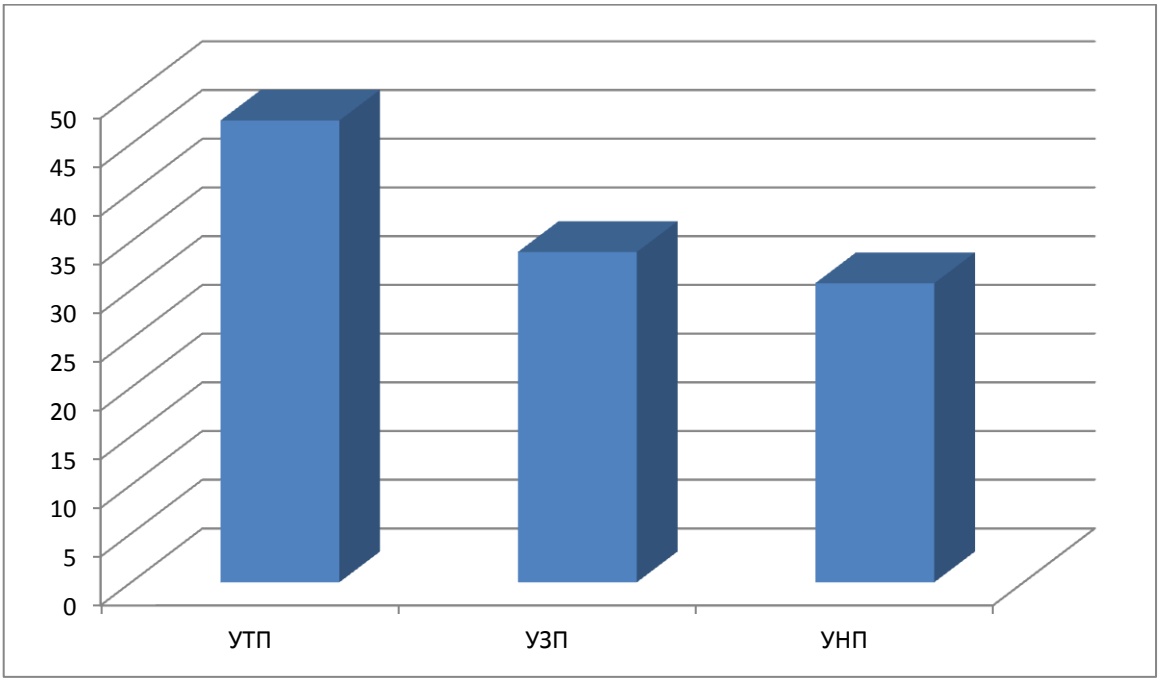


Рисунок 4.1 – Уменьшение уровня нарушений ИБ ЗАО «КОНТО»

На графике указаны проценты уменьшения последствий от количества нарушений ИБ. График демонстрирует, во-первых, что внедрение СЗИ и службы ИБ не может полностью исключить нарушения ИБ, в том числе и тяжелые. Это объясняется тем, что постоянно совершенствуются не только средства защиты, но и средства нападения. Причем нападающая сторона всегда имеет ряд преимуществ перед защищающейся.

Во-вторых, внедрение СЗИ и службы ИБ в большей степени уменьшает те нарушения ИБ, которые носят тяжелый характер, в средней степени - те

нарушения ИБ, которые носят заметный характер, в меньшей - те, которые носят незначительный характер.

Стоит отметить, что все участники опроса считают внедрение СЗИ и службы ИБ в компании полезным.

Таблица 4.3 демонстрирует положительные тенденции внедрения СЗИ на ООО «Лесной Двор».

Таблица 4.3 – Результаты анкетирования ООО «Лесной Двор»

УЭП	УТП	УЗП	УНП	ПОС	ПОЦ
94,1	46,8	23,7	18,8	100,0	100,0

Более наглядно эти результаты демонстрирует следующий график (рисунок 4.2).

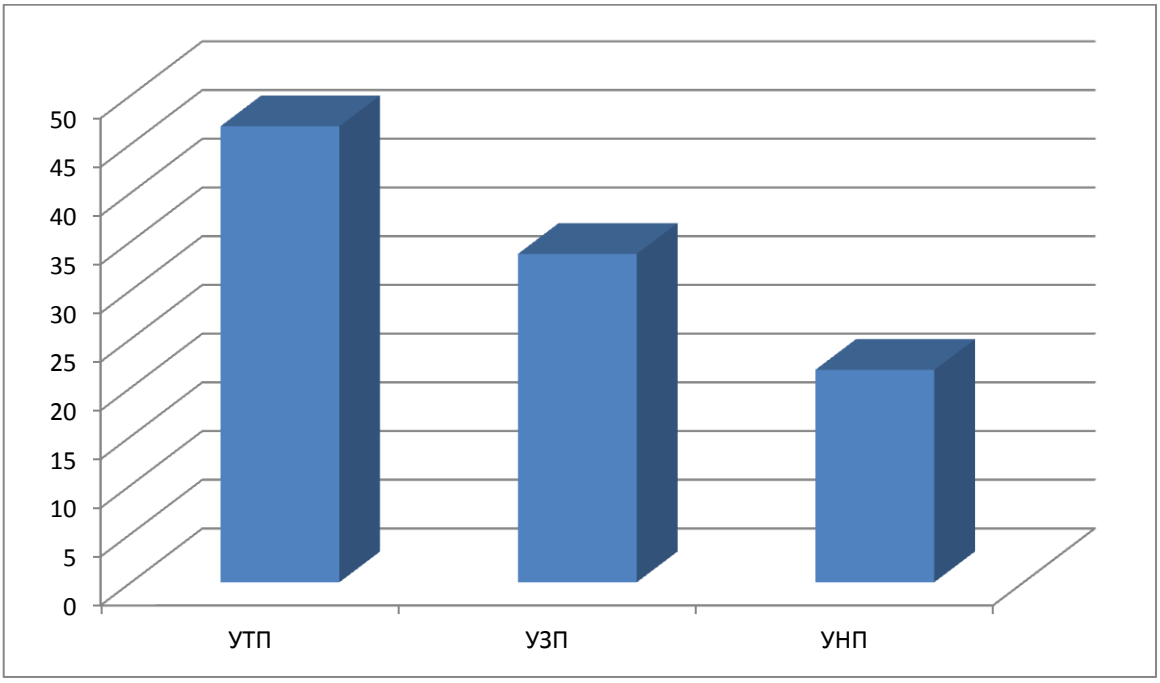


Рисунок 4.2 – Уменьшение уровня нарушений ИБ ООО «Лесной Двор»

На графике указаны проценты уменьшения последствий от количества нарушений ИБ. Здесь также можно говорить о том, что все сотрудники, принимавшие участие в опросе, считают внедрение СЗИ в компании полезным.

Таким образом, рассмотрев вышеприведенные результаты, можно говорить о том, что сотрудники на всех предприятиях, принимавшие участие в опросе, считают внедрение СЗИ в компании полезным для своей работы и работы компании в целом.

Посмотрим на изменение ущербов от нарушения ИБ до и после внедрения СЗИ. После проведения консультаций с сотрудниками предприятий, отвечающих за информационные технологии, были получены ущербы, причинённые предприятиям в результате нарушений информационной безопасности в 2014 г. и в 2015 г.

Предприятию ЗАО «КОНТО» в 2014 г. был причинён ущерб от нарушения ИБ 967 тыс. руб. в год, в 2015 г. был причинён ущерб 452 тыс. руб. (рисунок 4.3).

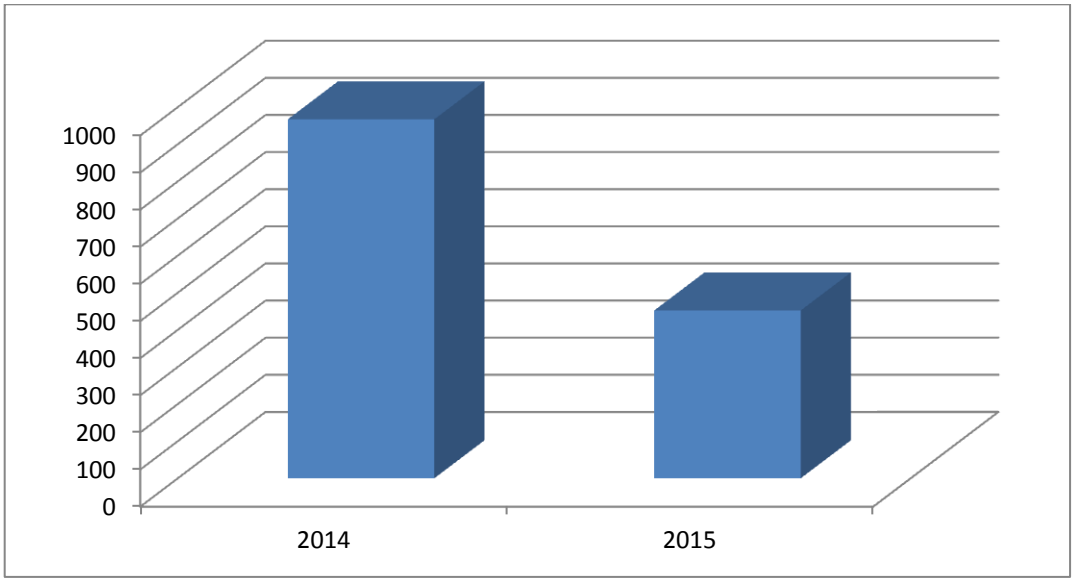


Рисунок 4.3– Динамика изменения ущерба по годам на предприятии ООО «СпецИнструментПоставка»

Предприятию ООО «Лесной Двор» в 2014 г. был причинён ущерб от нарушения ИБ 804 тыс. руб. в год, в 2015 г. был причинён ущерб 368 тыс. руб. (рисунок 4.4).

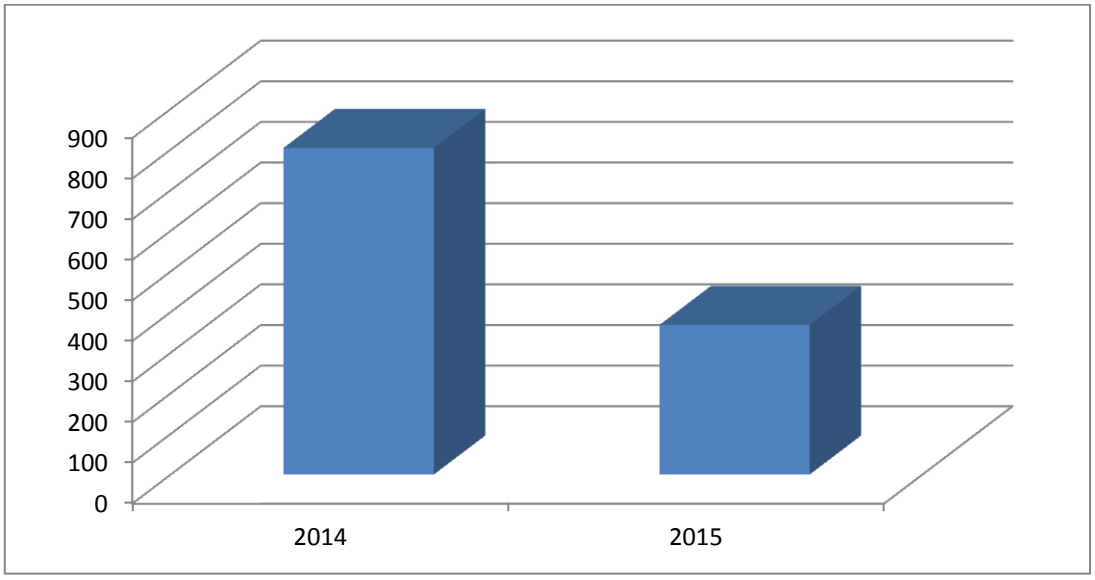


Рисунок 4.4– Динамика изменения ущерба по годам на предприятии ООО «Лесной Двор»

Анализируя графики, можно сделать вывод, что благодаря внедрению СЗИ существенно снизились ущербы от нарушений ИБ в 2015 г. по сравнению с 2014 г на всех трёх предприятиях.

4.3 Примеры реализации предложенных решений на предприятиях

На предприятии ЗАО «КОНТО» провели расчёты по внедрению теоретических разработок диссертационного исследования в хозяйственную деятельность предприятия. Это малое предприятие, проводящее операции с ценными бумагами, операции на фондовом рынке.

Информационные активы предприятия составляли сведения о динамике рынка акций, опционов, фьючерсов; сформированные портфели ценных бумаг; разработанные программы по реагированию на изменения котировок на фондовом рынке.

В модель угроз вошли угрозы конфиденциальности, целостности, доступности информации, угрозы несанкционированного доступа (НСД), угрозы вредоносных программ, с использованием уязвимости системного и прикладного ПО.

При обработке риска были выбраны уменьшение риска, то есть снижение вероятности реализации угрозы и наступившего в результате ущерба. Снижение вероятности возможно на стадии проектирования, при выборе оптимального варианта СЗИ. Уменьшение ущерба обеспечивается минимизацией коэффициента изменения конкурентоспособности.

Для нейтрализации угроз нарушения конфиденциальности, целостности, доступности информации, в СЗИ предложено использование файерволов, антивирусов, прокси-сервера, средств от НСД. Были сгенерированы три варианта СЗИ, удовлетворяющие условиям ограничения на рисунке 4.5.

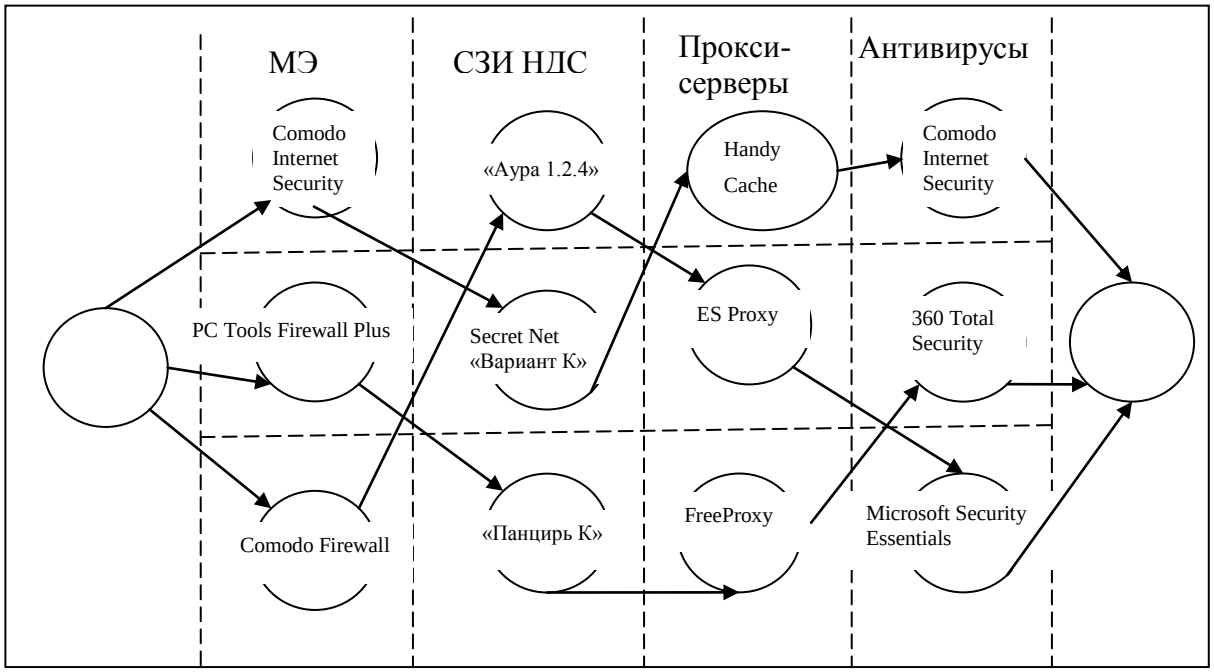


Рисунок 4.5 – Три альтернативных варианта сгенерированных средств ЗИ

В первый маршрут графа входили прокси–сервер Handy Cache, антивирус и файервол Comodo Internet Security, средство защиты информации от НСД Secret Net «Вариант К»; во второй – антивирус 360 Total Security, прокси-сервер FreeProxy, файервол PC Tools Firewall Plus, средство защиты информации от НСД «Панцирь К»; в третьем - прокси–сервер ES Proxy, антивирус Microsoft Security Essentials, файервол Comodo Firewall, средство защиты информации от

НСД «Аура 1.2.4». Установлены бесплатные е-мейл-клиенты Thunderbird для обеспечения ИБ при работе с почтой.

Было привлечено семь экспертов, из которых сформировали экспертную комиссию из трёх человек, коэффициент конкордации решений экспертов равен $W = 0{,}9$. Эксперты оценивают коэффициенты изменения конкурентоспособности для трёх вариантов СЗИ по выбранным показателям целостности, доступности и конфиденциальности. После опроса экспертов, представленного в Приложении 3, мы получаем пессимистичные нижнее и верхнее значения, и наиболее ожидаемые значения коэффициентов изменения конкурентоспособности (коэффициентов уменьшения ущерба), причём минимальные значения означают более предпочтительные оценки. Эксперты дают нам эти значения по сетке от 0 до 1 с шагом 0,1.

При оценивании коэффициента изменения конкурентоспособности для первой системы, даны каждым экспертом оценки $u_k^{(ij\,l)}$ в опорных точках $k = 1, \ldots, 4$ для объектов $j = 1,2,3$ по критериям при $i = 1$ целостности информации, $i = 2$ - конфиденциальности, $i = 3$ – доступности. Применяя принцип обобщения, получена выходная функция принадлежности трёх входных функций принадлежности для первого варианта СЗИ по трём критериям, на основе которой сформирована таблица 4.4. Пример расчёта для критерия доступности для первого варианта СЗИ приведён в Приложении Г.

Таблица 4.4 – Оценки для первой системы по трём критериям

первый вариант системы	наименее возможная нижняя оценка	наиболее ожидаемая минимальная оценка	наиболее ожидаемая максимальная оценка	наименее возможная верхняя оценка	дефаззифицированное значение
конфиденциальность	0,267	0,300	0,500	0,533	0,400
целостность	0,367	0,400	0,700	0,733	0550
доступность	0,367	0,400	0,667	0,700	0,534

Затем функции принадлежности трапецеидальных чисел подвергались дефаззификации. Дефаззификация проводилась интегральным представлением градуированного среднего значения.

Итоговые значения для трёх систем приведены в таблице 4.5.

Таблица 4.5 – Центроидные значения функций принадлежности трёх вариантов СЗИ по трём критериям

j	$\rho_1^{(j)}$	$\rho_2^{(j)}$	$\rho_3^{(j)}$
1	0,400	0,550	0,534
2	0,533	0,306	0,645
3	0,700	0,467	0,316

Относительная значимость трёх показателей коэффициента изменения конкурентоспособности (m=3)» [90] измерялась вектором весовых коэффициентов $\boldsymbol{w} = (w_1, w_2, w_3)$, равномерно распределённым на области допустимых значений с шагом дискретизации $h = \frac{1}{4}$, $n = 4$. Множество всех возможных векторов весовых коэффициентов $\boldsymbol{w^{(t)}} = (w_1^{(t)}, w_2^{(t)}, w_3^{(t)})$ состояло из $N(m,n) = \frac{(n+m-1)!}{n!(m-1)!} = 15$ [136] вариантов, представленных в таблице 4.6.

Так как возрастание коэффициента изменения конкурентоспособности соответствует ухудшению обеспечения ИБ предприятия, то нормирующую функцию $q_i^{(j)}$ задали как монотонно убывающую (4.1)

$$q_i^{(j)} = \begin{cases} 0, \ \rho_i \geq \max \rho_i, \\ \frac{\max \rho_i - \rho_i}{\max \rho_i - \min \ \rho_i} \quad , \ \min \ \rho_i < \rho_i < \max \rho_i. \\ 1, \ \rho_i \ \leq \min \ \rho_i. \end{cases} \qquad (4.1)$$

Получили отдельные показатели $q_i^{(j)}$, представленные в таблице 4.7.

Таблица 4.6 – Дискретные значения весовых коэффициентов

t	$w_1^{(t)}$	$w_2^{(t)}$	$w_3^{(t)}$
1	0,000	0,000	1,000
2	0,000	0,250	0,750
3	0,000	0,500	0,500
4	0,000	0,750	0,250
5	0,000	1,000	0,000
6	0,250	0,000	0,750
7	0,250	0,250	0,500
8	0,250	0,500	0,250
9	0,250	0,750	0,000
10	0,500	0,000	0,500
11	0,500	0,250	0,250
12	0,500	0,500	0,000
13	0,750	0,000	0,250
14	0,750	0,250	0,000
15	1,000	0,000	0,000

Таблица 4.7 – Нормированные показатели коэффициентов изменения конкурентоспособности

j	$q_1^{(j)}$	$q_2^{(j)}$	$q_3^{(j)}$
1	0,761	0,381	0,421
2	0,424	1,000	0,140
3	0,000	0,591	0,975

Подсчитали значения сводных показателей в таблице 4.8 для трёх оцениваемых объектов $j = 1,2,3$ с помощью аддитивной формулы.

Таблица 4.8 – Значения рандомизированных сводных показателей

t	$\tilde{Q}^{(t)}(q^{(1)})$	$\tilde{Q}^{(t)}(q^{(2)})$	$\tilde{Q}^{(t)}(q^{(3)})$
1	0,421	0,140	0,975
2	0,411	0,355	0,879
3	0,401	0,570	0,783
4	0,391	0,785	0,687
5	0,381	1,000	0,591
6	0,506	0,211	0,731
7	0,601	0,461	0,879
8	0,486	0,641	0,539
9	0,476	0,856	0,443
10	0,591	0,282	0,488
11	0,581	0,497	0,392
12	0,571	0,712	0,296
13	0,676	0,353	0,244
14	0,666	0,568	0,148
15	0,761	0,424	0,000

Рандомизированные сводные показатели являются случайными величинами, в качестве искомых стохастических оценок трёх оцениваемых объектов, подсчитали математические ожидания (4.2)

$$\bar{Q}^{(j)} = \frac{1}{N(m,n)} \sum_{t=1}^{N(m,n)} \tilde{Q}^{(t)}(q^{(j)}). \quad (4.2)$$

В качестве мер точности таких оценок взяли стандартные отклонения (4.3)

$$S^{(j)} = \sqrt{\frac{1}{N(m,n)} \sum_{t=1}^{N(m,n)} [\tilde{Q}^{(t)}(q^{(j)}) - \bar{Q}^{(j)}]^2}. \quad (4.3)$$

Получили следующие значения (таблица 4.9).

Таблица 4.9 – Математические ожидания и дисперсии сводных показателей коэффициентов изменения конкурентоспособности трёх вариантов СЗИ

j	$\bar{Q}^{(j)}$	$S^{(j)}$
1	0,528	0,114
2	0,524	0,234
3	0,538	0,242

Сосчитали вероятности попарного доминирования рандомизированных сводных показателей по формуле (4.4)

$$P(j,l) = P\left(\left\{\tilde{Q}^{(j)} > \tilde{Q}^{(l)}\right\}\right). \quad (4.4)$$

Получили следующие значения (таблица 4.10).

Таблица 4.10 – Достоверность выявленного доминирования

j\l	1	2	3
1	0,000	0,600	0,467
2	0,400	0,000	0,600
3	0,533	0,400	0,000

В стохастической дискретной модели неопределённости задания весовых коэффициентов мы получили сводные оценки объектов $\bar{Q}^{(j)}$, меры точности этих объектов $S^{(j)}$, вероятности попарного доминирования рандомизированных сводных показателей $P(j,l)$. Все вычисления сделаны при дефиците информации о весовых коэффициентах, что послужило причиной малой точности (большие *S* и *P*, близкие к 0,5).

Условие приемлемой точности не соблюдается, так как максимальное значение математического ожидания с вычетом стандартного отклонения не превосходит суммы среднего по значению математического ожидания и его стандартного отклонения.

В результате опроса экспертов у нас появилась дополнительная *ннн*-информация (4.5).

$$I = \{0{,}000 \le w_1 \le 0{,}250;\quad 0{,}000 \le w_2 \le 0{,}500;\ \ 0{,}250 \le w_3 \le 0{,}750\} \qquad (4.5)$$

Она редуцирует число всех возможных числовых коэффициентов до числа допустимых (таблица 4.11) весовых коэффициентов.

Таблица 4.11 – Редуцированные значения весовых коэффициентов с учётом *ннн*-информации

t	$w_1^{(t)}$	$w_2^{(t)}$	$w_3^{(t)}$
1	0,000	0,250	0,750
2	0,000	0,500	0,500
3	0,250	0,000	0,750
4	0,250	0,250	0,750
5	0,250	0,500	0,250

Сосчитали все допустимые значения сводных показателей (таблица 4.12) для трёх оцениваемых объектов.

Таблица 4.12 – Значения сводных показателей с учётом *ннн*-информации

t	$\tilde{Q}^{(t)}(q^{(1)})$	$\tilde{Q}^{(t)}(q^{(2)})$	$\tilde{Q}^{(t)}(q^{(3)})$
1	0,411	0,355	0,879
2	0,401	0,57	0,783
3	0,506	0,211	0,73125
4	0,60125	0,461	0,879
5	0,486	0,641	0,53925

В связи с этим математические ожидания $\bar{Q}^{(j)}(I)$ и стандартные отклонения $S^{(j)}(I)$ представлены в таблице 4.13.

Таблица 4.13 – Математические ожидания и дисперсии сводных оценок с учётом *ннн*-информации

j	$\bar{Q}^{(j)}(I)$	$S^{(j)}(I)$
1	0,481	0,073
2	0,445	0,153
3	0,762	0,125

Нашли вероятности попарного доминирования $P(j,l)(I)$ (таблица 4.14).

Таблица 4.14– Вероятности попарного доминирования с учётом *ннн*-информации

$j\backslash l$	1	2	3
1	0,000	0,600	0,000
2	0,400	0,000	0,200
3	1,000	0,800	0,000

Информация в таблицах 4.10 и 4.11 наглядно представлена на рисунке 4.6.

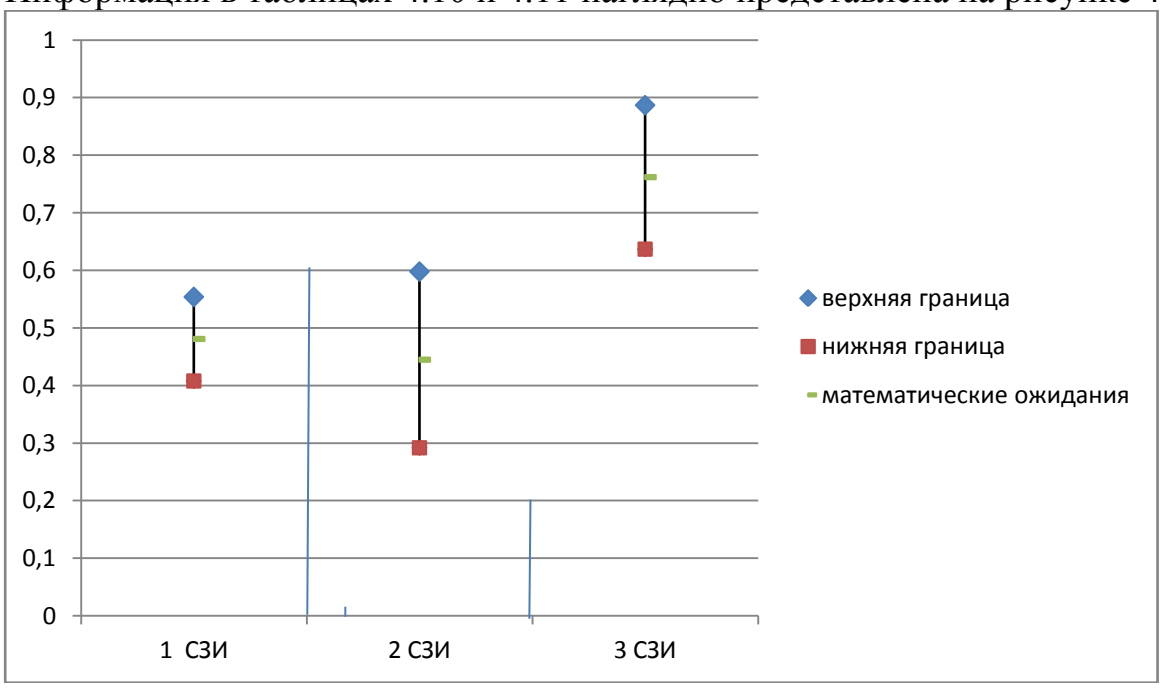


Рисунок 4.6 – Диаграмма для сводных показателей

Вертикальные линии, берущие начало на нулевом уровне, соответствуют вероятности доминирования, верхние и нижние границы соответствуют диапазону стандартного отклонения. Учёт *ннн*-информации повышает точность оценок сводных показателей, уменьшает стандартные отклонения и [1] достоверности доминирования приближает к единице. Мы выбираем СЗИ с наибольшим математическим ожиданием, небольшим стандартным отклонением и большой достоверностью. Получается третий вариант СЗИ.

Проводим операцию денормирования. Математическое ожидание $\bar{Q}^{(j)}(I) = 0{,}762$ выбранной СЗИ мы проецируем на нормировочную шкалу (Таблица 4.5) и

получаем значение коэффициента изменения конкурентоспособности для данной СЗИ (4.6)

$$\rho(\boldsymbol{x}) = 0{,}700 - (0{,}700 - 0{,}306) \times 0{,}762 = 0{,}400. \quad (4.6)$$

Коэффициент изменения конкурентоспособности в результате изменения информационной безопасности $\rho(\boldsymbol{x}) = 0{,}400$. Условный эффект (4.7) равен

$$Э_{уИБ} = У_{2014} \times (1 - \rho(\boldsymbol{x})). \quad (4.7)$$

Для данного предприятия $У_{2014} = 967$ тыс. руб. Тогда условный эффект и условный эффект для каждого из n товара или услуги равен (4.8)

$$Э_{уИБ} = У_{2014} \times (1 - \rho) = 967 \times (1 - 0{,}400) = 580{,}200 \text{ тыс. руб} = 580200 \text{ руб.}$$

$$Э^{i}_{\text{уИБ}} = \frac{580200}{n}, \quad (4.8)$$

где $i \in \{1, \dots, n\}$, n – количество производимых товаров или предоставляемых услуг на предприятии.

На данном предприятии один человек был назначен администратором информационной безопасности и получил прибавку к зарплате 96000 руб. в год, на приобретение средства защиты от НСД было потрачено 14000 руб. Поэтому затраты, приходящиеся на каждый из n товаров или услуг (4.9) равны

$$Z_i = \frac{Z}{n} = \frac{110000}{n}. \quad (4.9)$$

С учётом формул 4.8 и 4.9 конкурентоспособность предприятия (4.10) равна

$$К_{\text{пред}} = \sum_{i=1}^{n} a_i b_i \frac{\alpha_i F_i + \frac{580200}{n}}{\alpha^{б} F^{б}} \times \frac{С^{б} + Е^{б}}{C_i + E_i + \frac{110000}{n}} \quad (4.10)$$

Полностью значение конкурентоспособности данного предприятия не подсчитывалось, так как значения многих переменных, входящие в формулу составляют коммерческую тайну. Но очевидно обеспечение конкурентоспособности данного предприятия, так как в каждом слагаемом увеличение числителя превосходит увеличение знаменателя.

За результаты реализации конкретной СЗИ приняли максимальное значение условного эффекта при усилении ИБ. Тогда экономическая эффективность СЗИ [101] равна (4.11)

$$Эф_{сзи} = \frac{967000 \times (1-0{,}400)}{110000} - 1 = 4{,}275 > 0. \quad (4.11)$$

Таким образом, работу СЗИ можно считать эффективной.

Теоретические значения верифицировали реальными данными, полученными после внедрения выбранной систем защиты информации. В 2015 г. был получен реальный ущерб от нарушения ИБ после внедрения оптимального варианта СЗИ, который составил 452 тыс. руб. Подсчитали реальные значения по схеме процесса, представленного на рисунке 4.7.

Соотношения (4.12) показывают теоретические и реальные значения формул

$$\rho_{реал} = \frac{У_{2015}}{У2014} = \frac{452}{967} = 0{,}467,$$

$$Э_{уИБ,реал} = У_{2014} - У_{2015} = 515 \text{ тыс. руб.}$$

$$Эф_{сзи}^{реал} = \frac{515000}{110000} - 1 = 3{,}682 > 0. \quad (4.12)$$

$$\rho_{теор} = 0{,}400$$

$$Э_{уИБ,теор} = 580{,}200 \text{ тыс. руб}$$

$$Эф_{сзи}^{теор} = 4{,}275 > 0.$$

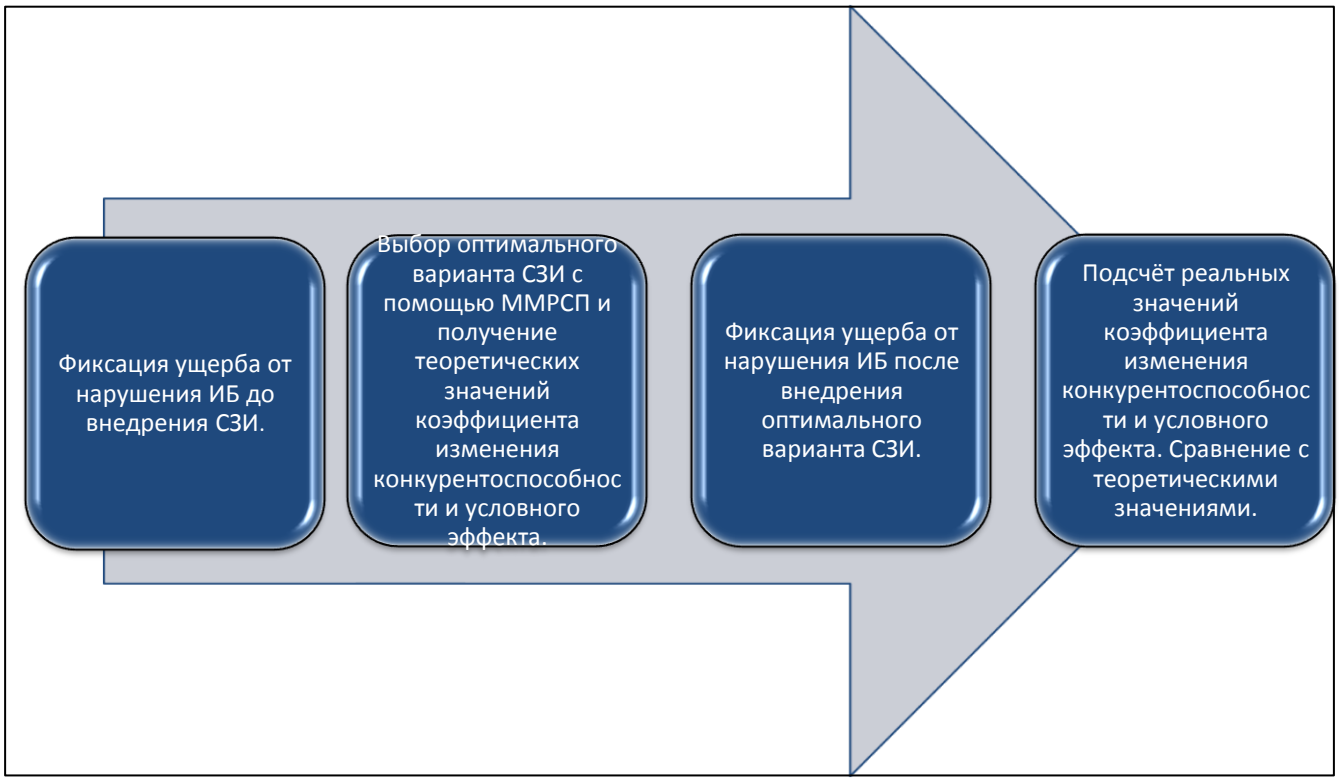


Рисунок 4.7 – Схема получения теоретических и реальных значений коэффициента изменения конкурентоспособности и условного эффекта

Разница между теоретическим условным эффектом (уменьшением ущерба) и реальным составляет 11%. Полученные соотношения отражены на рисунках 4.8–4.10.

Можно сделать вывод, что теоретические, результаты оказались близки к реальным. После внедрения оптимизационного варианта СЗИ, произошло снижение ущерба.

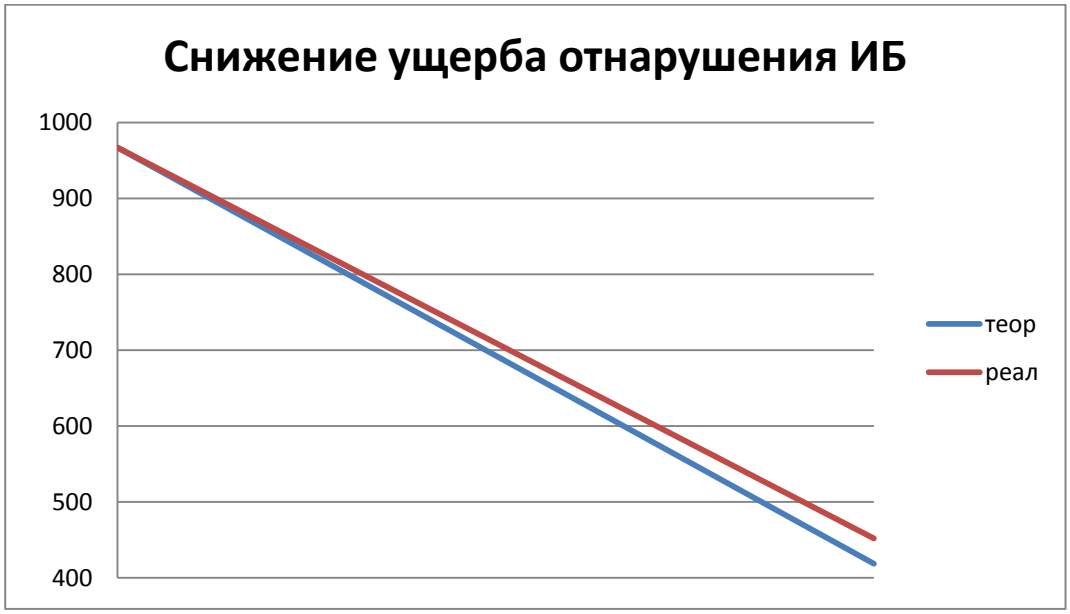


Рисунок 4.8 – Теоретическое и реальное снижение ущерба от нарушения ИБ после внедрения СЗИ

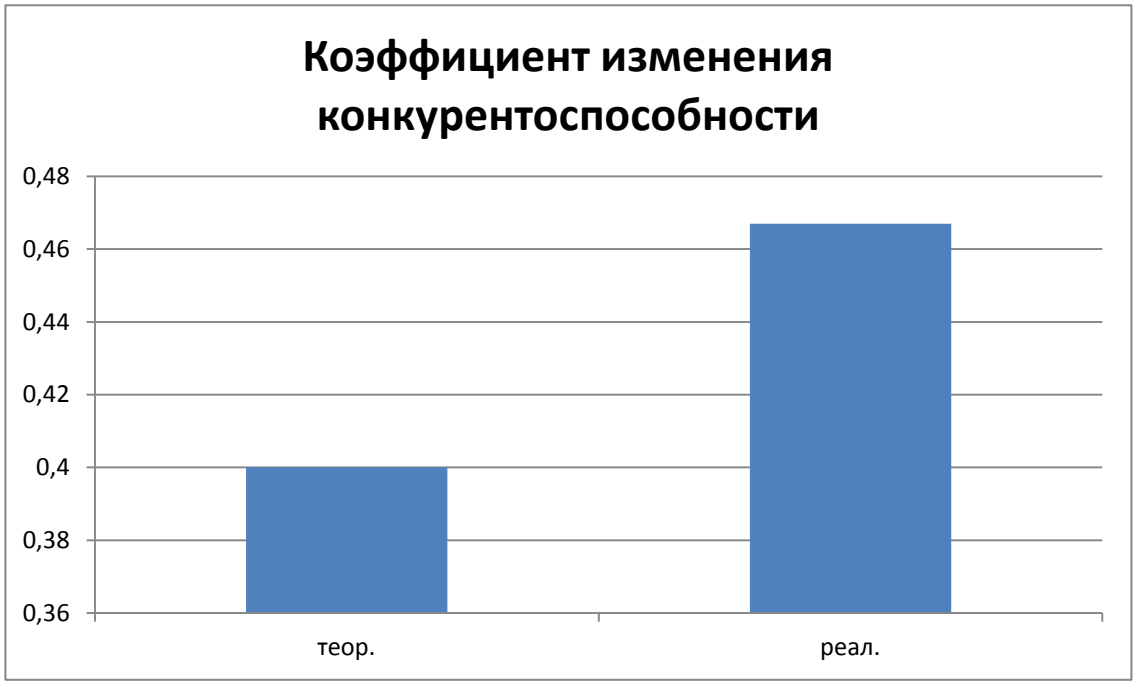


Рисунок 4.9 – Теоретическое и реальное значение коэффициента изменения конкурентоспособности

Рисунок 4.10 – Теоретический и реальный условный эффект от обеспечения ИБ

В компании ООО «Лесной Двор» максимальное математическое ожидание после использования *ннн*-информации получилось со следующим разбросом (таблица 4.15).

Таблица 4.15 – Стохастические оценки сводных показателей для оптимальной СЗИ и коэффициент изменения конкурентоспособности

$\bar{Q}^{(j)}(I)$	$S^{(j)}(I)$	$\rho(\boldsymbol{x})$
0,687	0,143	0,439

Два человека были назначены сотрудниками службы информационной безопасности и получили прибавку к зарплате 192000 руб. в год, на приобретение средства защиты от НСД было потрачено 40000 руб.

Соотношения (4.13) демонстрируют реальные и теоретические коэффициенты изменения конкурентоспособности, условные эффекты, затраты на организацию СЗИ, обеспечение конкурентоспособности предприятия:

$$\rho_{\text{теор}}(\boldsymbol{x}) = 0{,}439$$

$$\text{Э}_{\text{уИБ,теор}}(\boldsymbol{x}) = \text{У}_{2014} \times (1 - \rho(\boldsymbol{x})) = 451{,}044 \text{ тыс. руб}$$

(4.13)

$$Z = 232000 \text{ руб.}$$

$$\text{К}_{\text{пред}} = \sum_{i=1}^{n} a_i b_i \frac{\alpha_i F_i + \frac{451044}{n}}{\alpha^{б} F^{б}} \times \frac{\text{С}^{б} + \text{Е}^{б}}{C_i + E_i + \frac{232000}{n}}.$$

$$\text{Эф}_{\text{СЗИ}}^{\text{теор}} = \frac{\text{Э}_{\text{ИБу}} - Z}{Z} = \frac{451044}{232000} - 1 = 0,944 > 0.$$

Таким образом, работа СЗИ является эффективной. После внедрения оптимальной СЗИ были получены реальные значения ущерба, коэффициента изменения конкурентоспособности и условного эффекта (4.14)

$$\rho_{\text{реал}} = \frac{\text{У}_{2014}}{\text{У}_{2012}} = \frac{368}{804} = 0{,}458,$$

$$\text{Э}_{\text{уИБ,реал}} = У_{2014} - У_{2015} = 436 \text{ тыс. руб.} \qquad (4.14)$$

$$\text{Эф}_{\text{СЗИ}}^{\text{реал}} = 0{,}879 \text{ тыс. руб} > 0.$$

Разница между теоретическим условным эффектом (уменьшением ущерба) и реальным составляет 3%. Также можно сделать выводы о небольшой разнице теоретических и реальных значений.

Как видно из вычислений, во всех малых предприятиях после внедрения оптимального варианта СЗИ с учётом критерия обеспечения конкурентоспособности предприятия произошло снижение ущерба от нарушений ИБ и подтверждена эффективность, выбранных СЗИ. Все внедрённые СЗИ выполнили возложенные на них задачи.

В Автономной некоммерческой организации высшего образования «Смольный институт Российской Академии образования» научные результаты диссертационного исследования внедрены в учебный процесс института. При формировании программы дисциплины «Безопасность информационных

систем» разработан модуль «Метод обоснования СЗИ по критерию конкурентоспособности предприятия».

Выводы по главе 4

В данной главе описаны результаты внедрения разработанных методов и алгоритмов в хозяйственную деятельность малых предприятий Санкт-Петербурга, в учебный процесс «Смольного института Российской Академии Образования»; собраны и обработаны данные по внедрению; верифицированы полученные теоретические значения.

Таким образом, цель, поставленная в начале Главы 4, выполнена.

Заключение

Обоснование выбора наилучшего варианта СЗИ для повышения состояния защищённости предприятия от угроз нарушения ИБ по критерию конкурентоспособности является важной и актуальной задачей.

В диссертационной работе решена научно-техническая задача поиска способа (средства) ЗИ, при котором конкурентоспособность предприятия будет максимальной. Получены следующие результаты:

1. Получен алгоритм генерации допустимых вариантов системы защиты информации, который позволил сгенерировать допустимые варианты средств ЗИ. В дальнейшем возможно расширение алгоритма за счёт учёта эффективности совместного функционирования средств ЗИ (например, возможного замедления работы).

2. Разработан метод оптимизации вариантов защиты, который позволил выбрать оптимальный вариант. При дальнейших разработках можно увеличить количество критериев оптимизации, используя, например, устойчивость.

3. Разработан алгоритм обработки нечётких входных данных, который позволил использовать эвристическую информацию. При расширении алгоритма можно использовать нейронечёткие сети для настройки параметров нечёткой модели.

4. Получен метод обоснования СЗИ по критерию конкурентоспособности предприятия и алгоритм оценки эффективности СЗИ, в которых учитывался коэффициент изменения конкурентоспособности. В дальнейших разработках можно учитывать также суммарный стоимостной эффект.

5. Результаты исследований внедрены в хозяйственную деятельность двух малых предприятий Санкт-Петербурга. Произошло уменьшение ущерба после внедрения оптимального варианта СЗИ.

Полученные результаты соответствуют пунктам «9. Модели и методы оценки защищенности информации и информационной безопасности объекта», «10. Модели и методы оценки эффективности систем (комплексов) обеспечения

информационной безопасности объектов защиты» паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Результаты диссертационной работы рекомендуется применять для обеспечения ИБ в информационных инфраструктурах предприятий различных секторов экономики, отличающихся высоким уровнем конкуренции и имеющим ограниченные материальные ресурсы, в частности, в малых предприятиях. Дальнейшие исследования по тематики диссертационной работы предполагается целесообразным проводить в области развития и совершенствования полученных методов и алгоритмов в целях их распространения на обеспечение ИБ в более крупных предприятиях с учетом дополнительных критериев для выбора вариантов построения СЗИ.

Список сокращений и условных обозначений

RBAC	–	Role Based Access Control
ISO	–	International Organization for Standardization
IT	–	Information Technology
АСОИ	–	Автоматизированная система обработки информации
АСПИД	–	Анализ и синтез показателей при информационном дефиците
БД	–	База данных
ГОСТ	–	Государственный стандарт
ГТК	–	Государственная техническая комиссия при Президенте РФ
ЗИ	–	Защита информации
ИБ	–	Информационная безопасность
ИКТ	–	Информационно-коммуникационные технологии
ИС	–	Информационная система
ИСПДн	–	Информационная система персональных данных
ИР	–	Информационные ресурсы
ИТ	–	Информационные технологии
ЛИС	–	Локальная информационная система
МАС	–	Метод анализа и синтеза
МП	–	Метод прогнозирования
МР	–	Метод рейтингования
ММРСП	–	Модифицированный метод рандомизированных сводных показателей
МСП	–	Метод сводных показателей
МЭ	–	Межсетевой экран

НИОКР	–	Научно-исследовательская и опытно-конструкторская работа
ННН	–	Нечисловая, неполная, неточная (информация)
НСД	–	Несанкционированный доступ
ОК	–	Общие критерии
ОС	–	Операционная система
ПО	–	Программное обеспечение
ПП	–	Программный продукт
ПОС	–	Доля в процентах сотрудников, положительно оценивающих влияние системы защиты информации на свою работу
ПОЦ	–	Доля в процентах сотрудников, положительно оценивающих влияние системы защиты информации на работу компании
ПРД	–	Правила разграничения доступа
СВТ	–	Средства вычислительной техники
СЗ	–	Средства защиты
СЗИ	–	Система защиты информации
СЗИ НСД	–	Средства защиты информации от несанкционированного доступа
КСЗИ	–	Комплексная система защиты информации
СИБ	–	Служба информационной безопасности
СКЗИ	–	Средства криптографической защиты информации
СППР	–	Система поддержки принятия решений
ТП	–	Технический персонал
ТСОИ	–	Технические средства обработки информации
УБПДн	–	Угрозы безопасности персональных данных
УЗП	–	Процент уменьшения заметных последствий

УНП	–	Процент уменьшения незначительных последствий
УТП	–	Процент уменьшения тяжёлых последствий
УЭП	–	Доля в процентах участников эксперимента, применяющих информационные технологии в своей деятельности
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю
ЭВМ	–	Электронно-вычислительная машина
ЭЦП	–	Электронная цифровая подпись

Список литературы

1. Аверченков В. И. Системы защиты информации в ведущих зарубежных странах: учеб. пособие для вузов // В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – Брянск: БГТУ, 2007. – 225 С.

2. Агапьев Б. Д., Белов В. Н., Кесаманлы Ф. П., Козловский В. В., Марков С. И. Обработка экспериментальных данных // Учеб. Пособие. 2000. – 84 С.

3. Анн Х., Багиев Г. Л., Тарасевич В. М. Маркетинг: Учебник для вузов. 3-е изд. // Под общ. ред. Г. Л. Багиева. - СПб.: Питер, 2005. – 736 С.: ил. – (Серия «Учебник для вузов»).

4. Бабаш А. В., Шанкин Г. П. Криптография. Под редакцией В. П. Шерстюка, Э. А. Применко // А. В. Бабаш, Г. П. Шанкин. – М.: СОЛОН-Р, 2002. – 512 С.

5. Басовский Л. Е. Финансовый менеджмент: Учебник – М.: ИНФРА-М, 2008. – 240 С. (Высшее образование).

6. Бетелин В.Б., Галатенко В.А., Кобзарь М.Т., Сидак А.А., Трифаленков И.А. Профили защиты на основе «Общих критериев». // JetInfo, №3, -30 С., 2003.

7. Блинов А. О. Имидж организации как фактор конкурентоспособности / А. О. Блинов, В. Я. Захаров // Менеджмент в России и за рубежом. – 2003. - №4. – С. 35-43.

8. Борисов А.Н., Крумберг О.А., Федоров И.П. Принятие решений на основе нечетких моделей: примеры использования. – Рига: Знание, 1990 – 184С.

9. Василевский И.В, Болдырев А. И, Сталенков С. Е. Методические рекомендации по поиску и нейтрализации средств негласного съёма информации / Учебное пособие, 2001. – 138 С.

10. Воробьев В.И. Методология открытых систем и объектно-ориентированные технологии программирования. // Информационные технологии XXI века. Сб. тезисов докладов С-Петербургской конференции, посвященной 275-летию Российской Академии Наук. - СПб: СПбГУ, 1999. С.14-17.

11. Герасименко В.А., Малюк А. А. Основы защиты информации. – М.: МИФИ, 1997, 537 С.

12. Герасимова Л.В., Погожев И.Б. Комплексная оценка качества проектов и выбор оптимального варианта по методу академика А.Н. Крылова // Стандарты и качество. 1972. №8. С.37-39.

13. Городецкий С. Ю. ННГУ. Учебный курс «Модели и методы конечномерной оптимизации». Часть 2. Нелинейное программирование и многоэкстремальная оптимизация. // Учебно-исследовательская лаборатория "Математические и программные технологии для современных компьютерных систем (Информационные технологии)". 2003. 157 С.

14. Горшков А. С., Мясников А. В., Хованов Н. В. Прогнозирование эволюции сложных систем в условиях неопределённости // Материалы 6-й

международной конференции «Анализ, прогнозирование и управление в сложных системах» Т. 2. СПб., СЗАГС, 2005. С. 168-174.

15. ГОСТ 28806–90 «Качество программных средств. Термины и определения» [Электронный ресурс]– Режим доступа к рес.: http://files.stroyinf.ru/Data1/30/30786/ (дата обращения: 01.06.16).

16. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. [Электронный ресурс]– Режим доступа к рес.: http://docs.cntd.ru/document/gost-r-50922-2006 (дата обращения 18.04.16).

17. ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. [Электронный ресурс]– Режим доступа к рес.: http://allgosts.ru/35/020/gost_r_56546-2015 (дата обращения 19.04.16).

18. ГОСТ Р ИСО / МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Введение и общая модель. – Госстандарт России, Москва, 2008, 40 с. [Электронный ресурс]– Режим доступа к рес.: http://www.belgiss.org.by/russian/pered/index.php?UrlOr__=&UrlOrder=1&UrlDesc=1&entrant=73&UrlBD=22 (дата обращения: 30.04.16).

19. ГОСТ Р ИСО / МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Госстандарт России, Москва, 2002. 158 с. [Электронный ресурс]– Режим доступа к рес.: http://www.complexdoc.ru/scan/%D0%93%D0%9E%D0%A1%D0%A2%20%D0%A0%20%D0%98%D0%A1%D0%9E%7C%D0%9C%D0%AD%D0%9A%2015408-2-2002 (дата обращения: 06.02.16).

20. ГОСТ Р ИСО / МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Госстандарт России, Москва, 2002, 113 с. [Электронный ресурс]– Режим доступа к рес.: http://comsec.spb.ru/matherials/gosts/gost15408-3-2002.pdf (дата обращения: 30.03.16).

21. ГОСТ Р ИСО / МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – 31 С. [Электронный ресурс]– Режим доступа к рес.: http://vsegost.com/Catalog/57/5736.shtml (дата обращения: 30.04.16).

22. ГОСТ Р ИСО / МЭК 27005-20010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – 51 С. [Электронный ресурс]– Режим доступа к рес.: http://files.stroyinf.ru/data2/1/4293804/4293804268.pdf (дата обращения: 01.06.16).

23. ГОСТ Р ИСО / МЭК 27002-20012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента

информационной безопасности. -51 с. [Электронный ресурс]– Режим доступа к рес.: http://docs.cntd.ru/document/1200103619 (дата обращения: 01.06.16).

24. Гостехкомиссия России. Аттестационные испытания АС по требованиям безопасности информации. Типовая методика испытаний объектов информатики по требованиям безопасности информации (Аттестация АС). 1995. [Электронный ресурс]– Режим доступа к рес.:

http://www.s-system.ru/main/subject-2050/ (дата обращения: 30.01.16).

25. Грибов В. Д., Грузинов В. П. Экономика предприятия: учебник. Практикум. – 3-е изд., перераб. и доп. –М.: Финансы и статистика, 2008. – 336 С.: ил..

26. Грибунин В. Г. Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений // В. Г. Грибунин, В. В. Чудовский. – М. Издательский центр «Академия», 2009, - 416 С.

27. Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 С.

28. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М.: Яхтсмен, 1996. – 192 С.

29. Девянин П. Н. Модели безопасности компьютерных систем. уч. пособие. – М. Издательский центр «Академия», 2005. – 144 С.

30. Джохансон Джеспер М. Обеспечение безопасности. Ресурсы Windows Server 2008.// Пер. с англ.- М.: Издательство «Русская Редакция»; СПб.: БХВ – Петербург, 2009.-544 стр.: ил. ISBN 978-5-7502-0381-9 («Русская Редакция»).

31. Дмитриев П. А., Финкова М. А. Настройки BIOS.- 3-е изд., перераб. и доп. СПб.: Наука и Техника, 2007. – 288 С.: ил.

32. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО «ТИД «ДС», 2001. – 688 С.

33. Домарев В.В. Оценка эффективности систем защиты информации. [Электронный ресурс]– Режим доступа к рес.: https://bozza.ru/art-73.html (дата обращения: 03.02.16).

34. Доценко С.М., Шпак В.Ф. Комплексная информационная безопасность объекта: от теории к практике. / Учебное пособие, – СПб.: ООО «Издательство Полигон», - 2000, - 542 С.

35. Жук А. П., Жук Е. П., Лепёшкин О. М., Тимошкин А. И. Защита информации./ Учеб. Пособие. – 2-е изд. – М.: РИОР: ИНФРА-М, 2015. – 392 С.

36. Жук С.Н. Оценка эффективности функционирования сложных систем по иерархической системе показателей // Труды СПИИРАН. 2013. Вып. – 26. С. 194-203.

37. Зайнашева З. Г. Основы обеспечения конкурентоспособности системы сервиса: Монография – М.: ИКЦ «Маркетинг», 2009. – 362 С.

38. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. № 149-ФЗ. [Электронный ресурс]– Режим доступа к рес.: http://base.garant.ru/12148555/ (дата обращения: 29.05.16).

39. Закон РФ от 21.07.1993 г. №5485-1 «О государственной тайне». [Электронный ресурс]– Режим доступа к рес.: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=121414 (дата обращения: 09.06.16).

40. Закон РФ от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне». [Электронный ресурс]– Режим доступа к рес.: http://www.zakonprost.ru/zakony/98-fz-ot-2004-07-29-o-kommercheskoj-tajne (дата обращения: 24.04.16).

41. Закон от 27.07.2006 № 152-ФЗ «О персональных данных». [Электронный ресурс]– Режим доступа к рес.: http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html (дата обращения: 30.05.16).

42. Закутина Г. П., Кедровская Л. Г., Шумов Ю. А. Информационное обеспечение конкурентоспособности продукции и услуг (Методическое пособие). Изд – е 2 – е испр. и доп., М. 1992. ИПКИР УДК 002.55.339.137.2 (07) Л8к (03) – 92 С.

43. Закутный А. С. Оценка эффективности и анализ защищённости систем защиты информации. [Электронный ресурс]– Режим доступа к рес.: http://sbornik.dstu.education/articles/RU/283.pdf (дата обращения: 30.06.16).

44. Зегжда Д.П. Основы безопасности информационных систем, М.: Горячая линия - Телеком, 2000 г. — 452 С.

45. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. – 2-е изд.- СПб.: БХВ-Петербург, 2003. – 368 С.: ил.

46. Информационные системы и технологии в экономике и управлении: учебник под ред. проф. В. В. Трофимова. – 2-е изд., перераб. и доп. – М.: Высшее образование, 2007 – 480 С.

47. Канаев С. А. Информационные технологии и конкурентоспособность компании. – М.: МАКСПресс, 2011. – 136 С. (Серия : Исследования слушателей и выпускников программы «Доктор делового администрирования»).

48. Качество и конкурентоспособность в системе предпринимательства: Препринт. -СПб.: Изд-во СПбГУЭФ, 1999. – 44 С.

49. Кивиристи А. Новые подходы к обеспечению информационной безопасности сети. / А. Кавериcти // Компьютер-пресс, - 2000, - №7. – С. 3-8.

50. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 06.07.2016) [Электронный ресурс] – Режим доступа к рес.: http://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 30.05.16).

51. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линия-Телеком, 2002. – 336 С.: ил.

52. Колисниченко Д. Н. Блоги: создание, раскрутка, заработок. – М.: ООО «И. Д. Вильямс», 2010. – 336 С.: ил.

53. Колесов Д. Н., Михайлов М. В., Хованов Н. В., Оценка сложных финансово – экономических объектов с использованием системы поддержки принятия решений АСПИД-3W.СПб., ОЦЭиМ, 2004, - 64 С.

54. Число киберпреступлений в России выросло в шесть раз за три года. // Коммерсант.ru. - Режим доступа к рес.: https://www.kommersant.ru/doc/3391770 (дата обращения: 30.06.16).

55. Кондратюков С. В. Методика повышения конкурентоспособности предприятий сервиса : Монография / - Омск : «Омский научный вестник», 2007. – 142 С.

56. Конеев И. Р., Беляев А. В. Информационная безопасность предприятия. – СПб.: БХВ – Петербург, 2003. – 752 С.: ил.

57. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. – М.: Изд-во «Наука», 1978. – 831 С.

58. Корников В. В., Серёгин И. А., Хованов Н. В. Многокритериальное оценивание финансовых рисков в условиях неопределённости: Учеб. Пособие. – СПб.: Изд-во С.-Петерб. ун-та, 2002. – 96С.

59. Кудрявцев В. В. Повышение конкурентоспособности предприятий при помощи коммуникационных воздействий. Экономика и управление.// Пищевая промышленность. – 2006. №7 – С. 18.

60. Литвак Б.Г. Экспертная информация: методы получения и анализа. – М.: Радио и связь, 1982 – 184С.

61. Лифиц И. М. Формирование и оценка конкурентоспособности товара и услуг / И. М. Лифиц. – М.: Юрайт-Издат. 2004. – 335 С.

62. Лукацкий А.В. Атаки на информационные системы. Типы и объекты воздействия. //Электроника: Наука, Технология, Бизнес, №1, 2000.

63. Мак-Федрис Развёртывание безопасных сетей в WindowsVista.: Пер. с англ. – М.: ООО «И. Д. Вильямс», 2009. – 528 С.: ил.

64. Малюк А. А. Введение в защиту информации в автоматизированных системах / А. А. Малюк, С. В. Пазинин, Н. С. Погожин. – М.: Горячая линия – Телеком, 2001, - 148 С.

65. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М: Горячая линия – Телеком, 2004. – 280 С. Ил.

66. Масленников М. Е. Практическая криптография. – СПб.: БХВ-Петербург, 2003. – 464 С.: ил.

67. Маслова Н.А. Методы оценки эффективности систем защиты информационных систем / Н.А. Маслова // Штучний інтелект. — 2008. — № 4. — С. 253-264.

68. Мескон М. Х. , Альберт М., ХедоуриФ М53 Основы менеджмента: Пер с англ. – М.: Дело, 2006. – 720 С.

69. Миронов М. Г. Ваша конкурентоспособность/ М. Г. Миронов. – М.: Альфа-пресс, 2004, - 160 С.

70. Михайлов М. В. Модель оценки качества институтов высшего профессионального образования // Вестник Санкт-Петербургского университета. Сер. 5. Вып. 4. 2006. С. 74-82.

71. Михайлов М. В. Построение множества согласованных допустимых векторов весовых коэффициентов в методе сводных показателей. Деп. ВИНИТИ, Ш 3645-В96. М., 1996. – 12 С.

72. Могилёв А. В. Методы программирования. Компьютерные вычисления / А. В. Могилёв, Л. В. Листрова. – СПб.: БХВ-Петербург, 2008. – 320 С.: ил. – (ИиКТ)

73. Моисеева Н. К. Международный маркетинг: Учебн. пособие /Н. К. Моисеева. –М.: Центр экономики и маркетинга, 1998. ISBN 5-85873-010-9, М-74, ББК 65.050.9(2)2, - 320 С.

74. Ногин В. Д. Обобщённый принцип Зджворта-Парето и границы его применимости // Экономика и математические методы, «Издательство Наука», М. 2005. С. 128-134.

75. Молдовян А.А., Молдовян Н.А., Советов Б.Я. "Криптография." - Спб.: Издательство "Лань", 2001. – 224 С.

76. Нестерук Г. Ф., Молдовян А. А., Осовецкий Л. Г., Нестерук Ф. Г.; Фархутдинов Р. Ш. К разработке модели адаптивной защиты информации // Вопросы защиты информации. 2005, № 3. С. 11 – 16.

77. Ожегов // Толковый словарь. URL: http://tolkslovar.ru/ie672.html (дата обращения 18.07.16).

78. Олифер В. Г., Олифер Н. А. Сетевые операционные системы. – СПб.: Питер, 2007. – 539 С.: ил.

79. Официальный сайт Международного стандарта финансовой отчётности URL: http://www.msfofm.ru/transformation/137-cost-of-employees (дата обращения 17.03.16).

80. Официальный сайт Федеральной службы государственной статистики. URL: www.gks.ru (дата обращения 15.06.17).

81. Приказ ФСТЭК России от 18 февраля 2013 г. № 21. Официальный сайт Федеральной службы по техническому и экспертному контролю. www.fstec.ru (дата обращения 18.02.16).

82. Информационное сообщение ФСТЭК России от 15 июля 2013 г. № 24/22/2637. Официальный сайт Федеральной службы по техническому и экспертному контролю. www.fstec.ru (дата обращения 18.02.16).

83. Официальный сайт Hewlett Packard Enterprise. URL: http://www8.hp.com/ru/ru/software-solutions/ponemon-cyber-security-report/ (дата обращения 16.02.16).

84. Официальный сайт Защита и нападение в сети. URL: www.securitylab.ru (дата обращения 17.02.16).

85. Официальный сайт Измерительные приборы. URL: http://kipinfo.ru/info/opred/metrolog/ (дата обращения 17.02.16).

86. Пащенко И. Г. Интернет / И. Г. Пащенко. – 2-е изд., перераб. и доп. – М.: Эксмо, 2009. – 480 С. ил.

87. Пегат А. Нечеткое моделирование и управление; пер. с англ.-2-е изд.- М.: БИНОМ. Лаборатория знаний, 2013. – 798 С. ил. - (Адаптивные и интеллектуальные системы).

88. Петров В. Н. Информационные системы / - СПб.: Питер, 2003. – 688 С.: ил.

89. Петров В.А., Пискарев А.С., Шеин А.В. Информационная безопасность. Защита информации от несанкционированного доступа в автоматизированных системах / Учебное пособие. Изд. 2-е, испр. и доп. М.: МИФИ. 1995. – 84 С.

90. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009. – 352 С.

91. Попова Е. В. Влияние информационной безопасности на повышение конкурентоспособности малых предприятий сферы услуг. Журнал «Теория и практика сервиса», №3(13), сентябрь 2012, С. 220-226.

92. Попова Е. В. Выбор варианта системы защиты информации по критерию обеспечения конкурентоспособности предприятия// Научно-технический вестник информационных технологий, механики и оптики. – 2014. – № 2 (90). – С. 155-160.

93. Попова Е. В. Повышение конкурентоспособности малых предприятий сферы услуг путём усиления информационной безопасности после принятия закона о персональных данных. Журнал «Журнал правовых и экономических исследований», №3, С. 106-110 Сентябрь 2012.

94. Попова Е. В. Проблемы информационной безопасности малых предприятий сферы услуг в эпоху начинающихся кибервойн. // Конференции «Региональная информатика (РИ-2012)», -СПб.: Изд-во СПбГУСЭ, С. 306.

95. Попова Е. В. Роль информационной безопасности при построении инновационной экономики.// V Межвузовская научно-практическая конференция студентов, магистрантов и аспирантов «Социально-экономические аспекты сервиса: современное состояние и перспективы развития», -СПб.: Изд-во СПбГУСЭ, 2011г, С. 244-246.

96. Попова Е. В. Экономическая безопасность в период выхода из кризиса.// Всероссийская научно-практическая конференция «Проблемы развития предпринимательства 2010», -СПб.: Изд-во СПбГУСЭ, С. 344-347.

97. Попова Е. В. Экономическая и информационная безопасность сферы сервиса.// Международной научной конференции – Вторых Санкт – Петербургских социологических чтений 2010, -СПб.: Изд-во СПбГУСЭ, С. 192-193.

98. Попова Е. В.Непрерывность бизнеса как следствие экономической и информационной безопасности предприятия. // Конференция «Актуальные проблемы современной науки и образования» 2010.

99. Попова Е. В. Влияние информационного риска на бизнес.// Конференция "Социально-экономические аспекты сервиса: современное состояние и перспективы развития", -СПб.: Изд-во СПбГУСЭ, 2010, С. 155-158.

100. Попова Е. В. Информационная безопасность от древней истории до современных инновационных центров.// II Международная научно-практическая конференция «Инновационные процессы в сфере сервиса: проблемы и перспективы» 2010.

101. Попова Е. В. Метод выбора системы защиты информации с учётом критерия конкурентоспособности предприятия // Информационно-управляющие системы. – 2016. – № 6 (85). – С. 85-90.

102. Попова Е. В. Переход от индустриального общества к обществу информационных услуг.// II Всероссийская научная конференция «Научное творчество XXI века» с международным участием 2010.

103. Попова Е. В. Повышение конкурентоспособности предприятий путём усиления информационной безопасности при дистанционной занятости работника.// III Международная научно-практическая конференция «Инновационные технологии в сервисе» ITS 2012, -СПб.: Изд-во СПбГУСЭ, С. 251-252.

104. Попова Е. В. Расчёт конкурентоспособности малых предприятий сферы сервиса при усилении информационной безопасности. Журнал «Вестник российской академии естественных наук». Сентябрь 2012, 16(3): С. 48-51.

105. Попова Е. В. Электронная цифровая подпись и электронная безопасность малых предприятий. Журнал «Теория и практика сервиса» №2(8)/2011. УДК 004.056.53 ББК 32.97, С.107-114.

106. Попова Е. В. Эффективность системы защиты информации, выбранной по критерию обеспечения информации.//Приборостроение №9/2014,С. 19-22.

107. Попова Е. В. Многокритериальный оптимизационный выбор системы защиты информации (СЗИ) для малых предприятий.// Конференция ISRR-2013, VIII St. Petersburg Interregional Conference, октябрь 2013. С. 191–192.

108. Попова Е. В. Метод экспертной оценки для формирования измерений при многокритериальном выборе системы защиты информации (РИ-2016). Юбилейная XV Санкт- Петербургская международная конференция «Региональная информатика (РИ-2016)». Санкт-Петербург, 26-28 октября 2016 г.: Материалы конференции.\ СПОИСУ. - СПб, 2016. С. 382-383.

109. Попова Е. В. Алгоритм получения экспертных оценок при выборе оптимального варианта системы защиты информации на основе нечётких множеств.// Региональная информатика и информационная безопасность. Сборник трудов. Выпуск 2 / СПОИСУ. – СПб, 2016. С. 279-281.

110. Постников В. М. Спиридонов С. Б. Методы выбора весовых коэффициентов локальных критериев // Наука и Образование. МГТУ им. Н. Э. Баумана, Электрон. журн. 2015. № 06. С. 267-287.

111. Решение Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте

РФ. «Положение о государственном лицензировании деятельности в области защиты информации» от 27.04.1994 г. №10[Электронный ресурс]– Режим доступа к рес.: http://www.ekey.ru/info_def/legally_concerned/5/1 (дата обращения: 09.06.16).

112. Риз Дж. Облачные вычисления: Пер. с англ. – СПб.: БХВ – Петербург, 2011. – 288 С.: ил.

113. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 С.: ил.

114. Российская газета. [Электронный ресурс]– Режим доступа к рес.: http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html (дата обращения: 09.06.16).

115. Россия в глобальном пространстве : Национальная безопасность и конкурентоспособность : Материалы XXIV Международ. науч. – практ. конфр. : в 4 ч. / Урал. Соц. – экон. ин-т АТиСО. – Челябинск, 2007. –М. – 444 С.

116. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий (приказ Гостехкомиссии России от 19.06.2002г. № 187). [Электронный ресурс]– Режим доступа к рес.: http://www.detektor.ru/about/regulations/organizacionno-rasporyaditel_nye_dokumenty_po_tehnicheskoj_zawite_informacii1/ (дата обращения: 19.02.16).

117. Руководящий документ. Средства вычислительной техники, защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. (приказ Гостехкомиссии России от 30.03.1992г.) [Электронный ресурс] – Режим доступа к рес.: http://fstec.ru/normativnye-i-metodicheskie-dokumenty-tzi/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2 (дата обращения: 20.04.16).

118. Рыбаков И. Н. Качество и конкурентоспособность продукции при рыночных отношениях. Вопросы теории. // Стандарты и качество. – 1995. №12. – С. 43 – 47.

119. Системы нечёткого вывода [Электронный ресурс]– Режим доступа к рес.: http://nrsu.bstu.ru/chap27.html (дата обращения: 20.11.16).

120. Скляров И. С. Головоломки для хакера. – СПб.: БХВ-Петербург, 2007. – 320 С.: ил.

121. Социальная информатика: Основания, методы, перспективы/ Отв. ред. Н. И. Лапин. Изд. 3-е. – М.: Книжный дом «ЛИБРОКОМ», 2010. – 216 С.

122. Социально-экономическая и финансовая политика России в процессе перехода на инновационный путь развития: Материалы международной научно-практической конференции 2008 г. Пленарное заседание. -М.:ВЗФЭИ, 2008.- 320 С.

123. Суханов А. В. Оценки защищённости информационных систем. [Электронный ресурс] – Режим доступа к рес.: http://www.jurnal.org/articles/2008/inf33.html. (дата обращения: 02.04.16).

124. Тарасюк М. В. Защищённые информационные технологии. Проектирование и применение – М.: СОЛОН-Пресс, 2004. – 192 С.: ил.

125. Топольский Н.Г., Бутузов С.Ю. Основы создания проводящих сред для сверхскоростных информационных модулей автоматизированных систем безопасности. – М.: Ак. ГПС МВД России, 2001.

126. Третьяк О. А. Маркетинг: новые ориентиры модели управления: Учебник. – М.: ИНФРА-М, 2005. –XII, 403 С.

127. Указ Президента РФ от 26.08.1996 г. №1268 «О контроле за экспортом из Российской Федерации товаров и технологий двойного назначения» [Электронный ресурс] – Режим доступа к рес.: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=142660 (дата обращения: 01.07.16)

128. Фатхутдинов Р. А. Управление конкурентоспособности организации: учеб пособие. – М.: Изд-во ЭКСМО, 2004. – 544С.

129. Федеральная служба по техническому и экспертному контролю. [Электронный ресурс]. – Режим доступа к рес. http://fstec.ru/ (дата обращения: 29.02.16).

130. Фатхутдинов Р. А. Управленческие решения: Учебник.- 6-е изд., перераб. и доп. – М.: ИНФРА- М, 2007. – 344 С. – (Высшее образование).

131. Федеральная служба по техническому и экспертному контролю 11 февраля 2013 г. N 17 об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения 18.06.16).

132. Федеральная служба по техническому и экспертному контролю 15 февраля 2008 г. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. URL: http://fstec.ru/component/attachments/download/289 (дата обращения 18.06.16).

133. Федеральный закон РФ «Об электронной подписи» 2011 г. /Сайт Президента России: [Электронный ресурс]. – Режим доступа к рес.: http://www.kremlin.ru (дата обращения: 01.04.16).

134. Федеральный закон РФ от 4 июля 1996 года 85-ФЗ "Об участии в международном информационном обмене. /Сайт информационного правового обеспечения Гарант: [Электронный ресурс]. – Режим доступа к рес.: http://base.garant.ru/135401/1/#block_2 (дата обращения: 03.06.16).

135. Флёнов М. Е. Web-сервер глазами хакера: 2-е изд., перераб. и доп. – СПб.: БХВ- Петербург, 2009. – 320 С.: ил.

136. Фильчаков П. В. Справочник по высшей математике / «Наукова думка», Киев, 1974. – 743 С.

137. Хованов Н. В., Федотов Ю. В. Модели учёта неопределённости при построении сводных показателей эффективности деятельности сложных производственных систем № 28(R)-2006 СПбГУ Научно-исследовательский институт менеджмента научные доклады. Электронный ресурс]– Режим доступа к рес.: http://dspace.gsom.pu.ru/jspui/bitstream/123456789/91/1/28%28R%29_2006.pdf (дата обращения: 09.03.16)

138. Чайников В. Н. Прогнозирование конкурентоспособности продукции в региональной социально – экономической системе: монография / В. Н. Чайников. –Чебоксары : Изд-во Чуваш. Ун-та, 2006. – 150 С.

139. Шальминова А. С. Инновационное бизнес-планирование развитие приоритетной отрасли : автореф. дис. канд. экон. наук / А. С. Шальминова.- Казань : Изд-во КФЭИ, 2000.

140. Шепитько Г. Е. Комплексная система защиты информации на предприятии. Часть1. Учебное пособие / Г. Е. Шепитько, А. А. Локтев, Г. Н. Гудов. – М.: МФЮА, 2008, - 127 С.

141. Штовба С. Д. Fuzzy Logic Toolbox. Введение в теорию нечётких множеств. URL: http://matlab.exponenta.ru/fuzzylogic/book1/ (дата обращения: 16.01.2017).

142. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и Техника, 2004. – 384 С. ил.

143. Юсупов Р. М. Наука и национальная безопасность// 2-е издание, переработанное и дополненное. - СПб.: Наука, 2011. – 369 С. 45ил.

144. Ярочкин В.И. Информационная безопасность. Учебник для вузов. – Академический проект, Мир, Серия: Gaudeamus Ось-98, 2008, -544 С.

145. Armaghan Behnia, Rafhana Abd Rashid, Junaid Ahsenali Chaudhry A Survey of Information Security Risk Analysis Methods / Smart Computing Review, vol. 2, no. 1, February 2012, pp. 81-94.

146. Common Criteria for Information Technology Security Evaluation. Version 2.2. Revision 256. Part 1: Introduction and general model. – January 2004. [Электронный ресурс] – Режим доступа к рес.: http://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.2.pdf (дата обращения: 10.03.16)

147. CRAMM (CCTA Risk Analysis and Management Method) [Электронный ресурс]. URL: http://rm-inv.enisa.europa.eu/methods/m_cramm.html, свободный. Яз. англ. (дата обращения 08.02.16).

148. Feinstein H., Sandhu R., Coyne E., Youman C. Role-based access control models / IEEE Computer, tom 29, № 2, 1996, pp. 38-47.

149. Hovanov N/ ASPID-method: Analysis and Synthesis of Parameters under Iformation Deficiency // Lecters on Eurosummer School “Sustainability Assessment of Clean Air Technologies”. Lisbon, Instituto Superior Technico, 2000. P. 2-64.

150. Hovanov N., Yudaeva M., Hovanov K. “Multicriteria estimation of probabilities on basis of expert non-numeric, non-exact and non-complete knowledge

// Abstracts of 18-th International Conference on Multiple Criteria Decision Making". Chania (Greece), June 19-23, 2006. P.102.

151. Hovanov N. V., Yudaeva M. S., Kotov N. V. Event-Tree with randomized transition probabilities as a new tool for alternatives probabilities estimation under uncertainty // Proceedings of the Sixth International Scientific school "Modeling and Analysis of s Safety and Risk in Complex Systems". St.Petersburg, July 4-8, 2006. SPb., RAS, 2006. P. 118-125.

152. IEEE Std 1003.1, 2004 Edition / The Open Group cite. [Электронный ресурс] – Режим доступа к рес.: http://www.unix.org/version3/ieee_std.html (дата обращения: 03.06.16).

153. ISO/IEC 19791 "Security assessment of operational systems"[Электронный ресурс] – Режим доступа к рес.: http://docs.cntd.ru/document/gost-r-iso-mek-to-19791-2008 (дата обращения: 03.09.16).

154. Landwehr Carl Formal models for computer security / Carl Landwehr ACM Computing Surveys (CSUR), tom 13, № 3, 1981/9/1, pp. 247-278.

155. Leon J. Osterweil, Matt Bishop, Heather M. Conboy, Huong Phan, Borislava I. Simidchieva, George S. Avrunin, Lori A. Clarke, Sean Peisert Iterative Analysis to Improve Key Properties of Critical Human-Intensive Processes: An Election Security Example / ACM Transactions on Privacy and Security (TOPS), Volume 20 Issue 2, March 2017, Article No. 5.

156. NIST SP 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000. [Электронный ресурс] – Режим доступа к рес.: http://csrc.nist.gov/publications/nistir/ir7497/nistir-7497.pdf (дата обращения: 09.03.16).

157. NIST SP 800-30, Risk Management Guide for Information Technology Systems, January 2002. [Электронный ресурс] – Режим доступа к рес.: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf (дата обращения: 09.05.16).

158. Peltier, Thomas R. Information security risk analysis / Thomas R. Peltier -- 2nd ed. p. cm. Includes bibliographical references and index. ISBN 0-8493-3346-6 1. Computer security. p. 361. [Электронный ресурс]– URL.: http://www.antoanthongtin.vn/Portals/0/UploadImages/kiennt2/Sach/Sach-CSDL4/Information%20Security%20Risk%20Analysis,%202%20Ed..pdf (дата обращения: 03.02.16).

159. Prahalad C. K., Hamel G. The Core Competence of the Corporation//Harvard Business Rev.,1990, 66. P.82.

160. Shan Huo Chen, Shu Man Chang, Shiu Tung / // Some Properties of Graded Mean Integration Representation of L-R Type Fuzzy Numbers. Tamsui Wang Oxford Journal of Mathematical Sciences Aletheia University 22(2) (2006) 24 p.

161. Social sciences collection guides official publications [Электронный ресурс] –Режим доступа к рес.: http://www.bl.uk/britishlibrary/~/media/subjects%20images/government%20publications/pdfs/united-states-government-publications.pdf (дата обращения: 29.02.16).

162. Standard: Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, DoD 5200.28-STD, December 26, 1985. P. 116. [Электронный ресурс] – Режим доступа к рес.: http://csrc.nist.gov/publications/history/dod85.pdf (дата обращения: 20.05.16).

163. Standard: ISO/IEC 7498-4:1989. Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management framework. P. 9. [Электронный ресурс] – Режим доступа к рес.: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?ics1=35&ics2=100&ics3=70&csnumber=14258 (дата обращения: 20.04.16).

164. Standard: ISO/IEC 27001 - Titles: The Information Security Standard. Renamed in 2007. [Электронный ресурс] – Режим доступа к рес.: http://www.itgovernance.co.uk/iso27001.aspx (дата обращения: 25.04.16).

165. ISO/IEC 13335-1: 2004 Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management (IDT). [Электронный ресурс] – Режим доступа к рес.: http://www.iso27001security.com/html/others.html (дата обращения: 29.04.16).

166. Zadeh L. Fuzzy Sets//Information and Control. -1965. –Vol.8 –P. 338-353.

Приложение А

Список возможных угроз нарушения ИБ предприятий

По виду несанкционированных действий:

- угрозы конфиденциальности информации;
- угрозы целостности информации;
- угрозы доступности информации.

По видам источников угроз безопасности персональных данных (УБПДн):

- угрозы, создаваемые физическим лицом;
- аппаратной закладкой;
- вредоносными программами.

По способам реализации УБПДн:

- угрозы специальных воздействий на информационную систему персональных данных (ИСПДн);
- угрозы несанкционированного доступа (НСД) в ИСПДн;
- угрозы утечки информации по техническим каналам.

По используемой уязвимости:

- с использованием уязвимости системного программного обеспечения (ПО);
- с использованием уязвимости прикладного ПО;
- с использованием аппаратной закладки;
- с использованием уязвимости протоколов сетевого взаимодействия и каналов передачи данных;
- с использованием уязвимости технических средств обработки информации (ТСОИ);
- с использованием уязвимости СЗИ.

Случайные угрозы:

- воздействие магнитных полей на магнитные носители информации, дефекты оборудования, которые приводят к разрушению информации;
- невыявленные ошибки в программах обработки информации;
- ошибки при вводе данных;
- сбои в работе аппаратуры, вызванные воздействием напряжения, перебоями энергоснабжения;
- случайные действия, приводящие к разрушению аппаратных, программных, информационных ресурсов (ИР), носителей информации;
- некомпетентное использование технологических программ, способных к потере работоспособности системы;
- использование неучтенных, нелицензионных программ;
- некомпетентные действия, приводящие к разглашению конфиденциальной информации;
- потеря, передача атрибутов разграничения доступа;
- разработка прикладных программ, представляющих опасность для информационной системы (ИС) и информации;
- некомпетентная настройка или отключение средств защиты (СЗ) персоналом СИБ;
- передача данных по ошибочному адресу;
- непреднамеренное повреждение каналов связи;

Умышленные угрозы:

- умышленный доступ к системе с целью совершения запрещенных действий;
- маскировка под пользователя, обладающего большими полномочиями;
- использование служебного положения с целью увеличить свои полномочия;

- умышленное физическое разрушение системы;
- отключение подсистем обеспечения безопасности ИС;
- изменение режимов работы устройств и программ для совершения злонамеренных действий;
- подкуп, шантаж пользователей, имеющих определенные полномочия;
- кража носителей информации или несанкционированное их копирование;
- чтение остаточной информации из оперативной памяти;
- неправомерное получение паролей, других реквизитов разграничения доступа;
- незаконное дешифрование информации;
- внедрение аппаратных и программных закладок, для дальнейшего воздействия на ИС;
- незаконное подключение к линиям связи с вводом ложных сообщений или модификацией передаваемых сообщений;
- незаконное подключение к линиям связи, подмена законного пользователя после аутентификации для ввода;
- воздействие на каналы связи, для имитации законных пользователей и проникновения в систему;
- внедрение агентов в СИБ;
- применение подслушивающих устройств;
- хищение производственных отходов.

Приложение Б

Анкетирование сотрудников предприятий с целью мониторинга последствий внедрения системы защиты информации на предприятии

ИС – информационная система
ИБ – информационная безопасность
СЗИ – система защиты информации

1. Применяете ли Вы информационные технологии в своей профессиональной деятельности?

Да / Нет

2. Сталкивались ли Вы с нарушениями работы ИС, связанными с ИБ до внедрения СЗИ?

Да / Нет

3. Если да, то укажите процент уменьшения последствий (по количеству нарушений ИБ) в 2015 г. по сравнению с 2014 г. Тяжёлые последствия вызывают большие потери материальных активов и наносит большой урон репутации компании. Заметные последствия вызывают существенные потери материальных активов и умеренно влияют на репутацию компании. Незначительные последствия приводят к несущественным потерям материальных активов, которые быстро восстанавливаются, или к слабому влиянию на репутацию компании.

Тяжелых - __ %

Заметных - __ %

Незначительных - __ %

4. Считаете ли Вы, что внедрение СЗИ и службы ИБ для Вас лично было полезным?

Да / Нет

5. Считаете ли Вы, что внедрение СЗИ и службы ИБ для работы компании было полезным?

Да / Нет

Приложение В

Анкета по предприятиям, участвующим во внедрении научных разработок диссертационного исследования.

Анкета по предприятию ……., в котором предлагается к внедрению система защиты информации:

……

Просьба оценить наименее возможную нижнюю, наименее возможную верхнюю и интервал наиболее ожидаемых значений коэффициента уменьшения ущерба (коэффициент изменения конкурентоспособности) в результате обеспечения информационной безопасности по трём факторам: конфиденциальность, целостность, доступность информации.

Просьба указывать коэффициент только по значениям сетки:

0.0; 0.1; 0.2; … 0.9; 1.0.

Вариант системы защиты информации

характеристика системы защиты информации	наименее ожидаемая нижняя оценка	наиболее ожидаемая минимальная оценка	наиболее ожидаемая максимальная оценка	наименее ожидаемая верхняя оценка
конфиденциальность				
целостность				
доступность				

Приложение Г

Опорные точки коэффициента изменения конкурентоспособности

В таблице Г.1 представлены опорные точки функции принадлежности коэффициента изменения конкурентоспособности для первого варианта СЗИ по критерию целостности информации, полученные от экспертов.

Таблица Г.1 – Опорные точки коэффициента изменения конкурентоспособности

первый вариант системы защиты информации	наименее возможная нижняя оценка	наиболее ожидаемая минимальная оценка	наиболее ожидаемая максимальная оценка	наименее возможная верхняя оценка
1-й эксперт	0,2	0,3	0,7	0,8
2-й эксперт	0,3	0,4	0,6	0,7
3-й эксперт	0,4	0,5	0,8	0,9

Преобразование изменений входных значений в выходные в нечёткой модели с использованием оператора min проиллюстрировано на рисунке Г.1.

Значение дефаззифицированной выходной функции принадлежности затем участвует в дальнейших расчётах ММРСП.

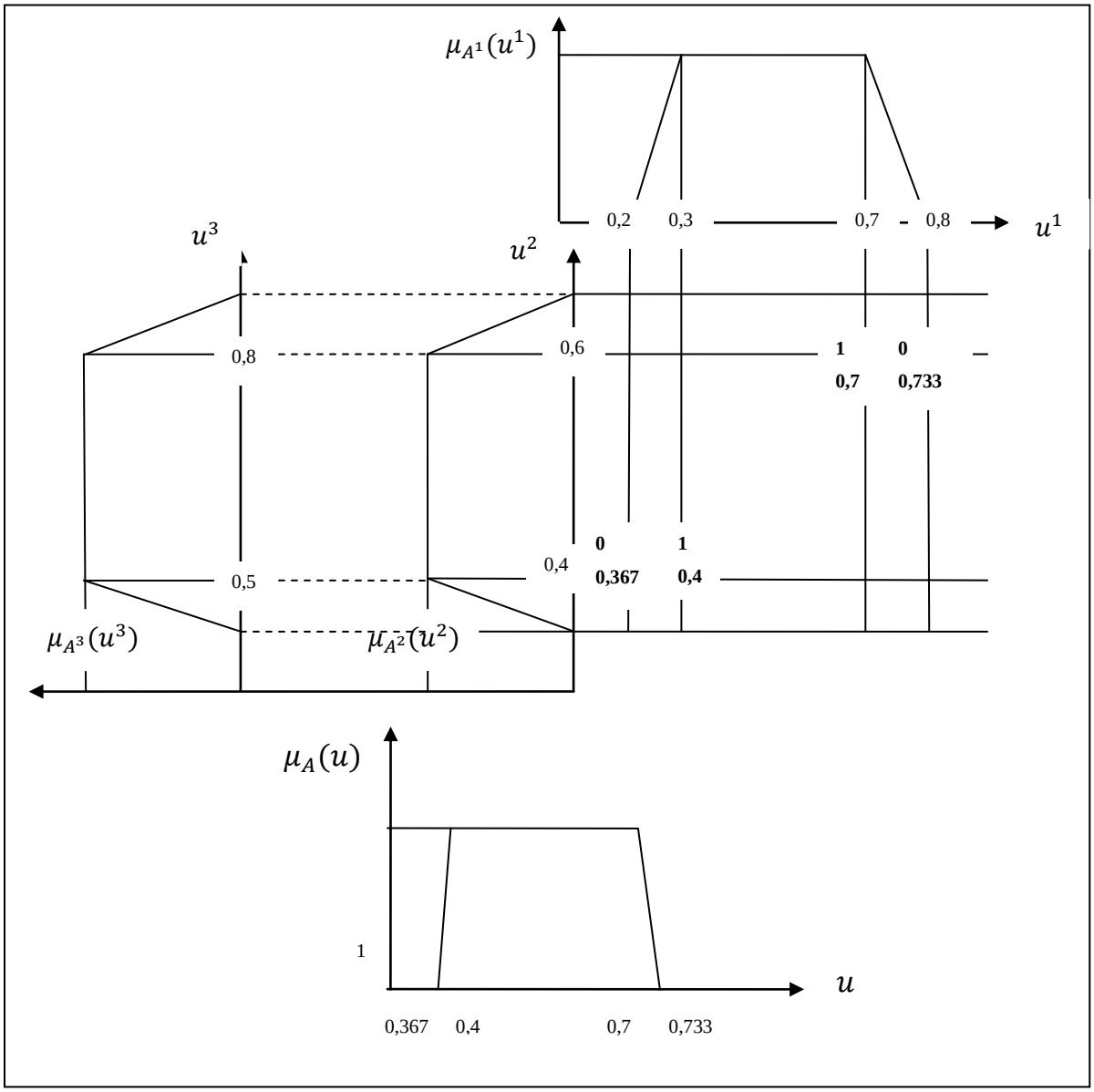


Рисунок Г.1 – Функция принадлежности выходного нечёткого числа при трёх входных нечётких числах, полученная с использованием операторов max и min.

Приложение Д

Копии актов о внедрении результатов работы

Закрытое акционерное общество «КОНТО»
191023, Россия, Санкт-Петербург, ул. Караванная, д. 1, офис 418
ИНН:7805029742, ОГРН:1027809186745
Тел.: (812)310-25-30, факс: (812) 310-25-30, e-mail: konto@mail.wplus.net
www/rjntj.sp.ru

АКТ
о внедрении научных результатов,
полученных в диссертации
Поповой Елены Владимировны

Комиссия в составе:

1. Забиякин Владимир Сергеевич, генеральный директор ЗАО «КОНТО»;
2. Ковалёв Павел Александрович, директор бэк-офиса;

составила настоящий акт о том, что научные результаты, полученные Поповой Еленой Владимировной в её диссертационной работе «Методы и алгоритмы обоснования системы защиты информации по критерию конкурентоспособности предприятия», а именно: метод обоснования системы защиты информации по критерию конкурентоспособности предприятия, алгоритм генерации допустимых вариантов системы защиты информации, алгоритм обработки нечётких входных данных, метод оптимизации вариантов защиты внедрены в деятельность данного предприятия. После внедрения оптимального варианта системы защиты информации были достигнуты положительные результаты в обеспечении состояния защищённости предприятия от угроз нарушения информационной безопасности.

Комиссия подтверждает практическую значимость и новизну результатов данной работы.

Генеральный директор — Забиякин В. С.

Директор бэк-офиса — Ковалёв П. А.

ИНН 7801382668 КПП 7801001
199106. Санкт-Петербург, Гаванская ул., д.3. лит.А
р/с 40702810900000007288
Банк «Таврический» (ОАО)
к/с 30101810700000000877
БИК 044030877

Комиссия в составе:

1. Галкин Игорь Михайлович, генеральный директор ООО «Лесной Двор»;
2. Зорин Андрей Борисович, инженер-программист;

составила настоящий акт о том, что научные результаты, полученные Поповой Еленой Владимировной в её диссертационной работе «Методы и алгоритмы обоснования системы защиты информации по критерию конкурентоспособности предприятия», а именно: метод обоснования системы защиты информации по критерию конкурентоспособности предприятия, алгоритм генерации допустимых вариантов системы защиты информации, алгоритм обработки нечётких входных данных, метод оптимизации вариантов защиты внедрены в деятельность данного предприятия. После внедрения научных разработок были достигнуты положительные результаты в обеспечении состояния защищённости предприятия от угроз нарушения информационной безопасности.

Комиссия подтверждает практическую значимость и новизну результатов данной работы.

Генеральный директор Галкин Игорь Витальевич.

Специалист Зорин Андрей Борисович.

Автономная некоммерческая организация высшего образования
СМОЛЬНЫЙ ИНСТИТУТ
РОССИЙСКОЙ АКАДЕМИИ ОБРАЗОВАНИЯ
195197, Российская Федерация, Санкт-Петербург, Полюстровский пр., д.59
Телефон: +7(812) 540-6984; факс: +7(812) 540-1403; Приемная комиссия: +7(812) 541-1111
E-mail: smun@smun.spb.ru, www.smun.spb.ru

УТВЕРЖДАЮ
Вр.И.О. ректора Смольного института РАО
Казанцев В. П.
30 августа 2016

АКТ
о внедрении научных результатов,
полученных в диссертации
Поповой Елены Владимировны

Комиссия, назначенная приказом ректора Автономной некоммерческой организации высшего образования «Смольный институт Российской академии образования» №65/п-1/16 от 26.08.16 составила настоящий акт о том, что научные результаты, полученные Поповой Еленой Владимировной в её диссертационной работе «Методы и алгоритмы обоснования системы защиты информации по критерию конкурентоспособности предприятия» внедрены в учебный процесс института. Комиссия подтверждает, что при изучении дисциплины «Безопасность информационных систем» разработана программа, в которую вошли модули по внедрению метода обоснования системы защиты информации по критерию конкурентоспособности предприятия, алгоритм генерации допустимых вариантов системы защиты информации, алгоритм обработки нечётких входных данных, метод оптимизации вариантов защиты.

Комиссия подтверждает практическую значимость и новизну результатов данной работы.

Председатель Комиссии: проректор по непрерывному образованию в учебно-воспитательной работе Черкасова Екатерина Павловна

Члены миссии:

декан факультета Информационных технологий
Барабаш Павел Александрович.

Заведующая кафедрой информационных систем
Титова Юлияна Францевна