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

На правах рукописи

Нурдинов Руслан Артурович

Модель количественной оценка рисков безопасности корпоративной информационной системы на основе метрик

05.13.19 – Методы и системы защиты информации,
информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
д.в.н., профессор
Каторин Юрий Федорович

Санкт-Петербург – 2016

ОГЛАВЛЕНИЕ

Введение

Актуальность темы

Высокие требования к обеспечению безопасности и надежности корпоративных информационных систем (КИС), обусловленные характером решаемых задач, а также регулярные изменения корпоративной среды, требуют тщательного подхода к формированию и постоянному совершенствованию системы защиты информации (СЗИ) КИС, состоящей из комплекса технических и организационных защитных мер.

Основное предназначение КИС заключается в повышении эффективности деятельности предприятия, следовательно, формируемый комплекс защитных мер для КИС должен быть рациональным с точки зрения выгод и затрат.

Во многих стандартах по информационной безопасности (ИБ) предлагается риск-ориентированный подход, в соответствии с которым защитные меры выбираются для снижения неприемлемых рисков. Это утверждение справедливо для международных стандартов [150, 173, 180], национальных стандартов [141, 142, 146, 162, 166-168], в том числе национальных стандартов Российской Федерации [41, 46], а также стандартов организаций [117, 129].

Риски могут оцениваться качественно и количественно (в стоимостном выражении). Количественная оценка рисков позволяет обосновать затраты на реализацию защитных мер. Вместе с тем, существует целый ряд проблем, затрудняющих выполнение на практике количественной оценки рисков безопасности КИС:

- недостаточная формализация правил оценки рисков и, как следствие, необходимость постоянного привлечения экспертов;
- трудоемкость детализированной оценки рисков на уровне отдельных элементов КИС (технических средств, программного обеспечения и прочих) и с учетом их взаимосвязей;
- неопределенность правил использования статистических данных для оценки вероятности рисковых событий.

Данные проблемы зачастую приводят к тому, что результаты оценки рисков носят приближенный характер и не могут быть использованы для формирования рационального комплекса защитных мер. Это снижает интерес к риск-ориентированному подходу как среди специалистов подразделений ИБ и информационных технологий (ИТ), так и среди руководителей предприятий.

В свою очередь, развитию риск-ориентированного подхода к выбору защитных мер для КИС способствуют совершенствование средств автоматизированной инвентаризации ИТ-активов и развитие технологий и систем анализа данных. Появление централизованных баз угроз, уязвимостей и инцидентов ИБ делает возможным применение сложных обучающихся математических моделей для оценки рисков безопасности КИС. Стоит отдельно отметить наметившуюся в последние годы тенденцию по созданию российских центров мониторинга, таких как банк угроз и уязвимостей ФСТЭК России [7] и центр FinCert Банка России.

Актуальность темы исследования следует из указанной выше необходимости рационального выбора защитных мер для КИС, осуществляемого на основе количественной оценки рисков, возникающих при этом трудностей и противоречий, а также возможностей по совершенствованию применяемых на практике методов и моделей оценки рисков.

Степень разработанности темы

Основные теоретические аспекты проблемы управления рисками ИБ нашли отражение в работах А.М. Астахова, Я.Д. Вишнякова, В.Н. Вяткина, Ю.Ф. Каторина, А.П. Ныркова, С.А. Петренко, Н.В. Хованова, В.М. Шишкина, D. Ashenden, A. Jones, T.L. Peltier, а также в работах ряда зарубежных университетов и коммерческих структур: BSI, CMU, IEC, ISO, MITRE, NIST. Вопросы оценки рисков и выбора защитных мер для информационных и автоматизированных систем и компьютерных сетей отражены в работах А.Н. Атаманова, Е.В. Дойниковой, И.А. Зикратова, Д.А. Котенко, И.В. Котенко, И.В. Машкиной, А.Г. Остапенко, И.Б. Саенко, Р.М. Юсупова, H. Joh, X. Ou, N. Poolsappasit, I. Ray, A. Singhal. Разработано большое количество нормативных

документов, регламентирующих вопросы оценки рисков и анализа защищенности информационных и автоматизированных систем. Теоретические основы ИБ отражены в трудах А.А. Варфоломеева, В.А. Герасименко, В.В. Домарева, Д.П. Зегжды, А.А Малюка, Д.С. Черешкина, А.И. Ярочкина.

Отечественными и зарубежными специалистами предложены различные модели и методы количественной оценки рисков, основанные на нечеткой логике [24, 57, 62, 78, 80, 124], линейном программировании [55], статистическом анализе [58, 132], байесовских сетях [176], нейронных сетях [5], логико-вероятностном моделировании [68], моделировании с использованием когнитивных карт [127] и имитационном моделировании [73].

Анализ работ специалистов в области оценки рисков ИБ показал, что при всей значимости проведенных исследований, проблема количественной оценки рисков безопасности КИС изучена и практически проработана не в полной мере. В первую очередь, для повышения качества выбора защитных мер необходимо разработать формализованную модель количественной оценки рисков, учитывающую связи между рисковыми событиями и способную к обучению с применением интеллектуальных технологий, что позволит избежать необходимости постоянного привлечения экспертов для оценки рисков.

Цель исследования – повышение качества выбора защитных мер для корпоративных информационных систем за счет детализированной количественной оценки рисков информационной безопасности.

Научная задача состоит в разработке методического аппарата, позволяющего осуществлять рациональный выбор защитных мер для корпоративных информационных систем за счет применения научно-обоснованной формализованной модели количественной оценки рисков.

Достижение цели путем решения поставленной научной задачи потребовало ее разделения на следующие **частные задачи**:

- сравнительный анализ подходов и математических методов количественной оценки рисков информационной безопасности, выявление ограничений в применении рассмотренных решений;

- разработка научно-обоснованной формализованной модели количественной оценки рисков безопасности корпоративной информационной системы;
- разработка методики формирования рационального комплекса защитных мер для корпоративной информационной системы;
- повышение точности прогнозирования вероятности реализации угроз нарушителем на основе данных об инцидентах информационной безопасности;
- разработка программного модуля управления рисками безопасности корпоративной информационной системы.

Объект исследования – защитные меры корпоративных информационных систем, создающих, хранящих и обрабатывающих информацию, важную с точки зрения обеспечения ее конфиденциальности, целостности и доступности.

Предмет исследования – математические методы и модели оценки рисков и выбора защитных мер для информационных систем.

Методы исследования

Для формирования понятий в работе используются логические приемы, определения, анализ и синтез. Для разработки модели оценки рисков и методики формирования рационального комплекса защитных мер для корпоративной информационной системы используются методы системного и структурного анализа, теории множеств, теории оптимизации и теории графов. Для количественной оценки вероятности реализации угроз нарушителем применяются методы математической статистики, теории вероятностей, теории нейронных сетей и метод анализа иерархий.

На защиту выносятся следующие **основные результаты научного исследования**:

1. Модель оценки рисков безопасности корпоративной информационной системы на основе определения деструктивных состояний ее элементов.

2. Методика формирования рационального комплекса защитных мер для корпоративной информационной системы на основе минимизации значения показателя затратоемкости активов.
3. Методика количественной оценки вероятности реализации угроз нарушителем на основе экспертно-нейросетевого определения метрик.

Научная новизна результатов исследования заключается в следующем:

1. Разработана оригинальная формализованная модель количественной оценки рисков безопасности КИС, отличающаяся набором связанных переходов ее элементов в деструктивные состояния, рассматриваемых в качестве рисковых событий.
2. Разработана методика, позволяющая повысить качество выбора защитных мер для корпоративной информационной системы, отличающаяся применением предложенного в работе показателя затратоемкости активов.
3. Для повышения точности прогнозирования вероятности реализации угроз нарушителем впервые применен специальный вариант алгоритма обратного распространения ошибки на основе диагонального метода Левенберга-Марквардта.

Обоснованность полученных результатов достигается использованием современного и апробированного математического аппарата, системно-структурным анализом описания объекта исследования, непротиворечивостью полученных выводов и их согласованностью с современными практиками в области информационной безопасности.

Достоверность предлагаемых моделей и методик подтверждается совпадением полученных в ходе экспериментального исследования результатов теоретическим положениям, практической апробацией на научно-технических конференциях и внедрением результатов в образовательных учреждениях и коммерческих предприятиях.

Практическую значимость исследования составляют предложенные модели и методики, которые позволяют повысить качество выбора защитных мер

для корпоративной информационной системы и могут быть реализованы в виде модуля управления рисками безопасности корпоративной информационной системы.

Внедрение результатов

Предложенные модели и методики внедрены в практику деятельности ООО «Газинформсервис» и ООО «Газпром трансгаз Санкт-Петербург». Кроме того, основные результаты, полученные в ходе диссертационного исследования, используются в учебном процессе ЧОУ ДПО «Центр предпринимательских рисков» и в учебном процессе кафедры безопасных информационных технологий Университета ИТМО.

Апробация работы

Основные результаты диссертационной работы представлены на 12 научных и практических конференциях, среди которых:

- V Всероссийский конгресс молодых ученых, V сессия научной школы «Технология программирования и защита информации», апрель 2016;
- XLV научная и учебно-методическая конференция НИУ ИТМО, Подсекция 45 «Управление и информатика в технических системах», февраль 2016;
- The First Information Security and Protection of Information Technologies (ISPIT) conference, ноябрь 2015;
- IX Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России», октябрь 2015;
- XIV Санкт-Петербургская международная конференция «Региональная информатика», октябрь 2014;
- III Международная научно-практическая конференция «Информационные управляющие системы и технологии», Украина, г. Одесса, сентябрь 2014.

Публикации

По результатам диссертационного исследования опубликовано 17 работ, из них статей в журналах, рекомендованных Высшей аттестационной комиссией при Министерстве образования и науки Российской Федерации, – 5.

Структура и объем работы

Диссертационная работа изложена на 186 страницах машинописного текста, содержит 37 иллюстраций и 21 таблицу, состоит из введения, четырех глав, заключения, списка сокращений и условных обозначений, списка литературы (180 наименований) и четырех приложений.

1 Анализ предметной области оценки рисков безопасности информационных систем

1.1 Оценка рисков информационной безопасности

Под риском, в общем смысле этого слова, понимают возможность или вероятность наступления событий с отрицательными или положительными последствиями в результате определенных решений или действий [21, 79].

Все риски являются случайными событиями, что зачастую обусловлено недостатком качественной информации о них. Получение всей необходимой информации ограничивается отсутствием соответствующих инструментальных средств, времени на сбор и обработку данных, действием внешних сил, а также отсутствием полных научных знаний о сущности рисковых процессов или явлений.

Риск присущ любой сфере человеческой деятельности, что обусловлено множеством условий и факторов, влияющих на исход принимаемых людьми решений. Наибольшее распространение оценка рисков получила в экономической, природной, политической, военной сферах деятельности.

О рисках в области ИБ всерьез заговорили в конце XX века, что обусловлено значительным совершенствованием средств вычислительной техники (СВТ) и увеличением объемов обрабатываемой, хранимой и передаваемой информации. Управление рисками в области ИБ имеет свои специфические особенности. Однако стоит отметить, что многие положения теории рисков ИБ берут свое начало из общей теории рисков.

В нормативных документах и методической литературе часто встречаются расхождения в используемой терминологии, составе типовых процедур оценки рисков и наборе оцениваемых параметров. Это делает необходимым проведение анализа предметной области оценки рисков безопасности информационных систем (ИС).

1.1.1 Основные понятия предметной области

В настоящее время термин «риск информационной безопасности» или «информационный риск» нашел широкое применение. Однако пока не существует принятой большинством ученых и практиков трактовки данного понятия [15]. Приведем лишь некоторые из них:

- «возможность наступления случайного события в информационной системе предприятия, приводящего к нарушению ее функционирования, снижению качества информации, в результате которых наносится ущерб предприятию» [4];
- «опасность возникновения убытков или ущерба в результате применения информационных технологий» [91];
- «неопределенность, предполагающая возможность потерь (ущерба)» [128]:
- «неопределенность, предполагающая возможность ущерба, связанного с нарушением информационной безопасности» [129];
- «потенциальная угроза эксплуатации уязвимости актива, вызывающая, таким образом, вред организации» [152].

Далее в диссертационной работе под риском понимается риск ИБ, представляющий собой комбинацию вероятности возникновения рискового события (например, реализации угрозы) и возникающего при этом ущерба.

Риски, как правило, связывают с активами, под которыми понимается «что-либо, имеющее ценность для организации и, следовательно, нуждающееся в защите» [42]. В ISO/IEC 27005:2011 активы подразделяются на первичные и вторичные. К первичным активам относят информацию и бизнес-процессы, а к вторичным – технические средства (ТС), программное обеспечение (ПО), сеть, персонал, места функционирования и организационную структуру [152].

В диссертационной работе в качестве активов рассматриваются ИС и их элементы. Вопросы безопасности ИС освещены в работах [14, 23, 50, 54, 140].

Общепринятого понятия термина «информационная система», равно как и однозначности в вопросе того, что входит в состав ИС, нет. В Федеральном законе 149-ФЗ «Об информации, информационных технологиях и о защите информации» дается следующее определение: «информационная система – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» [102].

При этом под ИС может пониматься как отдельная прикладная система, так и вся информационная инфраструктура предприятия. Чаще всего под ИС понимается одна или несколько прикладных систем, необходимых для реализации одного или нескольких связанных бизнес-процессов предприятия, например, ИС «Бухгалтерия и кадры», построенная на базе прикладного ПО «1С: Предприятие» и банк-клиента.

Зачастую термин «информационная система» путают с термином «автоматизированная система». В соответствии с ГОСТ 34.003-90: «автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций» [27]. Таким образом, можно выделить два основных различия между ИС и АС:

– в состав ИС, в отличие от АС, не входит персонал;

– в состав ИС входит информация или информационные активы (ИА).

Несмотря на это, некоторые авторы включают в состав ИС персонал [64].

Вопрос отнесения к ИС систем, в которых информация хранится и обрабатывается без использования ИТ и ТС, является противоречивым. В соответствии с определением, данным в Федеральном законе 149-ФЗ, в диссертационной работе под ИС подразумеваются только системы, реализованные с использованием ИТ и ТС. Вопросы защиты информации, хранящейся на бумажных и иных нетехнических носителях и обрабатывающейся без использования ИТ и ТС, относятся к области организации защищенного бумажного документооборота, регламентируемого стандартами [99, 101, 102].

КИС, как отдельный класс ИС, обладают определенными особенностями, такими как масштабируемость, высокая степень интеграции и другими, рассмотренными подробно в разделе 2 диссертационной работы. Поскольку данные особенности не играют существенной роли при проведении оценки рисков, анализ предметной области осуществляется для ИС в целом, а все сделанные в разделе 1 выводы справедливы для различных классов ИС, в том числе для КИС.

Под угрозой (безопасности информации) понимается «совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации» [45]. Угроза безопасности ИС может заключаться в неправомерном доступе к ней третьих лиц с целью нарушения конфиденциальности, целостности и доступности информации [14]. В ГОСТ Р 50922-2006 приводятся следующие определения данных свойств информации [45]:

- конфиденциальность – «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя»;
- целостность – «состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право»;
- доступность – «состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно».

Понятие «угроза» тесно связано с понятием «инцидент ИБ». В нормативных документах приводятся следующие определения термина «инцидент ИБ»:

- «появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ» [39];
- «любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность» [41].

Угроза безопасности ИС может возникнуть при наличии уязвимости, под которой понимается «свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации» [45]. Уязвимости подразделяются на технические (слабости кода и конфигурации ПО, низкая надежность ТС и прочие) и организационные (уязвимости, связанные с персоналом, слабости нормативно-документационного обеспечения, контроля и прочие) [34, 115].

Под источником угроз понимается «субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации» [87], а также «сущность, которая негативно воздействует на активы» [37]. По характеру происхождения угроз источники угроз подразделяются на естественные и антропогенные [42, 115, 159, 174].

Естественные источники угроз – это объективные физические процессы или стихийные природные явления, приводящие к нарушению целостности и доступности информации, и не зависящие или слабо зависящие от человека. В свою очередь, естественные источники угроз подразделяются на стихийные и техногенные [115, 162].

Стихийные источники угроз – это различные катастрофы природного и человеческого происхождения. К стихийным источникам угроз относятся климатические (наводнения, ураганы), термические (пожары, температурные воздействия), механические (землетрясения, обвалы), электромагнитные (магнитные бури, радиационное облучение), биологические (эпидемии, микроорганизмы) и химические (окисление) явления.

Под техногенными источниками угроз понимаются ТС и технологии, которые могут выйти из-под контроля человека. В теории надежности принято различать независимые и зависимые отказы [1, 31, 120]. Источниками независимых отказов являются сами элементы КИС, которые могут выйти из строя, например, в результате естественного старения ТС или ошибок ПО. Источниками зависимых отказов служат различные поддерживающие средства и

системы, оказывающее непосредственное воздействие на элементы КИС, например, системы электропитания, отопления и кондиционирования [166].

Антропогенные источники угроз, называемые также нарушителями ИБ [33], – это люди или группы лиц, в результате действий либо бездействия которых произошло нарушение безопасности КИС.

По характеру осуществляемых действий антропогенные нарушители подразделяются на тех, которые осуществляют свои действия преднамеренно (умышленно), и тех, кто способствует реализации угрозы непреднамеренно (случайно) [42, 115, 162, 166].

Под групповым нарушителем следует понимать группу преднамеренных одиночных нарушителей, осуществивших сговор с целью реализации угроз.

Описание существующих угроз безопасности информации, их актуальности, возможности реализации и последствий называется моделью угроз.

Под последствиями понимаются различные материальные и нематериальные потери, которые может понести предприятие в результате рискового события (реализации угрозы). Качественная или количественная (стоимостная) оценка всех последствий рискового события называется величиной ущерба.

Защитные меры – «это действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление активов» [36]. Защитные меры могут быть направлены как на уменьшение вероятности реализации угроз (за счет устранения или затруднения использования уязвимостей), так и на снижение величины последствий (ущерба) от реализации угроз.

Совокупность защитных мер, а также деятельность на их основе, направленную на выявление, отражение и ликвидацию последствий реализации угроз безопасности ИС, называют системой защиты информации [22].

Таким образом, предметная область оценки рисков безопасности ИС может быть представлена диаграммой классов в нотации Unified Modeling Language

(UML), как показано на рисунке 1. Между объектами предметной области установлены связи «многие ко многим», подразделяемые на ассоциации (прямые линии) и зависимости (пунктирные линии).

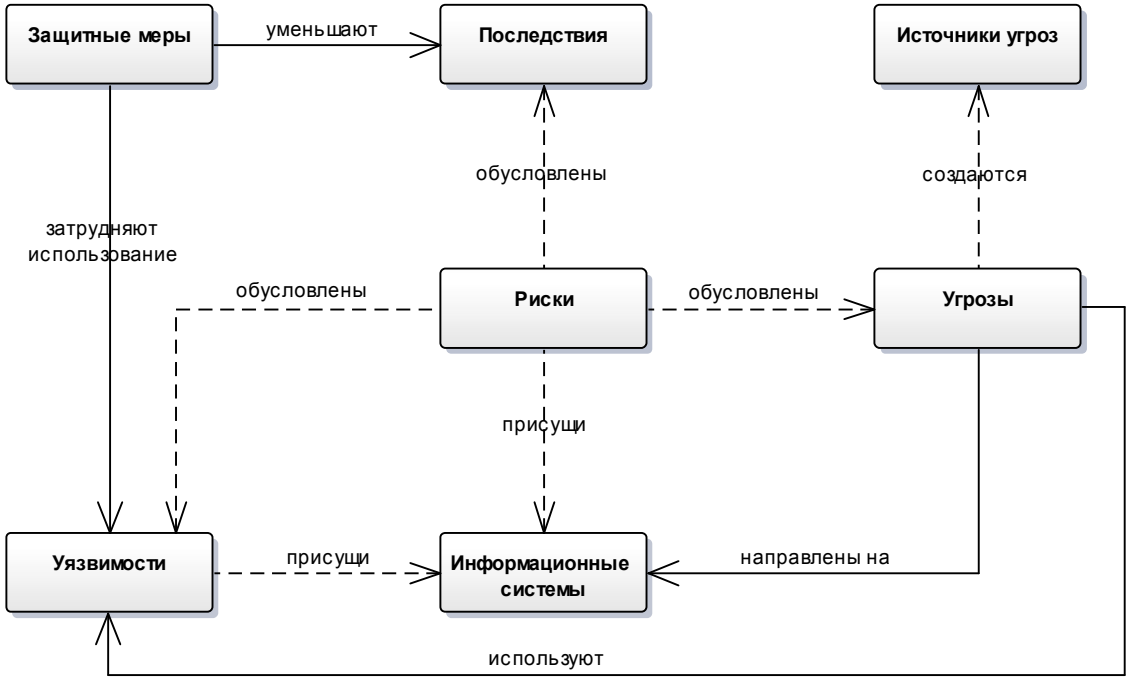

Рисунок 1 – Предметная область оценки рисков безопасности ИС

1.1.2 Качественная и количественная оценка рисков

Наиболее распространенной на практике является качественная оценка рисков, суть которой заключается в определении значений параметров риска (вероятности возникновения угрозы, вероятности использования уязвимости и величины ущерба) по некоторым, сформированным заранее, качественным шкалам. Классическим примером является трехуровневая шкала оценки параметров риска со значениями «высокий», «средний» и «низкий». Уровень риска определяется по специальной матрице, в которой возможные уровни риска проставлены на пересечениях значений, принимаемых его параметрами.

Качественная оценка рисков дает лишь грубые, трудно интерпретируемые результаты и, тем самым, не позволяет аргументировать размер инвестиций в ИБ и сформировать рациональный комплекс защитных мер. Распространенность качественной оценки рисков обусловлена тем, что количественная оценка вероятности рискового события весьма затруднена ввиду отсутствия четких

требований к составу исходных данных, правил оценки (математической модели) и достаточного количества статистических данных [15, 49].

Количественная оценка риска R в простейшем случае осуществляется по формуле [166]:

$$R = p \cdot q, \quad (1)$$

где p – вероятность рискового события;

q – величина ущерба.

Чаще всего под рисковым событием понимается реализация угрозы. Вероятность реализации угрозы принимает значения в интервале [0; 1] и определяется при помощи экспертных, статистических и прочих методов, рассмотренных подробнее в пункте 1.3.2 диссертационной работы. Прогнозирование вероятности рисковых событий с приемлемой точностью является весьма трудоемкой задачей, вследствие чего получить точную количественную оценку сложно. Вместе с тем объективная количественная оценка рисков позволяет повысить качество выбора защитных мер для ИС.

Величина ущерба в результате реализации угрозы при количественной оценке рисков определяется в стоимостных показателях. Поскольку вероятность является безразмерной величиной, единица измерения риска соответствует выбранной единице измерения ущерба.

При оценке величины ущерба от реализации угрозы необходимо учитывать различные последствия, подразделяемые на материальные (финансовые) и нематериальные (репутационные, ущерб окружающей среде и прочие). Для оценки величины ущерба должны привлекаться профильные специалисты: экономисты, юристы, экологи, специалисты по охране труда и другие.

Показатели вероятности и ущерба могут быть по-разному декомпозированы, в результате чего формула (1) становится более детализированной. Зачастую в литературе, посвященной вопросам ИБ, риск определяется по формуле [4, 74]:

$$R = p_T \cdot p_V \cdot q, \quad (2)$$

где p_T – вероятность возникновения угрозы;

p_V – вероятность использования уязвимости.

Формула (2) может быть детализирована посредством добавления в нее показателей, характеризующих эффективность реализованных защитных мер [115]:

$$R = p_T \cdot (1 - E_v) \cdot p_V \cdot (1 - E_q) \cdot q, \quad (3)$$

где E_v – эффективность защитных мер, направленных на предотвращение уязвимости;

E_q – эффективность защитных мер, направленных на снижение последствий.

Стоит отметить, что формулы (1)-(3) справедливы, если риск определяется для одной угрозы и одной уязвимости. Пусть модель угроз безопасности ИС, состоящей из K элементов, содержит X угроз и Y уязвимостей. Угроза может быть реализована посредством использования одной из нескольких уязвимостей. Если предположить, что данные уязвимости независимы, то вероятность нарушения безопасности k-го элемента ИС в результате реализации x-ой угрозы $p(k \mid x)$ можно определить по формуле:

$$p(k \mid x) = p_T(x) \cdot \left(1 - \prod_{y=1}^{Y} (1 - p_V(x \mid y))\right), \quad (4)$$

где $p_T(x)$ – вероятность возникновения x-ой угрозы;

$p_V(x \mid y)$ – вероятность использования y-ой уязвимости x-ой угрозой.

Если предположить, что угрозы независимы, то риск безопасности k-го элемента ИС $R(k)$ может быть определен по формуле:

$$R(k) = \sum_{x=1}^{X} p(k \mid x) \cdot q(k), \quad (5)$$

где $q(k)$ – величина ущерба от нарушения безопасности k-го элемента ИС.

Формула (5) имеет существенный недостаток – в ней многократно учитываются одни и те же последствия, наступающие при реализации разных угроз. Например, повреждение сервера может быть вызвано пожаром,

затоплением, физическим воздействием со стороны человека, неправильной эксплуатацией либо естественным износом оборудования. При этом значение риска, определенного по формуле (5), может превысить реальный ущерб от повреждения сервера.

Если предположить, что угрозы приводят к одинаковым последствиям, то риск безопасности элемента ИС может быть определен по формуле:

$$R(k) = \left(1 - \prod_{x=1}^{X} \left(1 - p(k \mid x)\right)\right) \cdot q(k) . \qquad (6)$$

Формула (6) основана на трудновыполнимом ограничении, поскольку, как правило, различные угрозы приводят к разным последствиям.

В случае если величина ущерба определяется отдельно для нарушения каждого из свойств безопасности элемента ИС, риск быть определен по формуле [91]:

$$R(k) = p(k_C) \cdot q(k_C) + p(k_M) \cdot q(k_M) + p(k_U) \cdot q(k_U) , \qquad (7)$$

где $p(k_C)$, $p(k_M)$, $p(k_U)$ – значения вероятности нарушения конфиденциальности, целостности и доступности k-го элемента ИС;

$q(k_C)$, $q(k_M)$, $q(k_U)$ – значения ущерба, возникающего при нарушении конфиденциальности, целостности и доступности k-го элемента ИС.

Полный риск R_{IS} определяется как сумма рисков безопасности элементов ИС до внедрения защитных мер:

$$R_{IS} = \sum_{k=1}^{K} R(k) . \qquad (8)$$

В методике оценки рисков компании Microsoft [164] и методике RiskWatch [4] вместо показателя «риск» используется показатель *ALE* (*Annual Loss Expectancy*), определяемый по формуле:

$$ALE = Asset\,Value \cdot Explosure\,Factor \cdot Frequency , \qquad (9)$$

где *Asset Value* – стоимость элемента ИС;

Exposure Factor – коэффициент воздействия, характеризующий, какая часть (в процентах) от стоимости элемента ИС подвергается риску;

Frequency – частота реализации угрозы.

Показатель *ALE* может быть также рассчитан по формуле:

$$ALE = ARO \cdot SLE, \quad (10)$$

где *ARO* (*Annualized Rate of Occurrence*) – ожидаемая годовая частота реализации угрозы;

SLE (*Single Loss Expectancy*) – ожидаемый единичный ущерб, определяемый как разница между первоначальной стоимостью элемента ИС и его остаточной стоимостью после реализации угрозы.

Таким образом, во всех рассмотренных формулах риска (1)-(7) и близкого к нему показателя *ALE* (9)-(10), можно выделить две главные составляющие:

- вероятность (частота) возникновения рискового события (реализации угрозы, нарушения свойства элемента ИС);
- величина ущерба от возникновения рискового события.

1.1.3 Характеристика процесса оценки рисков информационной безопасности

Оценка рисков представляет собой набор взаимосвязанных действий, преобразующих исходные данные (сведения об активах, угрозах, уязвимостях и прочие) в выходные данные (перечень и значения рисков), то есть является процессом. В свою очередь, процесс оценки рисков является частью (подпроцессом) процесса управления рисками.

Схема процесса управления рисками в соответствии с международными стандартами ISO/IEC 27005:2011 [152] и ISO 31000:2009 [155] приведена на рисунке 2. Процесс оценки рисков состоит из последовательных процедур идентификации, анализа и сравнительной оценки рисков.

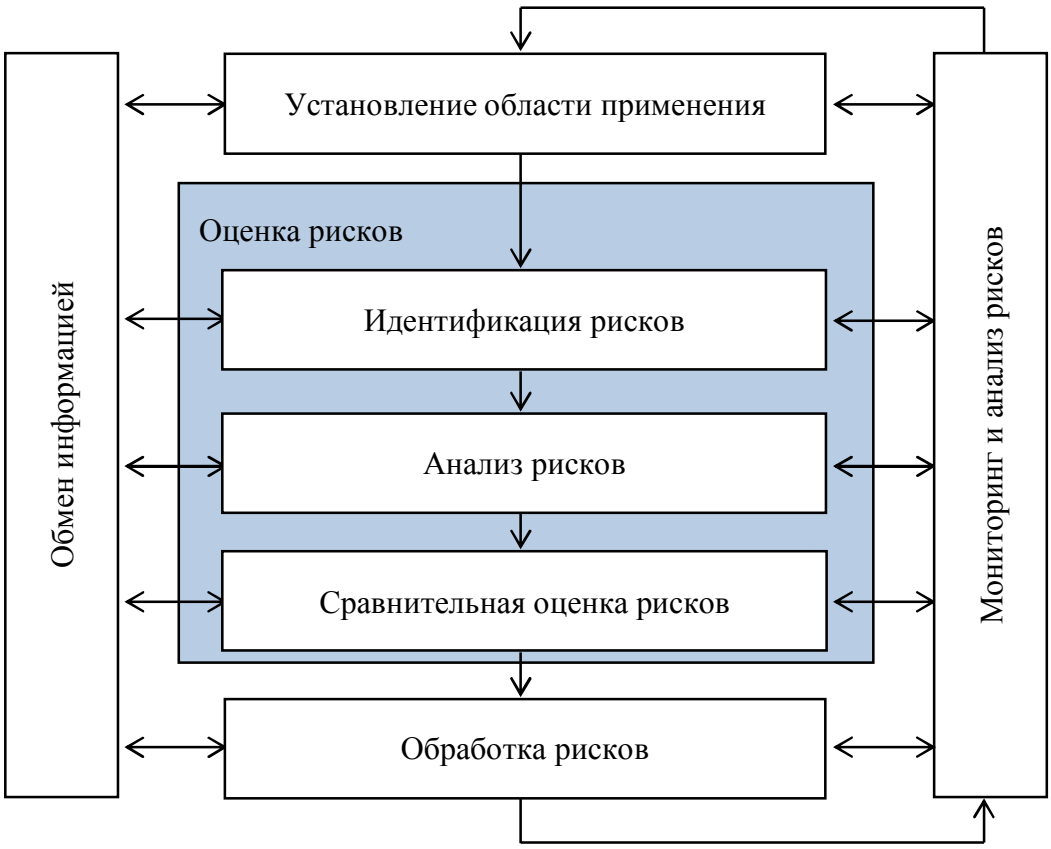

Рисунок 2 – Схема процесса управления рисками

Идентификация рисков проводится с целью сбора информации об активах (объектах защиты), уязвимостях, реализованных защитных мерах, угрозах, источниках угроз и последствиях. В ходе анализа рисков определяются значения параметров: вероятности возникновения угрозы, вероятности использования уязвимости, величины ущерба и прочих. Процедура сравнительной оценки рисков с установленными уровнями проводится с целью определения значимости рисков для деятельности предприятия и необходимости их дальнейшей обработки. Особенности выполнения процедур процесса оценки рисков рассмотрены в подразделе 1.2 диссертационной работы.

Процесс оценки рисков может быть применен на всех стадиях жизненного цикла ИС [38, 156]. Кроме процесса оценки рисков выделяют следующие процессы в рамках управления рисками:

– установление области применения (контекста) заключается в определении критериев оценки и принятия рисков, а также границ и области применения процесса управления рисками;

- обработка рисков представляет собой процесс выбора и реализации мер по модификации рисков [129];
- обмен информацией о рисках направлен на достижение договоренности во всех аспектах процесса управления рисками между причастными сторонами;
- мониторинг и анализ рисков проводится с целью контроля изменений факторов, влияющих на оценку рисков и принятие решений по обработке рисков.

1.2 Сравнительный анализ стандартов и методик в части реализации процедур оценки рисков

За последние двадцать лет появился целый ряд стандартов в области ИБ, в которых освещены вопросы управления рисками. Наибольшее распространение получил международный стандарт ISO/IEC 27005:2011 [152], прародителем которого является Британский стандарт BS 7799-2:2002 [141]. В США для управления рисками ИБ используются стандарты NIST SP серии 800 [166-168]. При этом база нормативно-методических документов в области управления рисками продолжает пополняться.

Помимо стандартов большой вклад в развитие теории информационных рисков внесли научные группы и компании в сфере ИТ, разработавшие различные методики оценки рисков [8]. В диссертационной работе рассматриваются наиболее значимые из них: CRAMM, RiskWatch, OCTAVE, ГРИФ и руководство Microsoft.

Проведен сравнительный анализ стандартов и методик в части выполнения процедур идентификации, анализа и сравнительной оценки рисков, в ходе которого рассмотрены следующие документы:

а) международные стандарты ISO/IEC серий 27000 и 31000, в том числе:
   - ISO/IEC 27005:2011. Information technology. Security techniques. Information security risk management [152];

- ISO/IEC 31000:2009. Risk management. Principles and guidelines. ISO, 2009 [154];
- ISO/IEC 31010:2009. Risk management. Risk assessment techniques [155];

б) стандарты NIST SP серии 800 в области управления рисками, в том числе:

- NIST SP 800-30. Risk Management Guide for Information Technology Systems [166];
- NIST 800-37. Guide for Applying the Risk Management Framework to Federal Information Systems [167];
- NIST SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View [168];

в) стандарты и рекомендации ПАО «Газпром», в том числе:

- Р Газпром 4.2-3-003-2015. Система обеспечения информационной безопасности ОАО «Газпром». Методика оценки рисков [115];
- СТО Газпром 4.2-3-003-2009. Система обеспечения информационной безопасности ОАО «Газпром». Анализ и оценка рисков [129];

г) РС БР ИББС-2.2-2009. Методика оценки рисков нарушения информационной безопасности [117];

д) BSI Standard 100-3. Risikoanalyse auf der Basis von IT-Grundschutz [142];

е) Metodología de Análisis y Gestiónde Riesgos de los Sistemas de Información (MAGERIT) [162];

ж) Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS). Méthode de Gestion des Risques [146];

з) Payment Card Industry Data Security Standard (PCI DSS). Risk Assessment Guidelines [173];

и) методология Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [170];

к) CCTA Risk Analysis and Management Method (CRAMM) [3, 4];

л) методика ГРИФ компании «Digital security» [88];

м) методика анализа и контроля рисков RiskWatch [3, 4];

н) руководство по управлению рисками от компании Microsoft [164];

При описании результатов сравнительного анализа при перечислении стандартов и методик для удобства восприятия используются буквенные обозначения из приведенного выше нумерованного списка.

1.2.1 Процедура идентификации рисков

Процедура идентификации рисков является неотъемлемой частью оценки рисков и проводится с целью сбора информации о следующих элементах:

- активы (а, б, в, г, д, е, ж, з, и, к, л, м, н);
- угрозы (а, б, в, г, д, е, ж, з, и, к, л, м, н);
- уязвимости (а, б, в, ж, з, и, к, л, м, н);
- защитные меры (а, б, в, г, д, е, ж, з, и, к, л, м, н);
- последствия (а, б, в, г, д, е, ж, з, и, к, л, м, н).

Набор идентифицируемых элементов одинаков во всех рассмотренных стандартах и методиках, за исключением того, что в (г, д, е) не рассматриваются уязвимости.

В качестве активов обычно рассматриваются:

- информация, данные (а, б, в, г, д, е, ж, з, и, к, л, м, н);
- бизнес-процессы (а, б, г, д, е, з, и, л);
- технические средства (а, б, в, г, д, е, ж, з, и, к, л, м, н);
- программное обеспечение (а, б, в, г, д, е, ж, з, и, к, м, н);
- каналы связи и сети передачи данных (а, б, г, д, е, ж, з, и, л, м, н);
- персонал (а, б, д, е, ж, з, и, к, л, м);
- помещения, здания, сооружения (а, г, д, е, ж, к);
- организационная структура (а, д, л);
- обеспечивающие системы (электропитание, кондиционирование) (д, е);
- третьи стороны (е, ж).

Для сбора исходных данных проводятся следующие мероприятия:

– интервьюирование (а, б, в, г, д, е, ж, з, и, к, л, м, н);
– опросные листы (а, б, в, г, д, е, ж, з, и, к, л, м, н);
– физический осмотр (а, в, ж);
– анализ документации (а, б, в, ж);
– анализ инцидентов (а, б, в, е, з, м);
– инструментальный анализ (а, б, в, ж, и, м, н);
– мозговой штурм (е, и).

Суть интервьюирования заключается в устном опросе персонала, третьих сторон и прочих заинтересованных лиц. Зачастую интервьюирование может быть заменено письменным заполнением опросных листов.

Физический осмотр проводится для идентификации активов и существующих защитных мер. Он может быть заменен или проведен совместно с анализом документации.

Различные инструментальные средства и техники позволяются получить более точные сведения о состоянии защищенности ИС. С помощью инструментального анализа осуществляется идентификация технических уязвимостей, проведение инструментального анализа защищенности, выполнение тестирования на проникновение и анализ кода ПО.

Еще одним мероприятием, выполняемым с целью идентификации рисков, является проведение коллективного обсуждения или, так называемого, мозгового штурма, в ходе которого группой специалистов определяются элементы (активы, угрозы и прочие) и существующие связи между ними.

Результаты сравнительного анализа стандартов и методик в части идентификации рисков представлены в таблице 1.

Таблица 1 – Анализ стандартов и методик в части идентификации рисков

Стандарт / методика	Идентифицируемые элементы					Типы активов										Проводимые мероприятия						
	Активы	Угрозы	Уязвимости	Защитные меры	Последствия	Информация	Бизнес-процессы	Технические средства	Программное обеспечение	Каналы и сети передачи данных	Персонал	Помещения	Организационная структура	Обеспечивающие системы	Третьи стороны	Интервьюирование	Опросные листы	Анализ документации	Физический осмотр	Анализ инцидентов	Инструментальный анализ	Мозговой штурм
а) ISO/IEC серий 27000 и 31000	+	+	+	+	+	+	+	+	+	+	+	+	+	–	–	+	+	+	+	+	+	–
б) NIST SP серии 800	+	+	+	+	+	+	+	+	+	+	+	–	–	–	–	+	+	+	–	+	+	–
в) Стандарты ПАО «Газпром»	+	+	+	+	+	+	–	+	+	–	–	–	–	–	–	+	+	+	+	+	+	–
г) РС БР ИББС-2.2-2009	+	+	–	+	+	+	+	+	+	+	–	+	–	–	–	+	+	–	–	–	–	–
д) BSI-Standard 100-3	+	+	–	+	+	+	+	+	+	+	+	+	+	+	–	+	+	–	–	–	–	–
е) MAGERIT	+	+	–	+	+	+	+	+	+	+	+	+	–	+	+	+	+	–	–	+	–	+
ж) EBIOS	+	+	+	+	+	+	–	+	+	+	+	+	–	–	+	+	+	+	+	–	+	–
з) PCI DSS	+	+	+	+	+	+	+	+	+	+	+	–	–	–	–	+	+	–	–	+	–	–
и) OCTAVE	+	+	+	+	+	+	+	+	+	+	+	–	–	–	–	+	+	–	–	–	+	+
к) CRAMM	+	+	+	+	+	+	–	+	+	–	+	+	–	–	–	+	+	–	–	–	–	–
л) ГРИФ	+	+	+	+	+	+	+	+	+	+	+	–	+	–	–	+	+	–	–	–	–	–
м) RiskWatch	+	+	+	+	+	+	–	+	+	+	+	–	–	–	–	+	+	–	–	+	+	–
н) Microsoft	+	+	+	+	+	+	–	+	+	+	–	–	–	–	–	+	+	–	–	–	+	–

1.2.2 Процедура анализа рисков

Как уже упоминалось выше, различают качественные и количественные способы оценки рисков. Иногда выделяют также полуколичественную оценку рисков, при котором уровень риска определяется по качественной шкале, значениям которой соответствуют диапазоны количественных значений.

На практике наиболее распространена качественная оценка (а, б, в, г, д, е, ж, з, и, к, л, н), тогда как полуколичественная (а, б, в, г, з, к, н) и количественная (а, б, з, л, м) оценки проводятся реже. При этом полноценная количественная оценка с приведением формул и правил расчета описана лишь в двух подходах (л, м), тогда как в остальных встречается только упоминание о возможности проведения количественной оценки.

Большинство подходов к оценке рисков основано на экспертном оценивании, которое заключается в определении параметров риска на основе мнений специалистов (экспертов).

Суть статистических методов оценки заключается в определении вероятности рисковых событий на основе статистических данных предшествующего периода. Несмотря на то, что во многих подходах (а, б, в, г, е, ж, з, и, к, л, м, н) упоминается возможность использования статистических данных для оценки рисков, полноценное описание статистических методов оценки приведено лишь в трех из них (а, в, м).

Прочие методы оценки параметров риска, например, структурные методы или методы, основанные на моделировании, не освещены в рассмотренных источниках, за исключением стандарта ISO/IEC 31010:2009 (а).

Во всех подходах в том или ином виде риск определяется как комбинация вероятности возникновения рискового события (реализации угрозы) и величины ущерба от данного события. При оценке угрозы определяются следующие показатели:

- вероятность, возможность (а, б, в, г, е, ж, з, и, л);
- частота реализации (е, к, м, н);

– актуальность (д).

Зачастую в зарубежных методиках оценки рисков (б, е) используется термин «likelihood», который переводится дословно как «возможность», вместо используемого в российских методиках (в, л) термина «вероятность». «Вероятность» реализации угрозы, предполагает установление определенного временного периода оценки, например, год или квартал. Под «возможностью» реализации угрозы понимается то, насколько реализуема данная угроза в отношении объекта воздействия при данных условиях.

При оценке вероятности реализации угрозы чаще всего учитываются такие факторы, как:

– мотивация (а, б, в, г, ж, з, и), осведомленность (в) и возможности (а, б, в, г, ж, з) источников угроз;
– имеющиеся уязвимости (а, б, в, ж, з, и, к, л, м, н);
– реализованные защитные меры (а, б, в, г, д, е, ж, з, и, к, л, м, н).

В качестве критических (важных) свойств активов рассматриваются:

– основные свойства: конфиденциальность, целостность, доступность (а, б, в, г, д, е, ж, з, и, к, л, м, н);
– дополнительные свойства: аутентичность, подотчетность, надежность, неотказуемость (а, в, е);

Чаще всего при оценке ущерба учитываются следующие категории последствий:

– финансовые (а, б, в, г, е, ж, з, и, к, л, м, н);
– правовые (а, в, г, е, и, к, н);
– репутационные (а, б, в, г, е, и, к, м, н);
– ущерб жизни и здоровью людей (а, б, в, е, и, к, м);
– ущерб окружающей среде (природе) (а, в, е).

Результаты сравнительного анализа стандартов и методик в части анализа рисков представлены в таблице 2.

Таблица 2 – Анализ стандартов и методик в части анализа рисков

Стандарт / методика	Способы оценки[1)]			Методы оценки			Оценка вероятности								Оценка ущерба						
							Оцениваемые показатели			Учитываемые факторы					Значимые свойства		Категории последствий				
	Качественные	Полуколичественные	Количественные	Экспертные	Статистические	Прочие	Вероятность	Частота	Актуальность	Мотивация источника	Возможности источника	Осведомленность источника	Уязвимости	Защитные меры	Основные свойства	Дополнительные свойства	Финансовые	Правовые	Репутационные	Ущерб жизни и здоровью	Ущерб природе
а) ISO/IEC серий 27000 и 31000	+	±	±	+	+	+	+	–	–	+	+	–	+	+	+	+	+	+	+	+	+
б) NIST SP серии 800	+	+	±	+	–	–	+	–	–	+	+	–	+	+	+	–	+	–	+	+	–
в) Стандарты ПАО «Газпром»	+	+	–	+	+	–	+	–	–	+	+	+	+	+	+	+	+	+	+	+	+
г) РС БР ИББС-2.2-2009	+	+	–	+	–	–	+	–	–	+	+	–	–	+	+	–	+	+	+	–	–
д) BSI-Standard 100-3	+	–	–	+	–	–	–	–	+	–	–	–	–	+	+	–	–	–	–	–	–
е) MAGERIT	+	–	–	+	–	–	+	+	–	–	–	–	–	+	+	+	+	+	+	+	+
ж) EBIOS	+	–	–	+	–	–	+	–	–	+	+	–	+	+	+	–	+	–	–	–	–
з) PCI DSS	+	±	±	+	–	–	+	–	–	+	+	–	+	+	+	–	+	–	–	–	–
и) OCTAVE	+	–	–	+	–	–	+	–	–	+	–	–	+	+	+	–	+	+	+	+	–
к) CRAMM	+	+	–	+	–	–	–	+	–	–	–	–	+	+	+	–	+	+	+	+	–
л) ГРИФ	+	–	+	+	–	–	+	–	–	–	–	–	+	+	+	–	+	–	–	–	–
м) RiskWatch	–	–	+	+	+	–	–	+	–	–	–	–	+	+	+	–	+	–	+	+	–
н) Microsoft	+	+	–	+	–	–	–	+	–	–	–	–	+	+	+	–	+	+	+	–	–

[1)] Знак «±» означает, что в стандарте упоминается данный способ оценки, но не приводятся конкретные рекомендации (шкалы, формулы)

1.2.3 Процедура сравнительной оценки рисков

В ходе сравнительной оценки рисков чаще всего выполняются следующие операции:

– объединение рисков (в, е);

– ранжирование рисков (а, б, в, д, е, ж, з, и, к, л, м, н);

– принятие решения по обработке рисков (а, б, в, д, е, ж, з, и, к, л, м, н).

В зависимости от целей и задач, риски могут быть объединены для определенной угрозы, актива, ИС, бизнес-процесса или предприятия в целом.

Ранжирование рисков ИБ позволяет определить приоритеты и последовательность их обработки.

Результаты сравнительной оценки рисков используются в качестве исходных данных для принятия решений по обработке рисков. В рассмотренных источниках встречаются следующие способы обработки рисков:

– принятие (а, б, в, д, е, ж, з, и, к, л, м, н);

– передача (а, б, в, д, е, ж, з, н);

– избежание (а, б, в, д, е, ж, з, н);

– снижение (а, б, в, д, е, ж, з, и, к, л, м, н);

– планирование (б);

– исследование и уведомление (б).

При обработке риска может быть принято решение о его принятии, то есть сохранении текущего уровня риска. Как правило, принимаются приемлемые риски, величина которых не превышает некоторое пороговое значение.

Еще один способ обработки риска – передача его другой стороне, которая может наиболее эффективно контролировать данный риск. Выделяют два основных способа передачи риска:

– страхование, представляющее собой «отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет

денежных фондов, формируемых из уплачиваемых ими страховых взносов (страховых премий)» [103];

– передача на аутсорсинг деятельности, вызывающей риск, организации, которая должным образом способна контролировать этот риск.

Избежание риска подразумевает отказ от деятельности или условия, вызывающего данный риск. Чаще всего избежание риска выбирается в том случае, если риск превышает выгоду, которая может быть получена от деятельности, вызывающей данный риск, или когда другие способы обработки риска неприменимы.

Снижение риска достигается за счет выбора и применения защитных мер. Выбор защитных мер может быть осуществлен исходя из соблюдения требований стандартов либо путем сопоставления затрат и выгод от их использования.

Планирование риска заключается в разработке плана обработки рисков, который может предусматривать введение определенных приоритетов, реализацию и поддержку защитных мер.

Следующим способом обработки рисков является уведомление о наличии уязвимости или недостатков в системе разработчиков для дальнейшего исследования возможностей исправления данной уязвимости.

Результаты сравнительного анализа стандартов и методик в части сравнительной оценки и обработки рисков представлены в таблице 3.

Таким образом, рассмотренные стандарты и методики оценки рисков отличаются используемыми шкалами оценки, перечнями угроз и уязвимостей, составом исходных данных, необходимых для оценки, и перечнем мероприятий, проводимых для получения исходных данных. Вместе с тем, почти во всех рассмотренных источниках оценка рисков проводится посредством пошаговой оценки параметров рисков экспертом или группой экспертов на основании собственных знаний и опыта, а иногда – статистических данных, что существенно затрудняет формализацию процесса оценки рисков безопасности ИС.

Таблица 3 – Анализ стандартов и методик в части сравнительной оценки и обработки рисков

Стандарт / методика	Операции			Способы обработки рисков					
	Объединение рисков	Ранжирование рисков	Принятие решение по обработке рисков	Принятие	Передача	Избежание	Снижение	Планирование	Исследование и уведомление
а) ISO/IEC серий 27000 и 31000	–	+	+	+	+	+	+	–	–
б) NIST SP серии 800	–	+	+	+	+	+	+	+	+
в) Стандарты ПАО «Газпром»	+	+	+	+	+	+	+	–	–
г) РС БР ИББС-2.2-2009	–	–	–	–	–	–	–	–	–
д) BSI-Standard 100-3	–	+	+	+	+	+	+	–	–
е) MAGERIT	+	+	+	+	+	+	+	–	–
ж) EBIOS	–	+	+	+	+	+	+	–	–
з) PCI DSS	–	+	+	+	+	+	+	–	–
и) OCTAVE	–	+	+	+	–	–	+	–	–
к) CRAMM	–	+	+	+	–	–	+	–	–
л) ГРИФ	–	+	+	+	–	–	+	–	–
м) RiskWatch	–	+	+	+	–	–	+	–	–
н) Microsoft	–	+	+	+	+	+	+	–	–

1.3 Существующие проблемы количественной оценки рисков безопасности информационных систем и способы их решения

Как упоминалось выше, объективная количественная оценка рисков способствует повышению качества выбора защитных мер для ИС. Вместе с тем, получение точных количественных значений рисков затруднено рядом проблем. Рассмотрим основные проблемы и возможные способы их решения.

1.3.1 Декомпозиция рисков безопасности информационных систем

Проведенный анализ стандартов и методик оценки рисков показал, что чаще всего риск отождествляется с угрозой или с комбинацией угрозы и уязвимости, а, следовательно, под рисковым событием понимается реализация угрозы. Это влечет за собой следующие недостатки и ограничения:

- число возможных угроз, вероятность реализации которых нужно оценить, может быть велико и зависит от степени детализации перечня угроз;
- регулярно появляются новые угрозы и способы их реализации, поэтому ни один из существующих перечней угроз нельзя считать полным;
- угроза чаще всего является внешней по отношению к ИС и зависит от многих неконтролируемых факторов, вследствие чего вероятность ее реализации трудно спрогнозировать;
- трудно учесть причинно-следственные связи между рисковыми событиями, поскольку необходимо учитывать связи как между элементами ИС, так и между угрозами;
- возникает проблема объединения рисков и расчета полного риска безопасности ИС с использованием формул (5) и (6).

Для устранения обозначенных недостатков и ограничений в диссертационной работе в качестве рискового события предлагается рассматривать не реализацию отдельной угрозы, а переход элемента КИС в деструктивное состояние. Понятие «деструктивное состояние», предложенное в диссертационной работе, означает нежелательное и незапланированное состояние элемента КИС, в котором он оказался в результате реализации одной или нескольких угроз [97].

Соответственно, риск предлагается определять как произведение вероятности перехода элемента КИС в деструктивное состояние на величину возникающего при этом ущерба. Например, если для элемента определено три деструктивных состояния, соответствующих нарушению его

конфиденциальности, целостности и доступности, то риск безопасности данного элемента рассчитывается по формуле (7).

Данный подход требует, во-первых, проведения классификации элементов КИС, а во-вторых, определения деструктивных состояний для элементов каждого типа. Данные вопросы рассмотрены в разделе 2 диссертационной работы.

1.3.2 Прогнозирование вероятности рискового события

Одна из главных проблем существующих подходов к оценке рисков ИБ заключается в сложности получения объективных количественных оценок. И если величину ущерба посчитать можно, то прогнозирование вероятности рискового события с приемлемой точностью является весьма трудоемкой и трудновыполнимой задачей [15].

Рассмотрим применяемые на практике методы прогнозирования вероятности случайного события. Все многообразие методов прогнозирования можно разделить на экспертные (интуитивные) и формализованные [130].

На практике, чаще всего, вероятность рискового события определяется экспертными методами, что вызывает скептическое отношение к таким оценкам ряда специалистов, ориентированных на решение практических задач [4, 110]. Это обусловлено, прежде всего, следующими недостатками экспертных методов оценки [4, 16]:

- субъективность экспертных суждений;
- высокая степень неопределенности и отсутствие гарантии достоверности полученных результатов;
- невозможность динамической переоценки без повторного привлечения экспертов.

Тем не менее, экспертные методы оценки обладают радом преимуществ, среди которых стоит отметить простоту реализации и нетребовательность к исходным данным.

Экспертные методы прогнозирования подразделяется на индивидуальные и коллективные (групповые) методы [122]. В стандарте ISO/IEC 31010:2009

выделяются следующие экспертные методы, позволяющие осуществлять количественную оценку вероятности рискового события: метод Дельфи, анализ сценариев, анализ дерева событий, анализ причин и последствий, анализ «галстук-бабочка», мультикритериальный анализ и другие [155]. В настоящее время также применяются экспертные методы оценки рисков, основанные на использовании нечеткой логики [1, 24, 57, 62, 78, 80,116, 124]. В работе [137] для оценки рисков ИБ используется метод анализа иерархий.

Формализованные методы прогнозирования подразделяются на статистические методы, структурные методы и методы моделирования.

В статистических методах зависимость будущего значения от прошлого задается в виде некоторого уравнения. К статистическим относятся такие методы прогнозирования как экстраполяция и интерполяция, корреляционный и регрессионный анализ, факторный анализ и многие другие [10, 81, 82, 123]. Методы статистического анализа для оценки рисков применяются в стандарте [164], а также в работах [58, 138, 139]. Байесовские методы оценки вероятности рискового события используются в работах [5, 57, 107, 163].

Сложность использования статистических методов для прогнозирования вероятности рискового события обусловлена следующими причинами:

- недостаток статистических данных об инцидентах (реализованных угрозах) в открытых источниках;
- большое количество угроз, для прогнозирования вероятности реализации которых необходимо учитывать разные факторы (признаки);
- быстро меняется окружение (элементы ИС, уязвимости, инфраструктура), что также препятствует сбору статистических данных;
- в опубликованных обзорах чаще всего приводятся только результирующие значения (количество или частота реализации определенных угроз), при этом редко учитываются факторы (признаки), влияющие на реализацию угрозы, например, уязвимости и реализованные защитные меры.

В структурных методах зависимость значения прогнозируемой величины задается в виде некоторой структуры и правил перехода по ней. К методам данной группы относятся нейросетевые методы [109, 134], методы на базе конечных автоматов [12, 47], цепей Маркова [56], сетей Петри [112] и прочие. В работе [5] прогнозирование вероятности рискового события осуществляется на базе модели, представляющей многослойный персептрон, а в работе [73] предложена методика моделирования рисков ИБ на основе сети Петри.

Использование структурных методов для прогнозирования вероятности рискового события затруднено, поскольку модель оценки вероятности реализации для каждой угрозы имеет свои особенности, которые необходимо учитывать. В то же время процедура формирования модели оценки трудоемка, а для корректного обучения модели, как правило, требуется большой объем обучающей выборки.

Моделирование заключается в построении и изучении математической модели процесса или явления. Выделяют следующие методы моделирования: математическое, имитационное, структурное, сетевое, матричное, моделирование методом Монте-Карло и другие. Для оценки рисков применяются методы моделирования с использованием когнитивных карт [127], логико-вероятностного моделирования [68] и имитационного моделирования [73].

Стоит отметить, что для прогнозирования вероятности рискового события на практике сравнительно редко используются методы моделирования, что обусловлено, во-первых, сложностью моделей, а во-вторых, как правило, низкой точностью получаемых с их помощью результатов.

Формализованные методы прогнозирования также подразделяются на:

- параметрические, применение которых требует обязательного знания закона распределения изучаемых признаков в совокупности и вычисления их основных параметров;
- непараметрические, применение которых не требует знания закона распределения изучаемых признаков в совокупности и вычисления их основных параметров.

Интерес представляют работы [48, 65, 69, 70, 71, 72, 96, 148, 158, 171, 176], в которых рассмотрена возможность количественной оценки рисков безопасности корпоративной сети на основе графов атак и общей методики оценки уязвимостей Common Vulnerability Scoring System (CVSS) [161].

Для компенсирования недостатков одних методов при помощи других в диссертационной работе предлагается использовать комбинированный подход к оценке рисков, сочетающий экспертные, статистические и структурные методы прогнозирования. Функция вероятности рискового события может быть задана аналитически группой квалифицированных экспертов, а ее дальнейшая аппроксимация осуществляться с использованием статистических и структурных методов.

Также в разрабатываемой модели оценки рисков следует учесть различия, характерные для естественных и антропогенных источников угроз. Прогнозирование вероятности рисковых событий, вызванных естественными источниками угроз, целесообразно осуществлять на основе имеющихся статистических данных с применением некоторого закона распределения, характерного для случайных событий. При оценке вероятности рисковых событий, вызванных нарушителями, необходимо учитывать ряд показателей, характеризующих степень опасности нарушителей и степень реализации защитных мер, направленных на обнаружение и предотвращение угроз.

Выводы по разделу 1

1. Проведенный анализ существующих стандартов и методик оценки рисков показал, что чаще всего оценка параметров риска осуществляется по некоторым качественным шкалам экспертом или группой экспертов, что затрудняет формализацию процесса оценки рисков.
2. Распространенность качественной оценки рисков связана с тем, что количественная оценка вероятности рискового события весьма затруднена ввиду отсутствия четких требований к составу исходных

данных, правил оценки (математической модели) и недостатка статистических данных.

3. Выявлены следующие ограничения в применении рассмотренных подходов к оценке рисков безопасности ИС:
   - сложность получения объективной количественной оценки рисков;
   - трудоемкость детализированной оценки рисков;
   - невозможность динамической переоценки рисков при изменении входных данных без повторного привлечения экспертов.
4. В качестве рискового события предлагается рассматривать переход элемента КИС в деструктивное состояние, возникающий в результате реализации одной или нескольких угроз.
5. Прогнозирование вероятности рискового события с приемлемой точностью является нетривиальной задачей, для решения которой предлагается использовать комбинацию экспертных, статистических и структурных методов.
6. Для повышения качества выбора защитных мер для КИС необходимо разработать формализованную модель оценки рисков, учитывающую связи между рисковыми событиями.

2 Разработка модели оценки рисков и методики формирования рационального комплекса защитных мер для корпоративной информационной системы

2.1 Корпоративные информационные системы

В конце XX века появился новый класс ИС, приобретающий особую популярность в наши дни, – корпоративные информационные системы. На сегодняшний день КИС являются важным инструментом повышения эффективности бизнес-процессов для многих крупных и средних предприятий топливно-энергетического комплекса, транспортной и финансовой сферы и сферы государственного управления.

2.1.1 Характерные особенности и отличительные признаки корпоративной информационной системы

Наиболее полное определение КИС приведено в [95]: «это открытая интегрированная система реального времени, автоматизирующая бизнес-процессы компании всех уровней и направлений деятельности, в том числе бизнес-процессы принятия управленческих решений».

Выделяют следующие отличительные признаки КИС [17, 95]:

- широкий круг решаемых задач, включающий задачи информационного обеспечения, планирования и управления деятельностью предприятия;
- охват различных сфер управления предприятием (управление производством, финансами, персоналом и так далее);
- поддержка всех или большинства основных и обеспечивающих бизнес-процессов предприятия;
- открытость и масштабируемость как по охватываемым функциям, так и по охватываемым территориям.

КИС являются многопользовательскими распределенными системами, состоящими из множества модулей, автоматизирующих различные бизнес-

процессы предприятия. Допускаются различные варианты реализации КИС, однако предпочтение отдается клиент-серверной многозвенной архитектуре, что обусловлено большим объемом данных, обрабатываемых в КИС [17, 114].

В литературе встречаются различные мнения по поводу того, какие системы следует относить к КИС. Так, в [95] сказано, что КИС формируется на базе единой интеграционной платформы, например, SAP или 1С, и состоит из модулей, для которых характерна сквозная интеграция. В [114] допускается, что КИС может состоять из множества аппаратно-программных платформ и приложений различных разработчиков, интегрированных в единую ИС предприятия. В диссертационной работе под КИС понимается интегрированная ИС, состоящая из множества взаимосвязанных модулей, которые могут быть реализованы с использованием различных программно-аппаратных платформ.

Как правило, КИС содержит различные учетные модули (модуль бухгалтерского учета, модуль кадрового учета и прочие), модуль электронного документооборота, модуль ведения договорной деятельности и ряд других модулей, автоматизирующих основные и обеспечивающие бизнес-процессы предприятия. Пример модульной структуры КИС представлен на рисунке 3.

Рисунок 3 – Пример модульной структуры КИС

КИС включает в себя инфраструктуру и прикладные системы и сервисы. К инфраструктуре относятся серверы, автоматизированные рабочие места (АРМ),

активное сетевое оборудование (АСО), системное и сетевое ПО, сети связи. Прикладные системы могут быть представлены в виде модулей интеграционной платформы либо в виде прикладного ПО. К прикладным сервисам относятся сервис электронной почты, сервис сетевой печати, сервис удаленного доступа и другие.

Еще одной особенностью КИС является использование единого корпоративного хранилища данных [17, 95, 114]. Для небольших предприятий корпоративное хранилище данных может быть реализовано в виде одной или нескольких взаимосвязанных баз данных (БД), а для крупных предприятий с распределенной филиальной структурой – в виде центра обработки данных (ЦОД). Пример структурной схемы КИС с ЦОД представлен на рисунке 4.

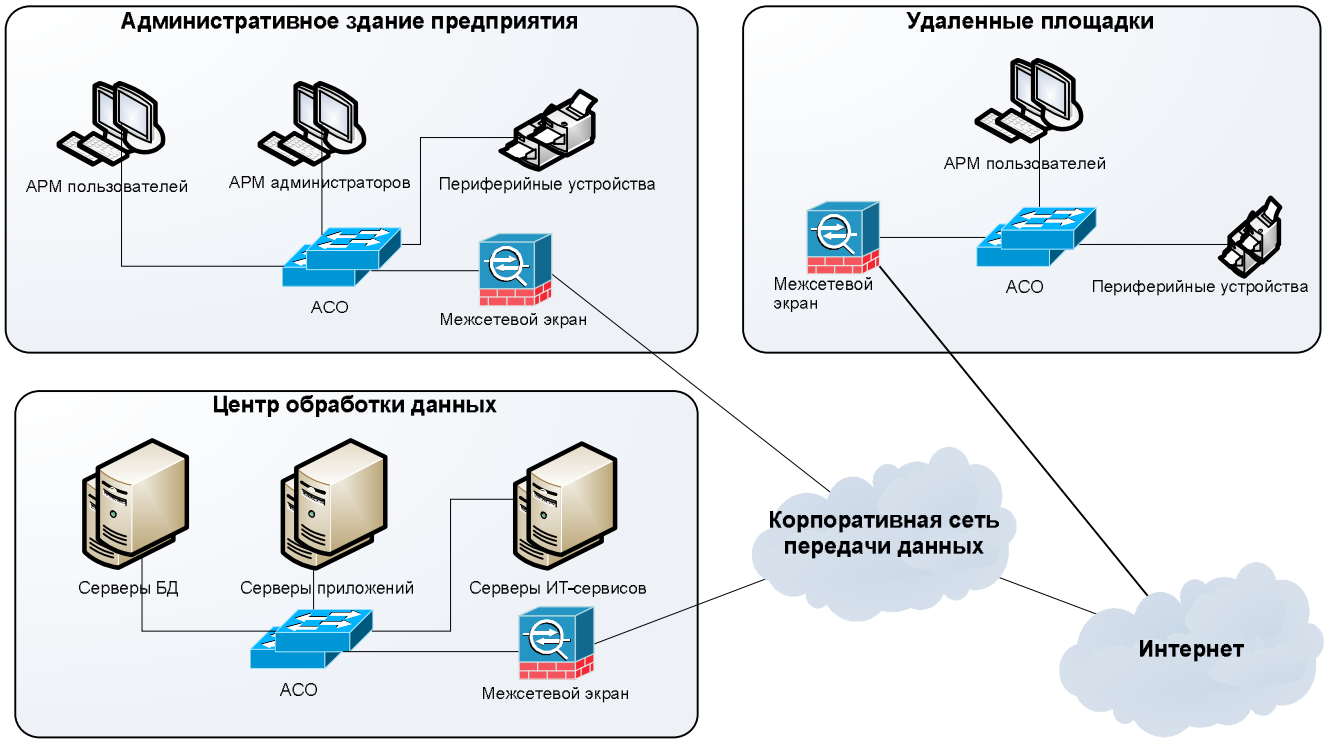

Рисунок 4 – Пример структурной схемы КИС с ЦОД

К КИС, как правило, предъявляются повышенные требования к обеспечению ИБ, включая требования к обеспечению конфиденциальности, целостности и доступности ИА, что обусловлено характером решаемых задач. Модули КИС рекомендуется размещать на разных физических серверах, а серверы БД и серверы приложений наиболее критичных модулей рекомендуется резервировать.

КИС ориентирована, прежде всего, на повышение эффективности бизнеса и максимизацию прибыли компании [95], поэтому выбор защитных мер для обеспечения безопасности КИС должен исходить из позиции рациональности затрат на их реализацию.

2.1.2 Стадии жизненного цикла корпоративной информационной системы

Жизненный цикл любой ИС – это «непрерывный процесс, начинающийся с момента принятия решения о создании информационной системы и заканчивающийся в момент полного изъятия ее из эксплуатации» [111]. Следовательно, жизненный цикл КИС, как и любой системы, можно представить в виде «…последовательности стадий, которые могут перекрываться и (или) повторяться циклически…» [35].

Анализ стандартов [29, 35, 38, 153] и прочих источников [17, 53, 111, 114], в которых рассматриваются вопросы жизненного цикла АС, ИС и ПО, показал, что на данный момент нет единого мнения о составе стадий жизненного цикла КИС. Последовательность стадий жизненного цикла КИС, сформированная на основе анализа указанных выше источников и опыта проектирования и внедрения систем, представлена на рисунке 5.

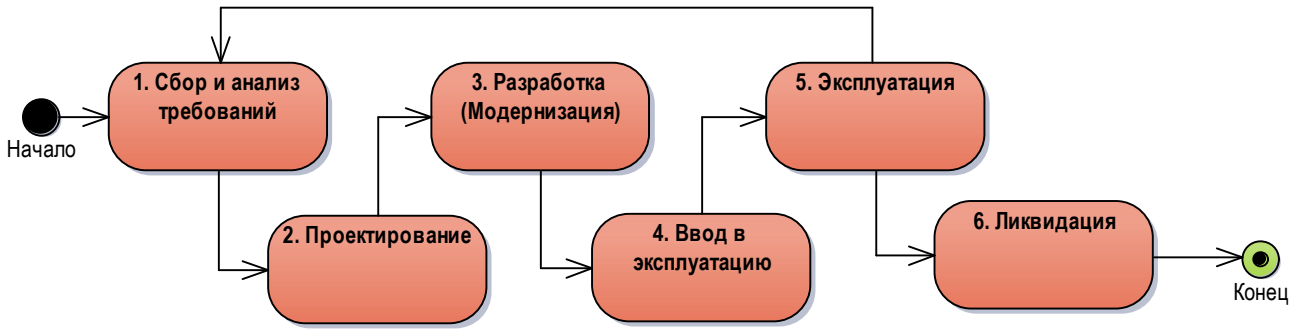

Рисунок 5 – Стадии жизненного цикла КИС

Прежде всего, к разрабатываемой или модернизируемой КИС должны быть предъявлены требования со стороны заинтересованных сторон. В соответствии с ISO/IEC/IEEE 29148:2011 заинтересованная сторона – это «физическое лицо или организация, имеющая права, долю, требования или интересы

относительно системы или ее свойств, удовлетворяющих их потребностям и ожиданиям» [153]. Таким образом, заинтересованными сторонами могут быть заказчики, пользователи системы, инвесторы, разработчики, поставщики, кредиторы, регулирующие органы и прочие лица и организации.

Требования подразделяются на функциональные, определяющие состав выполняемых системой действий (функций), и нефункциональные, определяющие критерии работы системы в целом, а не отдельные сценарии поведения. Примерами нефункциональных требований являются требования к производительности, расширяемости, надежности, удобству сопровождения и безопасности системы.

Собранные требования анализируются, группируются и документируются. На основе данных требований формируется техническое задание на создание (модернизацию) КИС [30].

На стадии проектирования осуществляется выбор проектных решений и разработка комплекта проектной документации. Типовой состав проектной документации приведен в ГОСТ 34.201-89 [28].

На стадии разработки происходит получение и установка ТС и ПО, а также разработка эксплуатационной документации. Кроме того, стадия разработки включает процедуры тестирования и отладки. Модернизация существующей КИС, как правило, включает тот же набор процедур, что и разработка КИС.

На стадии ввода в эксплуатацию КИС осуществляется ввод ТС и ПО в эксплуатацию, обучение персонала, опытная эксплуатация КИС и подписание актов приемки-сдачи работ.

Стадия эксплуатации включает, непосредственно, повседневную эксплуатацию КИС и ее техническое сопровождение. Поскольку основным предназначением КИС является обеспечение бизнес-процессов предприятия и повышение эффективности бизнеса, она может быть подвержена частым изменениям. Некоторые из этих изменений достаточно существенные и требуют реализации полноценного проекта по модернизации КИС, то есть повторного прохождения стадий 1-4 жизненного цикла. Примером модернизации КИС может

служить переход на новую интеграционную платформу. Чаще всего модернизация КИС происходит параллельно с ее эксплуатацией, а применение обновлений, влияющих на работу КИС, осуществляется в наименее критичное время, например, ночью или в выходные дни.

На стадии ликвидации осуществляется вывод КИС из эксплуатации. При необходимости осуществляется удаление ПО и информации, демонтаж ТС, подписание актов ликвидации.

Формирование СЗИ КИС начинается, как правило, на стадии проектирования КИС, а ликвидация СЗИ осуществляется совместно с ликвидацией КИС. Следовательно, для формирования и поддержания в актуальном состоянии СЗИ, состоящей из рационального комплекса защитных мер, необходимо осуществлять оценку рисков, начиная со стадии проектирования и заканчивая стадией ликвидации КИС.

2.1.3 Классификация защитных мер для корпоративных информационных систем

В зависимости от масштабов, характера обрабатываемой информации, области применения и прочих особенностей КИС осуществляется выбор защитных мер для обеспечения безопасности ее элементов. По способам осуществления защитные меры подразделяются на:

- технические, реализуемые за счет применения средств защиты информации (СрЗИ), под которыми понимаются «технические, программные, программно-технические средства, вещества и (или) материалы, предназначенные или используемые для защиты информации» [45];
- организационные, включающие законодательные, административные и процедурные меры и мероприятия, направленные на обеспечение ИБ;
- организационно-технические, сочетающие технические СрЗИ и организационные меры.

По характеру воздействия на угрозы защитные меры подразделяются на превентивные и корректирующие [157]. Превентивные меры направлены на обнаружение возможных угроз, определение динамики их эволюции и последующее предотвращение [93]. Корректирующие меры направлены на снижение ущерба от реализованных угроз. Таким образом, значение риска можно уменьшить как за счет использования превентивных защитных мер, снижающих вероятность реализации угроз, так и за счет использования корректирующих защитных мер, снижающих величину ущерба.

В последние годы появился целый ряд стандартов, посвященных защите различных видов информационных и автоматизированных систем, в частности, ИС персональных данных [104], АС управления производственными и технологическими процессами [105] и государственных ИС [106].

При этом в российских нормативных документах не приводится перечень защитных мер для КИС. При проектировании СЗИ КИС чаще всего ориентируются на требования документов [104, 118], а также на требования документа [106], если речь идет о государственных ИС. Защитные меры, имеющие схожие цели и принципы функционирования, группируются в категории.

В диссертационной работе сформирован перечень защитных мер для КИС основанный на перечне защитных мер, приведенных в Приказе ФСТЭК России от 18.02.2013 № 21 [104] со следующими изменениями:

- исключены защитные меры, относящиеся к категории «Защита средств виртуализации», поскольку они применимы только для средств виртуализации и дублируют защитные меры других категорий;
- добавлены защитные меры категории «Криптографическая защита», приведенные в нормативном документе [118].

Перечень категорий защитных мер для КИС, используемый в диссертационной работе, представлен в таблице 4. Данный перечень при необходимости может быть дополнен и детализирован.

Таблица 4 – Перечень категорий защитных мер для КИС

Наименование категории	Условное обозначение	Краткое описание	Число мер	Тип мер
1. Идентификация и аутентификация субъектов доступа и объектов доступа	ИАФ	Использование механизмов идентификации и аутентификации пользователей, процессов, устройств	6	Превентивные
2. Управление доступом субъектов доступа к объектам доступа	УПД	Управление правами и привилегиями субъектов доступа, разграничение доступа на основе установленных правил	17	Превентивные
3. Ограничение программной среды	ОПС	Установка и запуск только разрешенного к использованию ПО	4	Превентивные
4. Защита машинных носителей информации	ЗНИ	Контроль использования съемных носителей информации, защита от несанкционированного доступа (НСД) к машинным носителям информации	8	Превентивные
5. Регистрация событий безопасности	РСБ	Сбор, запись, хранение и защита информации о событиях безопасности	8	Превентивные
6. Антивирусная защита	АВЗ	Обнаружение и реагирование на вирусы	2	Превентивные
7. Обнаружение вторжений	СОВ	Обнаружение и реагирование на действия, направленные на получение НСД к информации	2	Превентивные
8. Контроль (анализ) защищенности информации	АНЗ	Проведение мероприятий по анализу защищенности КИС и тестированию СЗИ	5	Превентивные
9. Обеспечение целостности ИС и информации	ОЦЛ	Обнаружение фактов несанкционированного нарушения целостности информации, а также ее последующее восстановление	8	– превентивные; – корректирующие
10. Обеспечение доступности информации	ОДТ	Обеспечение авторизованного доступа пользователей к информации	7	Корректирующие
11. Защита ТС	ЗТС	Физическая защита ТС от НСД, обеспечение условий, необходимых для безопасной эксплуатации ТС	5	Превентивные
12. Защита ИС, ее средств, систем связи и передачи данных	ЗИС	Защита информации при взаимодействии КИС или ее отдельных сегментов с иными ИС и сетями передачи данных	20	Превентивные

Наименование категории	Условное обозна-чение	Краткое описание	Число мер	Тип мер
13. Выявление инцидентов и реагирование на них	ИНЦ	Обнаружение, идентификация, регистрация, анализ, устранение последствий и предотвращение повторного возникновения инцидентов ИБ	6	Корректирую-щие
14. Управление конфигурацией ИС и СЗИ	УКФ	Организационное и техническое управление изменениями конфигурации КИС и СЗИ	4	Превентивные
15. Криптографическая защита информации	КЗИ	Использование средств шифрования и электронной подписи	2	Превентивные

2.1.4 Структура корпоративной информационной системы

Каждая КИС по-своему уникальна, и решает задачи, характерные для конкретного предприятия. Для того чтобы модель оценки рисков безопасности КИС обладала универсальностью, необходимо абстрагироваться от конкретных вариантов архитектуры и примеров реализации КИС и оперировать понятиями элементов КИС, их типов (подтипов) и связей между ними.

Под элементом понимается объект, являющий составной частью КИС. Исходя из определения КИС, данного выше, а также анализа источников [100, 102, 106, 111] можно выделить следующие типы элементов КИС: ТС, линии связи (ЛС), ПО и ИА. Структурная диаграмма типов элементов КИС представлена на рисунке 6 [60]. Рассмотрим подробнее каждый из типов элементов КИС.

Техническое средство – «любое электротехническое, электронное и радиоэлектронное изделие, а также любое изделие, содержащее электрические и (или) электронные составные части» [44]. ТС может быть радиоэлектронным средством, СВТ, средством электронной автоматики, электротехническим средством, изделием промышленного, научного или медицинского назначения.

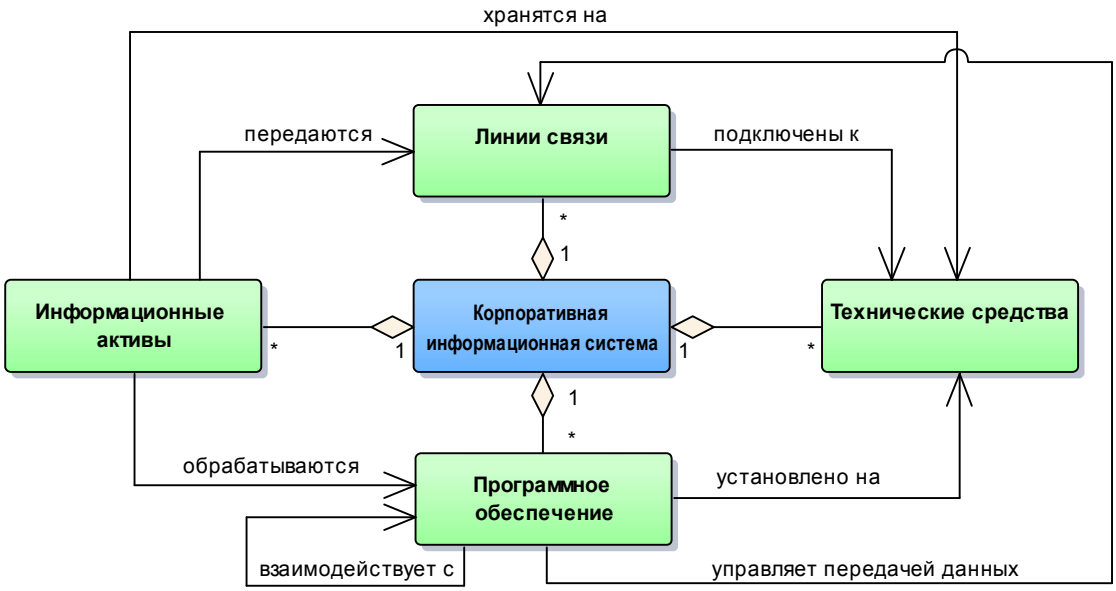

Рисунок 6 – Структурная диаграмма типов элементов КИС

Из перечисленных видов ТС в качестве элементов КИС чаще всего выступают СВТ, однако, чтобы не вводить подобное ограничение, в диссертационной работе используется более общий термин – «техническое средство».

Можно выделить следующие типы ТС, относящиеся к СВТ и наиболее часто встречающиеся в составе КИС:

– серверы;

– АРМ;

– АСО (коммутаторы, маршрутизаторы, концентраторы и так далее);

– мобильные устройства (планшеты, смартфоны и так далее);

– периферийные устройства (принтеры, сканеры, видеопанели и так далее);

– съемные носители (оптические диски, дисковые накопители и так далее);

– программируемые логические контроллеры;

– системы автоматического управления.

Серверы, АРМ и АСО входят в состав практически любой КИС. Основное отличие сервера от АРМ заключается в том, что сервер предназначен для предоставления некоторых вычислительных ресурсов другим системам (компьютерам или программам), называемым клиентами.

Также часто в составе КИС встречаются мобильные и периферийные устройства и съемные носители. Особенностью последних является то, что на них, как правило, не устанавливается ПО, а основное их предназначение ограничивается только хранением ИА.

Прочие типы ТС могут встречаться в зависимости от специфики КИС. Например, при наличии в составе КИС сегмента АС управления технологическими процессами, в ее состав могут входить системы автоматического управления и программируемые логические контроллеры.

В соответствии с классическим представлением ЛС состоит из физической среды, по которой передаются электрические информационные сигналы, и аппаратуры передачи данных [108].

Аппаратура передачи данных связывает компьютеры и АСО с ЛС, являясь пограничным оборудованием. При этом аппаратура передачи данных может быть отдельным ТС (модем) или частью других ТС (сетевой адаптер). Таким образом, в диссертационной работе под ЛС понимается только среда передачи данных.

В зависимости от физической среды передачи данных можно выделить следующие типы ЛС: проводные, кабельные (витая пара, коаксиальные, оптоволоконные), беспроводные (радиоканалы наземной и спутниковой связи) [108].

Под ПО понимается все или часть программ, процедур, правил системы обработки информации [149]. В зависимости от назначения выделяются следующие типы ПО [63]:

- системное, предназначенное для управления компонентами ТС (процессором, оперативной памятью, устройствами ввода-вывода);
- прикладное, предназначенное для выполнения определенных пользовательских задач;
- инструментальное, предназначенное для использования в ходе проектирования, разработки и сопровождения программ.

Ключевыми элементами КИС являются ИА, под которыми понимаются информационные ресурсы, данные, документы, обладающие ценностью для

предприятия [129, 152]. Выделяются следующие типы ИА: файл, каталог с файлами, база данных, технологическая информация (набор сигналов, команд), конфигурационная информация [152]. Кроме того, в [152] в качестве типа ИА выделены печатные документы, которые, однако, не входят в состав КИС.

Приведенные перечни типов ТС, ЛС, ПО и ИА (подтипов элементов КИС) не являются исчерпывающими и могут быть дополнены и скорректированы в зависимости от специфических особенностей КИС. На рисунке 7 приведена схема элементов сегмента ЦОД КИС, структурная схема которой представлена на рисунке 4.

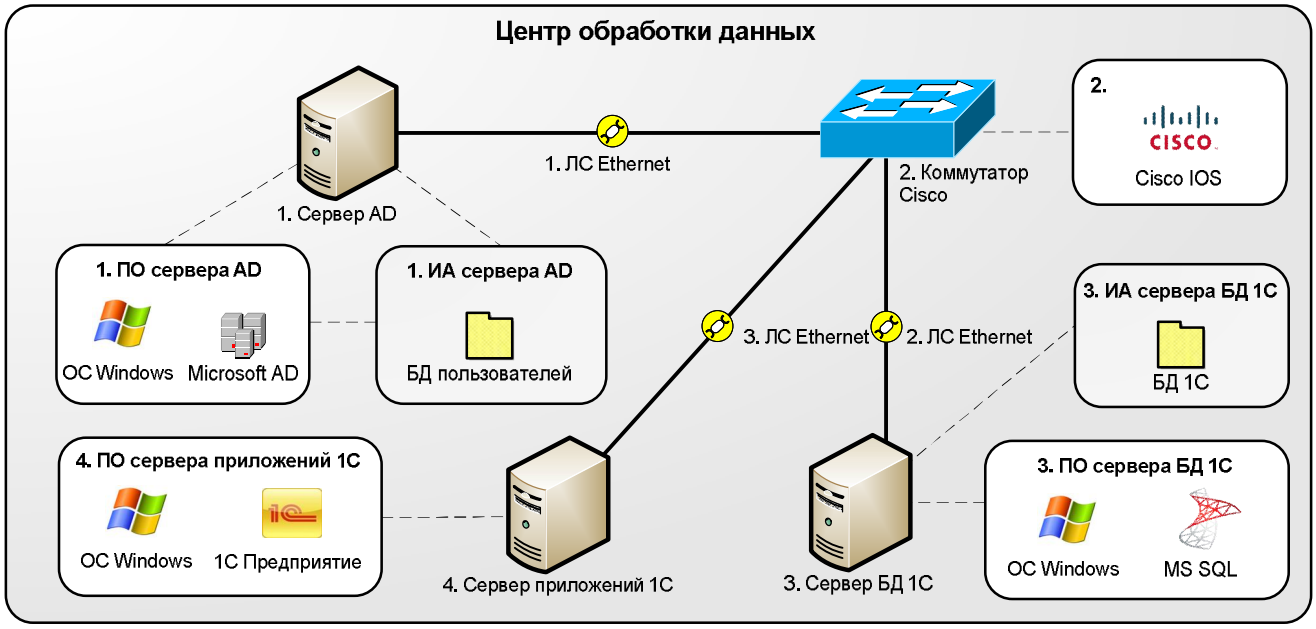

Рисунок 7 – Схема элементов сегмента ЦОД КИС

В диссертационной работе предлагается использовать инфраструктурную модель КИС, представленную в виде неориентированного графа:

$$G^{IS} = \{O^{IS}, L^{IS}\}, \tag{11}$$

где O^{IS} – множество элементов КИС;

L^{IS} – множество связей между элементами КИС.

Количество элементов КИС N_O определяется выражением:

$$N_O = N_{HW} + N_{HW} + N_{SW} + N_{IA}, \tag{12}$$

где N_{HW} – количество ТС;

N_{CL} – количество ЛС;

N_{SW} – количество ПО;

N_{IA} – количество ИА.

Множество элементов КИС, в свою очередь, можно представить кортежем:

$$O^{IS} = \{O^{HW}, O^{CL}, O^{SW}, O^{IA}\}, \quad (13)$$

где $O^{HW} = \{HW_1, HW_2, ..., HW_{N_{HW}}\}$ – подмножество ТС;

$O^{CL} = \{CL_1, CL_2, ..., CL_{N_{CL}}\}$ – подмножество ЛС;

$O^{SW} = \{SW_1, SW_2, ..., SW_{N_{SW}}\}$ – подмножество ПО;

$O^{IA} = \{IA_1, IA_2, ..., IA_{N_{IA}}\}$ – подмножество ИА, входящих в состав КИС.

Множество связей между элементами КИС определяется матрицей смежности $A^{IS} = [a_{ij}^{IS}]$, в которой $a_{ij}^{IS} = a_{ji}^{IS} = 1$, если между элементами O_i^{IS} и O_j^{IS} существует связь, и $a_{ij}^{IS} = a_{ji}^{IS} = 0$ в противном случае. Характер связей между типами элементов КИС определен на рисунке 6.

На рисунке 8 приведена инфраструктурная модель, соответствующая сегменту ЦОД КИС из рисунка 7.

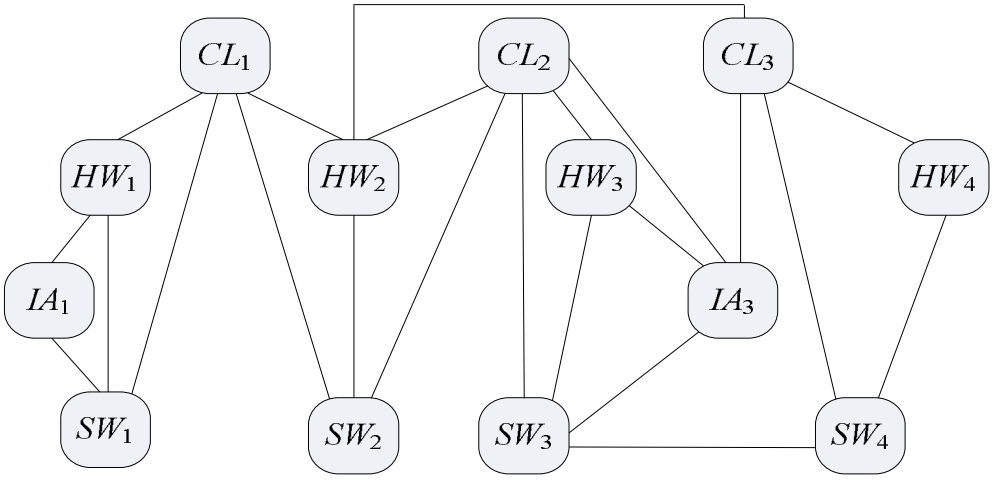

Рисунок 8 – Инфраструктурная модель сегмента ЦОД КИС

Инфраструктурная модель КИС на стадиях проектирования и разработки системы формируется на основе проектной документации, а на стадиях ввода в эксплуатацию, эксплуатации и ликвидации – на основе реальных данных об элементах КИС и их связях.

Множество источников угроз безопасности КИС ST^{IS} можно представить кортежем:

$$ST^{IS} = \{V^{NS}, V^{AS}\}, \quad (14)$$

где V^{NS} – подмножество (класс) естественных источников угроз;

V^{AS} – подмножество (класс) нарушителей.

Число источников угроз в модели угроз для КИС обозначим как N_{ST}.

Для учета связей между источниками угроз и элементами КИС определяется матрица $A^{ST} = [a_{ij}^{ST}]$ размерностью $N_O \times N_{ST}$, в которой $a_{ij}^{ST} = 1$, если источник угроз ST_i^{IS} может реализовать угрозу в отношении элемента КИС O_j^{IS} (например, нарушитель имеет доступ к ЛС), а иначе $a_{ij}^{ST} = 0$. Размерность матрицы A^{ST} и значения элементов a_{ij}^{ST} изменяются со временем.

2.2 Модель сценариев реализации угроз корпоративной информационной системе

В диссертационной работе в качестве рискового события предлагается рассматривать переход элемента КИС в деструктивное состояние, возникающий в результате реализации одной или нескольких угроз. Определим возможные деструктивные состояния для каждого типа элементов КИС, а также причинно-следственные связи между ними.

2.2.1 Деструктивные состояния элементов корпоративной информационной системы

Понятие «деструктивное состояние», используемое в диссертационной работе, связано с понятием «деструктивное действие», встречающимся в документах ФСТЭК России [6, 83, 86, 87] и означающим негативное воздействие со стороны источника угроз, направленное на информацию и носитель информации.

Число деструктивных состояний элементов КИС и связей между ними существенно влияет на сложность формируемой модели оценки рисков безопасности КИС. Следовательно, перечень деструктивных состояний должен быть сформирован исходя из принципа необходимой достаточности. В результате анализа документов по моделированию угроз [6], оценке рисков [152], теории надежности [1, 9, 31] и опроса специалистов в области ИТ и ИБ определены следующие деструктивные состояния для элементов КИС каждого типа:

1) техническое средство:
   - осуществлен НСД, $HW^{[I]}$;
   - нарушена доступность, $HW^{[U]}$;
2) линия связи:
   - осуществлен НСД, $CL^{[I]}$.
   - нарушена доступность, $CL^{[U]}$;
3) программное обеспечение:
   - осуществлен НСД, $SW^{[I]}$.
   - нарушена доступность, $SW^{[U]}$;
4) информационный актив:
   - нарушена конфиденциальность, $IA^{[C]}$;
   - нарушена целостность, $IA^{[M]}$;
   - нарушена доступность, $IA^{[U]}$.

Таким образом, для ИА определено три деструктивных состояния, соответствующих нарушению трех основных свойств ИБ: конфиденциальности, целостности и доступности. Для ТС, ЛС и ПО определено по два деструктивных состояния, первое из которых соответствует тому, что в отношении элемента КИС осуществлен НСД, а второе – нарушению доступности элемента КИС. Под НСД в соответствии с ГОСТ 53114–2008 понимается доступ к элементу КИС, осуществляемый с нарушением установленных прав доступа, в том числе неавторизованный доступ, повышение привилегий, несанкционированная модификация, удаление и так далее [33].

Множество деструктивных состояний элементов КИС, обозначаемое как DS^{IS}, можно представить как:

$$DS^{IS} = \left\{DS^{HW}, DS^{CL}, DS^{SW}, DS^{IA}\right\}, \quad (15)$$

где $DS^{HW} = \left\{HW^{[I]}, HW^{[U]}\right\}$ – подмножество деструктивных состояний ТС;

$DS^{CL} = \left\{CL^{[I]}, CL^{[U]}\right\}$ – подмножество деструктивных состояний ЛС;

$DS^{SW} = \left\{SW^{[I]}, SW^{[U]}\right\}$ – подмножество деструктивных состояний ПО;

$DS^{IA} = \left\{IA^{[C]}, IA^{[M]}, IA^{[U]}\right\}$ – подмножество деструктивных состояний ИА.

Деструктивные состояния, предложенные в диссертационной работе, не являются взаимоисключающими, то есть элемент КИС может находиться в нескольких деструктивных состояниях одновременно. Например, в результате кражи ТС нарушителем к нему осуществляется НСД, при этом ТС становится недоступным для его пользователей.

2.2.2 Переходы элементов в деструктивные состояния

Переход элемента КИС в деструктивное состояние осуществляется в результате реализации угроз источниками. В диссертационной работе под сценарием реализации угроз понимается один или несколько связанных переходов элементов КИС в деструктивные состояния.

Модель сценариев реализации угроз представляет собой множество всех сценариев, представленное ориентированным графом:

$$G^{TM} = \left\{V^{TM}, H^{TM}\right\}, \quad (16)$$

где V^{TM} – вершины графа G^{TM};

H^{TM} – дуги графа G^{TM}, соединяющие две его вершины.

Вершинами графа G^{TM} являются:

- начальные вершины $v'_i \in ST^{IS} \subset V^{TM}$, соответствующие классам источников угроз;
- промежуточные и конечные вершины $v'_i \in DS^{IS} \subset V^{TM}$, соответствующие деструктивным состояниям элементов КИС.

Переход элемента КИС в деструктивное состояние определяется парой вершин, первая из которых $v'_i \in V^{TM}$ является причиной, а вторая $v'_j \in DS^{IS}$ – результатом перехода. Причиной перехода может быть:

– связанный переход элемента КИС в деструктивное состояние, $v'_i \in DS^{IS}$;

– воздействие естественного источника угроз, $v'_i \in V^{NS}$;

– воздействие нарушителя, $v'_i \in V^{AS}$.

Вершины v'_i и v'_j соединяются дугой $h'_{ji} \in H^{TM}$ либо несколькими дугами через промежуточные вершины v'_r, называемые условиями перехода. Например, причиной НСД к ПО ($SW^{[I]}$) является воздействие нарушителя (V^{AS}), а условиями – наличие НСД нарушителя к связанным ТС ($HW^{[I]}$), ЛС ($CL^{[I]}$) или ПО ($SW^{[I]}$).

Множество дуг определяется матрицей смежности $A^{TM} = [a_{ij}^{TM}]$, в которой $a_{ij}^{TM} = 1$, если существует дуга, исходящая из вершины v'_i и входящая в вершину v'_j, в противном случае $a_{ij}^{TM} = 0$.

В результате анализа документов по моделированию угроз [6] и оценке рисков [4, 115, 152, 162] и опроса специалистов в данных областях сформирован перечень переходов элементов КИС в деструктивные состояния (таблица 5).

Таблица 5 – Перечень переходов элементов КИС в деструктивные состояния

Наименование перехода	**Результат, v'_j**	**Причина, v'_i**	**Условие[1)], v'_r**
НСД к ТС	$HW^{[I]}$	V^{AS}	–
Нарушение доступности ТС	$HW^{[U]}$	V^{NS}	–
		V^{AS}	$HW^{[I]}$
НСД к ЛС	$CL^{[I]}$	V^{AS}	–
Нарушение доступности ЛС	$CL^{[U]}$	V^{NS}	–
		V^{AS}	$CL^{[I]}$
		$HW^{[U]}$	–
НСД к ПО	$SW^{[I]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
Нарушение доступности ПО	$SW^{[U]}$	V^{NS}	–
		V^{AS}	$SW^{[I]}$
		$HW^{[U]}$	–
		$CL^{[U]}$	–
		$SW^{[U]}$	–
Нарушение конфиденциальности ИА	$IA^{[C]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$

Наименование перехода	Результат, v'_j	Причина, v'_i	Условие[1)], v'_r
Нарушение целостности ИА	$IA^{[M]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
		$HW^{[U]}$	–
		$CL^{[U]}$	–
		$SW^{[U]}$	–
Нарушение доступности ИА	$IA^{[U]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
		$HW^{[U]}$	–
		$CL^{[U]}$	–
		$SW^{[U]}$	–
[1)] Указываются возможные промежуточные вершины между причиной и результатом перехода			

Для проверки необходимости и достаточности предложенных в диссертационной работе деструктивных состояний и переходов определены возможные сценарии реализации угроз из перечня, приведенного в ГОСТ Р ИСО/МЭК 27005-2010 [42]. Результаты представлены в таблице А.1 приложения А.

Таким образом, разработанная модель, включающая два класса источников угроз, девять деструктивных состояний элементов КИС и 22 перехода (по количеству пар «причина / результат»), позволяет описать основные сценарии реализации угроз безопасности КИС в виде связанных переходов элементов КИС в деструктивные состояния. Исключение составила угроза «нарушение работоспособности персонала», которую не удалось представить в виде сценария, поскольку персонал не относится к элементам КИС.

2.2.3 Весовые функции переходов

Условная вероятность перехода v'_j в результате возникновения причины v'_i определяется весовой функцией $f_{ji} = p(v'_j \mid v'_i)$ с областью значений $E(f_{ji}) = [0;1]$. В зависимости от причины перехода можно определить три типа весовых функций.

Весовая функция зависимого перехода f_{ji}^{DS}, возникающего в результате связанного перехода элемента КИС в деструктивное состояние, определяется как:

$$f_{ji}^{DS} = 1, \forall v'_i \in DS^{IS}. \qquad (17)$$

Угрозы, реализуемые естественными источниками, носят случайный характер и возникают, как правило, достаточно редко и независимо друг от друга. Для прогнозирования условной вероятности переходов, вызванных естественными источниками угроз, в диссертационной работе предлагается использовать распределение Пуассона, описываемое для *i*-го источника угроз выражением [32]:

$$P_{П}(k) = \frac{\lambda^k}{k!} e^{-\lambda_i}, \qquad (18)$$

где $P_{П}(k)$ – вероятность того, что событие произойдет k раз за период оценки, $k = 0, 1, 2, ...$;

λ_i – среднее число опасных событий (отказов, аварий, катастроф) для *i*-го источника угроз за период оценки.

Выбор распределения Пуассона в диссертационной работе обусловлен тем, что оно позволяет достаточно точно прогнозировать частоту редких независимых событий [18, 25], к которым относятся переходы, вызванные естественными источниками угроз. Стоит также отметить успешный опыт использования распределения Пуассона для прогнозирования частоты аварий и отказов в теории надежности [1] и методиках оценки рисков [115].

Весовая функция перехода f_{ji}^{NS}, вызванного естественными источниками угроз, соответствует вероятности возникновения хотя бы одного опасного события за период оценки, приводящего к переходу, и определяется как:

$$f_{ji}^{NS} = 1 - e^{-\lambda_i}, \forall v_i' \in V^{NS}. \qquad (19)$$

Для стихийных источников угроз опасными событиями являются катастрофы и аварии, произошедшие в местах размещения ТС и ЛС. При этом учитываются только те катастрофы, масштаб которых превысил некоторый допустимый предел, например, землетрясения с интенсивностью, превышающей сейсмостойкость здания, в котором размещены ТС КИС, или ураганы с ветровой нагрузкой, превышающей предельно допустимую [125].

Для техногенных источников угроз среднее число опасных событий представляет собой интенсивность отказов ТС, ЛС и ПО [31]. Интенсивность отказов определяется для схожих элементов КИС, например, элементов одного подтипа. Для повышения точности результатов рекомендуется определять среднюю интенсивность отказов для конкретных моделей ТС, технологий ЛС и версий ПО. Для некоторых ТС интенсивность отказов указывается в технической документации, что делает необязательным сбор собственной статистики.

Одно из обязательных условий использования распределения Пуассона для прогнозирования вероятности случайных событий заключается в том, что в потоке учитываемых опасных событий должно отсутствовать последействие. Для этого при оценке λ_i необходимо удостовериться, что учитываемые опасные события независимы. В противном случае зависимые события, например, отказы одного и того же ТС по схожей причине в течение небольшого интервала времени, должны быть объединены или исключены.

Точное определение функции вероятности реализации угроз нарушителем, зависящей от многих признаков, является весьма нетривиальной и трудноразрешимой задачей. Определение вероятности реализации угроз нарушителем предполагает сравнение возможностей нарушителя для реализации угроз со степенью реализации защитных мер. В соответствии с данным утверждением в диссертационной работе в качестве аргументов функции f_{ji}^{AS} предлагается использовать два показателя:

- показатель степени опасности i-го нарушителя d_i;
- показатель степени реализации превентивных защитных мер, предотвращающих переход в j-ое деструктивное состояние, ψ_j.

Степенью опасности нарушителя называется интегральный количественный показатель, характеризующий желание и возможности нарушителя для реализации угроз и принимающий значения в интервале [0; 1]. Чем больше значение показателя d_i, тем большими возможностями для реализации угроз обладает нарушитель.

Степень реализации превентивных защитных мер представляет собой интегральный количественный показатель, характеризующий защищенность элемента КИС от перехода в *j*-ое деструктивное состояние и принимающий значения в интервале [0; 1]. Большее значение показателя ψ_j говорит о большей защищенности элемента КИС от перехода в *j*-ое деструктивное состояние.

В рассмотренных источниках встречается два наиболее распространенных подхода к определению функции вероятности реализации угроз нарушителем. С учетом того, что степень опасности нарушителя d_i характеризует возможность реализации угроз, а выражение $(1-\psi_j)$ – простоту использования уязвимостей [80], чаще всего функция вероятности реализации угроз нарушителем определяется как [4, 115]:

$$f_{ji}^{AS} = d_i \cdot (1-\psi_j), \forall v_i' \in V^{AS}. \quad (20)$$

Значения функции f_{ji}^{AS}, получаемые при использовании формулы (20), как правило, занижены. Например, при средней степени опасности нарушителя ($d_i = 0{,}5$) и средней степени реализации превентивных защитных мер ($\psi_j = 0{,}5$), значение f_{ji}^{AS} составляет всего 0,25.

В работе [5] используется пороговая функция, определяемая выражением:

$$f_{ji}^{AS} = \begin{cases} 1, \text{если } d_i \geq \psi_j \\ 0, \text{если } d_i < \psi_j \end{cases}, \forall v_i' \in V^{AS}. \quad (21)$$

Недостатками пороговой функции является ограниченность принимаемых значений и наличие точки разрыва, что не позволяет использовать для ее обучения градиентные методы [19].

В диссертационной работе весовую функцию перехода f_{ji}^{AS}, вызванного нарушителем, предлагается определять как логистическую функцию:

$$f_{ji}^{AS} = \frac{1}{1+e^{-z(d_i-\psi_j)}}, \forall v_i' \in V^{AS}, \quad (22)$$

где z – произвольный множитель, z > 0.

Можно выделить следующие преимущества использования логистической функции для оценки вероятности реализации угроз нарушителем:

– нелинейность и непрерывная дифференцируемость;

– производная может быть выражена через саму функцию;

– хорошая изученность и широкая применимость в различных методах обучения [19, 109];

– подходящая область значений функции: $E(f_{ji}^{AS}) = [0;1]$.

График логистической функции при некоторых значениях z представлен на рисунке 9. При $z \to \infty$ логистическая функция преобразуется в пороговую, представленную выражением (21).

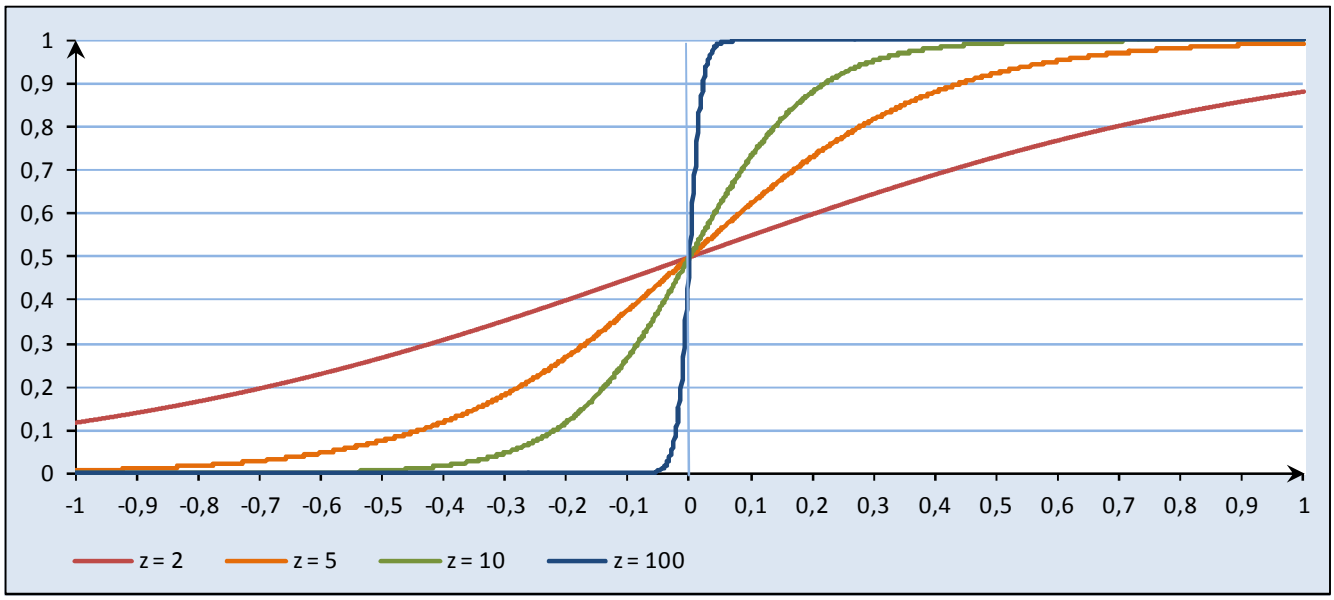

Рисунок 9 – График логистической функции

Таким образом, в диссертационной работе оценка условной вероятности перехода элемента КИС в деструктивное состояние, возникающего в результате реализации угроз нарушителем, осуществляется с использованием логистической функции (22), аргументом которой является разность между степенью опасности нарушителя d_i и степенью реализации превентивных защитных мер ψ_j. Значение множителя z определяется в ходе экспериментального исследования, результаты которого приведены в подразделе 3.2 диссертационной работы.

2.3 Оценка показателей защищенности корпоративной информационной системы

В диссертационной работе предлагается подход к определению совокупности взвешенных метрик для оценки показателей степени опасности нарушителя и степени реализации защитных мер.

Понятие «метрика», характерное в большей степени для работ в области менеджмента и проектного управления [175], в последнее время все чаще используется в трудах, посвященных вопросам ИБ [72, 96, 161, 169]. В диссертационной работе под метрикой понимается «количественное измерение, которое может быть интерпретировано в контексте ряда предыдущих или эквивалентных измерений» [89].

В стандарте COBIT 5 [175] определены основные свойства, которыми должна обладать метрика[1)]:

- конкретность: метрика должна быть ясной и иметь непосредственное отношение к измеряемому процессу;
- измеримость: должна существовать возможность однозначно измерить метрику;
- практическая применимость: должна существовать возможность изменения значения метрики;
- значимость: улучшение метрики должно означать повышение вклада в достижение целей безопасности;
- своевременность: должна существовать возможность своевременно измерить метрику.

Для определения функции f_{ji}^{AS} необходимо определить метрики нарушителей и метрики защитных мер, а также оценить значения их весовых коэффициентов.

[1)] При упоминании данных свойств метрики часто используется мнемоническая аббревиатура SMART

2.3.1 Общие принципы формирования метрик

В диссертационной работе под метрикой понимается мера, принимающая значение в интервале [0; 1], характеризующая степень соответствия фактического значения некоторого признака эталонному значению. Для расчета метрики в зависимости от значения соответствующего ей признака задается функция:

$$M = \varphi(F^a), \tag{23}$$

где M – значение метрики, $M \in [0; 1]$;

φ – функция оценки метрики;

F^a – фактическое значение признака.

Признаки, используемые в диссертационной работе при формировании метрик, можно классифицировать на бинарные, качественные и количественные. Рассмотрим функции оценки метрик в зависимости от соответствующих им признаков.

Для бинарного признака определяется целевое (эталонное) значение F^t. Значение метрики, при этом, определяется как:

$$M = \begin{cases} 1, \text{если } F^{\text{a}} = F^t \\ 0, \text{если } F^{\text{a}} \neq F^t \end{cases}. \tag{24}$$

Для количественного признака определяются рекомендуемый, допустимый и недопустимый интервалы значений. На основании данных интервалов строится кусочно-линейная функция:

$$M = \begin{cases} 1, \text{если } F^{\text{a}} \in \left[F^r; F^{r'}\right] \\ \dfrac{F^{p''} - F^{\text{a}}}{F^{p''} - F^{r'}}, \text{если } F^{\text{a}} \in \left(F^{r'}; F^{p''}\right] \\ \dfrac{F^{\text{a}} - F^p}{F^r - F^p}, \text{если } F^{\text{a}} \in \left[F^p; F^r\right) \\ 0, \text{если } F^{\text{a}} \in \left(-\infty; F^p\right) \cup \left(F^{p'}; +\infty\right) \end{cases}, \tag{25}$$

где $[F^r; F^{r'}]$ – интервал рекомендуемых значений признака;

$[F^p; F^{p'}]$ – интервал допустимых значений признака;

$\left(-\infty; F^{p}\right) \cup \left(F^{p'}; +\infty\right)$ – недопустимые значения признака.

При этом должны выполняться условия: $F^{r} \geq F^{p}$, $F^{r'} \leq F^{p'}$. В случае равенства верхних или нижних границ интервалов рекомендуемых и допустимых значений образуется точка разрыва функции.

При нелинейном характере зависимости значения метрики от количественного значения признака кусочно-линейная функция может быть заменена другой, например, экспоненциальной или степенной.

Для множества качественных значений признака определяются абсолютные весовые коэффициенты методом анализа иерархий согласно рекомендациям, приведенным в пункте 2.3.4 диссертационной работы. Значение метрики, соответствующей качественному признаку, равняется весовому коэффициенту фактического значения признака u^{a}.

В диссертационной работе рассматриваются метрики оценки степени опасности нарушителей и метрики оценки степени реализации защитных мер. Источниками для формирования данных метрик могут служить:

- требования и рекомендации национальных и международных стандартов;
- экспертное мнение специалистов в области ИБ;
- данные из различных АС, например систем мониторинга событий безопасности, систем предотвращения утечек информации и прочих.

2.3.2 Оценка степени опасности нарушителей

Для оценки степени опасности нарушителей предлагается использовать следующий набор метрик, сформированный на основе положений нормативных документов [40, 87]: мотивация, оснащенность (имеющееся оборудование), техническая компетентность, знание информации о КИС и СЗИ, права доступа (до реализации угроз), время доступа (до момента обнаружения и реагирования).

Степень опасности нарушителя является интегральным показателем, для оценки которого целесообразно использовать функцию среднего от значений метрик. В диссертационной работе для оценки степени опасности *i*-го нарушителя

предлагается использовать функцию средневзвешенного геометрического значений метрик:

$$d_i = \prod_h \left(M_{ih}^V \right)^{w_{ih}^V}, \quad (26)$$

где M_{ih}^V – значение *h*-ой метрики *i*-го нарушителя;

w_{ih}^V – весовой коэффициент *h*-ой метрики *i*-го нарушителя, $\sum_h w_{ih}^V = 1$.

Выбор функции (26) обусловлен следующими причинами:

– функция средневзвешенного геометрического часто используется для оценки интегральных показателей в теории принятия решений [162];
– при нулевых значениях метрик (мотивации, времени доступа и прочих) показатель степени опасности нарушителя также равен нулю.

Качественные значения признаков нарушителей, сформированные на основе положений нормативных документов [40, 87], и соответствующие им весовые коэффициенты приведены в таблице Б.1 приложения Б.

При оценке степени опасности группового нарушителя учитываются значения признаков входящих в его состав одиночных нарушителей с наибольшими весовыми коэффициентами.

2.3.3 Оценка степени реализации защитных мер

В диссертационной работе для оценки степени реализации защитных мер сформирован набор метрик на основе перечней защитных мер, приведенных в нормативных документах ФСТЭК России [104, 106, 118]. В свою очередь, защитные меры группируются по категориям, представленным ранее в таблице 4.

По аналогии с формулой (26), степень реализации превентивных защитных мер ψ_j предлагается определять как средневзвешенное геометрическое значений степени реализации связанных категорий по формуле:

$$\psi_j = \prod_g \left(K_{jg} \right)^{w_{jg}^K}, \quad (27)$$

где K_{jg} – значение g-ой категории защитных мер для j-го деструктивного состояния, $K_{jg} \in [0; 1]$;

w_{jg}^{K} – весовой коэффициент g-ой категории защитных мер относительно j-го деструктивного состояния, $\sum_{g} w_{jg}^{K} = 1$.

Степень реализации корректирующих защитных мер ψ'_j по аналогии с ψ_j определяется по формуле (27).

Весовые коэффициенты категорий защитных мер характеризуют степень их важности для предотвращения или снижения последствий от перехода. Результаты начальной оценки весовых коэффициентов категорий превентивных и корректирующих защитных мер с учетом их связи с деструктивными состояниями элементов КИС приведены в таблице Б.2 приложения Б.

На рисунке 10 на примере ПО веб-сервера показано, каким образом защитные меры различных категорий предотвращают угрозы, вызванные действиями нарушителей. Как правило, отсутствие защитных мер какой-либо категории делает возможной реализацию определенных угроз, в результате чего осуществляется переход элемента КИС в деструктивное состояние. Например, отсутствие защитных мер категории «антивирусная защита» делает возможной реализацию угрозы «внедрение вредоносного ПО», в результате чего нарушителем может быть получен НСД к ПО. Это подтверждает правильность выбора функции средневзвешенного геометрического для оценки степени реализации защитных мер в формуле (27).

Защитные меры одной категории, как правило, направлены на предотвращение схожих угроз и дополняют друг друга, а отсутствие защитной меры может быть компенсировано набором других мер категории. Исходя из этого степень реализации категории защитных мер предлагается определять как средневзвешенное арифметическое значений метрик данной категории по формуле:

$$K_{jg} = \sum_{l} w_{gl}^{C} \cdot M_{gl}^{C} \ , \qquad (28)$$

где M_{gl}^{C} – значение l-ой метрики g-ой категории;

w_{gl}^{C} – весовой коэффициент l-ой метрики g-ой категории, $\sum_{l} w_{gl}^{C} = 1$.

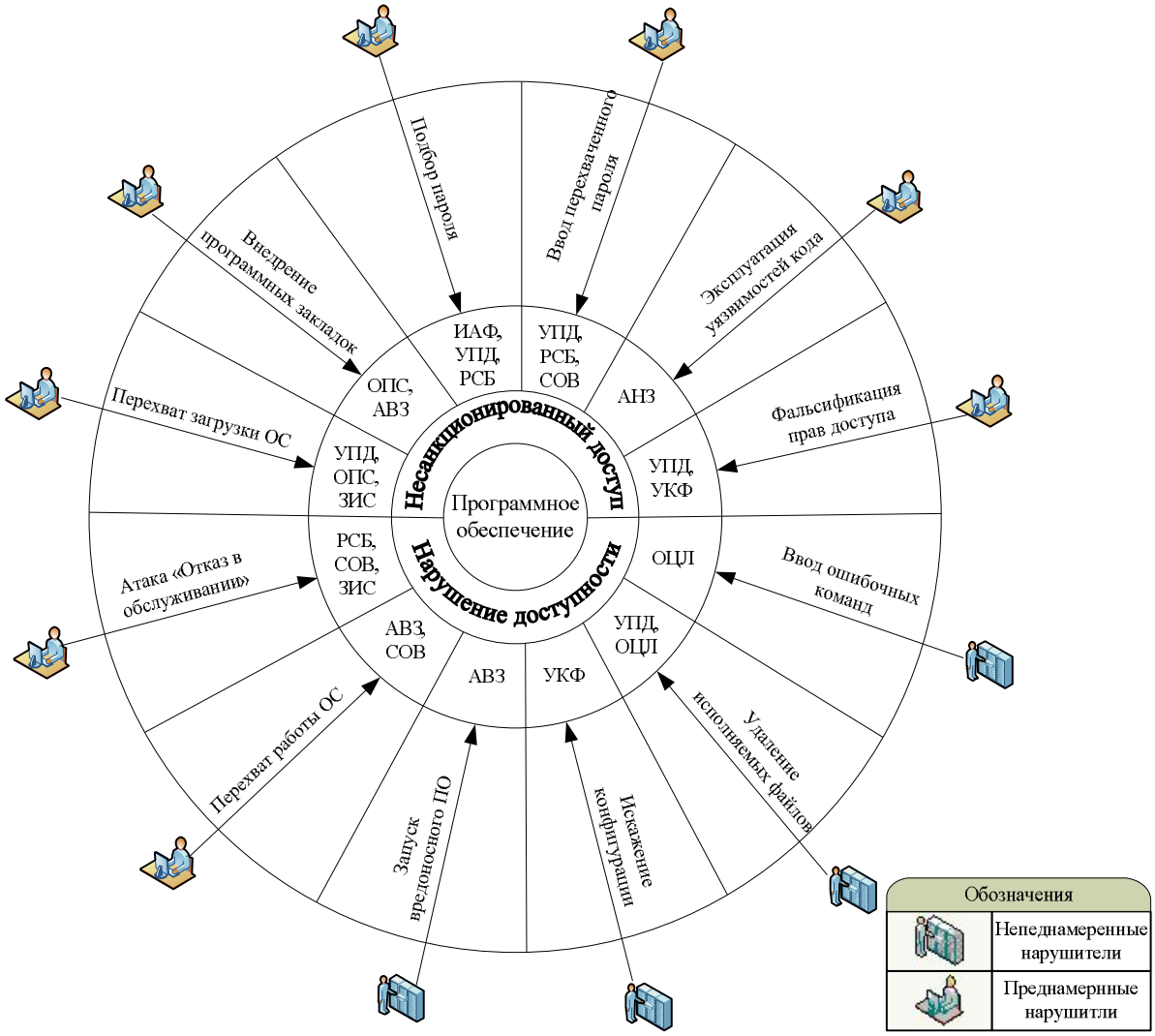

Рисунок 10 – Защитные меры, предотвращающие угрозы ПО веб-сервера

Весовые коэффициенты метрик защитных мер характеризуют степень их важности для данной категории. Набор метрик защитных мер и результаты оценки соответствующих им весовых коэффициентов приведены в таблице Б.3 приложения Б.

Метрики защитных мер, входящих в состав категорий УКФ, ИНЦ и КЗИ, определяются в зависимости от реализации соответствующих им защитных мер и принимают одно из двух значений: реализована (1) или не реализована (0). Метрики защитных мер прочих категорий, приведенных в документе [84],

определяются в зависимости от степени реализации требований, предъявляемых к соответствующей защитной мере, принимающей значения:

- «не реализована» – не реализованы базовые требования;
- «базовый уровень» – реализованы базовые требования;
- «усиленный уровень» – реализованы базовые требования и требования к усилению.

Базовые требования и требования к усилению, предъявляемые к защитным мерам, определены в методическом документе ФСТЭК России «Меры защиты информации в государственных информационных системах» [84].

2.3.4 Определение весовых коэффициентов методом анализа иерархий

Весовые коэффициенты характеризуют степень важности метрик и категорий относительно оцениваемого показателя. Для начальной оценки весовых коэффициентов целесообразно использовать один из методов экспертного оценивания. В дальнейшем корректировка весовых коэффициентов осуществляется с применением методов, основанных на коррекции ошибок, рассмотренных в разделе 3 диссертационной работы.

Оценку весовых коэффициентов можно осуществлять при помощи следующих методов: метод прямой расстановки, метод ранжирования, метод парных сравнений, метод анализа иерархий [67].

В методе прямой расстановки весовые коэффициенты напрямую оцениваются экспертами. Преимуществом данного метода является простота, а недостатками – сложность принятия решения при большом количестве элементов и отсутствие проверки качества полученных экспертных оценок.

Метод ранжирования заключается в упорядочивании элементов по степени возрастания или убывания их влияния на цель. Результирующие оценки весовых коэффициентов определяются в результате усреднения частных рангов, проставленных экспертами, и нормировки полученных усредненных значений. Выделяют следующие недостатки метода ранжирования [67]:

- не учитывается степень превосходства одного элемента над другим;

– не предусмотрена возможность равенства важности элементов;

– сложность принятия решения при большом количестве элементов;

– отсутствие проверки качества полученных экспертных оценок.

Метод парных сравнений заключается в попарном сравнении элементов в отношении некоторого свойства. В результате сравнения формируется матрица $C = [c_{ij}]$, называемая матрицей парных сравнений, где c_{ij} – оценка степени превосходства элемента x_i над элементом x_j. В классическом варианте метода парных сравнений, предложенных Л. Терстоуном, результат сравнения элемента x_i с элементом x_j определяется следующим образом:

$$c_{ij} = \begin{cases} 1, \text{если элемент } x_i \text{ лучше элемента } x_j \\ 0, \text{если элемент } x_i \text{ хуже элемента } x_j \end{cases}. \quad (29)$$

Результаты парных сравнений, как правило, являются более точными, чем результаты прямой расстановки или ранжирования [67]. Вместе с тем для классического метода парных сравнений характерны следующие недостатки: не предусмотрена оценка для элементов с равной важностью и не учитывается степень превосходства одного элемента над другим. Этих недостатков лишены многие модификации метода парных сравнений, одной из которых является метод анализа иерархий, предложенный Т. Саати [121].

В основе метода анализа иерархий лежит процедура парного сравнения элементов, осуществляемая по шкале, приведенной в таблице 6 [113].

Таблица 6 – Шкала оценки степени превосходства

Степень превосходства	Суждение	Пояснение
1	Отсутствие превосходства	Равная значимость двух элементов
3	Умеренное превосходство	Слабое (умеренное) превосходство одного элемента над другим
5	Существенное превосходство	Сильное (существенное) превосходство одного элемента над другим
7	Значительное превосходство	Очень сильное (значительное) превосходство одного элемента над другим
9	Абсолютное превосходство	Максимально возможное превосходство одного элемента над другим
2, 4, 6, 8	Промежуточные решения	Применяются в компромиссном случае
$\frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{9}$	Обратные величины	Обратные значения, характерные для уступающих в сравнении элементов

Выделяются следующие преимущества метода анализа иерархий: наглядность и интерпретируемость результатов, простота вычислений, возможность проверки качества полученных оценок. Данный метод успешно используется для решения различных задач, в том числе для оценки защищенности [75]. Таким образом, из рассмотренных методов для оценки весовых коэффициентов предпочтительно использовать метод анализа иерархий.

Основной недостаток метода анализа иерархий заключается в том, что при увеличении числа сравниваемых элементов происходит рост числа операций парных сравнений, близкий к экспоненциальному, что затрудняет работу экспертов и обработку результатов. В связи с этим рекомендуется, чтобы число сравниваемых элементов не превышало девяти [113].

Поскольку для защитных мер категорий УПД и ЗИС данное требование не выполняется, для оценки значений весовых коэффициентов защитных мер предлагается использовать метод сравнения относительно стандартов, являющийся модификацией метода анализа иерархий. Основная суть метода сравнения относительно стандартов заключается в разбиении множества сравниваемых элементов на небольшое число кластеров, соответствующих определенным стандартам, и замене процедуры парных сравнений элементов процедурой парных сравнений стандартов. При этом стандарты, используемые в диссертационной работе, характеризуют степень важности защитных мер.

Основываясь на суждениях из шкалы оценки степени превосходства, приведенной в таблице 6, сформирована пятиуровневая качественная шкала оценки степени важности защитных мер, приведенная в таблице 7.

Таблица 7 – Шкала оценки степени важности защитных мер

Значение степени важности	**Характеристика значения**	**Приоритет значения, b_i**
Критичная	Защитная мера крайне важна, а ее отсутствие почти наверняка приведет к реализации угроз нарушителем	0,51
Значительная	Защитная мера важна, а ее отсутствие, скорее всего, приведет к реализации угроз нарушителем	0,26
Существенная	Защитная мера рекомендуема, а ее отсутствие может привести к реализации угроз нарушителем	0,13
Умеренная	Защитная мера полезна, однако ее отсутствие может быть компенсировано другими защитными мерами	0,06

Значение степени важности	Характеристика значения	Приоритет значения, b_i
Незначительная	Защитная мера не играет существенной роли, но может незначительно усилить другие защитные меры категории	0,03

Оценка приоритетов значений степени важности защитных мер осуществлялась при помощи специализированной программы MPriority, интерфейс которой представлен на рисунке 11.

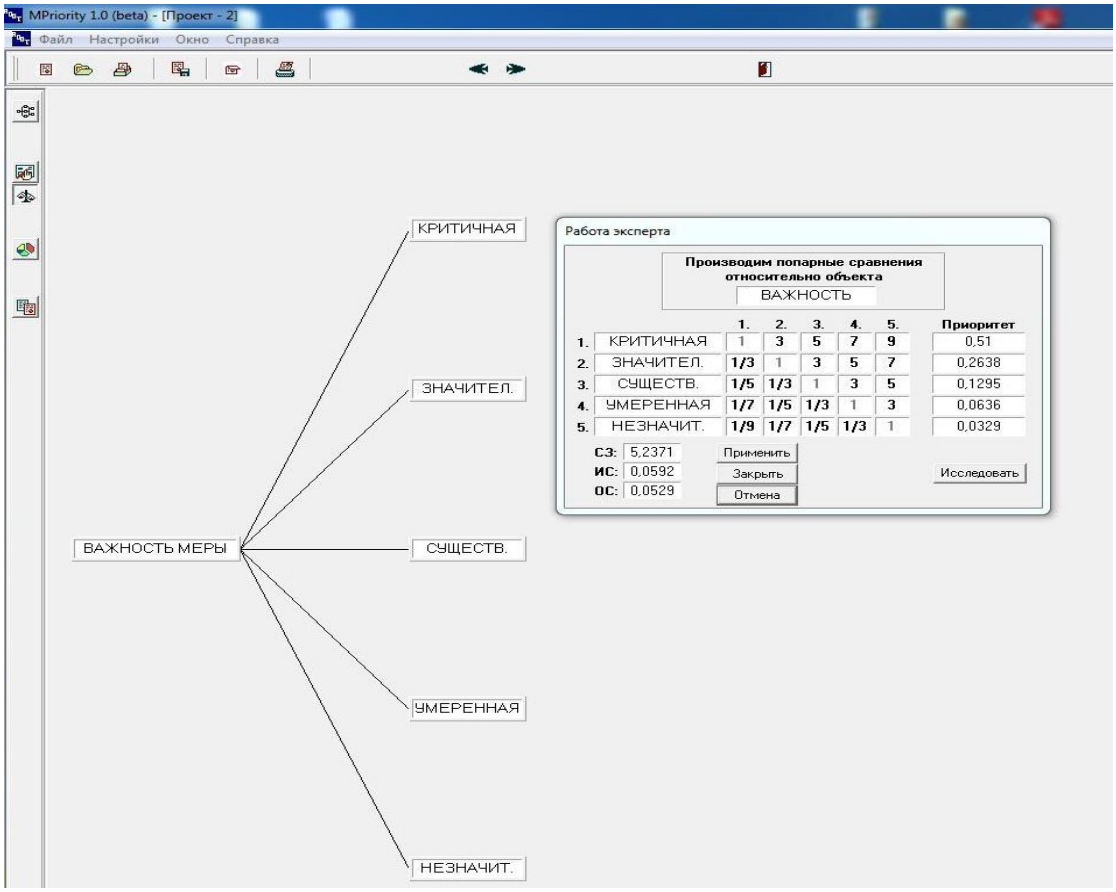

Рисунок 11 – Интерфейс программы MPriority

Существенное ограничение MPriority заключается в возможности расчета только относительных приоритетов, в то время как для оценки весовых коэффициентов качественных значений метрик в диссертационной работе используются абсолютные приоритеты. По этой причине для проведения опроса экспертов в Microsoft Excel разработаны следующие опросные листы (ОЛ):

– ОЛ-1 «Матрицы парных сравнений метрик нарушителей»;

– ОЛ-2 «Матрицы парных сравнений значений признаков нарушителей»;

– ОЛ-3 «Матрицы парных сравнений категорий защитных мер»;

– ОЛ-4 «Таблица оценки степени важности защитных мер».

Группа экспертов, включающая 18 специалистов в области ИБ, формировалась с учетом общих требований, предъявляемых к экспертам, приведенных в стандартах по оценке рисков [115, 117] и аудиту [43]:

– наличие высшего технического образования;
– наличие опыта работы не менее четырех лет, в том числе в области ИБ – не менее двух лет.

Заполнение ОЛ осуществлялось экспертами, соответствующими хотя бы одному частному требованию:

1) для ОЛ-1 и ОЛ-2:
   – наличие знаний по формированию модели нарушителя, подтверждаемых прохождением курса или наличием сертификата;
   – успешный опыт разработки модели нарушителя для ИС любого типа;
2) для ОЛ-3 и ОЛ-4:
   – наличие знаний в области защиты ИС, подтверждаемых прохождением учебного курса или наличием сертификата;
   – успешный опыт проектирования, внедрения и/или администрирования СЗИ ИС.

Минимальное число экспертов, участвовавших в заполнении одного ОЛ, составило 12 человек. Рассмотрим процедуру оценки весовых коэффициентов, состоящую из шести последовательных этапов, приведенных на рисунке 12.

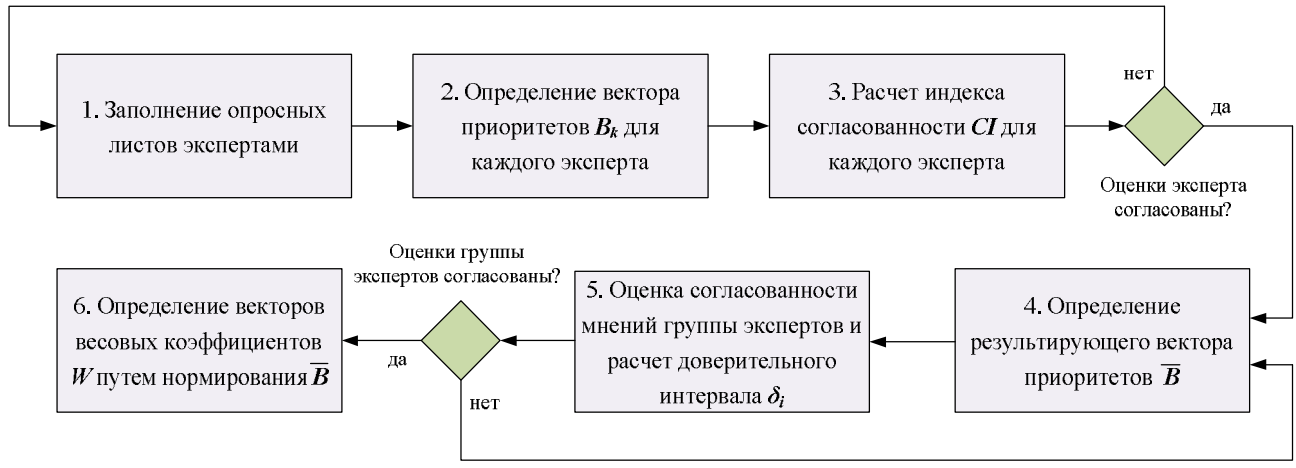

Рисунок 12 – Процедура оценки весовых коэффициентов

На первом этапе происходит заполнение ОЛ экспертами, соответствующими общим и частным требованиям. В ОЛ-1, ОЛ-2 и ОЛ-3 сравнительная степень важности элементов определяется в соответствии со шкалой, приведенной в таблице 6. В ОЛ-4 приоритеты элементов расставляются экспертами согласно шкале, приведенной в таблице 7, после чего осуществляется переход к четвертому этапу.

На втором этапе производится расчет векторов приоритетов $B_k = (b_{1k}, b_{2k}, ..., b_{mk})^T$ для каждого эксперта, исходя из равенства:

$$C_k \cdot B_k = \lambda_{k\max} \cdot B_k, \tag{30}$$

где C_k – матрица парных сравнений элементов x_i, полученная k-ым экспертом;

$\lambda_{k\max}$ – максимальное собственное число матрицы C_k.

На третьем этапе осуществляется проверка согласованности оценок каждого эксперта, для этого определяется индекс согласованности *CI* по формуле:

$$CI = \frac{\lambda_{k\max} - m}{m-1}, \tag{31}$$

где m – размерность матрицы парных сравнений.

Для оценки приемлемости полученных оценок используется отношение согласованности *CR*, определяемое по формуле:

$$CR = \frac{CI}{CIS}, \tag{32}$$

где *CIS* – среднее значение индекса согласованности как случайной величины.

Значения *CIS* и *CR* в зависимости от m представлены в таблице 8 [113].

Таблица 8 – Значения *CIS* и *CR* в зависимости от m

m	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
CIS	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48
CR	[0;0,05]	[0;0,08]	[0;0,1]							

Неприемлемые оценки должны быть скорректированы экспертом, в противном случае их не следует учитывать при расчете результирующего вектора приоритетов.

На четвертом этапе определяется результирующий вектор приоритетов $\overline{B}$:

$$\overline{B} = \left(\overline{b_1}, \overline{b_2}, ..., \overline{b_m}\right)^T, \ \overline{b_i} = \sqrt[K_E]{\prod_{k=1}^{K_E} b_{ik}}, \tag{33}$$

где $\overline{b_i}$ – результирующий приоритет элемента x_i;

K_E – число экспертов.

На пятом этапе определяется согласованность мнений группы экспертов. Мнения экспертов считаются согласованными, если все приоритеты b_{ik} лежат в интервале $\left(\overline{b_i} - 3\sigma_{gi}; \overline{b_i} + 3\sigma_{gi}\right)$, где σ_{gi} – геометрическое стандартное отклонение весового коэффициента b_{ik}, вычисляемое по формуле:

$$\sigma_{gi} = e^{\left(\sqrt{\frac{1}{K_E}\sum_{k=1}^{K_E}\left(\ln\frac{b_{ik}}{\overline{b_i}}\right)^2}\right)}. \tag{34}$$

Если мнения одного или нескольких экспертов признаются несогласованными на данном этапе, они отбрасываются и осуществляется возврат к четвертому этапу, то есть пересчитывается результирующий вектор приоритетов без учета оценок экспертов, мнения которых не согласованы с остальными. Доверительный интервал δ_i определяется по формуле:

$$\delta_i = t_{cm} \cdot \left(\frac{\sigma_{gi}}{\sqrt{K_E}}\right), \tag{35}$$

где t_{cm} – критерий Стьюдента. В диссертационной работе значение t_{cm} определяется в зависимости от K_E при доверительном уровне 0,95.

На шестом, заключительном этапе, определяются значения весовых коэффициентов. Для метрик нарушителей (ОЛ-1), категорий защитных мер (ОЛ-3) и метрик защитных мер (ОЛ-4) весовые коэффициенты определяются путем нормирования результирующего вектора приоритетов:

$$w_i = \frac{\overline{b_i}}{\sum_{i=1}^{m}\overline{b_i}}, \forall i \in [1; m]. \tag{36}$$

Для значений признаков нарушителей (ОЛ-2) определяются абсолютные весовые коэффициенты по формуле:

$$u_i = \frac{\overline{b_i}}{\overline{b}_{\max}}, \tag{37}$$

где $\overline{b}_{\max}$ – максимальное значение приоритета в составе вектора $\overline{B}$.

Результаты начальной оценки весовых коэффициентов метрик и категорий приведены в таблицах Б.1-Б.3 приложения Б.

Для оценки степени реализации требований, предъявляемых к защитной мере, сформирована трехуровневая шкала, представленная в таблице 9. Определение весовых коэффициентов осуществлялось путем преобразования вектора приоритетов по формуле [90]:

$$u_i = \frac{b_i - b_{\min}}{b_{\max} - b_{\min}}. \tag{38}$$

Таблица 9 – Шкала оценки степени реализации требований, предъявляемых к защитной мере

Степень реализации	**Усиленный уровень**	**Базовый уровень**	**Не реализована**	**Приоритет, b_i**	**Весовой коэффициент, u_i**
Усиленный уровень	1,00	2,00	7,00	2,41	1
Базовый уровень	0,50	1,00	5,00	1,357	0,5
Не реализована	0,14	0,20	1,00	0,306	0

2.4 Модель оценки рисков безопасности корпоративной информационной системы

Для повышения качества выбора защитных мер для КИС в диссертационной работе предлагается использовать формализованную модель количественной оценки рисков, учитывающую связи между рисковыми событиями и формируемую на основе представленных ранее инфраструктурной модели КИС и модели сценариев реализации угроз.

Рассмотрим правила формирования модели оценки рисков безопасности КИС, определения вероятности и величины ущерба от рисковых событий.

2.4.1 Формирование модели оценки рисков

Исходными данными для формирования модели оценки рисков безопасности КИС являются:

- сведения об элементах КИС и связях между ними (инфраструктурная модель КИС);
- правила оценки (модель сценариев реализации угроз).

Исходными данными для расчета показателей вероятности рисковых событий в модели являются:

- состав и характеристики (средняя частота реализации угроз) естественных источников угроз;
- состав и характеристики (значения метрик) нарушителей;
- состав и характеристики (значения метрик) превентивных и корректирующих защитных мер;

Исходными данными для расчета величины ущерба от рисковых событий являются значения стоимостных показателей последствий, приведенных в пункте 2.4.3 диссертационной работы.

Детализация и точность результатов оценки рисков зависят от того, насколько полны и достоверны исходные данные.

Модель оценки рисков безопасности КИС представлена в диссертационной работе ориентированным графом:

$$G^{RM} = \{V^{RM}, H^{RM}\}, \quad (39)$$

где V^{RM} – вершины графа G^{RM};

H^{RM} – дуги графа G^{RM}, соединяющие две его вершины.

Формирование графа G^{RM} осуществляется на основе инфраструктурной модели КИС G^{IS} и модели сценариев реализации угроз G^{TM} следующим образом.

1. Определяются вершины $v_i \in V^{DS} \subset V^{RM}$, соответствующие деструктивным состояниям элементов КИС, где $V^{DS} = \{O^{HW} \times DS^{HW}, \ O^{CL} \times DS^{CL}, \ O^{SW} \times DS^{SW}, \ O^{IA} \times DS^{IA}\}$. Рассмотрим правила определения попарных произведений. Пускай $O^{CL} = \{CL_1, CL_2\}$. Тогда, учитывая, что $DS^{CL} = \{CL^{[I]}, CL^{[U]}\}$, справедливо: $O^{CL} \times DS^{CL} = \{CL_1^{[I]}, CL_1^{[U]}, CL_2^{[I]}, CL_2^{[U]}\}$.
2. Определяются вершины $v_i \in V^{NS} \subset V^{RM}$, соответствующие естественным источникам угроз, и вершины $v_i \in V^{AS} \subset V^{RM}$, соответствующие нарушителям. Групповому нарушителю соответствует одна вершина v_i.
3. Для дуг $h_{ji} \in H^{NS}$, соединяющих вершины $v_i \in V^{NS}$ с вершинами $v_j \in V^{DS}$, и дуг $h_{ji} \in H^{AS}$, соединяющих вершины $v_i \in V^{AS}$ с вершинами $v_j \in V^{DS}$, в матрице смежности A^{RM} элемент $a_{ij}^{RM} = 1$, если выполняются условия:
   - в матрице A^{ST} для источника угроз $ST_x^{IS} \to v_i$ и элемента КИС $O_y^{IS} \to v_j$ справедливо: $a_{xy}^{ST} = 1$;
   - в матрице A^{TM} для источника угроз $ST_x^{IS} \to v_i$ и деструктивного состояния $DS_y^{IS} \to v_{ji}$ справедливо: $a_{xy}^{TM} = 1$.
4. Для дуг $h_{ji} \in H^{DS}$, соединяющих вершины $v_i \in V^{DS}$ с вершинами $v_j \in V^{DS}$, в матрице смежности A^{RM} элемент $a_{ij}^{RM} = 1$, если выполняются условия:
   - в матрице A^{IS} для элементов КИС $O_x^{IS} \to v_i$ и $O_y^{IS} \to v_j$ справедливо: $a_{xy}^{IS} = 1$;
   - в матрице A^{TM} для деструктивных состояний $DS_x^{IS} \to v_i$ и $DS_y^{IS} \to v_j$ справедливо: $a_{xy}^{TM} = 1$.

Для вершин графа G^{RM} осуществляется расчет следующих показателей:

- для $v_i \in V^{NS}$ определяются значения λ_i;
- для $v_i \in V^{AS}$ определяются значения d_i;
- для $v_i \in V^{DS}$ определяются значения ψ_i и ψ_i'.

Под полным риском безопасности КИС понимается сумма рисков безопасности всех ее элементов до внедрения защитных мер. Полный риск безопасности КИС R_{IS} определяется по формуле:

$$R_{IS} = \sum_{v_j \in V^{DS}} p(v_j) \cdot q(v_j) \,. \tag{40}$$

где $p(v_j)$ – безусловная вероятность рискового события;

$q(v_j)$ – величина ущерба от рискового события.

Представленная модель оценки рисков безопасности КИС обладает универсальностью, и при дополнительной проработке метрик нарушителей и защитных мер может быть использована для других типов систем, например, АС управления технологическими процессами [61].

2.4.2 Определение вероятности рисковых событий

Переход элемента КИС в деструктивное состояние происходит в результате реализации угроз источником. Принимая утверждение о независимости переходов, вызванных естественными источниками и нарушителями, безусловную вероятность рискового события $p(v_j)$ можно определить по формуле:

$$p(v_j) = 1 - (1 - p^{NS}(v_j)) \cdot (1 - p^{AS}(v_j)), \tag{41}$$

где $p^{NS}(v_j)$ – безусловная вероятность перехода, вызванного естественными источниками угроз;

$p^{AS}(v_j)$ – безусловная вероятность перехода, вызванного нарушителями.

Для оценки безусловной вероятности переходов, вызванных естественными источниками угроз, на основе графа G^{RM} строится ориентированный ациклический граф отказов $G^F = \{V^F, H^F\}$.

1. Из графа G^{RM} удаляются вершины, соответствующие нарушителям и деструктивным состояниям, переходы в которые осуществляются под воздействием нарушителей: $V^F = V^{RM} \setminus (V^{AS} \cup HW_i^{[I]} \cup CL_i^{[I]} \cup SW_i^{[I]} \cup IA_i^{[I]}), \forall i$.
2. Из графа G^{RM} удаляются дуги, соответствующие переходам, вызванным нарушителями: $H^F = H^{RM} \setminus H^{AS}$.

3. Из полученного графа удаляются циклы, образованные несколькими вершинами $v_i = SW_i^{[U]}$, путем слияния данных вершин.
4. Выполняется топологическая сортировка графа G^F поиском в глубину, в ходе которой вершинам v_i присваиваются номера, начиная с 1, чтобы для любой дуги h_{ji} выполнялось правило: $i < j$ [66]. При этом для любых $v_i \in V^{NS}$ и $v_j \in V^{DS}$ справедливо: $i < j$.

Поскольку переходы, вызванные естественными источниками угроз, носят случайный характер и происходят независимо друг от друга, значение $p^{NS}(v_j)$ определяется вероятностью реализации хотя бы одного из независимых сценариев, приводящих к данному переходу. Для каждой вершины $v_j \in V^{DS}$ в порядке увеличения j определяется безусловная вероятность перехода, вызванного естественными источниками угроз, по формуле:

$$p^{NS}(v_j) = 1 - \prod_{\forall i:\, a_{ij}^F = 1} \left(1 - p^{NS}(v_j \mid v_i)\right), \qquad (42)$$

где $A^F = [a_{ij}^F]$ – матрица смежности графа G^F;

$p^{NS}(v_j \mid v_i)$ – условная вероятность перехода элемента КИС в деструктивное состояние v_j в результате возникновения причины v_i, определяемая весовой функцией f_{ji}^{NS} по формуле (19).

На рисунке 13 показаны примеры сценариев реализации стихийным источником V_1^{NS} и техногенным источником V_2^{NS} угроз, приводящих к нарушению доступности ПО. Так, недоступность ПО может быть вызвана программным сбоем (h_{52}) либо нарушением доступности связанных ТС (h_{53}) и ЛС (h_{54}). В свою очередь, нарушение доступности ТС может быть вызвано его отказом (h_{32}) или повреждением в результате катастрофы (h_{31}), а нарушение доступности ЛС – отказом (h_{42}), повреждением в результате катастрофы (h_{41}) или отказом связанного ТС (h_{43}).

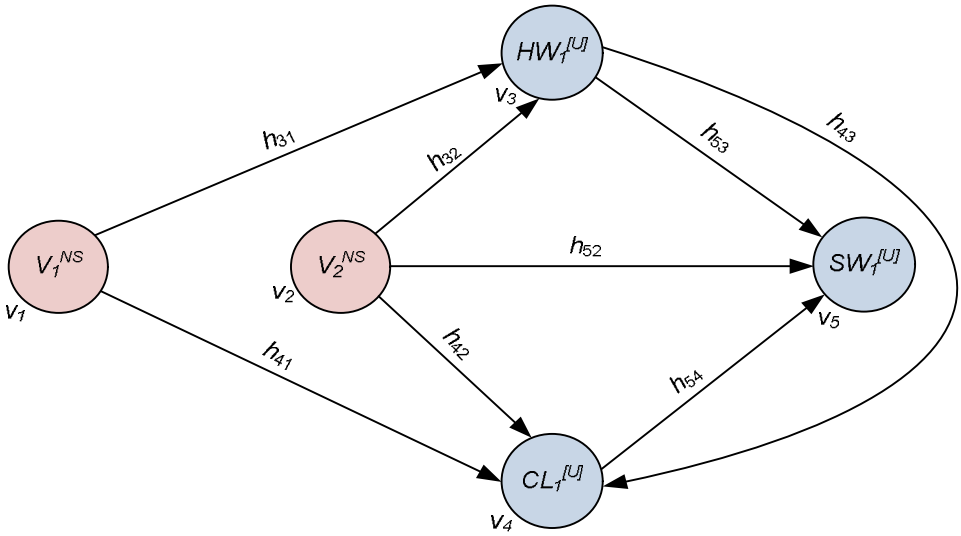

Рисунок 13 – Сценарии реализации угроз естественными источниками, приводящих к нарушению доступности ПО

Согласно формуле (42), значения безусловной вероятности нарушения доступности ТС, ЛС и ПО естественными источниками для примера, приведенного на рисунке 13, определяются выражениями:

$$p^{NS}(v_3) = 1 - \left(1 - p(v_3 \mid v_1)\right) \cdot \left(1 - p(v_3 \mid v_1)\right);$$
$$p^{NS}(v_4) = 1 - \left(1 - p(v_3 \mid v_1)\right) \cdot \left(1 - p(v_3 \mid v_1)\right) \cdot \left(1 - p^{NS}(v_3)\right);$$
$$p^{NS}(v_5) = 1 - \left(1 - p(v_5 \mid v_2)\right) \cdot \left(1 - p^{NS}(v_3)\right) \cdot \left(1 - p^{NS}(v_4)\right).$$

Для оценки значений безусловной вероятности переходов под воздействием нарушителей на основе графа G^{RM} строится ориентированный граф атак $G^A = \left\{V^A, H^A\right\}$.

1. Из графа G^{RM} удаляются вершины, соответствующие естественным источникам угроз: $V^A = V^{RM} \setminus V^{NS}$.
2. Из графа G^{RM} удаляются дуги, соответствующие переходам, вызванным естественными источниками угроз: $H^A = H^{RM} \setminus H^{NS}$.
3. Выполняется сортировка графа G^A, в ходе которой вершинам v_i присваиваются номера, начиная с 1, чтобы для любых $v_i \in V^{AS}$ и $v_j \in V^{DS}$ было справедливо: $i < j$.

К одному и тому же переходу могут привести сценарии реализации угроз, вызванные действиями различных нарушителей. Данные сценарии не являются независимыми, поскольку они содержат одинаковые вершины и дуги. В

соответствии с принципом гарантированного результата значение $p^{AS}(v_j)$ предлагается определять как наибольшее значение вероятности реализации сценария, приводящего к данному переходу:

$$p^{AS}(v_j) = \underset{v_i \in V^{AS}}{MAX} \left(p^{AS}(v_j \mid v_i) \right), \tag{43}$$

где $p^{AS}(v_j \mid v_i)$ – условная вероятность перехода элемента КИС в деструктивное состояние v_j под воздействием нарушителя v_i.

Для каждого нарушителя $v_i \in V^{AS}$ определяются наиболее вероятные сценарии реализации угроз, приводящие к переходам $v_j \in V^{DS}$. Прежде всего, рассчитываются значения весовых функций переходов f_{ji}^{AS} по формуле (22) и определяются соответствующие им длины дуг l_{ji} по формуле:

$$l_{ji} = -\ln(f_{ji}^{AS}). \tag{44}$$

Преобразование (44) позволяет свести задачу определения наиболее вероятных сценариев реализации угроз к задаче нахождения кратчайших путей из вершины $v_i \in V^{AS}$ во все достижимые из нее вершины $v_j \in V^{DS}$, для решения которой существуют такие алгоритмы как: алгоритмы Дейкстры, алгоритм Беллмана-Форда, алгоритм Джонсона, алгоритм Флойда-Уоршелла и другие [66]. Наиболее простым и распространенным на практике является алгоритм Дейкстры, позволяющий находить кратчайшие пути в графах, в которых отсутствуют дуги с отрицательными весами, таких как граф G^A.

В соответствии с алгоритмом Дейкстры кратчайший путь L_{ji} из вершины $v_i \in V^{AS}$ до каждой вершины $v_j \in V^{DS}$ должен удовлетворять условию [13]:

$$L_{ji} = \sum_{x,y=1} l_{xy} \cdot \chi_{xy} \to \min, \tag{45}$$

где $\chi_{xy} = 1$, если дуга h_{xy} входит в путь, $\chi_{xy} = 0$, если дуга h_{xy} не входит в путь.

Вероятность перехода элемента КИС в деструктивное состояние $v_j \in V^{DS}$ под воздействием нарушителя $v_i \in V^{AS}$ определяется по формуле:

$$p_{AS}(v_j \mid v_i) = e^{-L_{ji}}. \tag{46}$$

На рисунке 14 представлены возможные сценарии реализации угроз, приводящих к нарушению конфиденциальности ИА нарушителями V_1^{AS} и V_2^{AS}, между которыми отсутствует сговор.

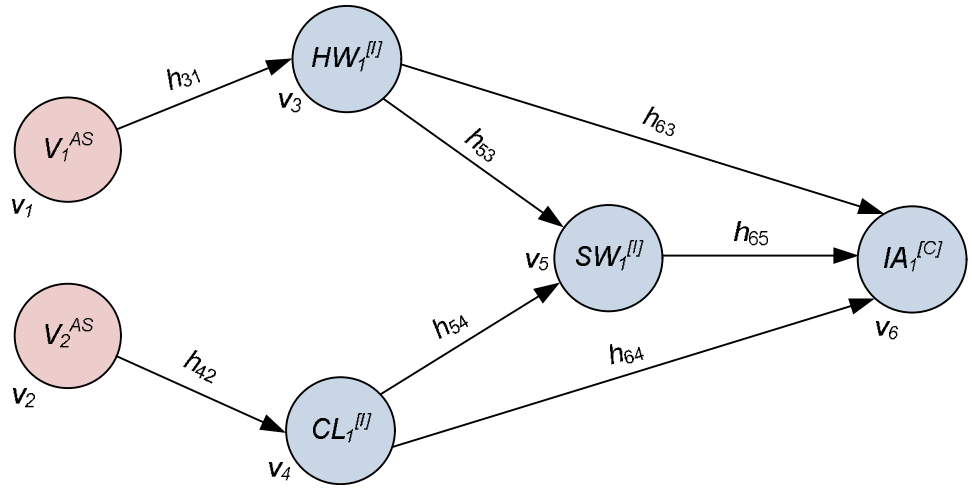

Рисунок 14 – Сценарии реализации угроз нарушителями, приводящих к нарушению конфиденциальности ИА

Так, нарушение конфиденциальности ИА может произойти в результате реализации одного из следующих сценариев:

– получение физического НСД к ТС первым нарушителем (h_{31}) и последующая кража носителя информации (h_{63});
– получение физического НСД к ТС первым нарушителем (h_{31}), взлом ПО (h_{53}) и последующее копирование информации (h_{65});
– получение НСД к ЛС вторым нарушителем (h_{42}) и перехват передаваемой по ней информации (h_{64});
– получение НСД к ЛС вторым нарушителем (h_{42}), взлом ПО (h_{54}) и последующее копирование информации (h_{65}).

Предложенные алгоритмы позволяют определить значения безусловной вероятности рисковых событий с учетом всех возможных связей между элементами КИС и источниками угроз.

2.4.3 Оценка величины ущерба от рисковых событий

Величина ущерба от перехода элемента КИС в деструктивное состояние $q(v_j)$ для $v_j \in V^{DS}$ определяется суммой возникающих при этом последствий,

выраженных в стоимостных показателях, с учетом степени реализации корректирующих защитных мер:

$$q(v_j) = \left(1 - \psi'_j\right) \cdot \sum_b J_{jb}\,, \tag{47}$$

где ψ'_i – степень реализации корректирующих защитных мер;

J_{jb} – b-ый показатель последствий.

Показатели последствий, предложенные в диссертационной работе, сформированы в результате анализа стандартов и методологий по оценке рисков, рассмотренных в подразделе 1.2, методических материалов в области экономики [74], методик оценки репутационного [51] и экологического [20] ущерба. Предложенные показатели последствий могут быть уточнены и дополнены с учетом функций, выполняемых КИС.

Величина ущерба от НСД к ТС, ЛС и ПО, а также от нарушения доступности ПО определяется по формуле:

$$q(v_j) = \left(1 - \psi'_j\right) \cdot J_{FW}\,, \forall v_j \in HW^{[I]} \cup DC^{[I]} \cup SW^{[I]} \cup SW^{[U]}\,, \tag{48}$$

где J_{FW} – затраты на восстановительные работы, определяемые по формуле:

$$J_{FW} = \left(1 + k_p\right) \cdot \left(1 + k_s\right) \cdot \sum_l z_l \cdot t_l\,, \tag{49}$$

где k_p – коэффициент премирования;

k_s – доля отчислений в социальные фонды;

z_l – часовая зарплата l-го сотрудника, восстанавливающего работоспособность элемента КИС;

t_l – время в часах, затраченное l-ым сотрудником на восстановление элемента КИС.

При оценке величины ущерба от нарушения доступности ТС и ЛС предлагается использовать формулу:

$$q(v_j) = \left(1 - \psi'_j\right) \cdot \left(J_{FW} + J_{FR}\right), \forall v_j \in HW^{[U]} \cup DC^{[U]}\,, \tag{50}$$

где J_{FR} – затраты на ремонт или замену элемента КИС.

Для оценки величины ущерба от нарушения конфиденциальности, целостности и доступности ИА предлагается учитывать последствия для связанных с ИА бизнес-процессов, подразделяемые на четыре категории (рисунок 15).

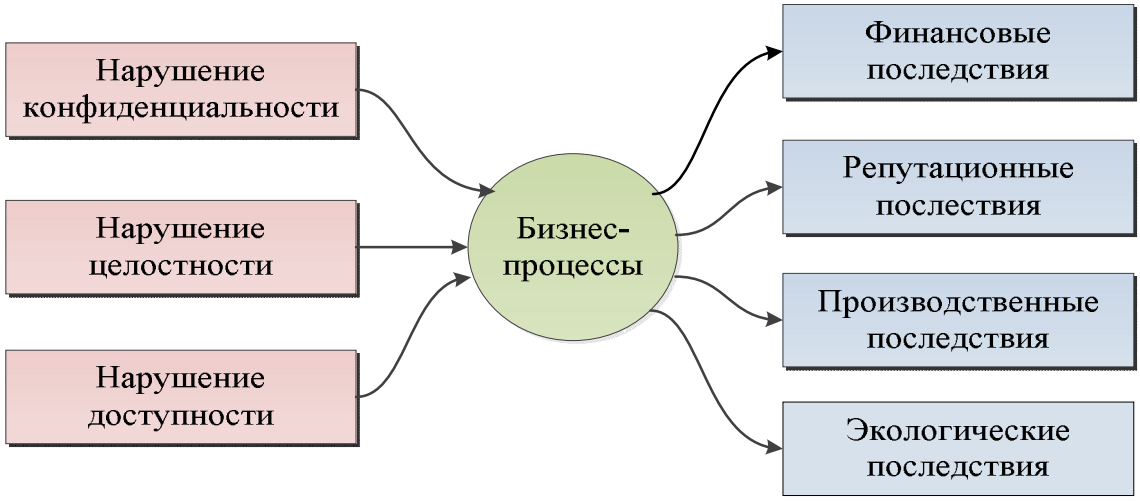

Рисунок 15 – Связь деструктивных состояний информационных активов с последствиями для бизнес-процессов

Величина ущерба от перехода ИА в деструктивное состояние, таким образом, может быть определена по формуле:

$$q(v_j) = \left(1-\psi'_j\right)\cdot\left(J_F + J_R + J_H + J_E\right), \forall v_j \in IA^{[C]} \cup IA^{[M]} \cup IA^{[U]}, \quad (51)$$

где J_F – финансовые последствия;

J_R – репутационные последствия;

J_H – производственные последствия;

J_E – экологические последствия;

Финансовые последствия J_F определяются как:

$$J_F = J_{FP} + J_{FL} + J_{FW}, \quad (52)$$

где J_{FP} – непредвиденные расходы;

J_{FL} – размер упущенной выгоды.

Непредвиденные расходы J_{FP}, в свою очередь, определяются как:

$$J_{FP} = J_{FPP} + J_{FPC} + J_{FPM}, \quad (53)$$

где J_{FPP} – штрафы за нарушение требований нормативно-правовых актов;

J_{FPC} – компенсационные выплаты за нарушение требований договоров;

J_{FPM} – прочие денежные выплаты.

Упущенная выгода возникает вследствие приостановки и затруднения выполнения бизнес-процессов при переходе ИА в деструктивное состояние. Например, бизнес-процесс «продажа товаров» может быть приостановлен или существенно затруднен при нарушении доступности БД интернет-магазина. Размер упущенной выгоды J_{FPL} определяется по формуле [52]:

$$J_{FPL} = t_d \cdot \sum_l D_l \cdot k_r , \tag{54}$$

где t_d – время нарушения функционирования элемента КИС;

D_l – средний часовой доход от реализации l-го бизнес-процесса;

k_r – степень зависимости бизнес-процесса от элемента КИС, $k_r \in [0; 1]$.

Репутационные последствия заключаются в снижении доверия, проявляемого к предприятию заинтересованными сторонами (клиентами, работниками, акционерами, партнерами и прочими). Для количественной оценки репутации используется понятие «гудвилл», характеризующее рыночную стоимость организации за вычетом балансовой стоимости ее активов. Существует несколько способов расчета гудвилла: оценка по объему реализации, оценка с позиций избыточной прибыли, оценка опционным методом [51]. Таким образом, репутационные последствия J_R определяются выражением:

$$J_R = \Delta Gw , \tag{55}$$

где ΔGw – изменение (снижение) гудвилла в результате нарушения свойства ИА, выраженное в стоимостных показателях.

При нарушении доступности или целостности технологической информации КИС, автоматизирующих производственные и технологические процессы на критически важных и потенциально опасных объектах, могут возникнуть производственные и экологические последствия.

Производственные последствия J_H определяются величиной страховых выплат при возникновении аварии по формуле:

$$J_H = S_I \cdot \sum_l d_l \,, \tag{56}$$

где S_I – страховая сумма (максимальная выплата для одного человека);

d_l – доля страховой суммы, выплачиваемая l-му потерпевшему.

Экологические последствия J_E определяются как:

$$J_E = J_{EA} + J_{EW} + J_{EL} + J_{EB}, \tag{57}$$

J_{EA} – последствия от загрязнения атмосферных ресурсов;

J_{EW} – последствия от загрязнения водных ресурсов;

J_{EL} – последствия от загрязнения земельных ресурсов;

J_{EB} – последствия от загрязнения биологических ресурсов.

Детализированные правила расчета экологических последствий приводятся в методике определения предотвращенного экологического ущерба [20].

Стоимость активов КИС S_{IS} определяется суммой последствий от нарушения безопасности ее элементов без учета корректирующих защитных мер:

$$S_{IS} = \sum_i \sum_b J_{ib}, \forall v_i \in V^{DS}. \tag{58}$$

2.4.4 Вычислительная сложность алгоритмов модели

Важным вопросом является определение вычислительной сложности алгоритмов, используемых в модели оценки рисков безопасности КИС. Большинство алгоритмов, предложенных в модели оценки рисков, имеют линейную сложность, а именно:

- алгоритмы поиска в глубину для сортировки графов G^A и G^F;
- оценка значений $p^{NS}(v_j)$ для вершин $v_j \in V^{DS}$;
- оценка величины ущерба для вершин $v_j \in V^{DS}$.

Следовательно, основную вычислительную сложность представляет задача нахождения кратчайших путей при оценке значений $p^{AS}(v_j)$ для вершин $v_j \in V^{DS}$.

Асимптотическая сложность алгоритма Дейкстры с использованием массива, как очереди приоритетов, при решении задачи нахождения кратчайших путей составляет $O\left(N_{DS}^2\right) \approx O\left(N_O^2\right)$, где N_{DS} – число вершин графа G^{RM}, соответствующих деструктивным состояния элементов КИС, N_O – количество элементов КИС.

Число обходов графа G^A с использованием алгоритма Дейкстры равняется числу нарушителей N_{AS}, следовательно, асимптотическая сложность задачи определения значений $p^{AS}(v_j)$ для вершин $v_j \in V^{DS}$ составляет $O\left(N_{AS} \cdot N_O^2\right)$. Как правило, число возможных нарушителей безопасности КИС не превышает нескольких десятков. Следовательно, при $N_O >> N_{AS}$ вычислительная сложность алгоритмов, используемых в предложенной модели оценки рисков, составляет:

$$T = O\left(N_O^2\right). \quad (59)$$

Следует отметить два способа снижения вычислительной сложности:

- использование для хранения непосещенных вершин фибоначчиевой кучи позволяет снизить вычислительную сложность до [66]: $T = O\left(N_O \cdot \log N_O\right)$;
- группировка идентичных элементов КИС, например, АРМ пользователей со схожей конфигурацией, позволяет снизить значение N_O.

2.5 Методика формирования рационального комплекса защитных мер

Защитные меры позволяют снизить риски безопасности КИС как за счет уменьшения вероятности реализации рисковых событий (превентивные меры), так и за счет снижения величины ущерба (корректирующие меры). Выбор защитных мер для таких сложных систем, как КИС, является нетривиальной задачей.

В диссертационной работе выполнен синтез методики, позволяющей сформировать рациональный комплекс защитных мер для КИС. Процедуры предлагаемой методики представлены в нотации UML на рисунке 16.

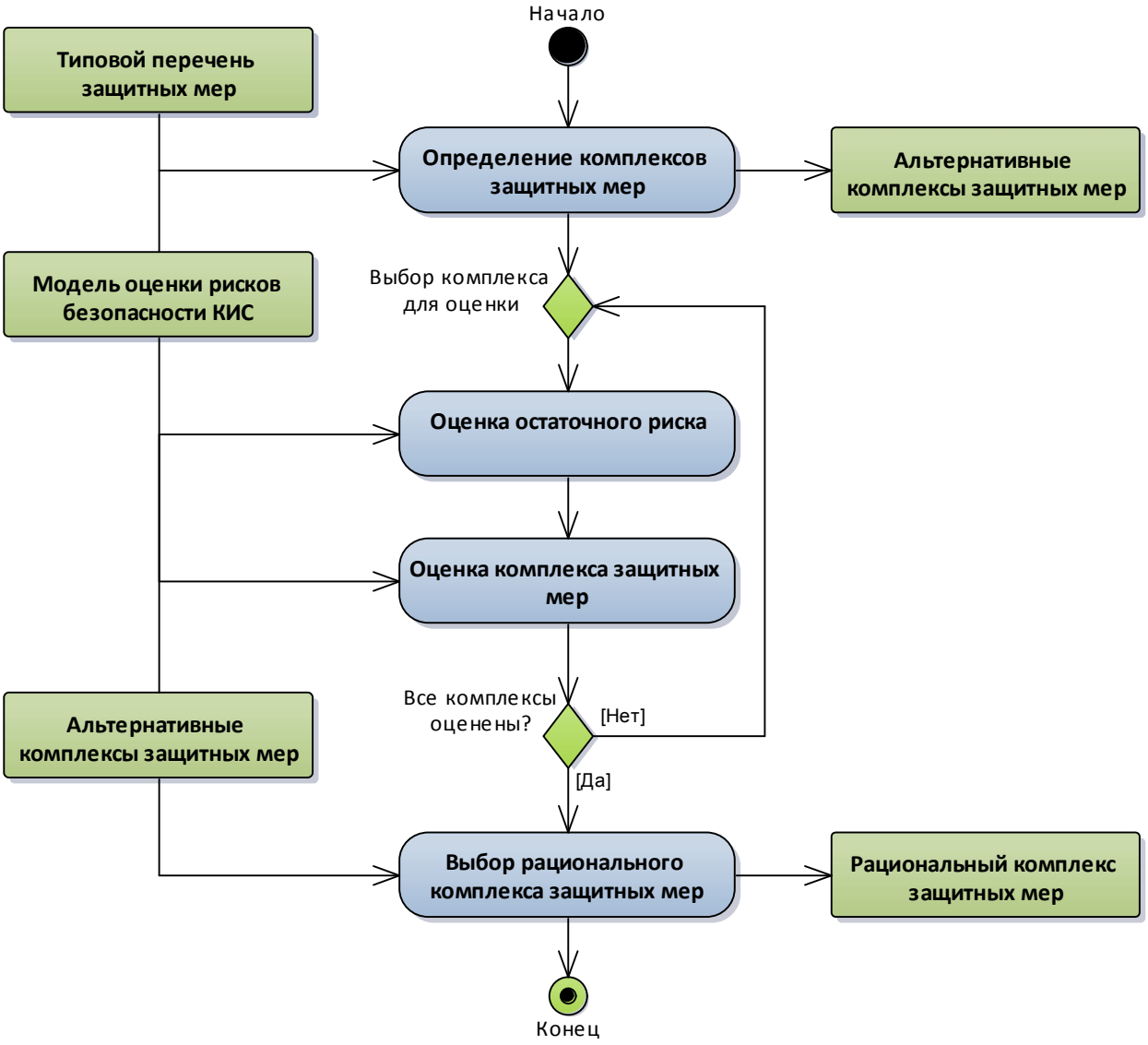

Рисунок 16 – Процедуры методики формирования рационального комплекса защитных мер

2.5.1 Определение альтернативных комплексов защитных мер

На основе типового перечня защитных мер, включающего различные СрЗИ и организационные меры, формируется множество альтернативных комплексов $Z_A = \{z_1, z_2, \ldots, z_x\}$, каждый из которых содержит определенный набор защитных мер $z_x = \{c_{x1}, c_{x2}, \ldots, c_{xy}\}$.

Формирование альтернативных комплексов защитных мер может осуществляться двумя способами:

– выборочное формирование комплексов защитных мер экспертом или группой экспертов;

– формирование всех допустимых наборов защитных мер.

При формировании допустимых наборов защитных мер в составе комплексов должны быть учтены следующие основные принципы, характерные, прежде всего, для СрЗИ:

- совместимость – выбираемые защитные меры должны быть совместимы друг с другом и с соответствующими элементами КИС;
- зависимость – одни защитные меры для реализации всех или части своих функций могут требовать обязательной реализации других защитных мер;
- взаимозаменяемость – необходимо избегать дублирования защитных мер, реализующих идентичный набор требований.

Кроме того, при формировании альтернативных комплексов защитных мер необходимо учитывать требования, предъявляемые нормативными документами. К таким документам могут относиться международные стандарты [150, 151], федеральные законы [100, 102], нормативные документы регуляторов [84, 104, 105, 106], отраслевые и корпоративные стандарты [128], а также локальные нормативные акты, например, политика ИБ предприятия.

Для каждого альтернативного комплекса защитных мер определяются затраты на реализацию S_z по формуле:

$$S_z = \sum_y S_{Cxy}, \tag{60}$$

где S_{Cxy} – затраты на y-ую защитную меру x-го комплекса.

Затраты на защитную меру могут включать прямые (капитальные и операционные) и косвенные затраты. К капитальным затратам относят расходы на приобретение, установку и обновление. К операционным относят затраты на проведение различных мероприятий по ИБ, включая затраты на обучение персонала, разработку документации, проведение аудита и другие. Кроме того, необходимо учитывать косвенные затраты, характеризующие потенциальные потери от различных плановых и внештатных ситуаций.

Затраты на защитную меру могут определяться с использованием одного из следующих показателей:

- показатель чистой приведенной стоимости *NPV* (*Net Present Value*);

– показатель совокупной стоимости владения *TCO* (*Total Cost of Ownership*), включающий затраты на планирование, реализацию, сопровождение и ликвидацию защитной меры [53].

Показатель *NPV* определяется величиной дисконтированных расходов на защитную меру по формуле:

$$NPV = \sum_t \frac{CF_t}{(1+r_d)^t}, \quad (61)$$

где CF_t – единовременные расходы на защитную меру в момент времени t;

r_d – ставка дисконтирования.

Поскольку бюджет, выделенный на формирование СЗИ КИС, как правило, ограничен, из числа альтернативных комплексов защитных мер следует исключить те, затраты на реализацию которых превышают допустимый бюджет S_B, то есть должно выполняться условие: $S_z < S_B$.

Значение риска безопасности КИС после внедрения комплекса защитных мер R_z называется остаточным риском. Как правило, при увеличении затрат на защитные меры остаточный риск постепенно снижается и стремится к нулю. Общий характер зависимости величины риска R от затрат на защитные меры S представлен на рисунке 17.

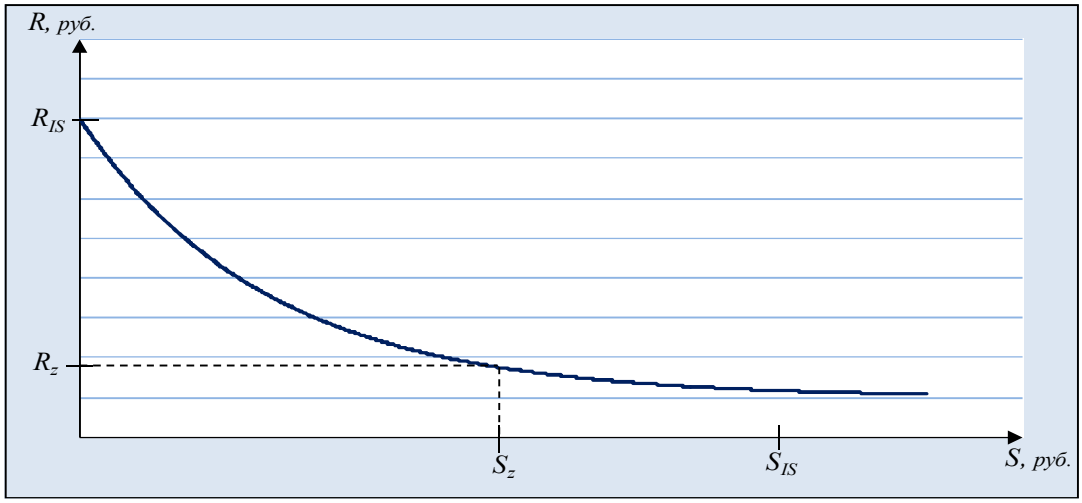

Рисунок 17 – Общий характер зависимости значения риска от затрат на защитные меры

Отметим, что затраты на реализацию комплекса защитных мер S_z не должны превышать стоимость активов КИС S_{IS}.

2.5.2 Постановка задачи выбора рационального комплекса защитных мер

В диссертационной работе слово «рациональный» используется как синоним таких слов как «оптимальный» и «эффективный». Вместе с тем, в условиях неопределенности и ограниченности рассматриваемого перечня защитных мер целесообразно говорить о рациональном, а не об оптимальном решении. Таким образом, под рациональным понимается наиболее подходящий в данных условиях комплекс защитных мер для КИС из всех рассмотренных.

Анализ стандартов и методологий по оценке рисков показал, что чаще всего для выбора защитных мер используются показатель возврата от инвестиций *ROI* (*Return on Investment*) и показатель экономической эффективности E_z.

Показатель возврата от инвестиций *ROI* рассчитывается по формуле:

$$ROI = \sum_{y} NPV(Benefits_{xy}) - \sum_{y} NPV(Costs_{xy}), \quad (62)$$

где $Benefits_{xy}$ – дисконтированные выгоды, определяемые снижением величины ущерба при использовании *y*-ой защитной меры x-го комплекса;

$Costs_{xy}$ – дисконтированные затраты на внедрение и поддержание *y*-ой защитной меры *x*-го комплекса;

Комплекс защитных мер целесообразно использовать в том случае, если $ROI > 0$. Трудность применения на практике показателя возврата от инвестиций обусловлена необходимостью прогнозирования не только затрат и выгод, но и времени их наступления, что далеко не всегда возможно.

Под экономической эффективностью понимается отношение выгоды от полученного результата к издержкам на достижение данного результата. Соответственно, показатель экономической эффективности комплекса защитных мер E_z может быть определен как отношение выгоды, выражаемой величиной, на которую уменьшился риск, к затратам на реализацию комплекса:

$$E_z = \frac{R_{IS} - R_z}{S_z}. \quad (63)$$

Целесообразность использования комплекса защитных мер определяется выражением: $E_z > 1$. Показатель экономической эффективности обратно пропорционален величине затрат на комплекс защитных мер и может принимать большие значения в том случае, если затраты на комплекс малы (например, при использовании бесплатных СрЗИ), что однако не свидетельствует о рациональности данного комплекса.

В диссертационной работе для выбора защитных мер предлагается использовать показатель затратоемкости активов ω_z, определяемый как [98]:

$$\omega_z = \frac{S_z + R_z}{S_{IS}}. \qquad (64)$$

Показатель затратоемкости активов определяется отношением суммы реальных затрат на защитные меры и предполагаемых затрат (величины остаточного риска) к стоимости защищаемых активов. Критерием выбора рационального комплекса защитных мер является минимизация показателя затратоемкости активов, достигаемая при оптимальном сочетании значения остаточного риска и затрат на реализацию комплекса защитных мер. Значения показателя ω_z при разных комплексах защитных мер, отсортированных в порядке уменьшения величины остаточного риска R_z, приведены на рисунке 18.

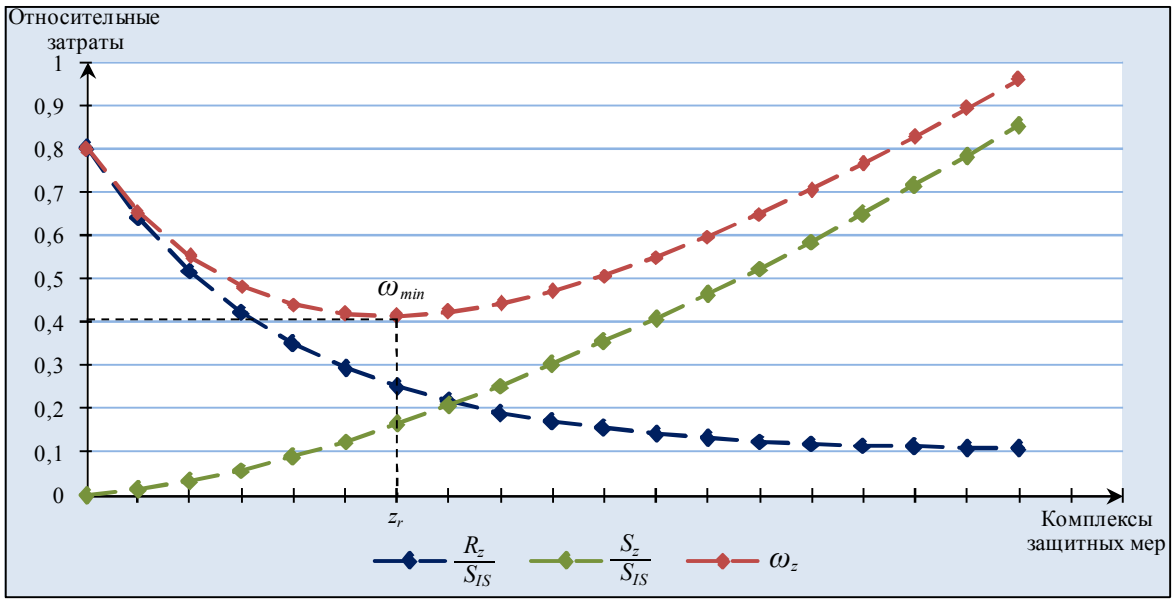

Рисунок 18 – Определение рационального комплекса защитных мер на основе показателя затратоемкости активов

Таким образом, в диссертационной работе выбор рационального комплекса защитных мер $z_r \in Z_A$ осуществляется в результате решения следующей задачи дискретной оптимизации:

$$\begin{cases} \omega_z \to \min\limits_{z_x \in Z_A}; \\ 0 \le S_z \le S_B. \end{cases} \quad (65)$$

Данная задача в простейшем случае решается полным перебором всех альтернативных комплексов защитных мер Z_A, соответствующих установленным ограничениям.

При равенстве показателей ω_z для нескольких альтернативных комплексов защитных мер выбор рационального комплекса среди них может осуществляться по одному из дополнительных критериев:

– минимизация величины остаточного риска: $R_z \to \min$;

– максимизация показателя экономической эффективности: $E_z \to \max$.

Показатель затратоемкости активов позволяет выбрать рациональный комплекс защитных мер из множества альтернативных вариантов. При этом формализованная модель количественной оценки рисков безопасности КИС, предложенная в подразделе 2.4 диссертационной работы, позволяет рассчитать значения остаточных рисков для комплексов защитных мер.

Практические результаты использования разработанной методики формирования рационального комплекса защитных мер приведены в подразделе 4.2 диссертационной работы.

Выводы по разделу 2

1. Проведен структурный анализ КИС, в результате которого определены основные типы элементов КИС и установлен характер связей между ними. Приведена унифицированная форма представления КИС в виде инфраструктурной модели.
2. Предложена научно-обоснованная модель сценариев реализации угроз КИС в виде ориентированного графа, вершинами которого являются

классы источников угроз и деструктивные состояния типов элементов КИС, а дугами – переходы элементов КИС в деструктивные состояния. Определены весовые функции переходов в зависимости от их причины.

3. Определена функция оценки вероятности реализации угроз нарушителем на основе показателей степени опасности нарушителя и степени реализации превентивных защитных мер. Для определения значений данных показателей сформированы наборы метрик и правил их оценки.
4. Проведена оценка начальных значений весовых коэффициентов метрик методом анализа иерархий с привлечением группы квалифицированных экспертов.
5. Предложена формализованная модель оценки рисков безопасности КИС, формируемая на основе инфраструктурной модели КИС и модели сценариев реализации угроз. Для оценки вероятности рисковых событий используются алгоритмы решения оптимизационных задач на графах. Для оценки величины ущерба от переходов элементов КИС в деструктивные состояния сформированы наборы показателей последствий и приведены правила их оценки.
6. Выполнен синтез методики формирования рационального комплекса защитных мер, основанной на минимизации значения показателя затратоемкости активов.

3 Повышение точности прогнозирования вероятности реализации угроз нарушителем на основе данных об инцидентах информационной безопасности

3.1 Настройка весовых коэффициентов метрик с использованием методов обучения нейронной сети

Для прогнозирования вероятности реализации угроз нарушителем в диссертационной работе используется функция f_{ji}^{AS}, определяемая формулой (22). Под обучением понимается процесс, в ходе которого осуществляется настройка свободных параметров функции f_{ji}^{AS}.

К свободным параметрам функции f_{ji}^{AS} относятся, прежде всего, весовые коэффициенты категорий w_{jg}^{K} и метрик w_{gl}^{C} защитных мер и метрик нарушителей w_{ih}^{V}, однако настройке могут подвергаться и другие свободные параметры, например, эталонные и пороговые значения признаков.

Качество решения задачи обучения зависит от выбранных параметров и метода обучения. Выбор метода обучения осуществляется исходя из специфики решаемой задачи и характеристики объектов обучающей выборки [19].

3.1.1 Характеристика объектов обучающей выборки

Объектами обучающей выборки для функции f_{ji}^{AS} являются данные о произошедших и предотвращенных инцидентах ИБ. В диссертационной работе под инцидентом ИБ понимается переход элемента КИС в деструктивное состояние в результате реализации одной или нескольких угроз нарушителем.

Данные об инциденте ИБ представляются кортежем:

$$I = [v_i, v_j, \{M_{ih}^{V}\}, \{M_{gl}^{C}\}, y_{ji}], \tag{66}$$

где $v_i \in V^{AS}$ – вершина-причина перехода;

$v_j \in V^{DS}$ – вершина-результат перехода;

$\{M_{ih}^{V}\}$ – множество метрик оценки степени опасности нарушителя;

$\{M_{gl}^{C}\}$ – множество метрик оценки степени реализации превентивных защитных мер;

y_{ji} – результат инцидента ИБ (y_{ji} = 1 – инцидент произошёл; y_{ji} = 0 – инцидент был предотвращен).

Таким образом, обучающая выборка представляет собой совокупность структурированных данных об инцидентах ИБ. Для повышения качества обучения база инцидентов ИБ КИС должна регулярно обновляться. Данные об инцидентах ИБ могут вноситься оператором вручную, либо импортироваться из различных АС, регистрирующих инциденты ИБ, таких как система мониторинга событий безопасности, система контроля защищенности, система предотвращения утечек информации и другие.

На рисунке 19 представлена диаграмма процесса обучения в нотации Engineering, Procurement and Construction (EPC).

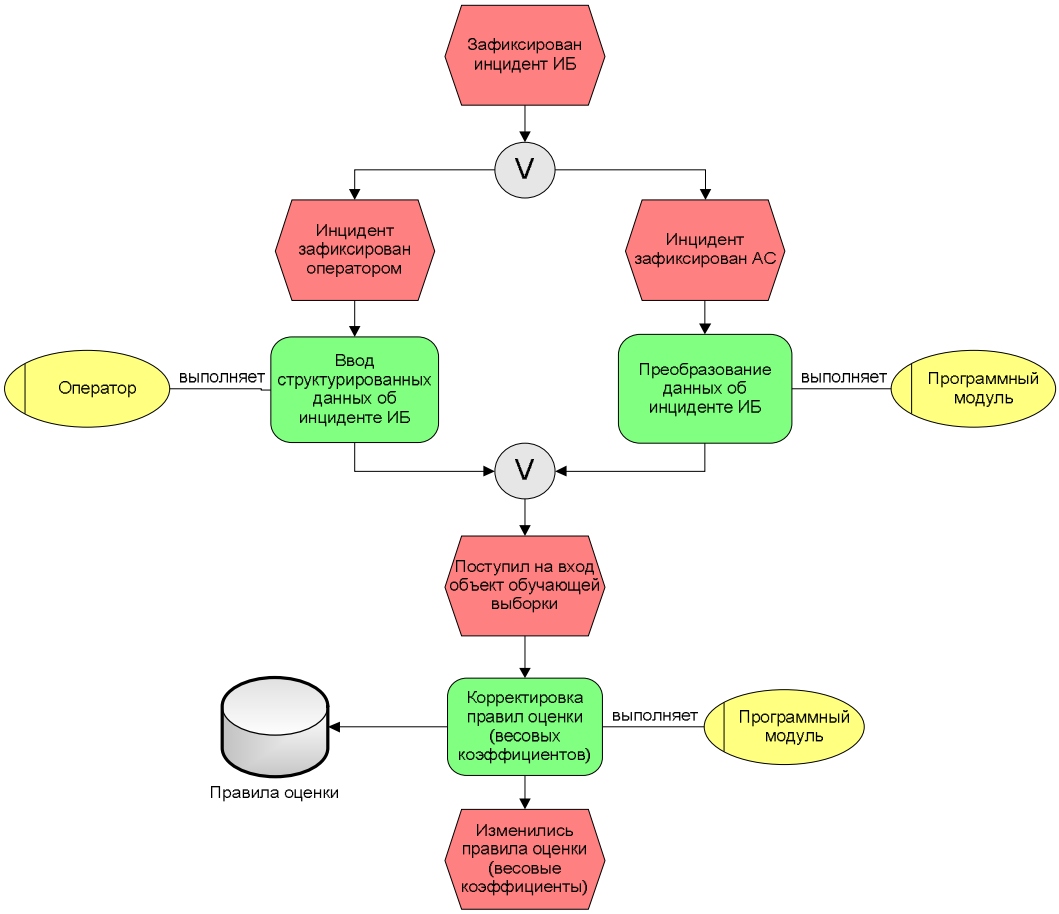

Рисунок 19 – Диаграмма процесса обучения

Стоит отметить важную особенность решаемой задачи обучения – небольшое число объектов обучающей выборки (инцидентов ИБ) для большинства переходов. Можно выделить следующие способы увеличения числа объектов обучающей выборки:

- выполнение тестирования на проникновение в КИС;
- использование данных об инцидентах ИБ, публикуемых в различных базах и аналитических отчетах;
- повторное использование объектов обучающей выборки.

Наиболее действенный способ увеличения числа объектов обучающей выборки без потери их качества – выполнение тестирования на проникновение, то есть имитация атакующих воздействий нарушителя на элементы КИС. Основная цель тестирования на проникновение – поиск уязвимостей, дающих нарушителю возможность реализовать угрозу или последовательность угроз, в результате которых произойдет один или несколько связанных переходов элементов КИС в деструктивные состояния. Результаты тестирования на проникновение используются в качестве объектов обучающей выборки.

Разработанная модель оценки рисков безопасности КИС достаточно универсальна, поэтому для обучения могут быть использованы данные об инцидентах ИБ КИС других предприятий. Это позволяет вести единую базу инцидентов ИБ. В мировой практике существуют и постоянно обновляются крупные базы инцидентов ИБ (Hackmageddon [147], OWASP [172] и другие).

При обучении можно также учитывать данные об инцидентах ИБ, публикуемые в аналитических отчетах компаний-разработчиков в области ИТ и ИБ. Примерами компаний, ежегодно публикующих статистические данные об инцидентах ИБ, являются Positive Technologies, Лаборатория Касперского, Microsoft, Cisco и другие.

Основными недостатками использования сведений из общедоступных баз аналитических отчетов являются:

- отсутствие гарантии достоверности сведений;
- как правило, отсутствие сведений о предотвращенных инцидентах ИБ;

– низкий уровень детализации и неполнота данных (отсутствие значений метрик).

Несмотря на отмеченные недостатки, очевидным преимуществом использования данных сведений является увеличение объема обучающей выборки, положительно сказывающееся на результатах обучения [19].

Анализ существующих баз инцидентов ИБ и аналитических отчетов, находящихся в свободном доступе, показал, что на сегодняшний день отсутствует открытая централизованная база инцидентов ИБ, данные из которой можно использовать в качестве обучающей выборки. В то же время, по мнению российских специалистов в области ИБ, создание национального центра мониторинга инцидентов ИБ – вопрос времени [76]. Вполне возможно, что подобная база скоро появится в дополнение к базам угроз и уязвимостей ФСТЭК России [7].

Качество результатов обучения можно также повысить за счет многократного использования данных об инцидентах ИБ, подаваемых на вход алгоритму обучения в произвольном порядке [109].

Еще одним важным вопросом является определение правил использования объектов обучающей выборки. Обычно обучение проводится в одном из двух режимов: последовательном или пакетном.

В последовательном режиме корректировка весовых коэффициентов осуществляется после подачи очередного объекта обучающей выборки, а в пакетном режиме – после подачи набора объектов, называемых «эпохой». Последовательный режим обучения является более медленным, поскольку требует пересчета весовых коэффициентов после каждого объекта обучающей выборки. В то же время, он менее подвержен остановкам в точках локальных минимумов, в отличие от пакетного режима.

Поскольку данные об инцидентах ИБ, как правило, поступают в режиме реального времени и их число сравнительно невелико, обучение целесообразно осуществлять в последовательном режиме.

3.1.2 Обоснование выбора метода обучения

Основываясь на приведенной характеристике объектов обучающей выборки и выводах, сделанных в разделе 2 диссертационной работы, сформированы требования, предъявляемые к методу обучения, приведенные ниже.

1. В процессе обучения должна осуществляться настройка свободных параметров функции f_{ji}^{AS} в последовательном режиме.
2. Существенное снижение величины остаточной ошибки (в несколько раз) должно достигаться при обучении на небольшом числе объектов обучающей выборки (от 100 до 1000 инцидентов ИБ).
3. Необходимо предусмотреть возможность обучения на неполных данных, когда для инцидента ИБ неизвестны значения части метрик.
4. В процессе обучения должен осуществляться отбор значимых признаков.
5. Алгоритм обучения должен выполняться за полиномиальное время.

Основываясь на приведенных требованиях, для решения поставленной задачи обучения целесообразно использовать методы, основанные на коррекции ошибок или минимизации целевой функции.

В основе данных методов обучения лежит информация о величине ошибки $\varepsilon^{(t)}$ для t-го объекта обучающей выборки, которая в общем случае определяется выражением:

$$\varepsilon^{(t)} = f_{ji}^{AS(t)} - y_{ji}^{(t)}. \quad (67)$$

где $f_{ji}^{AS(t)}$ – прогнозируемое значение вероятности реализации угроз нарушителем для t-го инцидента ИБ;

$y_{ji}^{(t)}$ – результат t-го инцидента ИБ.

Величина ошибки инициирует процедуру последовательной корректировки весовых коэффициентов путем минимизации целевой функции вида:

$$E = \frac{1}{2}\left(\varepsilon^{(t)}\right)^2 \to \min. \quad (68)$$

Поскольку f_{ji}^{AS} является сложной функцией, для ее обучения целесообразно использовать метод обратного распространения ошибки, применяемый для обучения многослойного персептрона.

Под многослойным персептроном понимается класс многослойных нейронных сетей прямого распространения, состоящих из элементарных единиц обработки информации (нейронов), накапливающих экспериментальные знания и предоставляющих их для последующей обработки. В литературе выделяют следующие преимущества многослойных персептронов [134, 178]:

- нелинейность (возможность строить более сложные и качественные модели нелинейных процессов);
- адаптивность (возможность обучения за счет изменения весовых коэффициентов);
- масштабируемость (возможность добавления и удаления нейронов в ходе обучения);
- сравнительная простота и глубокая изученность алгоритмов обучения.

В последовательном режиме обучения корректировка векторов весовых коэффициентов $w^{(t)}$ для t-го объекта обучающей выборки осуществляется по формуле [109]:

$$w^{(t)} = w^{(t+1)} + \Delta w^{(t)}. \qquad (69)$$

Вектор корректирующих значений весовых коэффициентов $\Delta w^{(t)}$ определяется на основе некоторого правила, выражаемого в виде равенства:

$$\Delta w^{(t)} = \eta \cdot l^{(t)}, \qquad (70)$$

где η – коэффициент, называемый темпом обучения [134];

l – направление в многомерном пространстве w.

Определение направления минимизации целевой функции осуществляется с помощью численных методов безусловной оптимизации, подразделяемых на безградиентные и градиентные [59, 131].

В безградиентных методах оптимизации направление минимизации целевой функции определяется последовательными вычислениями значений функции. К данным методам относятся: метод прямого поиска, метод деформируемого многогранника, метод покоординатного спуска, метод вращающихся координат, метод параллельных касательных и другие [131].

Безградиентные методы обладают меньшей вычислительной сложностью, но при этом и сравнительно меньшей скоростью сходимости, чем градиентные методы. Они обычно применяются для решения задач оптимизации, когда функция целевая функция не является непрерывной. Исходя из этого, следует сделать заключение о нецелесообразности выбора безградиентных методов для решения поставленной задачи обучения.

Градиентные методы оптимизации связаны с разложением целевой функции E в ряд Тейлора в ближайшей окрестности точки имеющегося решения w в направлении l, описываемого формулой [109]:

$$E(w+l) = E(w) + \left[g(w)\right]^T \cdot l + \frac{1}{2} l^T \cdot H(w) \cdot l + \ldots, \tag{71}$$

где $g(w)$ – вектор градиента, определяемый выражением:

$$g(w) = \nabla E = \left[\frac{\partial E}{\partial w_1}, \frac{\partial E}{\partial w_2}, \ldots, \frac{\partial E}{\partial w_L} \right]^T; \tag{72}$$

$H(w)$ – квадратная матрица производных второго порядка (гессиан):

$$H(w) = \begin{bmatrix} \partial^2 E / \partial w_1^2 & \ldots & \partial^2 / \partial w_1 \partial w_L \\ \ldots & \ldots & \ldots \\ \partial^2 / \partial w_L \partial w_1 & \ldots & \partial^2 E / \partial w_L^2 \end{bmatrix}. \tag{73}$$

На практике для решения задачи минимизации целевой функции с использованием градиентных методов чаще всего используются два или три первых члена ряда (71), а остальные игнорируются [109].

В методах оптимизации первого порядка используется два первых члена ряда (71). К данным методам, в частности, относятся [109]:

– метод градиентного спуска;

– метод градиентного спуска с моментом;

– метод сопряженных градиентов.

Самым простым методом оптимизации первого порядка является метод градиентного спуска, в соответствии с которым на каждом шаге обучения корректировка весовых коэффициентов осуществляется в направлении антиградиента и задается выражением:

$$\Delta w^{(t)} = -\eta \cdot g(w^{(t)}). \qquad (74)$$

Метод градиентного спуска применяется для решения широкого спектра задач, в том числе для оптимизации надежности [92] и оценки рисков [5]. Метод градиентного спуска применяется в классическом варианте метода обратного распространения ошибки [109].

Существенным недостатком данного метода является резкое замедление минимизации целевой функции в окрестности точки оптимального решения, то есть в точках, в которых градиент принимает малые значения. Повысить эффективность метода градиентного спуска можно путем различных модификаций выражения (74), определяющего направление изменения целевой функции.

В методе градиентного спуска с моментом уточнение весовых коэффициентов выполняется по правилу:

$$\Delta w^{(t)} = -\eta \cdot g(w^{(t)}) + \alpha \cdot \Delta w^{(t-1)}, \qquad (75)$$

где α – коэффициент момента, $\alpha \in [0; 1]$.

Второе слагаемое выражения (75) учитывает последнее изменение весовых коэффициентов и не зависит от фактического значения градиента, что позволяет осуществлять корректировку весовых коэффициентов вблизи локального минимума целевой функции.

Метод сопряженных градиентов аналогичен методу градиентного спуска с тем отличием, что направление спуска определяется не направлением антиградиента, а его линейной комбинацией с прежним направлением спуска. Корректировка весовых коэффициентов при использовании метода сопряженных градиентов осуществляется по правилу:

$$\Delta w^{(t)} = -\eta \cdot \left(- g(w^{(t)}) + \upsilon^{(t-1)} \cdot l^{(t-1)} \right), \tag{76}$$

где υ – коэффициент сопряжения.

Существуют различные формулы для оценки коэффициента сопряжения υ, например, формула Полака-Рибьера или формула Флетчера-Ривза. Метод сопряженных градиентов является достаточно эффективным алгоритмом оптимизации целевой функции, и при этом обладает относительно низкой вычислительной сложностью [109].

Ограничение применения метода сопряженных градиентов обусловлено предположением о неизменности целевой функции *E*, что, как правило, не выполняется в последовательном режиме обучения. Поэтому применение метода сопряженных градиентов ограничивается пакетным режимом обучения [19].

Основным преимуществом градиентных методов оптимизации второго порядка, в которых используются три первых члена ряда (71), является высокая сходимость, а главным недостатком – высокая вычислительная сложность, что ограничивает круг ими решаемых задач. Среди градиентных методов второго порядка следует выделить такие методы, как [109]:

- метод Ньютона-Рафсона;
- метод переменной метрики;
- метод Гаусса-Ньютона;
- метод Лавенберга-Маркара;

В соответствии с методом Ньютона-Рафсона корректировка весовых коэффициентов осуществляется согласно выражению:

$$\Delta w^{(t)} = -H(w^{(t)})^{-1} \cdot g(w^{(t)}). \tag{77}$$

Метод Ньютона-Рафсона обладает квадратичной сходимостью. Основной недостаток, существенно затрудняющий использование данного метода на практике, заключается в необходимости определения обратной матрицы $H(w^{(t)})^{-1}$. Для этого необходимо, чтобы гессиан, определяемый выражением (73), был положительно определенным на каждом шаге обучения, что практически неосуществимо [134]. По этой причине в других методах второго порядка вместо точно определенного гессиана $H(w^{(t)})$ используется его приближение $G(w^{(t)})$.

Основная суть метода переменной метрики заключается том, что на каждом шаге обучения гессиан или обратная ему величина, полученная на предыдущем шаге, модифицируется на величину некоторой поправки. Существуют различные алгоритмы для расчета значения этой поправки, наиболее известными из которых являются алгоритм Бройдена-Флетчера-Гольдфарба-Шанно (BFGS) и алгоритм Дэвидона-Флетчера-Пауэлла (DFP) [109].

В методе Гаусса-Ньютона для определения вектора корректирующих значений весовых коэффициентов используется матрица производных первого порядка целевой функции (Якобиан):

$$\Delta w^{(t)} = -\left(J(w^{(t)})^T \cdot J(w^{(t)})\right)^{-1} \cdot J(w^{(t)})^T \cdot \varepsilon^{(t)}, \tag{78}$$

где J – матрица производных первого порядка (Якобиан).

Для скалярной функции f_{ji}^{AS}, Якобиан представляет собой транспонированный вектор градиента [134], а выражение (78) принимает вид:

$$\Delta w^{(t)} = -\left(g(w^{(t)}) \cdot g(w^{(t)})^T\right)^{-1} \cdot g(w^{(t)}) \cdot \varepsilon^{(t)}. \tag{79}$$

Метод Гаусса-Ньютона обладает квадратичной сходимостью, и при этом не требует вычисления и обращения гессиана на каждом шаге обучения. Тем не менее, метод Гаусса-Ньютона в некоторых ситуациях некорректно работает и обладает медленной сходимостью [85]. Усовершенствованной версией метода Гаусса-Ньютона является метод Левенберга-Марквардта, согласно которому корректировка весовых коэффициентов осуществляется по правилу [109]:

$$\Delta w^{(t)} = -\left(g(w^{(t)}) \cdot g(w^{(t)})^T + \mu \cdot I_M\right)^{-1} \cdot g(w^{(t)}) \cdot \varepsilon^{(t)}, \tag{80}$$

где μ – неотрицательная переменная;

I_M – единичная матрица.

Существенным ограничением для большинства методов второго порядка является их применимость только в пакетном режиме обучения, когда функция E неизменна. Существуют различные модификации рассмотренных методов для последовательного режима обучения. Одной из таких модификаций является диагональный метод Левенберга-Марквардта, требующий для корректировки l-го весового коэффициента только один диагональный элемент матрицы вторых производных [19]:

$$\Delta w_l^{(t)} = -\frac{\eta}{\dfrac{\partial^2 E}{(\partial w_l^{(t)})^2} + \mu} \cdot \frac{\partial E}{\partial w_l^{(t)}} . \tag{81}$$

Применение диагонального метода Левенберга-Марквардта для обучения многослойного персептрона рассмотрено в работе ЛеКуна [160]. По сравнению с другими методами второго порядка данный метод обладает меньшей сложностью, сопоставимой со сложностью метода градиентного спуска, и в то же время обладает лучшей сходимостью, что подтверждено экспериментами [109].

Таким образом, для настройки свободных параметров функции f_{ji}^{AS} следует использовать различные вариации метода обратного распространения ошибки. В ходе экспериментального исследования целесообразно рассмотреть следующие методы корректировки весовых коэффициентов:

- метод градиентного спуска;
- метод градиентного спуска с моментом;
- диагональный метод Левенберга-Марквардта.

Вычислительная сложность данных методов имеет вид [19]:

$$T = O(N_W), \tag{82}$$

где N_W – число весовых коэффициентов многослойного персептрона, соответствующего функции f_{ji}^{AS}.

Основные результаты экспериментального исследования приведены в подразделе 3.2 диссертационной работы.

3.1.3 Представление функции вероятности реализации угроз нарушителем в виде многослойного персептрона

Задача обучения функции f_{ji}^{AS} равносильна задаче обучения многослойного персептрона, структура которого представлена на рисунке 20. Нейронами входного слоя рассматриваемого многослойного персептрона являются метрики нарушителей M_{ih}^{V} и метрики защитных мер M_{gl}^{C}.

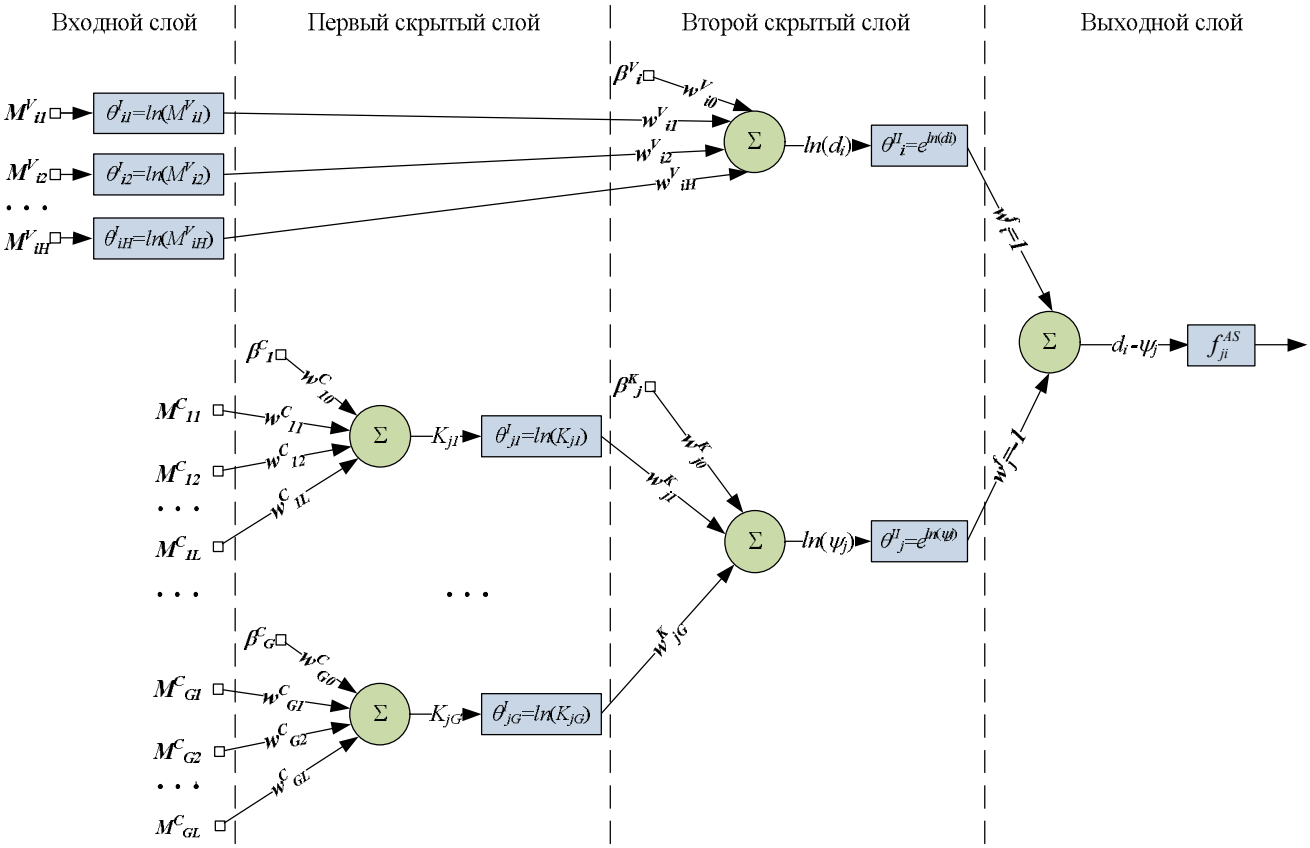

Рисунок 20 – Многослойный персептрон, соответствующий функции f_{ji}^{AS}

В структуре данного многослойного персептрона можно выделить два скрытых слоя. Нейроны первого скрытого слоя для метрик защитных мер соответствуют категориям K_{jg}. Для метрик нарушителей первый скрытый слой не используется. Второй скрытый слой состоит из двух нейронов, соответствующих показателям степени опасности нарушителя d_i и степени реализации

превентивных защитных мер ψ_j. Согласно формуле (22), весовые коэффициенты при d_i и ψ_j можно определить как: $w_i^f = 1$ и $w_j^f = -1$.

Выходной слой многослойного персептрона представлен одним нейроном, дающим на выходе прогнозируемое значение функции f_{ji}^{AS}.

В представленной модели многослойного персептрона используются пороговые элементы для метрик защитных мер β_g^C, метрик нарушителей β_i^V и категорий защитных мер β_j^K, равные 0,5. Добавление пороговых элементов позволяет решить две основные задачи:

- ограничение $w_{g0}^C > 0$ обеспечивает положительную определенность значений K_{jg}, что необходимо для вычисления натурального логарифма;
- существенный рост значений весовых коэффициентов при пороговых элементах служит поводом для добавления новых метрик и категорий.

Для замены мультипликатора в выражении (26) на сумматор используется логарифмическая функция активации $\theta_{ih}^I = \ln M_{ih}^V$. Для метрик нарушителей, используемых в диссертационной работе, выполняется условие: $M_{ih}^V > 0$.

По аналогии для замены мультипликатора в выражении (27) на сумматор используется логарифмическая функция активации $\theta_{jg}^I = \ln K_{jg}$. Условие $K_{jg} > 0$ выполняется за счет положительно определенных пороговых значений β_g^C и их весовых коэффициентов w_{g0}^C.

Для обратного преобразования сумм в нейронах второго скрытого слоя используются экспоненциальные функции активации: $\theta_i^{II} = e^{\ln(d_i)}$ для первого нейрона и $\theta_j^{II} = e^{\ln(\psi_j)}$ для второго нейрона.

В нейроне выходного слоя используется логистическая функция активации f_{ji}^{AS}, заданная выражением (22), аргументом которой является разность: $d_i - \psi_j$.

Инициализация векторов весовых коэффициентов осуществляется методом анализа иерархий в соответствии с процедурой, описанной в пункте 2.3.4

диссертационной работы. Качественная оценка начальных значений весовых коэффициентов существенно сокращает время обучения и требуемый объем обучающей выборки [134].

Под шагом обучения понимается процедура корректировки весовых коэффициентов для одного объекта обучающей выборки. На каждом шаге обучения последовательно выполняются две фазы: фаза прямого прохода и фаза обратного прохода [109, 134]. Схема шага обучения представлена на рисунке 21.

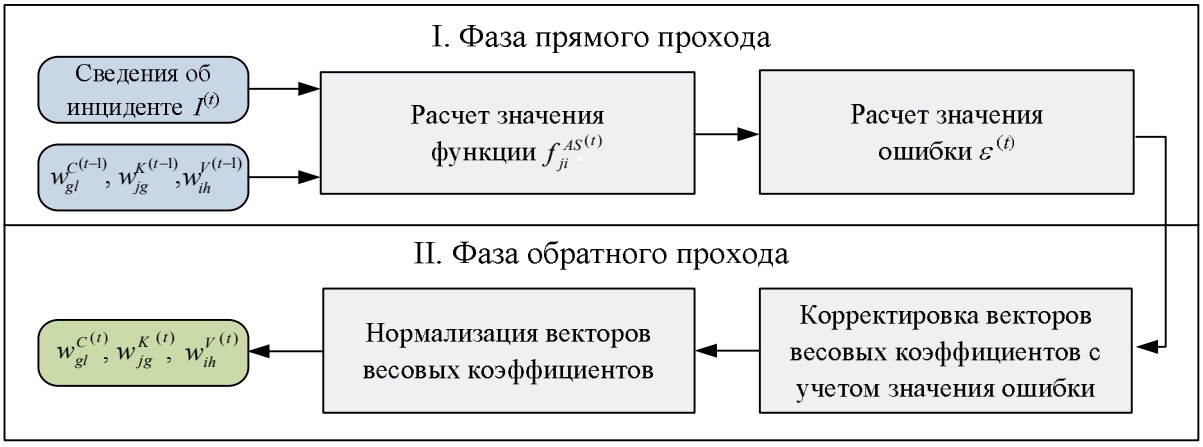

Рисунок 21 – Схема шага обучения

На фазе прямого прохода на вход подаются структурированные сведения о *t*-ом инциденте ИБ, представленные кортежем (66), и векторы весовых коэффициентов, определенные на предыдущем шаге обучения. На первом шаге обучения на вход подаются начальные векторы весовых коэффициентов, определенные методом анализа иерархий. Значение функции $f_{ji}^{AS(t)}$ на *t*-ом шаге обучения вычисляется по формуле:

$$f_{ji}^{AS(t)} = \left(1+\exp\left(-z\left(\prod_h \left(M_{ih}^{V(t)}\right)^{w_{ih}^{V(t)}} - \prod_g \left(\sum_l w_{gl}^{C(t)} \cdot M_{gl}^{C(t)}\right)^{w_{jg}^{K(t)}}\right)\right)\right)^{-1}. \quad (83)$$

Величина ошибки определяется как разность между значением функции $f_{ji}^{AS(t)}$ и результатом *t*-го инцидента ИБ $y_{ji}^{(t)}$ по формуле (67). При обучении используется целевая функция $E^{(t)}$, заданная выражением (68).

На фазе обратного прохода осуществляется корректировка весовых коэффициентов:

– по формуле (74) для метода градиентного спуска;

– по формуле (75) для метода градиентного спуска с моментом;

– по формуле (81) для диагонального метода Левенберга-Марквардта.

По правилам, приведенным в описании метода обратного распространения ошибки [19], определены значения первых производных:

– для весовых коэффициентов категорий защитных мер w_{jg}^{K}:

$$\frac{\partial E^{(t)}}{\partial w_{jg}^{K(t)}} = \frac{\partial E^{(t)}}{\partial f_{ji}^{AS(t)}} \cdot \frac{\partial f_{ji}^{AS(t)}}{\partial \psi_j^{(t)}} \cdot \frac{\partial \psi_j^{(t)}}{\partial w_{jg}^{K(t)}} = \varepsilon^{(t)} \cdot z \cdot f_{ji}^{AS(t)} \cdot \left(f_{ji}^{AS(t)} - 1\right) \cdot \psi_j^{(t)} \cdot \ln K_{jg}^{(t)}; \quad (84)$$

– для весовых коэффициентов метрик защитных мер w_{gl}^{C}:

$$\frac{\partial E^{(t)}}{\partial w_{gl}^{C(t)}} = \frac{\partial E^{(t)}}{\partial f_{ji}^{AS(t)}} \cdot \frac{\partial f_{ji}^{AS(t)}}{\partial \psi_j^{(t)}} \cdot \frac{\partial \psi_j^{(t)}}{\partial \left(\ln K_{jg}^{(t)}\right)} \cdot \frac{\partial \left(\ln K_{jg}^{(t)}\right)}{\partial w_{gl}^{C(t)}} = \varepsilon^{(t)} \cdot z \cdot f_{ji}^{AS(t)} \cdot \left(f_{ji}^{AS(t)} - 1\right) \cdot \psi_j^{(t)} \cdot w_{jg}^{K(t)} \cdot \frac{M_{gl}^{C(t)}}{K_{jg}^{(t)}}; \quad (85)$$

– для весовых коэффициентов метрик нарушителей w_{ih}^{V}:

$$\frac{\partial E^{(t)}}{\partial w_{ih}^{V(t)}} = \frac{\partial E^{(t)}}{\partial f_{ji}^{AS(t)}} \cdot \frac{\partial f_{ji}^{AS(t)}}{\partial d_i^{(t)}} \cdot \frac{\partial d_i^{(t)}}{\partial w_{ih}^{V(t)}} = \varepsilon^{(t)} \cdot z \cdot f_{ji}^{AS(t)} \cdot \left(1 - f_{ji}^{AS(t)}\right) \cdot d_i^{(t)} \cdot \ln M_{ih}^{V(t)}. \quad (86)$$

По правилам, приведенным в статье [160], определены значения вторых производных, используемые в диагональном методе Левенберга-Марквардта:

– для весовых коэффициентов категорий защитных мер w_{jg}^{K}:

$$\frac{\partial^2 E^{(t)}}{\partial \left(w_{jg}^{K(t)}\right)^2} = \frac{\partial^2 E^{(t)}}{\partial \left(f_{ji}^{AS(t)}\right)^2} \cdot \left(\frac{\partial f_{ji}^{AS(t)}}{\partial \psi_j^{(t)}}\right)^2 \cdot \left(\frac{\partial \psi_j^{(t)}}{w_{jg}^{K(t)}}\right)^2 + \frac{\partial E^{(t)}}{\partial f_{ji}^{(t)}} \cdot \frac{\partial^2 f_{ji}^{AS(t)}}{\partial \left(\psi_j^{(t)}\right)^2} \cdot \left(\frac{\partial \psi_j^{(t)}}{w_{jg}^{K(t)}}\right)^2 + \frac{\partial E^{(t)}}{\partial f_{ji}^{(t)}} \cdot \frac{\partial f_{ji}^{(t)}}{\partial \psi_j^{(t)}} \cdot \frac{\partial^2 \psi_j^{(t)}}{\partial \left(w_{jg}^{K(t)}\right)^2} =$$

$$= \varepsilon^{(t)} \cdot z^2 \cdot f_{ji}^{AS(t)} \cdot \left(f_{ji}^{AS(t)} - 1\right) \cdot \left(\psi_j^{(t)} \cdot \ln K_{jg}^{(t)}\right)^2 \cdot \left(\frac{f_{ji}^{AS(t)} \cdot \left(f_{ji}^{AS(t)} - 1\right)}{\varepsilon^{(t)}} + \left(1 - 2 f_{ji}^{AS(t)}\right) + \frac{1 + \left(\ln K_{jg}^{(t)}\right)^2}{z \cdot \psi_j^{(t)} \cdot \left(\ln K_{jg}^{(t)}\right)^2}\right); \quad (87)$$

– для весовых коэффициентов метрик защитных мер w_{gl}^{C}:

$$\frac{\partial^2 E^{(t)}}{\partial\left(w_{gl}^{C(t)}\right)^2}=\frac{\partial^2 E^{(t)}}{\partial\left(f_{ji}^{AS(t)}\right)^2}\cdot\left(\frac{\partial f_{ji}^{AS(t)}}{\partial\psi_j^{(t)}}\right)^2\cdot\left(\frac{\partial\psi_j^{(t)}}{\partial\left(\ln K_{jg}^{(t)}\right)}\right)^2\cdot\left(\frac{\partial\left(\ln K_{jg}^{(t)}\right)}{\partial w_{gl}^{C(t)}}\right)^2+\frac{\partial E^{(t)}}{\partial f_{ji}^{AS(t)}}\cdot\frac{\partial^2 f_{ji}^{AS(t)}}{\partial\left(\psi_j^{(t)}\right)^2}\cdot\left(\frac{\partial\psi_j^{(t)}}{\partial\left(\ln K_{jg}^{(t)}\right)}\right)^2\times$$

$$\times\left(\frac{\partial\left(\ln K_{jg}^{(t)}\right)}{\partial w_{gl}^{C(t)}}\right)^2+\frac{\partial E^{(t)}}{\partial f_{ji}^{AS(t)}}\cdot\frac{\partial f_{ji}^{AS(t)}}{\partial\psi_j^{(t)}}\cdot\frac{\partial^2\psi_j^{(t)}}{\partial\left(\ln K_{jg}^{(t)}\right)^2}\cdot\left(\frac{\partial\left(\ln K_{jg}^{(t)}\right)}{\partial w_{gl}^{C(t)}}\right)^2+\frac{\partial E^{(t)}}{\partial f_{ji}^{AS(t)}}\cdot\frac{\partial f_{ji}^{AS(t)}}{\partial\psi_j^{(t)}}\cdot\frac{\partial\psi_j^{(t)}}{\partial\left(\ln K_{jg}^{(t)}\right)}\cdot\frac{\partial^2\left(\ln K_{jg}^{(t)}\right)}{\partial\left(w_{gl}^{C(t)}\right)^2}=$$

$$=\varepsilon^{(t)}\cdot z^2\cdot f_{ji}^{AS(t)}\cdot\left(f_{ji}^{AS(t)}-1\right)\cdot\left(\psi_j^{(t)}\cdot w_{jg}^{K(t)}\right)^2\cdot\frac{\left(M_{gl}^{C(t)}\right)^2}{\left(K_{jg}^{(t)}\right)^2}\cdot\left(\frac{f_{ji}^{AS(t)}\cdot\left(f_{ji}^{AS(t)}-1\right)}{\varepsilon^{(t)}}+\left(2f_{ji}^{AS(t)}-1\right)+\right.$$

$$\left.+\frac{1+\left(w_{jg}^{K(t)}\right)^2}{z\cdot\psi_j^{(t)}\cdot\left(w_{jg}^{K(t)}\right)^2}-\frac{1}{z\cdot\psi_j^{(t)}\cdot w_{jg}^{K(t)}}\right);\tag{88}$$

– для весовых коэффициентов метрик нарушителей w_{ih}^{V}:

$$\frac{\partial E^{(t)}}{\partial\left(w_{ih}^{V(t)}\right)^2}=\frac{\partial^2 E^{(t)}}{\partial\left(f_{ji}^{AS(t)}\right)^2}\cdot\left(\frac{\partial f_{ji}^{AS(t)}}{\partial d_i^{(t)}}\right)^2\cdot\left(\frac{\partial d_i^{(t)}}{\partial w_{ih}^{V(t)}}\right)^2+\frac{\partial E^{(t)}}{\partial f_{ji}^{(t)}}\cdot\frac{\partial^2 f_{ji}^{AS(t)}}{\partial\left(d_i^{(t)}\right)^2}\cdot\left(\frac{\partial d_i^{(t)}}{\partial w_{ih}^{V(t)}}\right)^2+\frac{\partial E^{(t)}}{\partial f_{ji}^{(t)}}\cdot\frac{\partial f_{ji}^{(t)}}{\partial d_i^{(t)}}\cdot\frac{\partial^2 d_i^{(t)}}{\partial\left(w_{ih}^{V(t)}\right)^2}=$$

$$=\varepsilon^{(t)}\cdot z^2\cdot f_{ji}^{AS(t)}\cdot\left(1-f_{ji}^{AS(t)}\right)\cdot\left(d_i^{(t)}\cdot\ln M_{ih}^{V(t)}\right)^2\cdot\left(\frac{f_{ji}^{AS(t)}\cdot\left(1-f_{ji}^{AS(t)}\right)}{\varepsilon^{(t)}}+\left(1-2f_{ji}^{AS(t)}\right)+\frac{1+\left(\ln M_{ih}^{V(t)}\right)^2}{z\cdot d_i^{(t)}\cdot\left(\ln M_{ih}^{V(t)}\right)^2}\right).\tag{89}$$

В завершении шага обучения осуществляется нормализация векторов весовых коэффициентов, чтобы выполнялись условия:

$$\begin{aligned}&\sum_l w_{gl}^{C(t)}=1,\ \forall g\in[1;G];\\&\sum_g w_{jg}^{K(t)}=1;\\&\sum_h w_{ih}^{V(t)}=1.\end{aligned}\tag{90}$$

Для оценки результатов на *t*-ом шаге обучения используется показатель $Q_f^{(t)}$, определяемый как средний модуль отклонения текущих значений весовых коэффициентов от их целевых значений:

$$Q_f^{(t)} = \frac{\sum_{h=1}^{H} \left| w_{ih}^{V\,(t)} - \overline{w}_{ih}^{V} \right| + \sum_{g=1}^{G} \left| w_{jg}^{K\,(t)} - \overline{w}_{jg}^{K} \right| + \sum_{g=1}^{G} \sum_{l=1}^{L} \left| w_{gl}^{C\,(t)} - \overline{w}_{gl}^{C} \right|}{H + G + \sum_{g=1}^{G} L_g}, \qquad (91)$$

где H – число метрик нарушителя;

G – число категорий защитных мер;

L_g – число метрик g-ой категории защитных мер.

При корректном обучении с ростом значения t показатель $Q_f^{(t)}$ должен уменьшаться и стремиться к нулю.

Значение ошибки $\varepsilon^{(t)}$, определяемое выражением (67), зависит от объекта обучающей выборки. По этой причине величину остаточной ошибки предлагается определять как среднюю ошибку $\overline{\varepsilon^{(t)}}$ при текущих значениях весовых коэффициентов для 10^6 объектов обучающей выборки.

Корректировка весовых коэффициентов осуществляется каждый раз при поступлении новых данных об инцидентах ИБ, тем самым обеспечивается адаптация функции f_{ji}^{AS} к различным изменениям, например появлению новых угроз и способов их реализации.

3.2 Основные результаты экспериментального исследования

Проведено экспериментальное исследование, в ходе которого осуществлялась обучение функции f_{ji}^{AS}, определяющей вероятность реализации угроз НСД к ПО веб-сервера нарушителем через сеть Интернет. Для простоты рассматривались исключительно угрозы удаленного НСД, реализуемые нарушителями через сеть Интернет.

Рассматриваемая функция f_{ji}^{AS}, таким образом, является весовой функцией перехода с причиной $v'_i = V^{AS}$ и результатом $v'_j = SW^{[I]}$.

Эксперименты проводились посредством моделирования процедуры обучения многослойного персептрона, соответствующего функции f_{ji}^{AS}, с использованием разработанного для этой цели программного кода на языке C++.

3.2.1 Формирование обучающей выборки

Анализ открытых источников показал, что на момент проведения экспериментального исследования отсутствовали базы инцидентов ИБ, содержащие данные, необходимые для формирования объектов обучающей выборки, представленных кортежем (66). По этой причине в ходе моделирования осуществлялась генерация объектов обучающей выборки по заданным целевым значениям весовых коэффициентов и правилу вывода результата инцидента ИБ.

Начальные значения весовых коэффициентов метрик и категорий защитных мер и метрик нарушителей определялись методом анализа иерархий, в соответствии с процедурой, описанной в подпункте 2.3.4 диссертационной работы. Предварительно осуществлялась нормализация векторов весовых коэффициентов $w_{jg}^{K\,(0)}$, $w_{gl}^{C\,(0)}$ и $w_{ih}^{V\,(0)}$ с учетом добавления пороговых элементов β_j^K, β_g^C и β_i^V, начальные значения весовых коэффициентов которых равны 0,01.

Оценка степени реализации защитных мер осуществлялась на основе метрик четырех категорий защитных мер, направленных на предотвращение НСД к ПО, с наибольшими начальными значениями весовых коэффициентов (согласно таблице Б.2 приложения Б): идентификация и аутентификация (ИАФ), антивирусная защита (АВЗ), анализ защищенности (АНЗ) и управление конфигурацией (УКФ).

В открытых базах [147, 172] и аналитическом отчете [126] приведена краткая характеристика инцидентов ИБ. Для экспериментального исследования из данных источников были отобраны инциденты, связанные с осуществлением НСД к ПО веб-серверов, со следующими причинами возникновения:

- использование словарных и слабых паролей (слабости категории ИАФ);
- использование вредоносного ПО (слабости категории АВЗ);

– использование уязвимостей кода ПО (слабости категории АНЗ);

– ошибки конфигурации (слабости категории УКФ).

Для каждого источника определены относительные частоты использования слабостей отдельных категорий защитных мер. Целевые значения весовых коэффициентов (весов) категорий, приведенные в таблице 10, получены путем усреднения значений относительных частот для трех источников.

Таблица 10 – Весовые коэффициенты категорий защитных мер

Источник	**Категории защитных мер**				**Пороговый элемент,** $\boldsymbol{\beta_j^K = 0,5}$
	ИАФ, $\boldsymbol{K_{j1}}$	**АВЗ,** $\boldsymbol{K_{j2}}$	**АНЗ,** $\boldsymbol{K_{j3}}$	**УКФ,** $\boldsymbol{K_{j4}}$	
Отчет компании Positive Technologies [126]	0,33	0	0,58	0,09	–
Статистика ресурса Hackmageddon [147]	0,27	0,2	0,54	0	–
База данных OWASP/WASC [172]	0,2	0,21	0,48	0,1	–
Начальный вес, $\boldsymbol{w_{jg}^{K\,(0)}}$	**0,34**	**0,18**	**0,26**	**0,21**	**0,01**
Целевой вес, $\boldsymbol{\bar{w}_{jg}^K}$	**0,27**	**0,14**	**0,53**	**0,06**	**0**

Значения, принимаемые метриками защитных мер, определены в подразделе 2.3 диссертационной работы. Определение целевых значений весовых коэффициентов (весов) метрик защитных мер, приведенных в таблице 11, ввиду отсутствия необходимых статистических данных, осуществлялось по формуле:

$$\bar{w}_{gl}^{C} = \frac{УЗ_{gl} + 1}{\sum_l (УЗ_{gl} + 1)}, \tag{92}$$

где $УЗ_{gl}$ – число уровней (классов) защищенности системы, для которых должна быть реализована данная мера, определяемое согласно документам ФСТЭК России [104] и [118].

Таблица 11 – Весовые коэффициенты метрик защитных мер

Метрика / пороговый элемент	**Условное обозначение защитной меры**	**Принимаемые значения**	**Начальный вес,** $\boldsymbol{w_{gl}^{C\,(0)}}$	**Целевой вес,** $\boldsymbol{\bar{w}_{gl}^C}$
Идентификация и аутентификация				
β_1^C	–	{ 0,5 }	0,01	0
M_{11}^C	ИАФ.1	{ 0; 0,5; 1 }	0,38	0,2
M_{12}^C	ИАФ.3	{ 0; 0,5; 1 }	0,11	0,2
M_{13}^C	ИАФ.4	{ 0; 0,5; 1 }	0,11	0,2
M_{14}^C	ИАФ.5	{ 0; 0,5; 1 }	0,10	0,2

Метрика / пороговый элемент	Условное обозначение защитной меры	Принимаемые значения	Начальный вес, $w_{gl}^{C\,(0)}$	Целевой вес, $\bar{w}_{gl}^{C}$
M_{15}^{C}	ИАФ.6	{ 0; 0,5; 1 }	0,29	0,2
Антивирусная защита				
β_2^C	–	{ 0,5 }	0,01	0
M_{21}^{C}	АВЗ.1	{ 0; 0,5; 1 }	0,73	0,5
M_{22}^{C}	АВЗ.2	{ 0; 0,5; 1 }	0,26	0,5
Анализ защищенности				
β_3^C	–	{ 0,5 }	0,01	0,01
M_{31}^{C}	АНЗ.1	{ 0; 0,5; 1 }	0,27	0,2
M_{32}^{C}	АНЗ.2	{ 0; 0,5; 1 }	0,17	0,25
M_{33}^{C}	АНЗ.3	{ 0; 0,5; 1 }	0,15	0,2
M_{34}^{C}	АНЗ.4	{ 0; 0,5; 1 }	0,11	0,2
M_{35}^{C}	АНЗ.5	{ 0; 0,5; 1 }	0,29	0,15
Управление конфигурацией				
β_4^C	–	{ 0,5 }	0,01	0
M_{41}^{C}	УКФ.1	{ 0; 1 }	0,09	0,25
M_{42}^{C}	УКФ.2	{ 0; 1 }	0,41	0,25
M_{43}^{C}	УКФ.3	{ 0; 1 }	0,38	0,25
M_{44}^{C}	УКФ.4	{ 0; 1 }	0,12	0,25

Для метрик нарушителей, ввиду отсутствия необходимых статистических данных, определены одинаковые целевые значения весовых коэффициентов (весов), приведенные в таблице 12. Значения, принимаемые метриками нарушителей, определены в таблице Б.1 приложения Б.

Таблица 12 – Весовые коэффициенты метрик нарушителей

Метрика / пороговый элемент	Наименование метрики	Принимаемые значения	Начальный вес, $w_{ih}^{V\,(0)}$	Целевой вес, $\bar{w}_{ih}^{V}$
β_i^V	–	{ 0,5 }	0,01	0
M_{i1}^{V}	Мотивация	{ 0,08; 0,14; 0,19; 0,2; 0,25; 0,45; 0,57; 0,61; 0,92; 1 }	0,18	0,165
M_{i2}^{V}	Оснащенность	{ 0,09; 0,18; 0,44; 1 }	0,17	0,165
M_{i3}^{V}	Техническая компетентность	{ 0,11; 0,37; 1 }	0,24	0,165
M_{i4}^{V}	Знание информации о КИС и СЗИ	{ 0,13; 0,4; 1 }	0,14	0,165
M_{i5}^{V}	Права доступа	{ 0,09; 0,19; 0,42; 1 }	0,17	0,165
M_{i6}^{V}	Время доступа	{ 0,11; 0,22; 0,52; 1 }	0,10	0,165

Для определения результата инцидента ИБ при генерации объектов обучающей выборки использовалась пороговая функция:

$$\begin{cases} y_{ji}^{(t)} = 1, \ если \ \overline{f}_{ji}^{AS(t)} \geq 0 \\ y_{ji}^{(t)} = 0, \ если \ \overline{f}_{ji}^{AS(t)} < 0 \end{cases}, \quad (93)$$

где $\overline{f}_{ji}^{AS(t)}$ – значение функции $f_{ji}^{AS(t)}$, рассчитанной по формуле (83) для *t*-го объекта обучающей выборки при целевых значениях весовых коэффициентов.

Начальное значение среднего модуля отклонения значений весовых коэффициентов $Q_f^{(t)}$ (далее – среднее отклонение) при исходных данных, приведенных в таблицах 10-12, составило $Q_f^{(0)} = 1057 \cdot 10^{-4}$. В свою очередь, начальное значение средней ошибки составило $\overline{\varepsilon^{(0)}} = 0{,}2167$.

3.2.2 Выбор метода корректировки весовых коэффициентов и параметров обучения

В ходе экспериментального исследования осуществлялось сравнение методов корректировки весовых коэффициентов и определение рекомендуемых параметров обучения.

Для моделирования процедуры обучения разработан программный код на языке C++. Результаты обучения определялись значением среднего отклонения $Q_f^{(t)}$ на 100-ом и 1000-ом шагах обучения. Все приведенные результаты усреднены по 1000 циклам обучения.

Для определения наиболее подходящего значения переменной *z* логистической функции (22) проведен ряд экспериментов, в ходе которых осуществлялось обучение функции f_{ji}^{AS} методом градиентного спуска при $z \in [5; 100]$ с шагом 0,05. Чтобы компенсировать прямо-пропорциональную зависимость величин $\Delta w_{jg}^{K(t)}$, $\Delta w_{gl}^{C(t)}$ и $\Delta w_{ih}^{V(t)}$ от переменной *z*, темп обучения

определялся как $\eta = 1/z$. Результаты обучения функции f_{ji}^{AS} при некоторых значениях z представлены на рисунке 22.

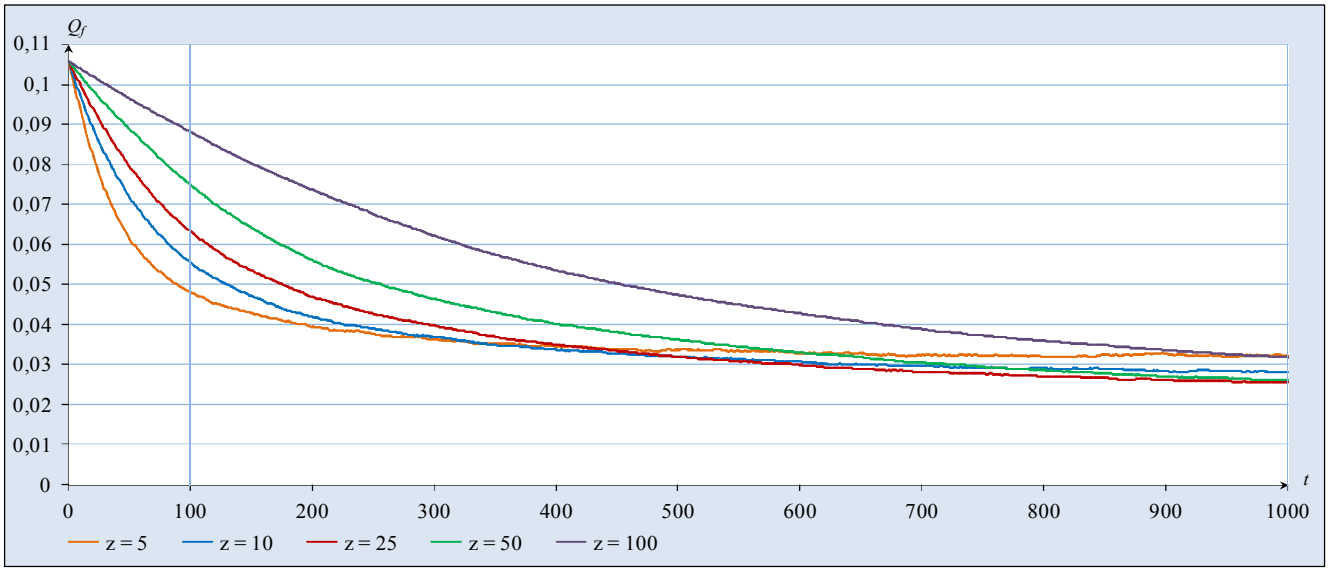

Рисунок 22 – Результаты обучения функции f_{ji}^{AS} в зависимости от значения переменной z

На 1000-ом шаге обучения наименьшее значение $Q_f^{(1000)} = 256 \cdot 10^{-4}$ было получено при $z = 25$ (кривая красного цвета). При проведении дальнейших экспериментов использовалось значение $z = 25$.

В ходе экспериментального исследования для обучения функции f_{ji}^{AS} использовались различные вариации метода обратного распространения ошибки, отличающиеся правилами выбора направления и величины корректировки векторов весовых коэффициентов.

Эксперименты по обучению функции f_{ji}^{AS} методом градиентного спуска с постоянным темпом обучения проводились при $\eta \in [0{,}005; 0{,}1]$ с шагом 0,005. Полученные при некоторых значениях η результаты представлены на рисунке 23.

Как видно из графика, большее значение темпа обучения позволяет добиться сравнительно лучших результатов на первых шагах обучения. Так, при $\eta =$ 0,07 значение среднего отклонения на 100-ом шаге обучения составило $Q_f^{(100)} = 589 \cdot 10^{-4}$, что почти в 1,8 раза меньше начального значения $Q_f^{(0)}$. Однако большое значение темпа обучения отрицательно влияет на сходимость, поэтому

при η = 0,07 среднее отклонение, достигнув значения $400 \cdot 10^{-4}$, существенно замедлило снижение. На 1000-ом шаге обучения наименьшее значение среднего отклонения $Q_f^{(1000)} = 136 \cdot 10^{-4}$ было получено при темпе обучения $\eta = 0{,}03$.

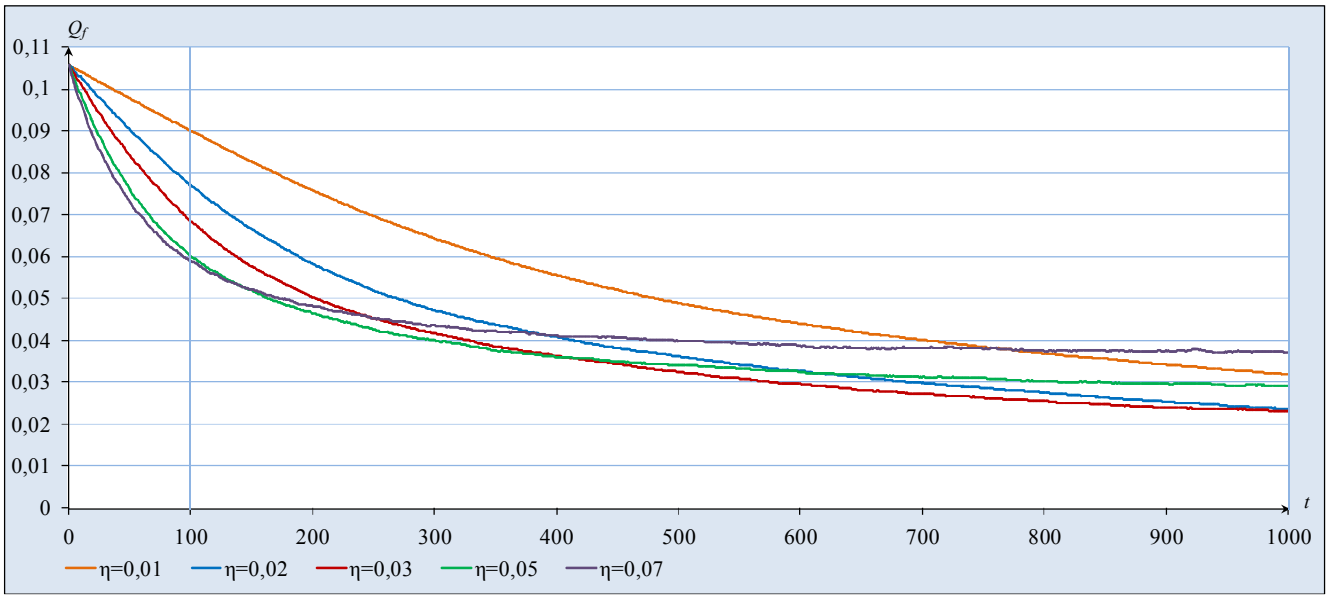

Рисунок 23 – Результаты обучения функции f_{ji}^{AS} методом градиентного спуска с постоянным темпом обучения

Результаты обучения функции f_{ji}^{AS}, представленные на рисунке 23, удалось улучшить за счет использования, так называемого, адаптивного или плавающего темпа обучения $\eta^{(t)}$. При этом базовый темп обучения обозначим как η_b. На практике используются различные способы определения адаптивного темпа обучения, основанные на задании некоторой зависимости $\eta^{(t)}$ от значений $\Delta w^{(t)}$, порядкового номера шага обучения *t* и прочих параметров [109, 134].

При проведении экспериментов были рассмотрены следующие способы определения адаптивного темпа обучения:

1) увеличение темпа обучения при повторении знаков $\Delta w^{(t)}$ на r_w последовательных шагах обучения в геометрической прогрессии по формуле: $\eta^{(t)} = \eta_b \cdot k_{gp}^{\ r_w}$, где k_{gp} – коэффициент геометрической прогрессии; r_w – число последовательных объектов обучающей выборки, для которых соответствующие значения $\Delta w \neq 0$ и имеют один знак;

2) увеличение темпа обучения при повторении знаков $\Delta w^{(t)}$ на r_w последовательных шагах обучения в арифметической прогрессии по формуле: $\eta^{(t)} = \eta_b \cdot k_{ap} \cdot r_w$, где k_{ap} – коэффициент арифметической прогрессии;
3) определение темпа обучения на основе порядкового номера шага обучения t по формуле: $\eta^{(t)} = \eta_b \cdot k_t$, где k_t – коэффициент, уменьшающийся с ростом шага обучения.

Для каждого способа в ходе моделирования задавались различные значения базового темпа обучения η_b и коэффициентов k_{gp}, k_{ap} и k_t. На рисунке 24 представлены лучшие результаты обучения функции f_{ji}^{AS}, полученные для каждого из способов.

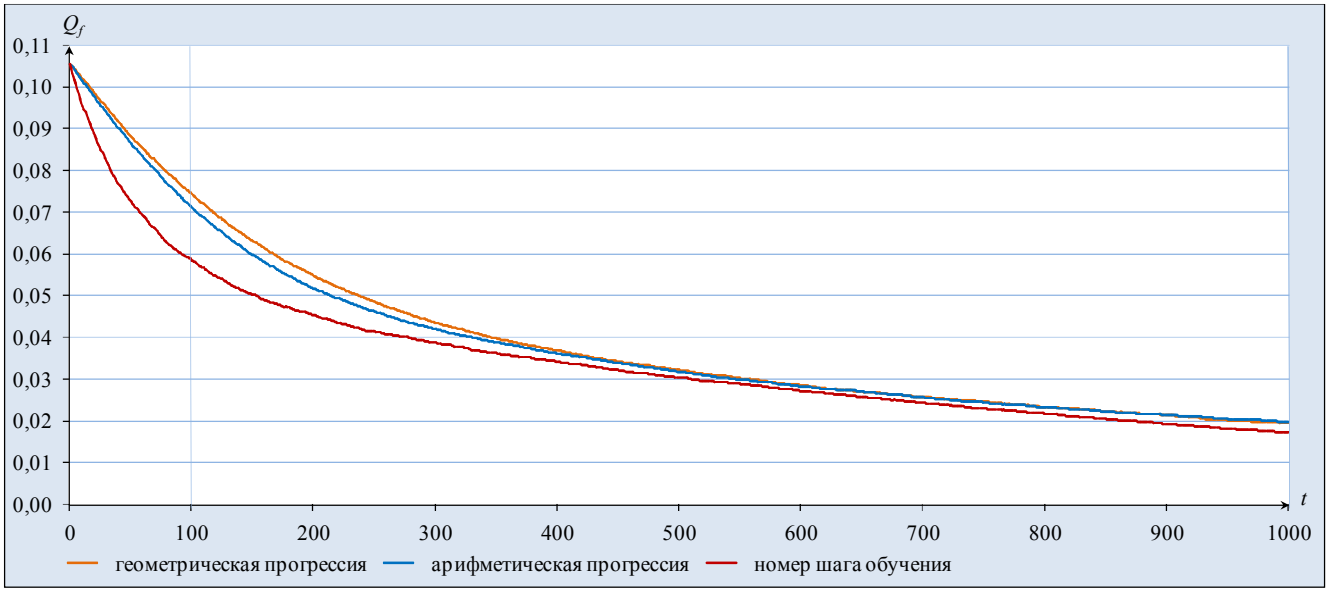

Рисунок 24 – Результаты обучения функции f_{ji}^{AS} методом градиентного спуска с адаптивным темпом обучения

Значения среднего отклонения при различных способах определения адаптивного темпа обучения приведены в таблице 13. Наименьшие значения $Q_f^{(t)}$ были получены при определении адаптивного темпа обучения на основе порядкового номера шага обучения t.

Таблица 13 – Значения $Q_f^{(t)}$ при различных способах определения $\eta^{(t)}$

Правило изменения темпа обучения	**Цвет кривой на рисунке 24**	**Базовый темп обучения, η_b**	**Значение коэффициента**	**Среднее отклонение, $Q_f^{(t)}$**	
				при $t = 100$	**при $t = 1000$**
Геометрическая прогрессия	Оранжевый	0, 015	$k_{gp} = 0{,}25$	$744 \cdot 10^{-4}$	$196 \cdot 10^{-4}$
Арифметическая прогрессия	Синий	0, 015	$k_{ap} = 0{,}5$	$713 \cdot 10^{-4}$	$198 \cdot 10^{-4}$
Номер шага обучения	Красный	0,07	$k_t = \frac{1000 - t}{1000}$	$586 \cdot 10^{-4}$	$174 \cdot 10^{-4}$

Эксперименты по обучению функции f_{ji}^{AS} методом градиентного спуска с моментом проводились при значениях момента $\alpha \in [0{,}05; 1]$ с шагом 0,05. При этом использовался адаптивный темп $\eta^{(t)}$, определяемый на основе порядкового номера шага обучения *t*. Результаты обучения функции f_{ji}^{AS} при некоторых значениях α представлены на рисунке 25.

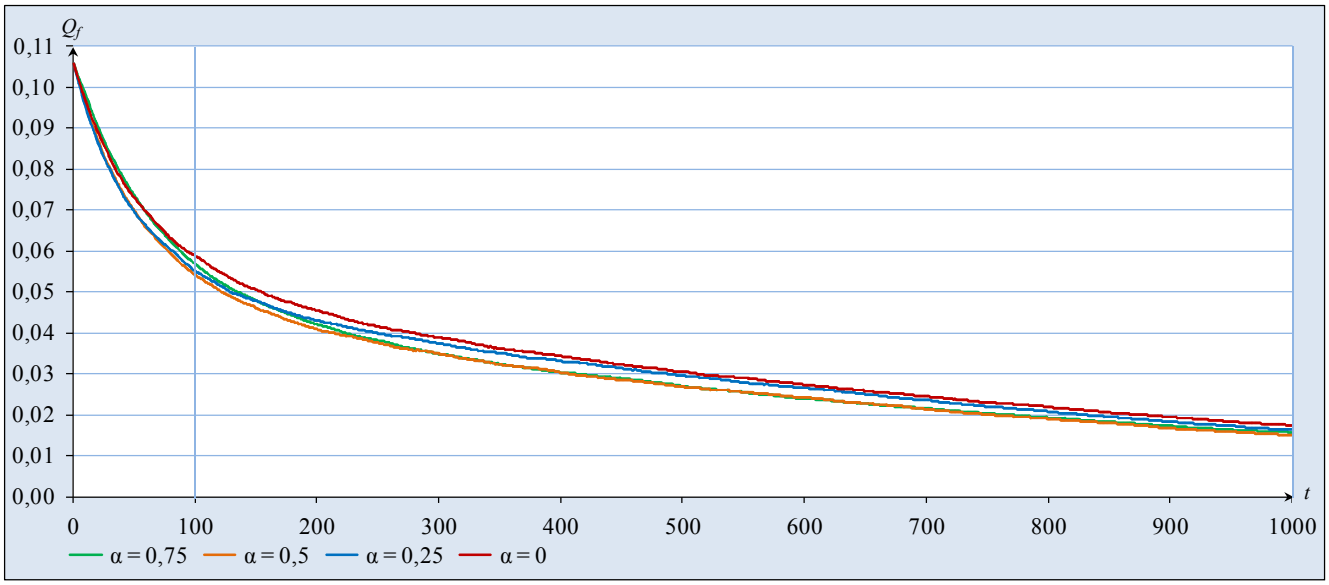

Рисунок 25 – Результаты обучения функции f_{ji}^{AS} методом градиентного спуска с моментом

Наименьшие значения среднего отклонения были получены при $\alpha = 0{,}5$ (кривая желтого цвета) и составили $Q_f^{(100)} = 540 \cdot 10^{-4}$ и $Q_f^{(1000)} = 150 \cdot 10^{-4}$.

Дальнейшего улучшения результатов обучения удалось добиться при использовании диагонального метода Левенберга-Марквардта. Эксперименты

проводились при значениях коэффициента $\mu \in [0{,}05; 1]$ с шагом 0,05. Результаты обучения функции f_{ji}^{AS} при некоторых значениях μ представлены на рисунке 26.

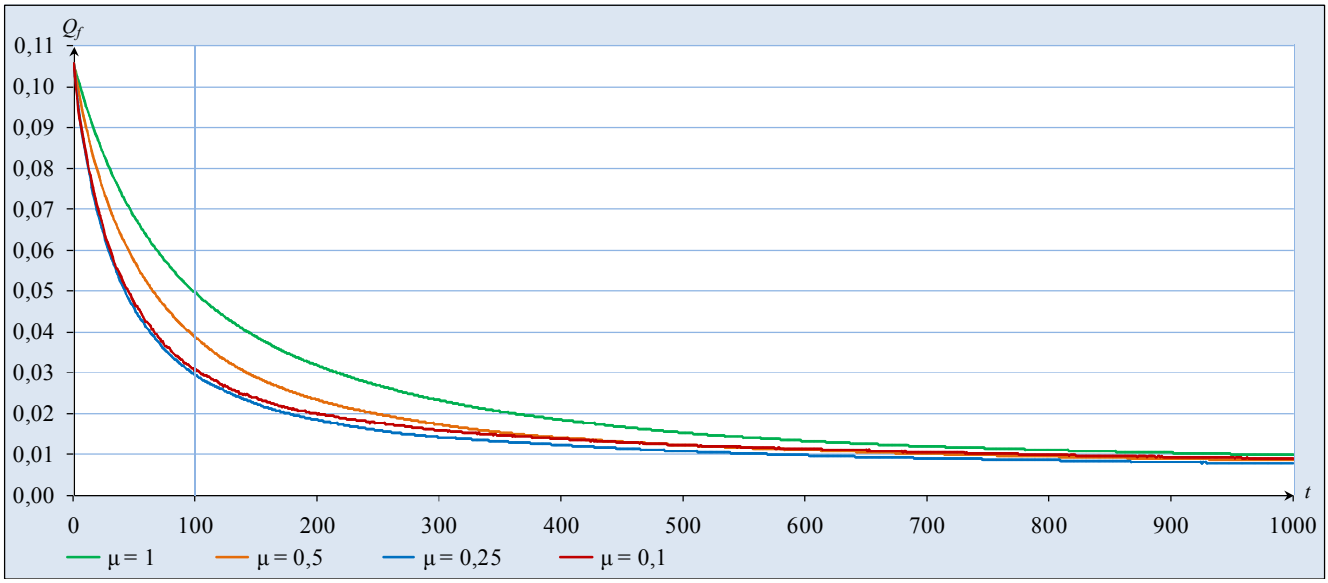

Рисунок 26 – Результаты обучения функции f_{ji}^{AS} диагональным методом Левенберга-Марквардта

Наименьшие значения среднего отклонения были получены при $\mu = 0{,}25$ (кривая синего цвета) и составили $Q_f^{(100)} = 294 \cdot 10^{-4}$ и $Q_f^{(1000)} = 77 \cdot 10^{-4}$. При $\mu < 0{,}2$ на некоторых циклах обучения наблюдалось резкое увеличение значений $Q_f^{(t)}$, вызванное большими изменениями отдельных весовых коэффициентов.

Использование диагонального метода Левенберга-Марквардта позволило добиться значительно лучших результатов обучения функции f_{ji}^{AS} по сравнению с градиентными методами, что полностью соответствуют теоретическим и экспериментальным выводам других авторов [19, 109].

При выборке из 100 инцидентов ИБ удалось снизить среднюю ошибку до $\overline{\varepsilon^{(100)}} = 0{,}0491$ (менее 5%), а при выборке из 1000 инцидентов ИБ – до $\overline{\varepsilon^{(1000)}} = 0{,}0098$ (менее 1%), то есть более чем в 22 раза.

Дальнейшие эксперименты по отбору значимых признаков и определению влияния различных факторов на результаты обучения проводились с использованием диагонального метода Левенберга-Марквардта при $\mu = 0{,}25$.

3.2.3 Отбор значимых признаков в процессе обучения

Проведено два эксперимента, в ходе которых определялась возможность отбора значимых признаков в процессе обучения функции f_{ji}^{AS}.

Цель первого эксперимента заключалась в определении среднего числа шагов обучения, необходимых для исключения незначимых категорий и метрик, в зависимости от начальных значений их весовых коэффициентов. Для этого целевые значения весовых коэффициентов категории K_{j4} и метрики M_{15}^{C} были приравнены к нулю, а их начальные значения задавались в интервале [0,1; 0,5].

Если в процессе обучения весовой коэффициент категории (метрики) становился меньше порога значимости $w_T = 0{,}01$, то она признавалась незначимой и не учитывалась при дальнейшей оценке показателя ψ_j. Результаты эксперимента представлены на рисунке 27.

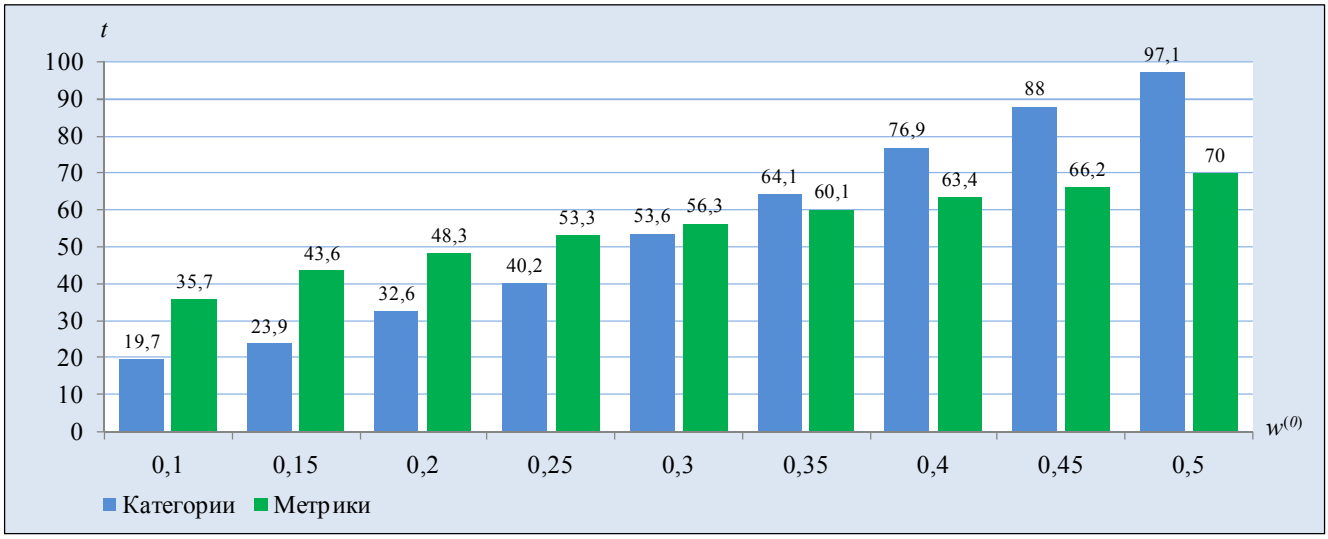

Рисунок 27 – Среднее число шагов обучения, необходимых для исключения незначимых категорий и метрик

По результатам проведенного эксперимента можно сделать вывод, что для исключения незначимых категорий и метрик, начальные значения весовых коэффициентов которых не превышают 0,5, требуется обучающая выборка менее чем из 100 инцидентов ИБ. Характер зависимости, представленной на рисунке 27, отличается для категорий и метрик. Для метрик данная зависимость напоминает логарифмическую, тогда как для категорий данная зависимость ближе к

экспоненциальной. Это обусловлено различием функций активации для первого скрытого слоя, соответствующего метрикам, и второго скрытого слоя, соответствующего категориям.

В ходе второго эксперимента определялось среднее число шагов обучения, требуемых для определения необходимости добавления новых категорий и метрик. Для этого в функцию f_{ji}^{AS} были добавлены категория K_{j5} и метрика M_{23}^{C}, принимающие случайные значения в интервале [0; 1]. Целевые значения весовых коэффициентов $\overline{w}_{j5}^{K}$ и $\overline{w}_{23}^{C}$ задавались в интервале [0,1; 0,5] с шагом 0,05. Целевые значения весовых коэффициентов других категорий и метрик изменялись таким образом, чтобы выполнялись условия, определенные выражением (90).

Корректировка весовых коэффициентов при пороговых элементах осуществляется исключительно в результате нормализации векторов весовых коэффициентов. Если существующая функция f_{ji}^{AS} плохо прогнозирует результат инцидента ИБ, весовые коэффициенты категорий и метрик уменьшаются, а весовые коэффициенты пороговых элементов увеличиваются, и наоборот.

В ходе эксперимента, результаты которого представлены на рисунке 28, превышение весовыми коэффициентами $w_{j5}^{K(t)}$ и $w_{23}^{C(t)}$ значения $w_S = 0{,}02$ являлось основанием для добавления новых категорий и метрик соответственно.

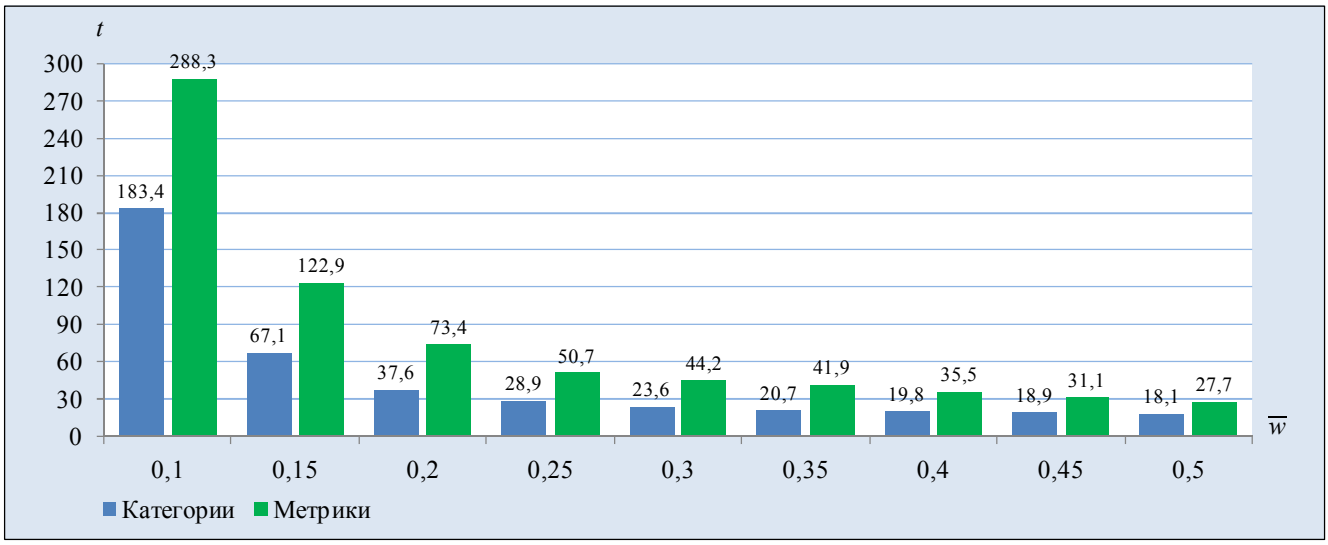

Рисунок 28 – Среднее число шагов обучения, требуемых для определения необходимости добавления значимых категорий и метрик

Исходя из полученных результатов можно сделать вывод, что отсутствие значимой категории существеннее сказывается на результатах, и, как следствие, может быть быстрее выявлено, чем отсутствие значимой метрики.

Таким образом, предложенный метод обучения позволяет осуществлять отбор значимых признаков в процессе обучения за счет:

- исключения незначимых категорий и метрик, не влияющих либо вносящих сравнительно малый вклад в результат оценки;
- определения необходимости добавления новых (значимых) категорий и метрик в том случае, если существующая функция f_{ji}^{AS} плохо прогнозирует результат инцидента ИБ.

3.2.4 Анализ влияния неполноты данных об инцидентах информационной безопасности на результаты обучения

Проведены эксперименты, целью которых являлось определение влияния на результаты обучения функции f_{ji}^{AS} следующих факторов:

- типы используемых признаков;
- число категорий защитных мер;
- неполнота данных об объектах обучающей выборки (инцидентах ИБ).

Цель первого эксперимента, результаты которого представлены на рисунке 29, заключалась в определении зависимости результатов обучения функции f_{ji}^{AS} от типов используемых признаков. Эксперимент включал три процедуры моделирования, в ходе которых метрикам, приведенным в таблицах 10-12, соответствовали:

- количественные признаки;
- качественные признаки;
- бинарные признаки.

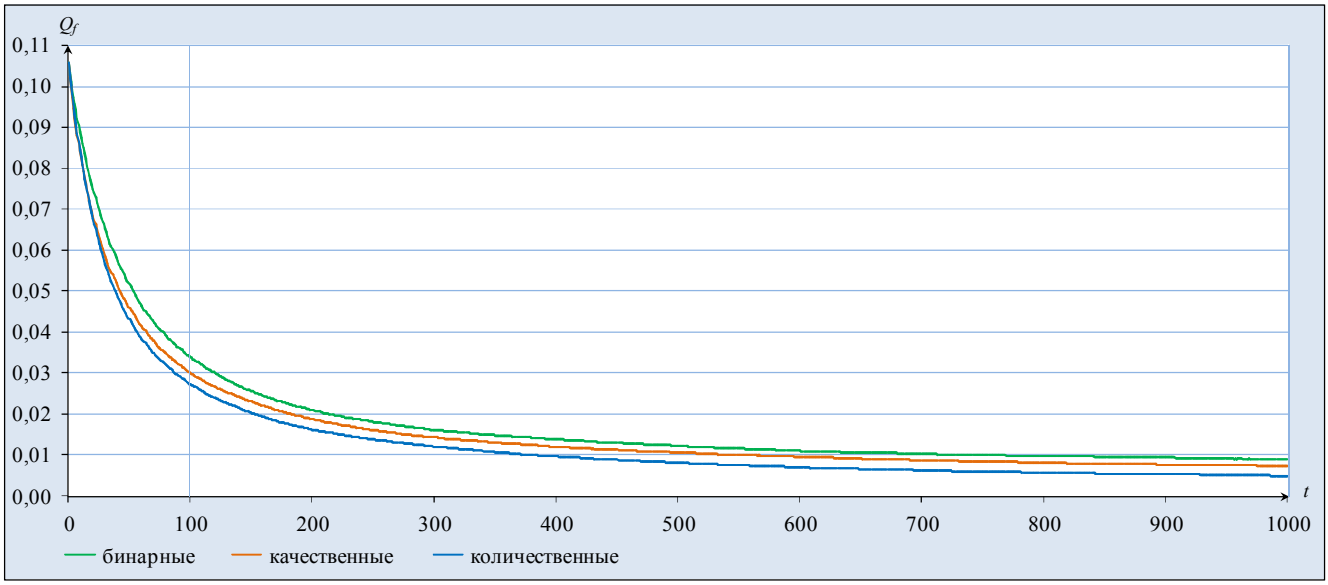

Рисунок 29 – Результаты обучения функции f_{ji}^{AS} в зависимости от типов признаков

Полученные значения $Q_f^{(t)}$ при использовании количественных признаков (кривая синего цвета) ниже, чем при использовании качественных (кривая оранжевого цвета) и бинарных (кривая зеленого цвета) признаков. Это объясняется большей вариативностью значений метрик, соответствующих количественным признакам, что позволяет осуществлять более точную настройку весовых коэффициентов. По этой причине при определении степени опасности нарушителей (26) и степени реализации защитных мер (27) вместо бинарных признаков рекомендуется использовать их количественные или качественные эквиваленты.

Цель второго эксперимента заключалась в определении зависимости результатов обучения функции f_{ji}^{AS} от числа категорий защитных мер. Эксперимент включал четыре процедуры моделирования, в ходе которых число учитываемых категорий защитных мер составляло:

– $G = 4$ (ИАФ, АВЗ, АНЗ, УКФ);
– $G = 3$ (ИАФ, АВЗ, АНЗ);
– $G = 2$ (ИАФ, АНЗ);
– $G = 1$ (АНЗ).

Предварительно осуществлялась нормализация вектора $\overline{w}_{jg}^{K}$, а значения $w_{jg}^{K(0)}$ задавались таким образом, чтобы начальное значение среднего отклонения $Q_f^{(0)} = 1057 \cdot 10^{-4}$ оставалось неизменным. При $G = 1$ с этой же целью были скорректированы начальные значения весовых коэффициентов метрик $w_{gl}^{C(0)}$. Неизменность величины $Q_f^{(0)}$ позволяет сопоставить результаты обучения функции f_{ji}^{AS} при разном числе категорий G, представленные на рисунке 30.

Эксперимент показал, что при $G \geq 2$ значения $Q_f^{(t)}$ отличаются несущественно. При $G = 1$ были получены существенно меньшие значения среднего отклонения: $Q_f^{(100)} = 125 \cdot 10^{-4}$ и $Q_f^{(1000)} = 38 \cdot 10^{-4}$. Это объясняется тем, что при наличии единственной категории защитных мер функция f_{ji}^{AS} и соответствующий ей многослойный персептрон существенно упрощаются.

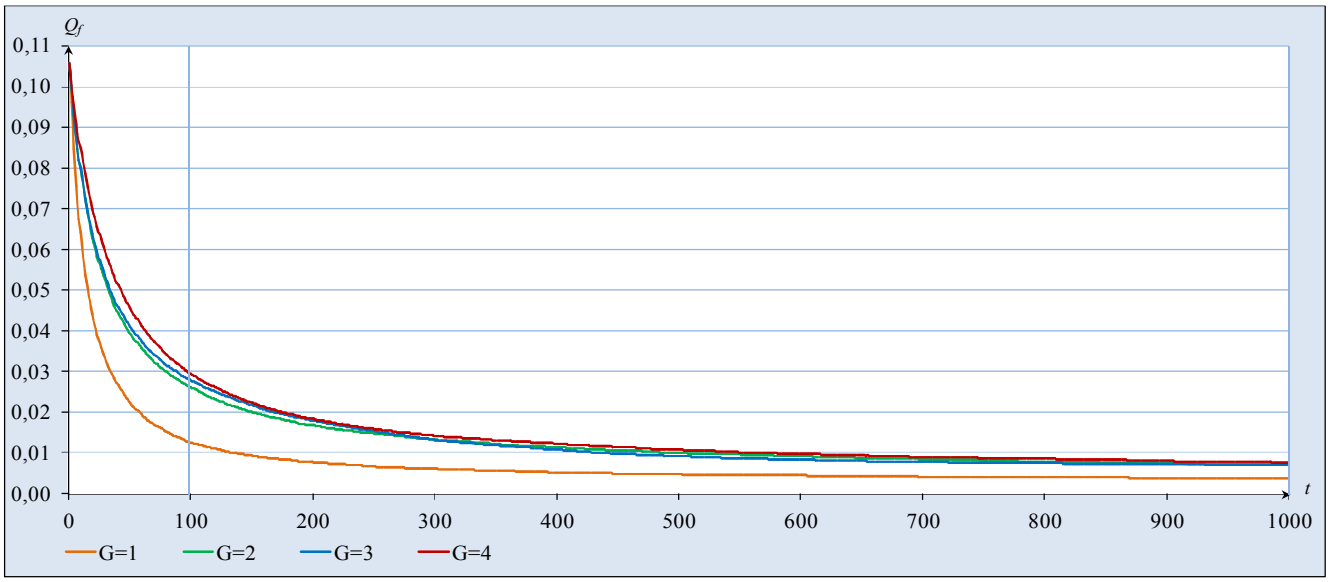

Рисунок 30 – Результаты обучения функции f_{ji}^{AS} в зависимости от числа категорий G

Цель третьего эксперимента заключалась в определении влияния неполноты данных об инцидентах ИБ на результаты обучения функции f_{ji}^{AS}, представленные на рисунке 31. Для произвольного инцидента ИБ обозначим как γ долю метрик, значения которых неизвестны, от общего числа метрик. Обучение функции f_{ji}^{AS}

осуществлялось при $\gamma \in [0; 0{,}95]$ с шагом 0,05, при этом с вероятностью γ значения подаваемых на вход метрик не были определены, а корректировка их весовых коэффициентов не осуществлялась на данном шаге обучения.

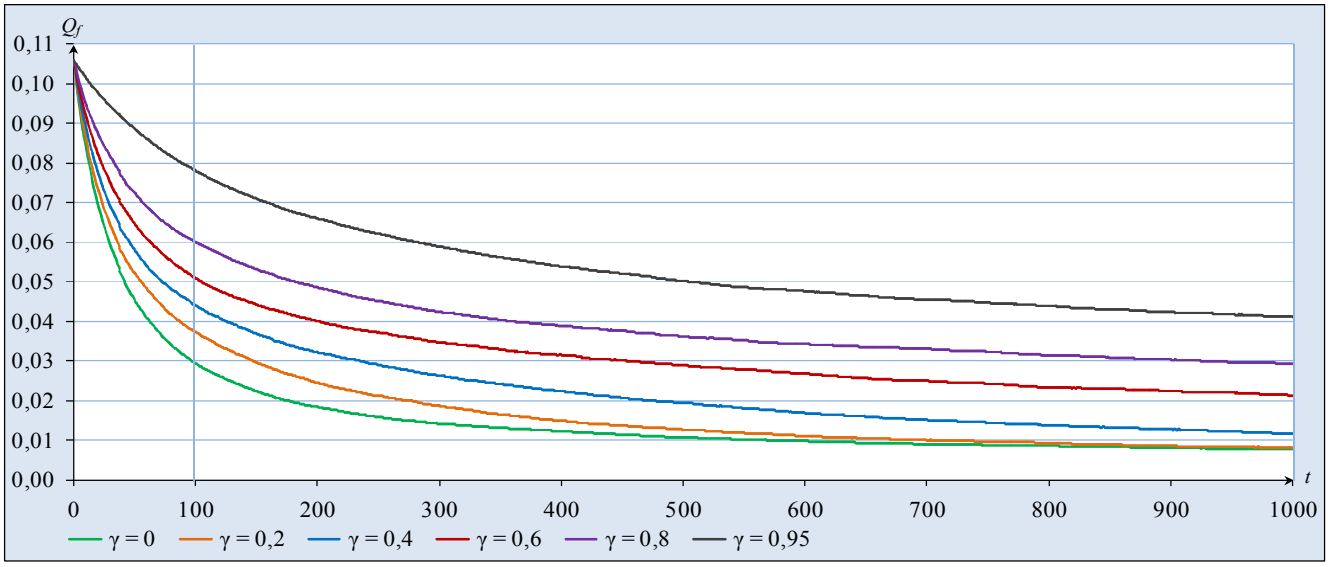

Рисунок 31 – Результаты обучения функции f_{ji}^{AS} в зависимости от доли метрик с неизвестными значениями γ

При $\gamma = 0$ (кривая зеленого цвета) и $\gamma = 0{,}2$ (кривая желтого цвета) значения среднего отклонения на 1000-м шаге обучения составили $Q_f^{(1000)} = 77 \cdot 10^{-4}$ и $Q_f^{(1000)} = 82 \cdot 10^{-4}$ соответственно. Следовательно, отсутствие значений 20% метрик при обучении несущественно влияет на результат. Обучение функции f_{ji}^{AS} осуществляется даже при $\gamma = 0{,}95$ (кривая серого цвета), а значения среднего отклонения при этом составили $Q_f^{(100)} = 779 \cdot 10^{-4}$ и $Q_f^{(1000)} = 410 \cdot 10^{-4}$.

Результаты экспериментального исследования показали, что предложенный метод обучения позволяет осуществлять аппроксимацию функции вероятности реализации угроз нарушителем в случае, когда данные об инцидентах ИБ неполные, неточные, неоднородные и нечисловые, что зачастую встречается при решении прикладных задач прогнозирования вероятности рисковых событий.

Выводы по разделу 3

1. Предложена методика, позволяющая повысить точность прогнозирования вероятности реализации угроз нарушителем за счет настройки весовых коэффициентов категорий и метрик защитных мер и метрик нарушителей.
2. Объектами обучающей выборки являются структурированные сведения об инцидентах ИБ. Обучение выполняется в последовательном режиме при поступлении данных об очередном инциденте ИБ, тем самым обеспечивая ответную реакцию на изменения окружающей среды.
3. Проведен ряд экспериментов, доказывающих возможность отбора значимых признаков в процессе обучения. Также доказана устойчивость предложенного метода к влиянию различных факторов, например, возможность обучения на объектах, данные о которых неполны.
4. Для решения задачи прогнозирования вероятности рискового события впервые применен специальный вариант метода обратного распространения ошибки, позволяющий значительно сократить требуемое число объектов обучающей выборки. Это преимущество является существенным, поскольку объем обучающей выборки, выраженный числом инцидентов ИБ, как правило, ограничен.
5. Предложенная методика количественной оценки вероятности реализации угроз нарушителем, при условии качественного отбора метрик и оценки значений их весовых коэффициентов методом анализа иерархий, позволяет снизить среднюю ошибку до 5% при наличии выборки из 100 инцидентов ИБ и до 1% при наличии выборки из 1000 инцидентов ИБ.

4 Применение результатов исследования при решении практических задач оценки рисков безопасности корпоративных информационных систем

4.1 Модуль управления рисками безопасности корпоративной информационной системы

Процессы оценки, обработки и мониторинга рисков безопасности КИС на уровне ее элементов являются весьма трудоемкими, особенно если при этом используются сложные математические модели и алгоритмы оценки рисков. В связи с этим возникает необходимость использования средств, автоматизирующих процедуры сбора, обработки и представления информации.

Для автоматизации процесса управления рисками могут быть использованы различные инструменты, обладающие необходимой функциональностью. При модульной архитектуре КИС на базе единой интеграционной платформы, например, SAP или 1С, модуль управления рисками безопасности КИС может быть реализован на базе данной платформы.

Предложенные в диссертационной работе модели и методы использованы при разработке модуля управления рисками в составе системы автоматизации процессов управления ИБ ООО «Газпром трансгаз Санкт-Петербург», что подтверждается актом, приведенным в приложении В.

В диссертационной работе приводится характеристика архитектуры и функциональных возможностей разработанного модуля управления рисками, а также реализованных коннекторов к смежным системам.

4.1.1 Архитектура модуля управления рисками

Модуль управления рисками на аппаратном уровне состоит из трех серверов: сервера приложений, сервера БД и сервера сервисов. Модуль обменивается данными со смежными системами, к которым относятся смежные модули и инфраструктурные сервисы КИС, а также общедоступные ресурсы сети

Интернет. Архитектура модуля управления рисками безопасности КИС представлена на рисунке 32.

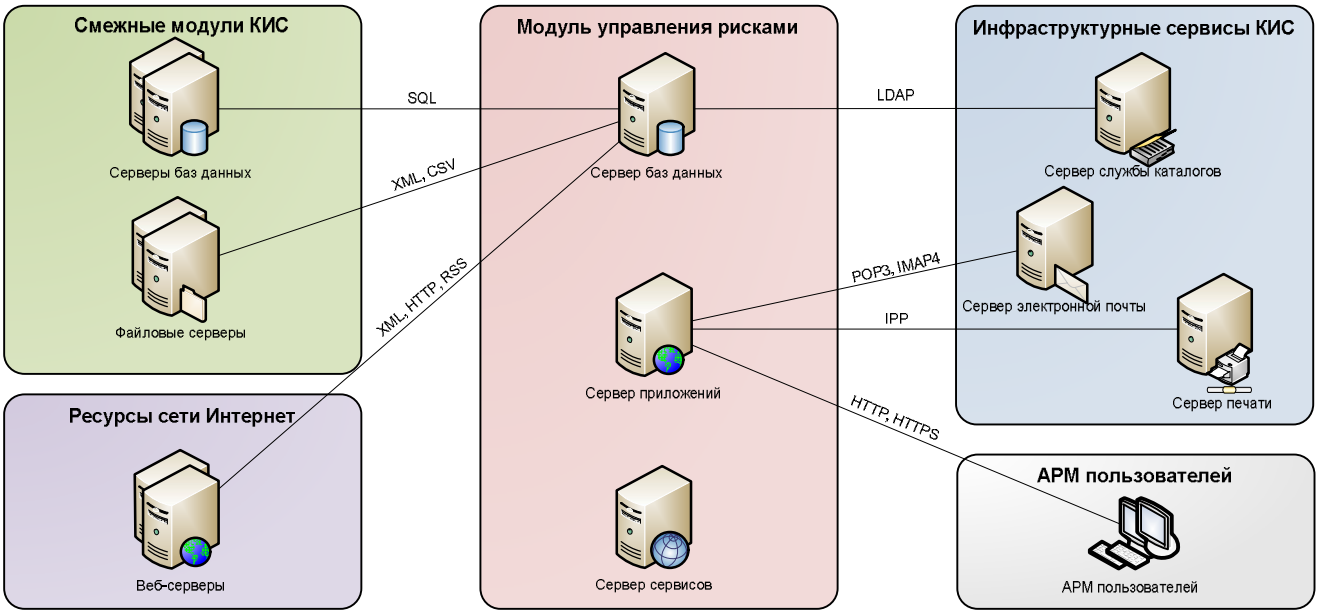

Рисунок 32 – Архитектура модуля управления рисками

Модуль управления рисками реализован на базе интеграционной платформы RSA Archer GRC версии 5.5, предназначенной для создания корпоративных систем стратегического управления, управления рисками и контроля соответствия требованиям регуляторов [11].

Для установки программных компонентов RSA Archer GRC на серверах помимо операционной системы (ОС) Windows Server должно быть установлено следующее ПО:

– Microsoft Internet Information Server (IIS) и .NET Framework на сервере приложений;
– система управления базами данных (СУБД) Microsoft SQL Server на сервере БД;
– .NET Framework и Java Runtime Environment на сервере сервисов.

Архитектура интеграционной платформы RSA Archer GRC включает три логических уровня:

– уровень СУБД – набор процедур хранения, обработки и представления данных, необходимых для функционирования модуля;

– уровень приложений – набор объектов C#, инкапсулирующих логику приложения и взаимодействующих с СУБД;
– уровень интерфейса – набор ASP.NET-страниц, написанных на языке C#, через которые осуществляется вызов уровня приложений для получения и обработки данных.

Сервер приложений реализует логические уровни интерфейса и приложений, взаимодействует с АРМ пользователей, выполняет обработку информации в различных приложениях и взаимодействует с СУБД. Доступ пользователей к серверу приложений осуществляется через браузер по протоколу HTTPS. Для возможности разработки и администрирования интеграционной платформы RSA Archer GRC на АРМ требуется установка Microsoft Silverlight.

Сервер БД реализует логический уровень БД. Структура данных модуля управления рисками безопасности КИС представлена на рисунке 33 в виде диаграммы классов в нотации UML.

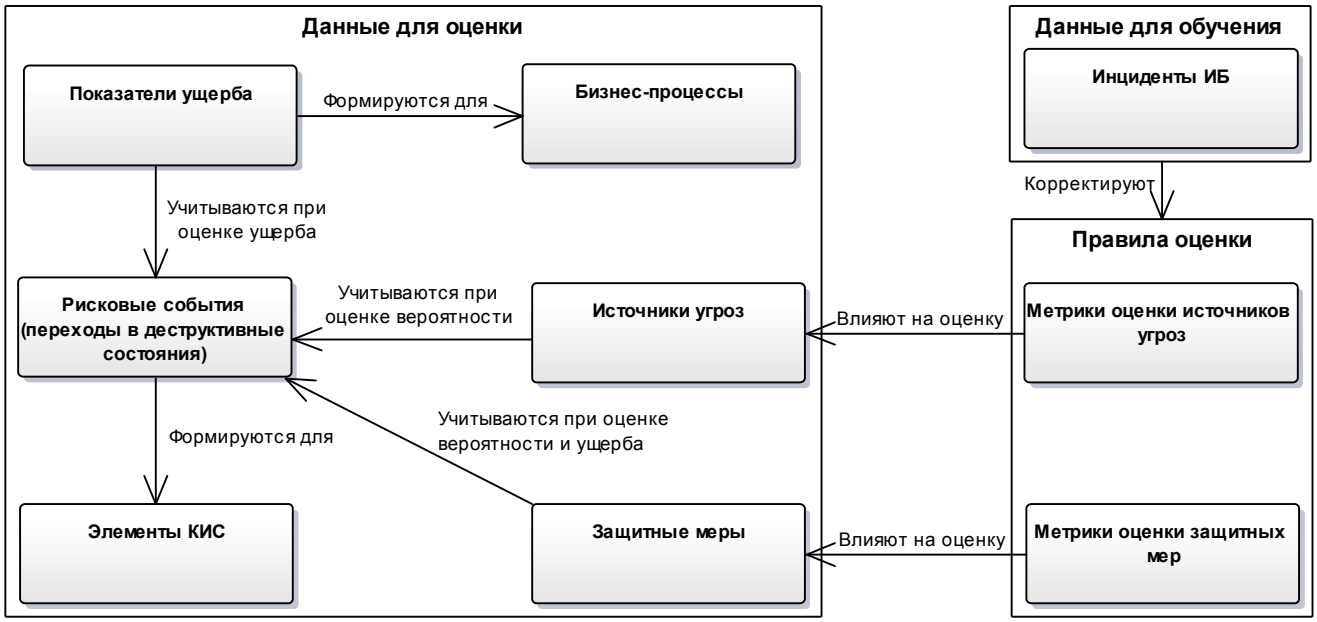

Рисунок 33 – Структура данных модуля управления рисками

Данные, необходимые для оценки и обработки рисков, вводятся оператором либо импортируются из внешних систем. В БД кроме таблиц с данными имеется обширный набор служебных представлений и служебных процедур, посредством которых осуществляется управление данными.

Сервер сервисов реализует логический уровень приложений и предназначен для выполнения ресурсоемких процедур (вычислений, импорта и экспорта данных и прочих). Кроме того, на сервере сервисов реализовано взаимодействие интеграционной платформы RSA Archer GRC с разработанным программным модулем обработки данных через операции ввода-вывода данных в файлы с форматом «.csv». Программный модуль обработки данных содержит два исполняемых файла на языке C++:

– файл «Learning.exe» выполняет процедуру обучения на основе данных об инцидентах ИБ;
– файл «Graph_traversal.exe» выполняет процедуру расчета вероятности рисковых событий с применением алгоритма поиска в глубину и алгоритма Дейкстры.

Интерфейс модуля управления рисками представлен на рисунке 34.

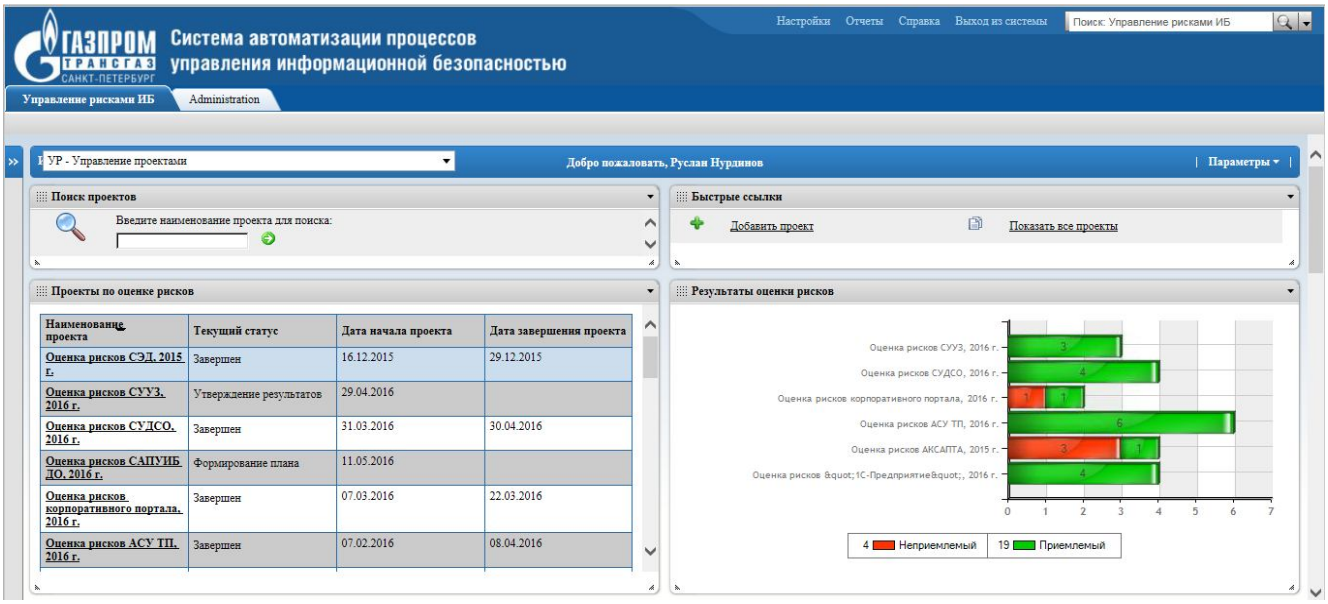

Рисунок 34 – Интерфейс модуля управления рисками

4.1.2 Функциональные возможности модуля управления рисками

Модуль управления рисками безопасности КИС включает три основных функциональных блока: оценка рисков, обработка рисков, мониторинг и контроль рисков.

Оценка рисков безопасности КИС осуществляется на основе модели, предложенной в подразделе 2.4 диссертационной работы. Кроме того,

выполняется корректировка правил оценки рисков на основе данных об инцидентах ИБ в соответствии с процедурой, описанной в подразделе 3.1 диссертационной работы. Диаграмма функций модуля в части оценки рисков представлена в нотации EPC на рисунке 35.

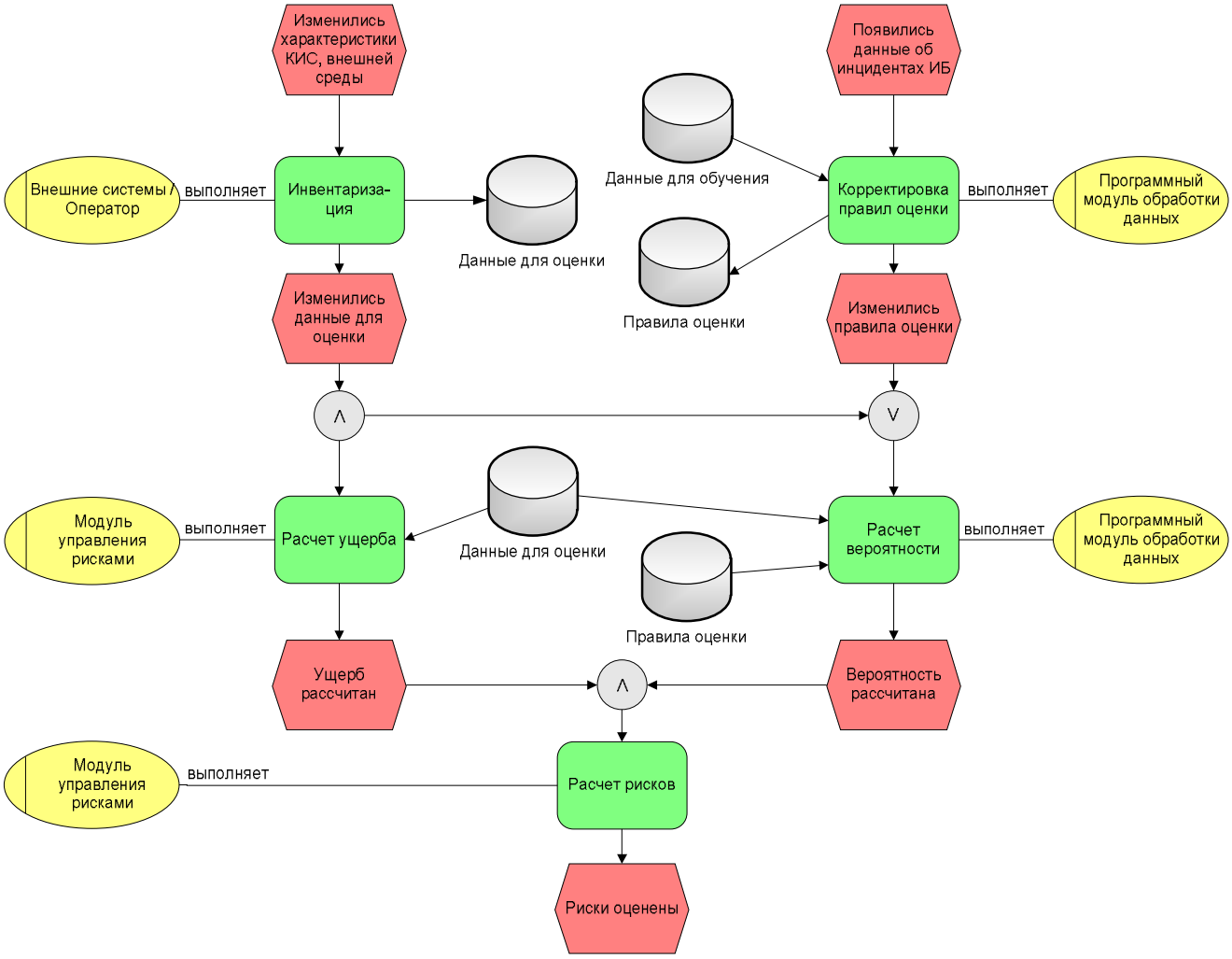

Рисунок 35 – Диаграмма функций модуля в части оценки рисков

Обработка рисков осуществляется в диалоговом режиме с оператором, который выбирает способ обработки для каждого неприемлемого риска. В том случае, если выбран способ обработки «снижение риска», оператор осуществляет выбор защитных мер из предложенного перечня. После обработки осуществляется переоценка рисков.

Мониторинг и контроль рисков осуществляется при помощи специальной информационной панели, на которой отображаются актуальные данные о рисках безопасности КИС.

Для реализации функций модуля управления рисками использованы следующие функциональные возможности интеграционной платформы RSA Archer GRC [177]:

- конструктор приложений, предоставляющий визуальный интерфейс для создания приложений и настройки интерфейса пользователей;
- средства создания отчетов и мониторинга, используемые для представления аналитической информации в форме таблиц, графиков и диаграмм;
- средства контроля доступа пользователей, используемые для настройки правил доступа пользователей к информации на уровне модуля, приложений, записей и полей;
- механизм формирования рабочих процессов, позволяющий реализовывать правила выполнения процессов обработки информации и отслеживания состояния выполнения процессов;
- средства формирования уведомлений, используемые для настройки правил и условий рассылки сообщений пользователям;
- механизмы интеграции, используемые для настройки потоков получения и алгоритмов обработки данных, поступающих из внешних систем;
- средства настройки пользовательского окружения, используемые для формирования интерфейсов пользователей в виде рабочих областей, информационных панелей и форм редактирования данных.

Недостатком интеграционной платформы RSA Archer GRC следует признать ограниченность возможностей встроенных механизмов обработки данных и сравнительно долгое время выполнения вычислительных расчетов. Для устранения этого недостатка реализован программный модуль обработки данных на языке C++.

4.1.3 Интеграция модуля управления рисками с внешними системами

Реализованный модуль позволяет осуществлять оценку рисков безопасности КИС на основе данных, структура которых приведена на

рисунке 33. Для сбора данных требуется интеграция модуля управления рисками со смежными системами, реализуемая за счет коннекторов.

Интеграционная платформа RSA eGRC Platform поддерживает следующие способы интеграции:

- взаимодействие с СУБД посредством SQL-запросов;
- использование веб-сервисов посредством протоколов REST и SOAP;
- использование файлов в форматах XLS, CSV, XML;
- взаимодействие по электронной почте посредством протоколов POP3/SMTP.

При загрузке данных платформой возможно их дополнительное преобразование и фильтрация по заданным правилам.

Данные, необходимые для оценки рисков безопасности КИС, импортируются из смежных систем, к которым могут относиться смежные модули и инфраструктурные сервисы КИС. Кроме того, возможна загрузка данных из общедоступных ресурсов сети Интернет, таких как:

- банк данных угроз ФСТЭК [7];
- базы уязвимостей [144, 145, 165];
- базы инцидентов ИБ [147, 172, 179].

В таблице 14 приведена характеристика коннекторов, обеспечивающих обмен данными между модулем управления рисками и смежными системами.

Таблица 14 – Характеристика коннекторов

Смежная система	Направление (импорт/экспорт)	Передаваемые данные	Способ интеграции
Система управления ресурсами	Импорт	Сведения об элементах КИС, бизнес-процессах, последствиях	– SQL; – XML
Система инвентаризации ИТ-активов	Импорт	Сведения об элементах КИС	– SQL; – XML
Система контроля защищенности	Импорт	Сведения об элементах КИС, защитных мерах	XML
Система мониторинга событий безопасности	Импорт	Сведения об угрозах, источниках угроз, инцидентах	XML
Система предотвращения утечек информации	Импорт	Сведения об угрозах, источниках угроз, инцидентах	XML

Смежная система	Направление (импорт/экспорт)	Передаваемые данные	Способ интеграции
Система анализа конфигурации АРМ	Импорт	Сведения об элементах КИС, защитных мерах	– XML; – CSV
Система электронного документооборота	– импорт; – экспорт	Приказы, акты, протоколы оценки и обработки рисков	XML
Система управления заявками	Импорт	Сведения об инцидентах	– SQL; – XML
	Экспорт	Сведения о заявках по оценке и обработке рисков	– SQL; – XML
Ресурсы сети Интернет	Импорт	Сведения об источниках угроз, угрозах, уязвимостях, защитных мерах и инцидентах	– XML; – CSV
Подсистема обработки данных	– импорт; – экспорт	Данные об элементах КИС, значениях метрик и весовых коэффициентов, инцидентах	CSV

4.2 Применение методики формирования рационального комплекса защитных мер для корпоративной информационной системы предприятия

Предложенная в диссертационной работе методика формирования рационального комплекса защитных мер используется при проектировании систем защиты информации для автоматизированных и информационных систем в ООО «Газинформсервис», что подтверждается актом, приведенным в приложении В.

В диссертационной работе представлены основные результаты применения данной методики при проектировании СЗИ ИС «Бухгалтерия и кадры», являющейся сегментом КИС предприятия нефтегазовой отрасли.

4.2.1 Характеристика защищаемой системы

ИС «Бухгалтерия и кадры» предназначена для кадрового и бухгалтерского учета и обрабатывает сведения, содержащие конфиденциальную информацию, в том числе персональные данные (ПДн) работников предприятия.

ИС «Бухгалтерия и кадры» является территориально распределенной, поскольку часть АРМ находятся в филиале и подключаются к терминальному серверу предприятия через сеть Интернет по технологии Remote Desktop Protocol.

Основу ИС «Бухгалтерия и кадры» составляют сервер 1С с установленным прикладным ПО «1С: Предприятие», сервер корпоративного портала с установленным прикладным ПО Microsoft Sharepoint и файловый сервер, на котором осуществляется хранение и обработка файлов пользователей, содержащих конфиденциальную информацию.

При оценке рисков безопасности ИС «Бухгалтерия и кадры» учитывались прочие ТС, в частности, серверы ИТ и ИБ, АСО и АРМ пользователей, а также установленное на них ПО. ТС объединены в локальную вычислительную сеть (ЛВС) предприятия с использованием ЛС Ethernet. Перечень элементов ИС «Бухгалтерия и кадры» приведен в таблице Г.1 приложения Г. Для упрощения расчетов проведена группировка идентичных элементов, например, АРМ пользователей со схожей конфигурацией.

Значения вероятности нарушения доступности элементов ИС «Бухгалтерия и кадры» в результате воздействия естественных источников угроз определялись на основе статистических данных, приведенных в таблице 15.

Таблица 15 – Результаты оценки вероятности нарушения доступности элементов ИС «Бухгалтерия и кадры» под воздействием естественных источников угроз

Наименование элемента (группы элементов)	**Среднее число отказов (нарушений доступности) в год, λ_j**	**Вероятность нарушения доступности, $p^{NS}(v_j)$**
Серверы	0,033	0,033
АРМ администрации	0,051	0,05
АРМ филиала	0,057	0,056
АСО администрации и филиала	0,05	0,049
ЛС администрации	0,137	0,128
ЛС филиала	0,150	0,139
ЛС Интернет	0,400	0,330
ОС Windows Server 2012	0,067	0,064
ОС Windows 7	0,064	0,062
Cisco IOS	0	0
ОС HP	0,067	0,064
СУБД SQL Server Standard 2014	0,100	0,095
MS SharePoint	0,132	0,124
Active Directory	0	0
1С: Предприятие	0,200	0,181

Сформирована модель нарушителей, на основе которой определялись значения показателей степени опасности, представленная в таблице 16.

Таблица 16 – Модель нарушителей безопасности ИС «Бухгалтерия и кадры»

Нарушитель	Способ доступа	Мотивация	Оснащенность	Техническая компетентность	Знание информации	Права доступа	Время доступа	Степень опасности
Специальные службы иностранных государств	Удаленный	Отсутствие мотива	Оборудование, сделанное на заказ	Профессионал	Отсутствие знаний	Отсутствуют	<1 дня	0,26
Террористические, экстремистские группировки	Удаленный	Идеологические / религиозные убеждения	Стандартное оборудование	Непрофессионал	Отсутствие знаний	Отсутствуют	<1 дня	0,16
Криминальные структуры	Удаленный	Корыстные интересы	Специализированное оборудование	Специалист	Отсутствие знаний	Отсутствуют	<1 дня	0,3
Квалифицированные взломщики (хакеры)	Удаленный	Профессиональное самоутверждение	Заказное оборудование	Профессионал	Отсутствие знаний	Отсутствуют	<1 дня	0,34
Конкурирующие организации	Удаленный	Корыстные интересы	Специализированное оборудование	Специалист	Отсутствие знаний	Отсутствуют	<0,5 часа	0,3
Разработчики, производители, поставщики ПО, ТС	Удаленный	Отсутствие мотива	Специализированное оборудование	Профессионал	Чувствительная информация	Отсутствуют	<1 дня	0,3
Посетители (физические лица)	Физический	Любопытство	Отсутствует	Непрофессионал	Отсутствие знаний	Отсутствуют	<1 дня	0,12
Подрядчики (лица, привлекаемые для пуско-наладочных работ и настройки)	Физический	Отсутствие мотива	Стандартное оборудование	Специалист	Чувствительная информация	Привилегированные	<1 месяца	0,28
Обслуживающий персонал (охрана, уборщики)	Физический	– халатность; – любопытство	Отсутствует	Непрофессионал	Отсутствие знаний	Отсутствуют	<1 месяца	0,14
Бывшие работники	Удаленный	Месть	Стандартное оборудование	Непрофессионал	Ограниченные знания	Отсутствуют	<1 дня	0,2

Нарушитель	Способ доступа	Мотивация	Оснащенность	Техническая компетентность	Знание информации	Права доступа	Время доступа	Степень опасности
Пользователи администрации	Удаленный и физический	– халатность; – любопытство	Стандартное оборудование	Непрофессионал	Ограниченные знания	Пользовательские	<1 месяца	0,21
Пользователи филиала	Удаленный и физический	– халатность; – любопытство	Стандартное оборудование	Непрофессионал	Ограниченные знания	Пользовательские	<1 месяца	0,21
Администраторы ИТ	Удаленный и физический	Отсутствие мотива	Специализированное оборудование	Специалист	Чувствительная информация	Административные	>1 месяца	0,41
Администраторы ИБ	Удаленный и физический	Отсутствие мотива	Специализированное оборудование	Специалист	Чувствительная информация	Привилегированные	>1 месяца	0,35
Пользователи с правами разработчиков 1С	Удаленный и физический	Отсутствие мотива	Специализированное оборудование	Специалист	Чувствительная информация	Административны	<1 месяца	0,41
Криминальные структуры совместно с хакерами	Удаленный	Корыстные интересы	Заказное оборудование	Профессионал	Отсутствие знаний	Отсутствуют	<1 дня	0,43
Конкурирующие организации совместно с разработчиками ПО	Удаленный	Корыстные интересы	Специализированное оборудование	Профессионал	Чувствительная информация	Отсутствуют	<1 дня	0,5
Хакеры совместно с разработчиками ПО	Удаленный и физический	Профессиональное самоутверждение	Заказное оборудование	Профессионал	Чувствительная информация	Отсутствуют	<1 дня	0,45
Конкурирующие организации совместно с бывшими работниками	Удаленный	Корыстные интересы	Специализированное оборудование	Специалист	Ограниченные знания	Отсутствуют	<1 дня	0,35

Для дальнейших расчетов выбраны внешний и внутренний нарушители, обладающие ненулевой мотивацией и наибольшей степенью опасности:

– конкурирующие организации совместно с разработчиками ПО, реализующие угрозы посредством удаленного доступа к элементам ИС «Бухгалтерия и кадры», со степенью опасности $d = 0{,}5$;

– пользователи администрации и филиала, реализующие угрозы посредством физического и удаленного доступа к элементам ИС «Бухгалтерия и кадры», со степенью опасности $d = 0{,}21$.

На рисунке 36 приведена структурная схема ИС «Бухгалтерия и кадры» с указанием начальных положений нарушителей.

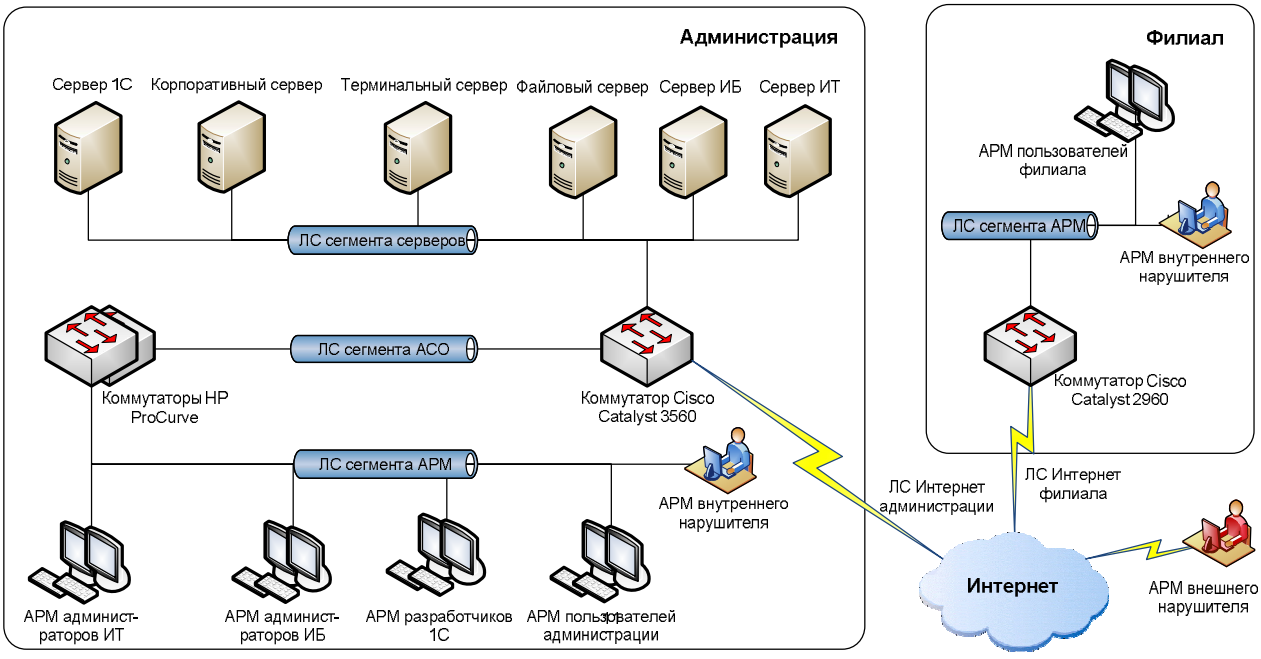

Рисунок 36 – Структурная схема ИС «Бухгалтерия и кадры»

Начальный комплекс защитных мер, реализованных до внедрения СЗИ ИС «Бухгалтерия и кадры», представлен в таблице 17.

Таблица 17 – Начальный комплекс защитных мер

Наименование средства / меры	Количество	Место размещения	Затраты, тыс. руб.	Связанные категории
Сертифицированная ОС Windows Server 2012 Standard	6	Серверы	53,1	ИАФ, УПД, ОПС, РСБ, АНЗ, ОЦЛ, ЗИС, УКФ
Сертифицированная ОС Windows 7 Professional	100	АРМ	118	ИАФ, УПД, ОПС, РСБ, АНЗ, ОЦЛ, ЗИС, УКФ

Наименование средства / меры	Количество	Место размещения	Затраты, тыс. руб.	Связанные категории
Встроенные средства BIOS	106	Серверы и АРМ	–	ИАФ, УПД
Netcheck	106	Серверы и АРМ	27,7	РСБ, АНЗ, УКФ
Kaspersky Endpoint Security	106	Серверы и АРМ	166,6	РСБ, АВЗ
Система контроля и управления доступом администрации	1	Администрация	517	ЗТС
Система контроля и управления доступом филиала	1	Филиал	151	ЗТС
Камеры видеонаблюдения	22	Администрация	39,6	ЗТС, ИНЦ
Источник бесперебойного питания для серверов	1	Администрация	203,5	ОДТ
Комплект документов по ИБ	–	Корпоративный портал	165	УПД, ЗНИ, ЗТС, ИНЦ, УКФ

4.2.2 Формирование и оценка рационального комплекса защитных мер

Формирование рационального комплекса защитных мер для ИС «Бухгалтерия и кадры» осуществлялось на основе типового перечня, включающего 72 СрЗИ, имеющих сертификаты соответствия ФСТЭК России, и 40 организационных мер. Для каждой защитной меры были определены значения метрик по правилам, приведенным в подразделе 2.3 диссертационной работы.

Задача выбора рационального комплекса защитных мер, определяемая выражением (65), решалась полным перебором комплексов защитных мер:

- сформированных с учетом принципов совместимости, зависимости и взаимозаменяемости защитных мер;
- выполняющих требования Приказа ФСТЭК России от 18.02.2013 № 21 [104], предъявляемые к четвертому уровню защищенности ПДн.

В результате сформирован рациональный комплекс дополнительных защитных мер, приведенный в таблице 18.

Таблица 18 – Рациональный комплекс дополнительных защитных мер

Наименование средства / меры	Количество	Место размещения	Затраты, тыс. руб.	Связанные категории
С-Терра Криптошлюз 1000V	1	Администрация	101	ИАФ, УПД, СОВ, ОЦЛ, ЗИС, КЗИ
С-Терра VPN клиент 4.1	14	АРМ филиала	61,6	ИАФ, УПД, СОВ, ОЦЛ, ЗИС, КЗИ
Электронный ключ SafeNet eToken	25	– АРМ филиала; – АРМ администраторов ИТ и ИБ; – АРМ разработчиков 1С	28,5	ИАФ, УПД, КЗИ
Secret Net 7.0	6	Серверы	54,76	ИАФ, УПД, ЗНИ, ОПС, РСБ, АНЗ, ОЦЛ, ЗИС, ИНЦ
DeviceLock Search Server	2	– сервер 1С; – файловый сервер	110	ЗНИ, ОЦЛ, ЗИС
Acronis Backup for Windows Server	3	– сервер 1С; – файловый сервер; – сервер портала	47,4	ОЦЛ, ОДТ

Для сравнения был рассмотрен альтернативный комплекс дополнительных защитных мер, приведенный в таблице 19 и предложенный разработчиками технического проекта на СЗИ ИС «Бухгалтерия и кадры».

Таблица 19 – Альтернативный комплекс дополнительных защитных мер

Наименование средства / меры	Количество	Место размещения	Затраты, тыс. руб.	Связанные категории
С-Терра Криптошлюз 1000V	2	– администрация; – филиал	202	ИАФ, УПД, СОВ, ОЦЛ, ЗИС, КЗИ
С-Терра VPN клиент	100	АРМ администрации и филиала	440	ИАФ, УПД, СОВ, ОЦЛ, ЗИС, КЗИ
Электронный ключ eToken PRO	100	АРМ администрации и филиала	150	ИАФ, УПД, КЗИ
Secret Net 7.0	106	Серверы и АРМ	784,4	ИАФ, УПД, ОПС, ЗНИ, РСБ, АНЗ, ОЦЛ, ЗИС, ИНЦ
DeviceLock 7.1	100	АРМ администрации и филиала	760	ЗНИ, ОЦЛ, ЗИС
DeviceLock Search Server	6	Серверы	330	ЗНИ, ОЦЛ, ЗИС
Сервер теневого копирования и журналирования	1	Администрация	270	РСБ, ИНЦ
Acronis Backup for Windows Server	6	Серверы	142,2	ОЦЛ, ОДТ

Оценка величины ущерба от переходов элементов ИС «Бухгалтерия и кадры» в деструктивные состояния осуществлялась с привлечением владельцев и пользователей системы. Стоимость активов ИС «Бухгалтерия и кадры» составила S_{IS} = 12 840 300 рублей.

Для каждого из рассматриваемых комплексов защитных мер определены значения вероятности переходов элементов КИС в деструктивные состояния. Результаты оценки рисков безопасности ИС «Бухгалтерия и кадры» при начальном, рациональном и альтернативном комплексах защитных мер приведены в таблице 20.

Таблица 20 – Результаты оценки рисков безопасности ИС «Бухгалтерия и кадры»

Наименование элемента	**Коли-чество**	**Деструктивное состояние**	**Величина ущерба, тыс. руб.**[1)]	**Вероятность перехода при комплексе защитных мер**		
				Началь-ный	**Рацио-нальный**	**Альтерна-тивный**
1. Сервер 1С	1	НСД	–	0,056	0,056	0,056
		Недоступно	220	0,033	0,033	0,033
2. Сервер корпоративного портала	1	НСД	–	0,056	0,056	0,056
		Недоступно	180	0,033	0,033	0,033
3. Терминальный сервер	1	НСД	–	0,056	0,056	0,056
		Недоступно	275	0,033	0,033	0,033
4. Сервер ИБ	1	НСД	–	0,056	0,056	0,056
		Недоступно	180	0,033	0,033	0,033
5. Файловый сервер	1	НСД	–	0,056	0,056	0,056
		Недоступно	180	0,033	0,033	0,033
6. Сервер ИТ-сервисов	1	НСД	–	0,056	0,056	0,056
		Недоступно	220	0,033	0,033	0,033
7. АРМ пользователей администрации	75	НСД	–	0,930	0,930	0,930
		Недоступно	37,5	0,050	0,050	0,050
8. АРМ администраторов ИТ	5	НСД	–	0,316	0,316	0,316
		Недоступно	48,2	0,050	0,050	0,050
9. АРМ администраторов ИБ	3	НСД	–	0,316	0,316	0,316
		Недоступно	37,5	0,050	0,050	0,050
10. АРМ разработчиков 1С	3	НСД	–	0,316	0,316	0,316
		Недоступно	45,3	0,050	0,050	0,050
11. АРМ пользователей филиала	14	НСД	–	0,930	0,930	0,930
		Недоступно	37,5	0,056	0,056	0,056
12. Коммутатор Cisco Catalyst 3560	1	НСД	–	0,056	0,056	0,056
		Недоступно	179,8	0,049	0,049	0,049

Наименование элемента	Коли-чество	Деструктивное состояние	Величина ущерба, тыс. руб.[1)]	Вероятность перехода при комплексе защитных мер		
				Началь-ный	Рацио-нальный	Альтерна-тивный
13. Коммутатор HP ProCurve Switch 2610-48	3	НСД	–	0,056	0,056	0,056
		Недоступно	58,4	0,049	0,049	0,049
14. Коммутатор Cisco Catalyst 2960	1	НСД	–	0,056	0,056	0,056
		Недоступно	35,2	0,049	0,049	0,049
15. ЛС сегмента серверов администрации	6	НСД	–	0,668	0,345	0,341
		Недоступно	0,6	0,128	0,128	0,128
16. ЛС сегмента АРМ администрации	86	НСД	–	1,000	1,000	1,000
		Недоступно	0,6	0,128	0,128	0,128
17. ЛС сегмента АСО администрации	6	НСД	–	0,668	0,345	0,341
		Недоступно	0,6	0,128	0,128	0,128
18. ЛС сегмента АРМ филиала	14	НСД	–	1,000	1,000	1,000
		Недоступно	0,6	0,139	0,139	0,139
19. ЛС Интернет администрации	2	НСД	–	0,983	0,992	0,983
		Недоступно	–	0,330	0,330	0,330
20. ЛС Интернет филиала	2	НСД	–	0,983	0,992	0,983
		Недоступно	–	0,330	0,330	0,330
21. ПО сервера 1С	1	НСД	–	0,362	0,016	0,016
		Недоступно	30	0,323	0,317	0,317
22. ПО сервера корпоративного портала	1	НСД	–	0,362	0,016	0,016
		Недоступно	30	0,277	0,272	0,272
23. ПО терминального сервера	1	НСД	–	0,362	0,016	0,016
		Недоступно	15	0,093	0,091	0,091
24. ПО сервера ИБ	1	НСД	–	0,362	0,016	0,016
		Недоступно	15	0,093	0,091	0,091
25. ПО файлового сервера	1	НСД		0,362	0,016	0,016
		Недоступно	15	0,093	0,091	0,091
26. ПО сервера ИТ	1	НСД	–	0,362	0,016	0,016
		Недоступно	15	0,093	0,091	0,091
27. ПО АРМ пользователей администрации	75	НСД	–	1,000	1,000	1,000
		Недоступно	3	0,107	0,107	0,105
28. ПО АРМ администраторов ИТ	5	НСД	–	0,242	0,090	0,005
		Недоступно	5,5	0,107	0,107	0,105
29. ПО АРМ администраторов ИБ	3	НСД	–	0,242	0,090	0,005
		Недоступно	4,5	0,107	0,107	0,105
30. ПО АРМ разработчиков 1С	3	НСД	–	0,242	0,090	0,005
		Недоступно	4,5	0,107	0,107	0,105
31. ПО АРМ филиала	14	НСД	–	1,000	1,000	1,000
		Недоступно	3	0,112	0,111	0,110

Наименование элемента	Коли-чество	Деструктивное состояние	Величина ущерба, тыс. руб.[1)]	Вероятность перехода при комплексе защитных мер		
				Началь-ный	Рацио-нальный	Альтерна-тивный
32. ПО коммутатора Cisco Catalyst 3560	1	НСД	–	0,668	0,345	0,341
		Недоступно	30	0,048	0,048	0,048
33. ПО коммутатора HP ProCurve	3	НСД	–	0,446	0,119	0,116
		Недоступно	15	0,108	0,107	0,107
34. ПО коммутатора Cisco Catalyst 2960	1	НСД	–	0,668	0,668	0,341
		Недоступно	15	0,048	0,048	0,048
35. БД 1С	1	Конфиденци-альность	1780	0,959	0,205	0,035
		Целостность	3520	0,059	0,000	0,017
		Доступность	370	0,169	0,002	0,159
36. БД корпоративного портала	1	Конфиденци-альность	10	0,962	0,223	0,035
		Целостность	920	0,312	0,000	0,033
		Доступность	85	0,153	0,001	0,128
37. БД пользователей	1	Конфиденци-альность	150	0,354	0,015	0,001
		Целостность	235	0,312	0,045	0,033
		Доступность	78	0,120	0,092	0,091
38. Каталог файлов пользователей с информацией ограниченного доступа	1	Конфиденци-альность	2750	0,354	0,090	0,001
		Целостность	520	0,312	0,000	0,033
		Доступность	45	0,120	0,000	0,091
Остаточный риск, тыс. руб.				**3971,6**	**683,4**	**342,3**

[1)] Указана верхняя граница величины ущерба для одного элемента КИС

Результаты оценки комплексов защитных мер, в том числе значения показателей затратоемкости активов и экономической эффективности, приведены в таблице 21.

Таблица 21 – Результаты оценки комплексов защитных мер

Комплекс защитных мер	Затраты на реализацию (тыс. руб.), S_z	Остаточный риск (тыс. руб.), R_z	Затратоемкость активов, ω_z	Экономическая эффективность, E_z
Начальный	1441,5	3971,6	0,423	6,15
Рациональный	425, 6 (1867,1)[1)]	(683,4)	(0,199)	7,73
Альтернативный	3007,5 (4449)	(342,3)	(0,360)	1,2

[1)] В скобках указаны значения показателей с учетом начального комплекса защитных мер

В результате использования методики формирования рационального комплекса защитных мер удалось снизить затраты на СЗИ ИС «Бухгалтерия и кадры» в 7 раз по сравнению с альтернативным комплексом защитных мер,

предложенным в техническом проекте. В то же время, использование рационального комплекса защитных мер позволило снизить остаточный риск в 5,8 раз по сравнению с начальным комплексом защитных мер.

На рисунке 37 приведен график, отражающий снижение показателя затратоемкости активов при пошаговом добавлении рациональных защитных мер из типового перечня.

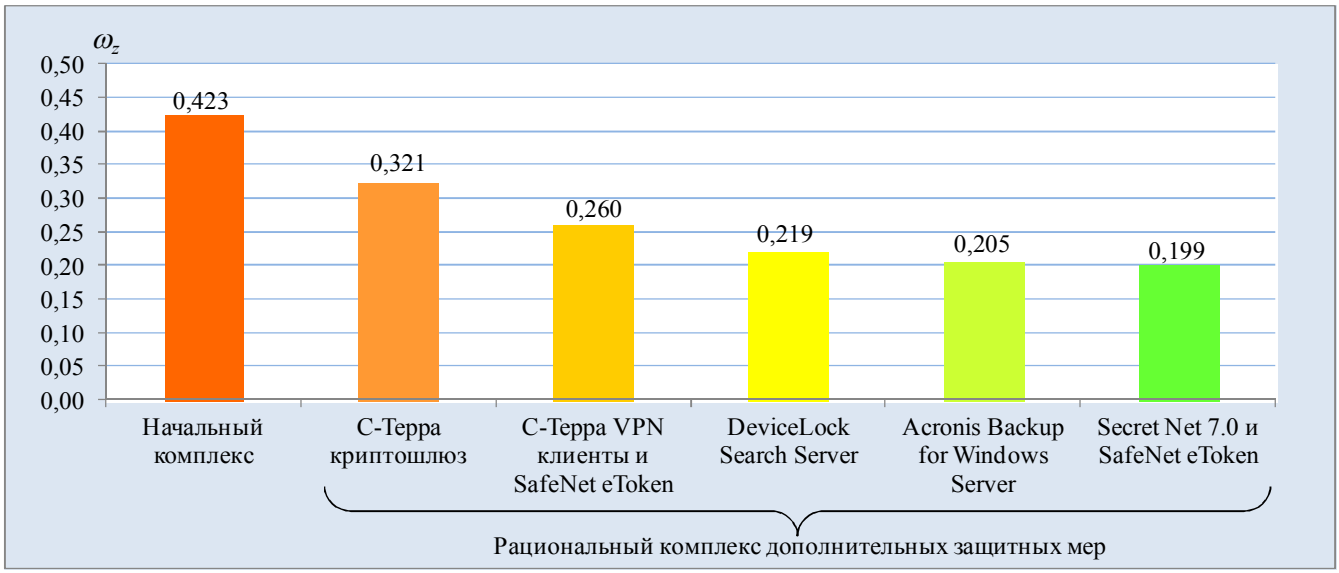

Рисунок 37 – Снижение показателя затратоемкости активов при пошаговом добавлении рациональных защитных мер

Таким образом, использование методики, предложенной в диссертационной работе, позволило оптимизировать затраты на реализацию СЗИ ИС «Бухгалтерия и кадры», являющейся сегментом КИС предприятия нефтегазовой отрасли. Полученные результаты свидетельствуют о том, что предложенная в подразделе 2.5 диссертационной работы методика позволяет сформировать рациональный комплекс защитных мер и предотвратить ненужные и необоснованные затраты на обеспечение безопасности КИС предприятия.

Выводы по разделу 4

1. Практическая значимость результатов исследования подтверждается успешным внедрением предложенных в диссертационной работе моделей и методик на коммерческих предприятиях и в учебных организациях.

2. Разработан модуль управления рисками безопасности КИС, подтверждающий адекватность предложенных в диссертационной работе модели оценки рисков и методики количественной оценки вероятности реализации угроз нарушителем на основе экспертно-нейросетевого определения показателей защищенности.
3. Использование методики формирования рационального комплекса защитных мер при проектировании и внедрении СЗИ сегмента КИС предприятия нефтегазовой отрасли позволило уменьшить показатель затратоемкости активов на 74 % по сравнению с альтернативным вариантом системы защиты, предложенным в техническом проекте.

Заключение

В диссертационной работе решена актуальная научная задача разработки методического аппарата, позволяющего повысить качество выбора защитных мер за счет применения научно-обоснованной формализованной модели количественной оценки рисков. При решении данной задачи получены следующие основные результаты.

1. Проведен сравнительный анализ подходов и математических методов количественной оценки рисков информационной безопасности, выявлены проблемы и ограничения в их применении.
2. Разработана оригинальная формализованная модель количественной оценки рисков, учитывающая связи между рисковыми событиями, определяемые в модели сценариев реализации угроз.
3. Предложен подход к определению совокупности взвешенных метрик для оценки показателей степени опасности нарушителя и степени реализации защитных мер.
4. Предложена методика, позволяющая повысить качество выбора защитных мер для корпоративной информационной системы за счет минимизации показателя затратоемкости активов с учетом установленных ограничений.
5. Выполнен синтез методики, позволяющей повысить точность прогнозирования вероятности реализации угроз нарушителем в условиях ограниченного набора данных об инцидентах информационной безопасности.
6. Значимость и эффективность разработанных моделей и методик подтверждается практическим опытом их использования.

Дальнейшим перспективным направлением исследования является адаптация предложенных моделей и методик для различных классов информационных и автоматизированных систем.

Полученные результаты соответствуют пункту 7 «Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения» и пункту 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».

Список сокращений и условных обозначений

В диссертационной работе используются следующие сокращения и условные обозначения:

ALE	–	Annual Loss Expectancy
ARO	–	Annualized Rate of Occurrence
CVSS	–	Common Vulnerability Scoring System
EPC	–	Engineering, Procurement and Construction
NPV	–	Net Present Value
ROI	–	Return on Investment
SLE	–	Single Loss Expectancy
TCO	–	Total Cost of Ownership
UML	–	Unified Modeling Language
АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
АСО	–	активное сетевое оборудование
БД	–	база данных
ИА	–	информационный актив
ИБ	–	информационная безопасность
ИС	–	информационная система
ИТ	–	информационные технологии
КИС	–	корпоративная информационная система
ЛВС	–	локальная вычислительная сеть
ЛС	–	линия связи
НСД	–	несанкционированный доступ
ОЛ	–	опросный лист
ОС	–	операционная система
ПДн	–	персональные данные

ПО	–	программное обеспечение
СВТ	–	средство вычислительной техники
СЗИ	–	система защиты информации
СрЗИ	–	средство защиты информации
СУБД	–	система управления базами данных
ТС	–	техническое средство
ЦОД	–	центр обработки данных

Список литературы

1. Агеев С.А., Саенко И.Б. Метод интеллектуального многоагентного управления рисками информационной безопасности в защищенных мультисервисных сетях специального назначения // T-Comm: Телекоммуникации и транспорт. 2015. Т. 9. № 1. С. 5-10.

2. Акимов В. А., Лапин В. Л., Попов В. М., Пучков В. А., Томаков В. И., Фалеев М. И. Надежность технических систем и техногенный риск. М.: ЗАО ФИД «Деловой экспресс», 2002. 368 с.

3. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft [Электронный ресурс] // Интуит: [сайт]. URL: http://www.intuit.ru/studies/courses/531/387/lecture/8996 (дата обращения: 26.12.2015).

4. Астахов А.М. Искусство управления информационными рисками. М.: ДМК Пресс, 2010. 312 с.

5. Атаманов А.Н. Динамическая итеративная оценка рисков информационной безопасности в автоматизированных системах: автореф. дис. ... канд. техн. наук: 05.13.19. М., 2012. 23 с.

6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. 2008-02-15. М.: ФСТЭК России, 2008. 69 с.

7. Банк данных угроз безопасности информации ФСТЭК [Электронный ресурс] // ФСТЭК России: [сайт]. URL: http://www.bdu.fstec.ru/ubi/vul (дата обращения: 02.06.2015).

8. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. № 1 (9). 2015. С. 73-79.

9. Беззатеев С.В., Волошина Н.В., Санкин П.С. Методика расчета надежности сложных систем, учитывающая угрозы информационной безопасности // Информационно-управляющие системы. 2014. № 3 (70). С. 78-83.

10. Бокс Д., Дженкинс Г. Анализ временных рядов: прогноз и управление. Вып. 1. М.: Мир, 1974. 405 с.

11. Борисенко П.С., Ильин И.В., Канев А.Н., Никифорова К.А., Нурдинов Р.А. Анализ современного рынка продуктов GRC [Электронный ресурс] // Электронный сборник статей по материалам XXXI студенческой международной научно-практической конференции. Новосибирск: СибАК, 2015. № 4 (30). С. 74-80. URL: http://sibac.info/studconf/tech/xxxi/41798 (дата обращения: 12.12.2015).

12. Брауэр В. Введение в теорию конечных автоматов: пер. с нем. М.: Радио и связь, 1987. 392 с.

13. Бурков В.Н., Заложнев А.Ю., Новиков Д.А. Теория графов в управлении организационными системами. М.: Синтег, 2001. 124 с.

14. Варфоломеев А.А. Основы информационной безопасности: учеб. пособие. М.: РУДН, 2008. 412 с.

15. Вихров Н.М., Ныркov А.П., Каторин Ю.Ф., Шнуренко А.А., Башмаков А.В., Соколов С.С., Нурдинов Р.А. Анализ информационных рисков // Морской вестник. 2015. № 3 (55). С. 81-85.

16. Вишняков Я.Д. Радаев Н.Н. Общая теория рисков: учеб. пособие для студ. высш. учеб. заведений. 2-е изд. М.: Академия, 2008. 368 с.

17. Волков Г.Г., Глинский О.Ю. Компьютерные информационные технологии: учеб.-метод. пособие, ч. 3. Бобруйск, 2010. 86 с.

18. Волков Ю.В., Самохин Д.С. Метод определения вида и параметров распределений случайных величин по эксплуатационным данным с объектов ядерной энергетики // Известия вузов. Ядерная энергетика. 2007. № 4. С. 15-23.

19. Воронцов К.В. Математические методы обучения по прецедентам [Электронный ресурс] // Информационно-аналитический ресурс MachineLearning: [сайт]. URL: http://machinelearning.ru/wiki/images/6/6d/Voron-ML-1.pdf (дата обращения: 11.10.2015).

20. Временная методика определения предотвращенного экологического ущерба [Электронный ресурс]. М.: Госкомэкология РФ, 1999. URL: http://envi.narod.ru/doc36.htm (дата обращения: 11.10.2015).

21. Вяткин В.Н., Гамза В.А. Маевский Ф.В. Риск-менеджмент: превентивное управление. М.: АП «Наука и образование», 2013. – 265 с.

22. Гатчин Ю.А., Карпик А.П., Ткачев К.О., Чиков К.Н., Шлишевский В.Б. Теоретические основы защиты информации от утечки по акустическим каналам: учеб. пособие. Новосибирск: СГГА, 2008. 194 с.

23. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: МИФИ, 1997. 537 с.

24. Гилльмулин Т.М. Модели и комплекс программ процесса управления рисками информационной безопасности: дис. ... канд. техн. наук: 05.13.18. Казань, 2010. 225 с.

25. Гончаренко В.А. Моделирование и оценивание характеристик случайных потоков событий в компьютерных сетях при параметрической неопределенности // Труды ВКА имени А.Ф.Можайского. 2015. Вып. 649. С. 16-22.

26. Городецкий В.И., Котенко И.В., Юсупов Р.М. Защита компьютерных сетей // Вестник Российской академии наук. 2006. Т. 76. № 7. С. 668-670.

27. ГОСТ 34.003-90. Автоматизированные системы. Термины и определения. Введ. 1992-01-01. М.: Стандартинформ, 2009. 16 с.

28. ГОСТ 34.201-89. Виды, комплектность и обозначение документов при создании автоматизированных систем. Введ. 1990-01-01. М.: ИПК Издательство стандартов, 2002. 11 с.

29. ГОСТ 34.601-90. Автоматизированные системы. Стадии создания. Введ. 1992-01-01. М.: Стандартинформ, 2009. 6 с.

30. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. Введ. 1990-01-01. М.: Стандартинформ, 2009. 12 с.

31. ГОСТ Р 27.002-2009. Надежность в технике. Термины и определения. Введ. 2011-01-01. М.: Стандартинформ, 2011. 32 с.

32. ГОСТ Р 50779.10-2000. Статистические методы. Вероятность и основы статистики. Термины и определения. Введ. 2001-07-01. М.: ИПК Издательство стандартов, 2001. 46 с.

33. ГОСТ Р 53114-2008. Обеспечение информационной безопасности в организации. Основные термины и определения. Введ. 2009-10-01. М.: Стандартинформ, 2009. 20 с.

34. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. Введ. 2016-04-01. М.: Стандартинформ, 2015. 12 с.

35. ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. Введ. 2012-03-01. М.: Стандартинформ, 2011. 105 с.

36. ГОСТ Р ИСО/МЭК ТО 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Ч. 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введ. 2008-07-01. М.: Стандартинформ, 2007. 18 с.

37. ГОСТ Р ИСО/МЭК 15408-1-2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. Введ. 2012-11-15. М.: Стандартинформ, 2014. 50 с.

38. ГОСТ Р ИСО/МЭК 16085-2007. Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения. Введ. 2008-09-01. М.: Стандартинформ, 2008. 31 с.

39. ГОСТ Р ИСО/МЭК 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Введ. 2008-07-01. М.: Стандартинформ, 2009. 50 с.

40. ГОСТ Р ИСО/МЭК 18045-2013. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. Введ. 2014-07-01. М.: Стандартинформ, 2014. 250 с.

41. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введ. 2008-02-01. М.: Стандартинформ, 2008. 31 с.

42. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Введ. 2011-12-01. М.: Стандартинформ, 2011. 51 с.

43. ГОСТ Р ИСО/МЭК 27006-2008. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Введ. 2009-10-01. М.: Стандартинформ, 2010. 40 с.

44. ГОСТ Р 50397-2011. Совместимость технических средств электромагнитная. Термины и определения. Введ. 2012-09-01. М.: Стандартинформ, 2013. 62 с.

45. ГОСТ Р ИСО/МЭК 50922-2006. Защита информации. Основные термины и определения. Введ. 2008-02-01. М.: Стандартинформ, 2008. 12 с.

46. ГОСТ Р ИСО/ТО 13569-2007. Финансовые услуги. Рекомендации по информационной безопасности. Введ. 2007-09-01. М.: Стандартинформ, 2009. 61 с.

47. Гуренко В.В. Введение в теорию автоматов. М.: МГТУ имени Н.Э. Баумана, 2013. 62 с.

48. Дойникова Е.В. Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов // Труды СПИИРАН, 2013. Вып. 3 (26). С. 54-68.

49. Дулатов И.Н., Ныркова А.П. Современные подходы к оценке рисков информационной безопасности // Материалы III Международной научно-практической конференции «Информационные управляющие системы и технологии». 2014. С. 155-157.

50. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО «ТИД ДС», 2002. 688 с.

51. Задорожко Д.С. Современные подходы к оценке деловой репутации и репутационного риска // УЭкС, 2013. № 8 (56).

52. Зайцева Н.М., Нурдинов Р.А. Оценка ущерба от правонарушений в информационной сфере // Вестник полиции. 2015. № 4. С. 124-132.

53. Зараменских Е.П. Управление жизненным циклом информационных систем: монография. Новосибирск: ЦРНС, 2014. 270 с.

54. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. М.:Горячая линия – Телеком, 2002. 452 с.

55. Зикратов И.А., Одегов С.В., Смирных А.В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования // Научно-технический вестник информационных технологий, механики и оптики. 2013. № 1 (83). С. 141-144.

56. Зорин А.В., Зорин В.А., Пройдакова Е.В., Федоткин М.А. Введение в общие цепи Маркова: учеб.-метод. пособие. Нижний Новгород: Нижегородский госуниверситет, 2013. 51 с.

57. Иванова И.В. Нечетко-логические и вероятностные инструменты компьютеризированного управления информационными рисками промышленных предприятий: автореф. дис. ... канд. экон. наук: 08.00.13, 08.00.05. М., 2013. 23 с.

58. Калашников А.О., Бурса М.В., Остапенко Г.А. Мультисервисные сети: дискретная риск-модель HTTP-флуда // Вопросы кибербезопасности. 2015. № 1 (9). С.49-54.

59. Карпушкин С.В. Теория принятия проектных решений: учеб. пособие. Тамбов: ТГТУ, 2015. 86 с.

60. Каторин Ю.Ф., Нурдинов Р.А., Зайцева Н.М. Модель количественной оценки рисков безопасности информационной системы // Yовый университет. Серия: технические науки. 2016. № 3 (49). С. 42-47.

61. Каторин Ю.Ф., Нурдинов Р.А., Зайцева Н.М., Канев А.Н., Иоффе М.А. Количественная оценка вероятности реализации угроз нарушения безопасности АСУ технологическими процессами террористическими группировками. Вопросы

оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. Т. 3-4 (93-94). С. 3-9.

62. Кащенко А.Г. Многокритериальные модели и алгоритмы управления рисками информационной безопасности автоматизированных систем: автореф. дис. ... канд. техн. наук: 05.13.19. Воронеж, 2008. 18 с.

63. Ключев А.О., Кустарев П.В., Ковязина Д.Р., Петров Е.В. Программное обеспечение встроенных вычислительные систем: учеб. пособие. СПб.: СПб НИУ ИТМО, 2009. 212 с.

64. Когаловский М.Р. Перспективные технологии информационных систем. М.: ДМК Пресс; Компания АйТи, 2003. 288 с.

65. Колегов Д.Н. Проблемы синтеза и анализа графов атак // Вестник ТГУ. Приложение. 2007. № 23. С. 180-188.

66. Кормен Т.Х., Лейзерсон Ч.И., Ривест Р.Л., Штайн К.Э. Алгоритмы. Построение и анализ: пер. с англ. 3-е изд. М.; СПб.; Киев: Вильямс, 2013. 1296 с.

67. Коробов В.Б. Сравнительный анализ методов определения весовых коэффициентов «влияющих факторов» // Социология: методология, методы, математические модели. 2005. № 20. С. 54-73.

68. Котенко Д.А. Метод оценки риска информационной безопасности на основе сценарного логико-вероятностного моделирования: автореф. дис. ... канд. техн. наук: 05.13.19. СПб., 2010. 16 с.

69. Котенко И.В., Дойникова Е.В. Система оценки уязвимостей CVSS и ее использование для анализа защищенности компьютерных систем // Защита информации. Инсайд. 2011. № 5. С. 54-60.

70. Котенко И.В., Дойникова Е.В., Чечулин А.А. Динамический перерасчет показателей защищенности на примере определения потенциала атаки // Труды СПИИРАН, 2013. Вып. 7 (30). С. 54-68.

71. Котенко И.В., Саенко И.Б., Дойникова Е.В. Оценка рисков в компьютерных сетях критических инфраструктур // «Инновации в науке»: материалы XVI международной заочной научно-практической конференции. Новосибирск: Изд. «СибАК», 2013. С.84-88.

72. Котенко И.В., Степашкин М.В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Проблемы управления рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). М.: УРСС, 2007. Т. 31. С. 126-207.

73. Криволапов В.Г. Комплексная методика моделирования рисков информационной безопасности открытых систем: автореф. дис. ... канд. техн. наук: 05.13.19. М., 2009. 23 с.

74. Ларина И.Е. Экономика защиты информации: учеб. пособие. М.: МГИУ, 2007. 92 с.

75. Лившиц И.И. Методы оценки защищенности систем менеджмента информационной безопасности, разработанных в соответствии с требованиями международного стандарта ИСО/МЭК 27001:2005: автореф. дис. ... канд. техн. наук: 05.13.19. СПб., 2012. 20 с.

76. Лукацкий А.В. Эффективное распределение информации об угрозах // Информационная безопасность банков. 2015. № 4 (19). С. 28-33.

77. Львова А.В. Метод анализа и управления рисками безопасности защищенной информационной системы: дис. ... канд. экон. наук: 08.00.05. М., 2009. 198 с.

78. Лысенко А.Г. Язык описания рисков для оценки безопасности информационных систем: автореф. дис. ... канд. техн. наук: 05.13.19. СПб., 2008. 18 с.

79. Марцынковский Д.А., Владимирцев А.В., Марцынковский О.А. Руководство по риск-менеджменту. СПб: Береста, 2007. 331 с.

80. Машкина И.В. Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий: автореф. дис. ... д-ра техн. наук: 05.13.19. Уфа, 2009. 32 с.

81. Мерков А.Б. Распознавание образов: Введение в методы статистического обучения. М.: УРСС, 2011. 256 с.

82. Мерков А.Б. Распознавание образов: Построение и обучение вероятностных моделей. М.: Ленанд, 2014. 240 с.

83. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры. Утв. 2007-05-18. М.: ФСТЭК России, 2007.

84. Меры защиты информации в государственных информационных системах. Утв. 2014-02-11. М.: ФСТЭК России, 2014. 176 с.

85. Метод Ньютона-Гаусса [Электронный ресурс] // Информационный ресурс MachineLearning: [сайт]. URL: http://www.machinelearning.ru (дата обращения: 09.10.2015).

86. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. 2008-02-14. М.: ФСТЭК России, 2008. 10 с.

87. Методика определения угроз безопасности информации в информационных системах (проект) [Электронный ресурс] // ФСТЭК России: [сайт]. URL: http://fstec.ru/component/attachments/download/812 (дата обращения: 12.05.2016).

88. Методика оценки риска ГРИФ [Электронный ресурс] // Digital Security: [сайт]. URL: http://dsec.ru/ipm-research-center/article/risk_assessment_method_vulture_2006_from_the_composition_of_the_digital_security_office (дата обращения: 22.05.2015).

89. Метрики безопасности [Электронный ресурс] // Информационная безопасность. Практика информационной безопасности: [сайт]. URL: http://dorlov.blogspot.ru/2009/11/blog-post.html (дата обращения: 25.05.2015).

90. Микони С.В. Системный анализ методов многокритериальной оптимизации на конечном множестве альтернатив // Труды СПИИРАН. 2015. Вып. 41. С. 180-199.

91. Мур М. Управление информационными рисками // Финансовый директор. 2003. № 9. С. 64-68.

92. Мусаев А.А., Скворцов М.С. Контроль и оптимизация надежности технических систем на стадии проектирования // Информационные системы и технологии. 2011. № 6 (68). С. 49-56.

93. Мусаев А.А., Тураносов А.В. Аналитическая система превентивного контроля безопасности нефтеперерабатывающего предприятия // Нефтепереработка и нефтехимия. Научно-технические достижения и передовой опыт. 2011. № 9. С. 35-40.

94. Нечаев Д.Ю., Черешкин Д.С. Управление комплексной безопасностью КВО на основе оценки рисков возникновения чрезвычайных ситуаций // Сборник научных трудов по итогам международной научно-практической конференции «Перспективы развития технических наук». 2015. С. 18-28.

95. Новикова Г.М. Корпоративные информационные системы: учеб. пособие. М.: РУДН, 2008. 94 с.

96. Нурдинов Р.А. Определение вероятности нарушения критических свойств информационного актива на основе CVSS метрик уязвимостей [Электронный ресурс] // Современные проблемы науки и образования. 2014. № 3. URL: http://www.science-education.ru/117-13290 (дата обращения: 30.05.2014).

97. Нурдинов Р.А. Оценка рисков безопасности информационной системы на основе модели деструктивных состояний и переходов // Материалы конференции ИБРР-2015. СПОИСУ. СПб, 2015. С. 372-373.

98. Нурдинов Р.А., Батова Т.Н. Подходы и методы обоснования целесообразности выбора средств защиты информации [Электронный ресурс] // Современные проблемы науки и образования. 2013. № 2. URL: http://www.science-education.ru/ru/article/view?id=9131 (дата обращения: 13.05.2013).

99. О коммерческой тайне: федеральный закон Российской Федерации от 29.07.2004 (ред. от 12.03.2014) № 98-ФЗ // СПС КонсультантПлюс: [сайт]. URL: http://www.consultant.ru/ document/cons_doc_LAW_48699 (дата обращения: 12.06.2016).

100. О персональных данных: федеральный закон Российской Федерации от 27.07.2006 (ред. от 21.07.2014) № 152-ФЗ // СПС КонсультантПлюс: [сайт]. URL:

http://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения: 12.06.2016).

101. Об архивном деле в Российской Федерации: федеральный закон Российской Федерации от 22 октября 2004 (ред. от 29.12.2015) № 125-ФЗ // СПС КонсультантПлюс: [сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_19559 (дата обращения: 12.06.2016).

102. Об информации, информационных технологиях и о защите информации: федеральный закон Российской Федерации от 27.07.2006 (ред. от 06.07.2016) № 149-ФЗ // СПС КонсультантПлюс: [сайт]. URL: http://www.consultant.ru/ document/cons_doc_LAW_61798 (дата обращения: 02.08.2016).

103. Об организации страхового дела в Российской Федерации: закон Российской Федерации от 27.11.1992 (в ред. от 03.07.2016) № 4015-1 // СПС КонсультантПлюс: [сайт]. URL: http://www.consultant.ru/document/cons_doc_LAW_1307 (дата обращения: 09.08.2016).

104. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 № 21. М.: ФСТЭК России, 2013. 20 с.

105. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: приказ ФСТЭК России от 14.03.2014 № 31. М.: ФСТЭК России, 2014. 42 с.

106. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11.02.2013 № 17. М.: ФСТЭК России, 2013. 37 с.

107. Одегов С.В. Методика снижения рисков информационной безопасности облачных сервисов на основе квантифицирования уровней защищенности и оптимизации состава ресурсов: автореф. дис. ... канд. техн. наук: 05.13.19. СПб., 2013. 18 с.

108. Олифер В. Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 4-е изд. СПб.: Питер, 2010. 944 с.

109. Осовской С. Нейронные сети для обработки информации: пер. с польского Рудинского И.Д. М.: Финансы и статистика, 2002. 344 с.

110. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи, ДМК-Пресс, 2004. 384 с.

111. Петров В.Н. Информационные системы. СПб.: Питер, 2003. 688 с.

112. Питерсон Дж. Теория сетей Петри и моделирование систем: пер. с англ. М: Мир, 1984. 264 с.

113. Подвесовский А.Г. Метод анализа иерархий // Брянск: БГТУ, 2013. 30 с.

114. Прокофьева М.А. Корпоративные информационные системы. Пятигорск: КМВИС ФГБОУ ВПО «ЮРГУЭС», 2013. 70 с.

115. Р Газпром 4.2-3-003-2015. Система обеспечения информационной безопасности ОАО «Газпром». Методика оценки рисков. М.: ОАО «Газпром», 2015. 178 с.

116. Родина Ю.В. Оценка риска нарушения информационной безопасности по модели нечёткой логики с корректировкой параметров её терм-множеств [Электронный ресурс] // Управление экономическими системами: электронный научный журнал. 2011 № 6. URL: http://www.uecs.ru (дата обращения: 24.05.2012).

117. РС БР ИББС-2.2-2009. Методика оценки рисков нарушения информационной безопасности. М., 2009. 23 с.

118. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация

автоматизированных систем и требования по защите информации. М.: Гостехкомиссия России, 1992. 21 с.

119. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. М.: Гостехкомиссия России, 1992. 16 с.

120. Рябинин И.А. Надежность и безопасность структурно-сложных систем. Спб., 2012. 276 с.

121. Саати Т.Л. Принятие решений: Метод анализа иерархий: пер. с англ. Вачнадзе Р.Г. М.: Радио и связь, 1993. 314 с.

122. Самылин А.И. Управление результатами деятельности // Проблемы современной экономики. 2009. № 3. С. 65-69.

123. Сизова Т.М. Статитстика: учеб. пособие. СПб.: СПб НИУ ИТМО, 2013. 176 с.

124. Сидоров А.О. Модель и метод структурированной оценки риска при анализе информационной безопасности: автореф. дис. ... канд. техн. наук: 05.13.19. СПб., 2008. 24 с.

125. СП 20.13330.2011. Нагрузки и воздействия. Введ. 2016-04-01. М.: Стандартинформ, 2011. 12 с.

126. Статистика уязвимостей веб-приложений (2014 г.). М.: Positive Technologies, 2015. 24 с.

127. Степанова Е.С. Модели и методы оценки рисков нарушения информационной безопасности с использованием нечетких когнитивных карт: автореф. дис. ... канд. техн. наук: 05.13.19. Уфа, 2013. 16 с.

128. СТО БР ИББС-1.0-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. М., 2009. 44 с.

129. СТО Газпром 4.2-3-003-2009. Система обеспечения информационной безопасности ОАО «Газпром». Анализ и оценка рисков. М.: ОАО «Газпром», 2009. 22 с.

130. Тихонов Э.Е. Прогнозирование в условиях рынка: учеб. пособие. Невинномысск, 2006. 221 с.

131. Трифонов А.Г. Постановка задачи оптимизации и численные методы ее решения [Электронный ресурс] // Информационный ресурс MATLAB.Exponenta: [сайт]. URL: http://matlab.exponenta.ru/optimiz/book_2/index.php (дата обращения: 25.02.2016).

132. Фаткиева Р.Р. Методы и алгоритмы прогнозирования поведения и оценки свойств информационной системы: автореф. дис. ... канд. техн. наук: 05.13.01. СПб., 2004. 20 с.

133. Хаббард Д.У. Как измерить все, что угодно. Оценка стоимости нематериального в бизнесе: пер. с англ. Пестеревой Е.М. 3-е изд. М.: ЗАО «Олимп-Бизнес», 2009. 320 с.

134. Хайкин С. Нейронные сети: полный курс: пер. с англ. 2-е изд. М.: Вильямс, 2006. 1104 с.

135. Хованов Н.В. Математические модели риска и неопределенности. Санкт-Петербург, 1998. 204 с.

136. Черешкин Д. С., Гадасин В. А., Елизаров О. И., Кононов А. А., Тищенко Д. В., Цыгичко В. Н. Оценка эффективности систем защиты информационных ресурсов. М.: Институт системного анализа РАН, 1998. 48 с.

137. Чусавитин М.О. Использование метода анализа иерархий при оценке рисков информационной безопасности образовательного учреждения // Фундаментальные исследования. 2013. № 10 (ч. 9). С. 2080-2084.

138. Шишкин В.М. Оценка рисков на сложных структурах факторов при дефиците информации // Труды международного симпозиума Надежность и качество. 2011. Т. 1. С. 273-277.

139. Шишкин В.М. Структурная информация и оценка факторов в риск-анализе // Сборник научных трудов X Международной школы-симпозиума АМУР-2016. 2016. С. 420-425.

140. Ярочкин В.И. Информационная безопасность: учебник. М.: Фонд «Мир», 2003. 639 с.

141. BS 7799-2:2002. Information security management. Specification with guidance for use. BSI, 2002. 38 p.

142. BSI Standard 100-3. Risikoanalyse auf der Basis von IT-Grundschutz. BSI, 2008. 23 p.

143. COBIT 5 for Risk. Rolling Meadows: ISACA, 2013. 245 p.

144. Common Configuration Enumeration [Электронный ресурс] // The Mitre Corporation: [сайт]. URL: https://cce.mitre.org (дата обращения: 11.05.2015).

145. Common Vulnerabilities and Exposures [Электронный ресурс] // The Mitre Corporation: [сайт]. URL: https://cve.mitre.org (дата обращения: 11.05.2015).

146. Expression des Besoins et Identification des Objectifs de Sécurité. Méthode de Gestion des Risques. Paris, 2010. 95 p.

147. Cyber attacks statistics [Электронный ресурс] // Hackmageddon: [сайт]. URL: http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics (дата обращения: 28.03.2016).

148. Houmb S.H., Franqueira V.N.L. Estimating ToE Risk Level Using CVSS // International Conference on Availability, Reliability and Security. 2009. P.718-725.

149. ISO/IEC 2382-1:1993. Information technology. Vocabulary: пер. с англ. Шуткина Л.В. ISO, 2005. 44 p.

150. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. ISO, 2013. 30 p.

151. ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls. ISO, 2013. 94 p.

152. ISO/IEC 27005:2011. Information technology. Security techniques. Information security risk management. ISO, 2011. 76 p.

153. ISO/IEC/IEEE 29148:2011. Systems and software engineering. Life cycle processes. Requirements engineering. ISO, 2011. 94 p.

154. ISO/IEC 31000:2009. Risk management. Principles and guidelines. ISO, 2009. 34 p.

155. ISO/IEC 31010:2009. Risk management. Risk assessment techniques. ISO, 2009. 34 p.

156. ITSC-33. Information Technology Security Guidance IT Security Risk Management: A Lifecycle Approach. Overview. CSE, Canada, 2012. 16 p.

157. Jenkins B.D. Security risk analysis and management. Countermeasures Inc., 1998. 16 p.

158. Joh H., Malaiya Y.K.A Framework for Software Security Risk Evaluation using the Vulnerability Lifecycle and CVSS Metrics // Proc. International Workshop on Risk and Trust in Extended Enterprises. 2010. P. 430-434.

159. Jones A., Ashenden D. Risk management for computer security. Elsevier Butterworth-Heinemann, 2005. 297 p.

160. LeCun Y., Bottou L., Orr G.B., Muller K.-R. Efficient backprop. Neural Networks: Tricks of the Trade. 1998. P: 9-50.

161. Mell P., Scarfone K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. 2007. 23 p.

162. Metodología de Análisis y Gestiónde Riesgos de los Sistemas de Información. Madrid, 2012. 127 p.

163. Metsis V., Androutsopoulos I., and Paliouras G. Spam filtering with naive Bayes-which naive bayes? // Proceedings of the 3rd Conference on Email and Anti-Spam. Mountain View, CA, 2006. 9 p.

164. Microsoft Solutions for Security and Compliance. The Security Risk Management Guide. San Francisco: Microsoft Corporation, 2006. 129 p.

165. National vulnerability database [Электронный ресурс] // National Institute of Standards and Technology: [сайт]. URL: https://nvd.nist.gov (дата обращения: 11.05.2015).

166. NIST SP 800-30. Risk Management Guide for Information Technology Systems. NIST, 2002. 56 p.

167. NIST 800-37. Guide for Applying the Risk Management Framework to Federal Information Systems. NIST, 2010. 93 p.

168. NIST SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. NIST, 2011. 88 p.

169. Nurdinov R.A., Kanev A.N. The Quantitative Information System Security Vulnerability Estimation Model Based on Metrics // First Information Security and Protection of Information Technologies (ISPIT) conference, St. Peterburg, November 5-6, 2015. P. 37-41.

170. OCTAVE Method [Электронный ресурс] // Software Engineering Ibstitute: [сайт]. URL: http://www.cert.org/resilience/products-services/octave (дата обращения: 28.05.2015).

171. Ou X., Singhal A. Quantitative Security Risk Assessment of Enterprise Networks. NY: Springer, 2011. 27 p.

172. OWASP WASC Web Hacking Incidents Database [Электронный ресурс] // OWASP Community [сайт]. URL: https://www.owasp.org/index.php (дата обращения: 28.03.2016).

173. PCI DSS Risk Assessment Guidelines. PCI security standard council, 2012. 24 p.

174. Peltier, T.L. Information security risk analysis: 2 ed. Auerbach Publications, 2005. 361 p.

175. Phelps B. Smart Business Metrics: Measure What Really Counts & Manage What Makes The Difference. 2004. 127 p.

176. Poolsappasit N., Dewri R., Ray I. Dynamic Security Risk Management Using Bayesian Attack Graphs // IEEE Trans. Dependable and Secure Computing. 2012. Vol. 9, no. 1. P. 61-74.

177. RSA Archer GRC. Platform 6.0. Administration Guide. USA, 2015. 1109 p.

178. Sejnowski T.J. Strong covariance with non lineary interacting neurons // Journal of Mathematical Biology. 1977. vol. 4. p. 303-321.

179. The Repository of Industrial Security Incidents [Электронный ресурс] // RISI: [сайт].URL: http://www.risidata.com (дата обращения: 28.02.2016).

180. The Risk IT Framework based on COBIT. Rolling Meadows: ISACA, 2009. 40 p.

Приложение А

(обязательное)

Примеры сценариев реализации угроз

Таблица А.1 – Примеры сценариев реализации угроз, приведенных в ГОСТ Р ИСО/МЭК 27005-2010

Наименование угрозы	Результат	Причина	Условие
1. Пожар	$HW^{[U]}$	– V^{NS}; – V^{AS}	–
2. Ущерб, причиненный водой	$HW^{[U]}$	– V^{NS}; – V^{AS}	–
3. Загрязнение	$HW^{[U]}$	– V^{NS}; – V^{AS}	–
4. Крупная авария	$HW^{[U]}$	– V^{NS}; – V^{AS}	–
5. Разрушение оборудования или носителей	$HW^{[U]}$	– V^{NS}; – V^{AS}	–
6. Пыль, коррозия, замерзание	$HW^{[U]}$	– V^{NS}; – V^{AS}	–
7. Климатическое явление	$HW^{[U]}$	V^{NS}	–
8. Сейсмическое явление	$HW^{[U]}$	V^{NS}	–
9. Вулканическое явление	$HW^{[U]}$	V^{NS}	–
10. Метеорологическое явление	$HW^{[U]}$	V^{NS}	–
11. Наводнение	$HW^{[U]}$	V^{NS}	–
12. Авария системы кондиционирования воздуха или водоснабжения	$HW^{[U]}$	V^{NS}	–
13. Нарушение энергоснабжения	$HW^{[U]}$	V^{NS}	–
14. Отказ телекоммуникационного оборудования	$CL^{[U]}$	V^{NS}	–
15. Электромагнитное излучение	– $HW^{[U]}$; – $CL^{[U]}$	V^{NS}	–
16. Тепловое излучение	– $HW^{[U]}$; – $CL^{[U]}$	V^{NS}	–
17. Электромагнитные импульсы	– $HW^{[U]}$; – $CL^{[U]}$	V^{NS}	–
18. Перехват компрометирующих сигналов	$IA^{[C]}$	V^{AS}	$CL^{[I]}$
19. Дистанционный шпионаж	$IA^{[C]}$	V^{AS}	– $CL^{[I]}$; – $SW^{[I]}$
20. Прослушивание	$IA^{[C]}$	V^{AS}	$CL^{[I]}$
21. Кража носителей или документов	– $IA^{[C]}$; – $IA^{[U]}$	V^{AS}	$HW^{[I]}$
22. Кража оборудования	– $HW^{[I]}$; – $HW^{[U]}$	V^{AS}	–
23. Поиск повторно используемых или забракованных носителей	$IA^{[C]}$	V^{AS}	$HW^{[I]}$

Наименование угрозы	Результат	Причина	Условие
24. Раскрытие	$IA^{[C]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
25. Данные из ненадежных источников	$IA^{[M]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
26. Преступное использование аппаратных средств	$HW^{[I]}$	V^{AS}	–
27. Преступное использование программного обеспечения	$SW^{[I]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$
28. Определение местонахождения	$IA^{[C]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
29. Отказ оборудования	$HW^{[U]}$	V^{NS}	–
30. Неисправная работа оборудования	$HW^{[U]}$	V^{NS}	–
31. Насыщение информационной системы	– $CL^{[U]}$; – $SW^{[U]}$	– V^{NS}; – V^{AS}	–
32. Нарушение функционирования программного обеспечения	$SW^{[U]}$	– V^{NS}; – V^{AS}	–
33. Нарушение сопровождения информационной системы	– $HW^{[U]}$; – $CL^{[U]}$; – $SW^{[U]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
34. Несанкционированное использование оборудования	$HW^{[I]}$	V^{AS}	–
35. Мошенническое копирование программного обеспечения	$SW^{[I]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$
36. Использование контрафактного или скопированного программного обеспечения	$SW^{[I]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$
37. Искажение данных	$IA^{[M]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
38. Незаконная обработка данных	– $IA^{[C]}$; – $IA^{[M]}$	V^{AS}	$SW^{[I]}$
39. Ошибка при использовании	– $IA^{[C]}$; – $IA^{[M]}$; – $IA^{[U]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
40. Злоупотребление правами	– $IA^{[C]}$; – $IA^{[M]}$; – $IA^{[U]}$	V^{AS}	$SW^{[I]}$
41. Фальсификация прав	$SW^{[I]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$;
42. Отказ в осуществлении действий	$IA^{[M]}$	V^{AS}	– $HW^{[I]}$; – $CL^{[I]}$; – $SW^{[I]}$
43. Нарушение работоспособности персонала	–	– V^{NS}; – V^{AS}	–

Приложение Б

(обязательное)

Результаты начальной оценки весовых коэффициентов методом анализа иерархий

Таблица Б.1 – Весовые коэффициенты метрик нарушителей

Наименование метрики (признака)	**Весовой коэффициент метрики**	**Значение признака**	**Весовой коэффициент значения признака**
Мотивация	0,18±0,06	Отсутствие мотива	0,08±0,01
		Халатность	0,14±0,03
		Любопытство	0,19±0,03
		Хулиганство	0,25±0,03
		Самоутверждение	0,45±0,06
		Принуждение	0,20±0,04
		Идеологические убеждения	0,61±0,08
		Месть	0,57±0,05
		Политические цели	0,92±0,06
		Корыстные интересы	1,00±0,01
Оснащенность	0,17±0,04	Отсутствует	0,09±0,02
		Стандартное оборудование	0,18±0,01
		Специализированное оборудование	0,44±0,04
		Заказное оборудование	1,00±0,00
Техническая компетентность	0,24±0,03	Непрофессионал	0,11±0,02
		Специалист	0,37±0,03
		Профессионал	1,00±0,00
Знание информации о КИС и СЗИ	0,14±0,04	Отсутствие знаний	0,13±0,03
		Ограниченные знания	0,40±0,04
		Чувствительная информация	1,00±0,00
Права доступа	0,17±0,05	Отсутствуют	0,09±0,02
		Пользовательские	0,19±0,04
		Привилегированные	0,42±0,04
		Административные	1,00±0,00
Время доступа	0,10±0,03	Менее 0,5 часа	0,11±0,05
		Менее 1 дня	0,22±0,05
		Менее 1 месяца	0,52±0,05
		Более 1 месяца	1,00±0,00

Таблица Б.2 – Весовые коэффициенты категорий защитных мер

Деструктивное состояние	**Тип защитных мер**	**Категория защитных мер**	**Весовой коэффициент**
Нарушение доступности ТС	Превентивные	ОДТ	0,51±0,07
		ЗТС	0,49±0,07
	Корректирующие	ОДТ	1,00±0,00

Деструктивное состояние	Тип защитных мер	Категория защитных мер	Весовой коэффициент
НСД к ТС	Превентивные	ЗНИ	0,40±0,12
		ЗТС	0,60±0,12
	Корректирующие	–	–
Нарушение доступности ЛС	Превентивные	ЗТС	1,00±0,00
	Корректирующие	ОДТ	1,00±0,00
НСД к ЛС	Превентивные	ИАФ	0,17±0,05
		УПД	0,23±0,04
		ЗТС	0,27±0,05
		ЗИС	0,33±0,06
	Корректирующие	–	–
Нарушение доступности ПО	Превентивные	УПД	0,30±0,06
		АВЗ	0,14±0,03
		СОВ	0,07±0,02
		АНЗ	0,12±0,05
		ЗИС	0,23±0,05
		УКФ	0,15±0,03
	Корректирующие	ОЦЛ	0,39±0,08
		ОДТ	0,61±0,08
НСД к ПО	Превентивные	ИАФ	0,21±0,04
		УПД	0,10±0,03
		ОПС	0,09±0,02
		РСБ	0,05±0,03
		АВЗ	0,11±0,03
		СОВ	0,07±0,02
		АНЗ	0,16±0,03
		ЗИС	0,08±0,02
		УКФ	0,13±0,03
	Корректирующие	ОЦЛ	1,00±0,00
Нарушение конфиденциальности ИС	Превентивные	УПД	0,17±0,04
		ЗНИ	0,14±0,01
		РСБ	0,06±0,03
		ОЦЛ	0,08±0,02
		ЗТС	0,10±0,02
		ЗИС	0,09±0,03
		ИНЦ	0,10±0,01
		КЗИ	0,26±0,04
	Корректирующие	–	–
Нарушение целостности ИА	Превентивные	УПД	0,24±0,05
		РСБ	0,07±0,01
		ОЦЛ	0,38±0,04
		ЗИС	0,18±0,03
		ИНЦ	0,13±0,01
	Корректирующие	ОДТ	1,00±0,00
Нарушение доступности ИА	Превентивные	УПД	0,54±0,07
		РСБ	0,12±0,02
		ОЦЛ	0,24±0,05
		ИНЦ	0,10±0,01
	Корректирующие	ОДТ	1,00±0,00

Таблица Б.3 – Весовые коэффициенты метрик защитных мер и их соответствие деструктивным состояниям

Условное обозначение	Наименование метрики (защитной меры)	Весовой коэффициент	Связанные деструктивные состояния[1)]								
			HW		*CL*		*SW*		*IA*		
			[*I*]	[*U*]	[*I*]	[*U*]	[*I*]	[*U*]	[*C*]	[*M*]	[*U*]
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)											
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	0,34±0,05	–	–	–	–	П	–	–	–	–
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных	0,11±0,02	–	–	П	–	–	–	–	–	–
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	0,10±0,03	–	–	П	–	П	–	–	–	–
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	0,10±0,03	–	–	–	–	П	–	–	–	–
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	0,09±0,04	–	–	–	–	П	–	–	–	–
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	0,26±0,06	–	–	–	–	П	–	–	–	–
Управление доступом субъектов доступа к объектам доступа (УПД)											
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	0,10±0,04	–	–	–	–	П	П	–	–	–
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	0,10±0,04	–	–	–	–	–	–	П	П	П
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами ИС, а также между ИС	0,10±0,04	–	–	П	–	–	–	–	–	–
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС	0,05±0,03	–	–	–	–	П	П	–	–	–
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС	0,09±0,05	–	–	–	–	П	П	–	–	–
УПД.6	Ограничение неуспешных попыток входа в ИС (доступа к ИС)	0,08±0,04	–	–	–	–	П	–	–	–	–

Условное обозначение	Наименование метрики (защитной меры)	Весовой коэффициент	Связанные деструктивные состояния[1)]								
			HW		*CL*		*SW*		*IA*		
			[*I*]	[*U*]	[*I*]	[*U*]	[*I*]	[*U*]	[*C*]	[*M*]	[*U*]
УПД.7	Предупреждение пользователя при его входе в ИС о том, что в ИС реализованы меры по обеспечению безопасности информации, и о необходимости соблюдения установленных оператором правил обработки информации	0,02±0,02	–	–	–	–	П	П	–	–	–
УПД.8	Оповещение пользователя после успешного входа в ИС о его предыдущем входе в ИС	0,02±0,02	–	–	–	–	П	–	–	–	–
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя ИС	0,02±0,02	–	–	–	–	П	–	–	–	–
УПД.10	Блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу	0,04±0,02	–	–	–	–	П	–	–	–	–
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	0,05±0,03	–	–	–	–	П	П	–	–	–
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки	0,02±0,02	–	–	–	–	–	–	П	П	П
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	0,07±0,05	–	–	П	–	–	–	–	–	–
УПД.14	Регламентация и контроль использования в ИС технологий беспроводного доступа	0,08±0,05	–	–	П	–	–	–	–	–	–
УПД.15	Регламентация и контроль использования в ИС мобильных ТС	0,05±0,02	–	–	П		П		–	–	–
УПД.16	Управление взаимодействием с ИС сторонних организаций (внешние информационные системы)	0,05±0,02	–	–	–	–	П	П	–	–	–
УПД.17	Обеспечение доверенной загрузки СВТ	0,06±0,06	–	–	–	–	П	–	–	–	–
Ограничение программной среды (ОПС)											
ОПС.1	Управление запуском (обращениями) компонентов ПО, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов ПО	0,27±0,06	–	–	–	–	П	–	–	–	–
ОПС.2	Управление установкой (инсталляцией) компонентов ПО, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов ПО	0,30±0,05	–	–	–	–	П	–	–	–	–

Условное обозначение	Наименование метрики (защитной меры)	Весовой коэффициент	Связанные деструктивные состояния[1)]								
			HW		*CL*		*SW*		*IA*		
			[*I*]	[*U*]	[*I*]	[*U*]	[*I*]	[*U*]	[*C*]	[*M*]	[*U*]
ОПС.3	Установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов	0,35±0,05	–	–	–	–	П	–	–	–	–
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов	0,08±0,02	–	–	–	–	П	–	–	–	–
Защита машинных носителей информации (ЗНИ)											
ЗНИ.1	Учет машинных носителей информации	0,11±0,03	П	–	–	–	–	–	–	–	–
ЗНИ.2	Управление доступом к машинным носителям информации	0,20±0,02	П	–	–	–	–	–	–	–	–
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны	0,13±0,04	П	–	–	–	–	–	–	–	–
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием информации, хранящихся на машинных носителях, и (или) использования носителей информации в иных ИС	0,09±0,02	–	–	–	–	–	–	П	–	–
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	0,08±0,02	П	–	–	–	–	–		–	–
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации	0,17±0,04	–	–	–	–	–	–	П	–	–
ЗНИ.7	Контроль подключения машинных носителей информации	0,16±0,03	–	–	–	–	–	–	П	–	–
ЗНИ.8	Уничтожение (стирание) или обезличивание информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания	0,06±0,02	–	–	–	–	–	–	П	–	–
Регистрация событий безопасности (РСБ)											
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	0,15±0,03	–	–	П	–	П	–	П	П	П
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	0,15±0,03	–	–	П	–	П	–	П	П	П
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	0,24±0,03	–	–	П	–	П	–	П	П	П
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема памяти	0,19±0,04	–	–	П	–	П	–	П	П	П

Условное обозначение	Наименование метрики (защитной меры)	Весовой коэффициент	Связанные деструктивные состояния[1)]								
			HW		*CL*		*SW*		*IA*		
			[*I*]	[*U*]	[*I*]	[*U*]	[*I*]	[*U*]	[*C*]	[*M*]	[*U*]
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	0,15±0,03	–	–	П	–	П	–	П	П	П
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в ИС	0,05±0,01	–	–	П	–	П	–	П	П	П
РСБ.7	Защита информации о событиях безопасности	0,07±0,02	–	–	П	–	П	–	П	П	П
Антивирусная защита (АВЗ)											
АВЗ.1	Реализация антивирусной защиты	0,73±0,04	–	–	–	–	П	П	–	–	–
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	0,26±0,03	–	–	–	–	П	П	–	–	–
Обнаружение вторжений (СОВ)											
СОВ.1	Обнаружение вторжений	0,68±0,04	–	–	П	–	П	П	–	–	–
СОВ.2	Обновление базы решающих правил	0,32±0,06	–	–	П	–	П	П	–	–	–
Контроль (анализ) защищенности информации (АНЗ)											
АНЗ.1	Выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей	0,27±0,06	–	–	–	–	П	П	–	–	–
АНЗ.2	Контроль установки обновлений ПО, включая обновление ПО СрЗИ	0,17±0,06	–	–	–	–	П	П	–	–	–
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования ПО и СрЗИ	0,15±0,03	–	–	–	–	П	П	–	–	–
АНЗ.4	Контроль состава ТС, ПО и СрЗИ	0,11±0,03	–	–	–	–	П	П	–	–	–
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИС	0,30±0,05	–	–	–	–	П	П	–	–	–
Обеспечение целостности ИС и информации (ОЦЛ)											
ОЦЛ.1	Контроль целостности ПО, включая ПО СрЗИ	0,12±0,02	–	–	–	–	К	К	–	–	–
ОЦЛ.2	Контроль целостности информации, содержащихся в базах данных ИС	0,19±0,06	–	–	–	–	–	–	–	П	–
ОЦЛ.3	Обеспечение возможности восстановления ПО, включая ПО СрЗИ, при возникновении нештатных ситуаций	0,16±0,05	–	–	–	–	К	К	–	–	–
ОЦЛ.4	Обнаружение и реагирование на поступление в ИС незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию ИС (защита от спама)	0,12±0,03	–	–	–	–	–	–	–	–	П

Условное обозначение	Наименование метрики (защитной меры)	Весовой коэффициент	Связанные деструктивные состояния[1)]								
			HW		*CL*		*SW*		*IA*		
			[*I*]	[*U*]	[*I*]	[*U*]	[*I*]	[*U*]	[*C*]	[*M*]	[*U*]
ОЦЛ.5	Контроль содержания информации, передаваемой из ИС (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из ИС	0,12±0,04	–	–	–	–	–	–	П	–	–
ОЦЛ.6	Ограничение прав пользователей по вводу информации в ИС	0,10±0,06	–	–	–	–	–	–	–	П	–
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в ИС	0,08±0,03	–	–	–	–	–	–	–	П	П
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях	0,11±0,03	–	–	–	–	–	–	П	П	П
Обеспечение доступности информации (ОДТ)											
ОДТ.1	Использование отказоустойчивых ТС	0,19±0,03	–	К	–		–		–	–	–
ОДТ.2	Резервирование ТС, ПО, каналов передачи информации, средств обеспечения функционирования ИС	0,20±0,04	–	К	–	К	–	К	–	–	–
ОДТ.3	Контроль безотказного функционирования ТС, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	0,17±0,02	–	К	–	К	–	–	–	–	–
ОДТ.4	Периодическое резервное копирование информации на резервные машинные носители информации	0,22±0,05	–	–	–	–	–	–	–	К	К
ОДТ.5	Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала	0,22±0,05	–	–	–	–	–	–	–	К	К
Защита технических средств (ЗТС)											
ЗТС.1	Защита информации, обрабатываемой ТС, от ее утечки по техническим каналам	0,10±0,03	–	–	–	–	–	–	П	–	–
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные ТС, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	0,26±0,06	П	П	П	П	–	–	–	–	–
ЗТС.3	Контроль и управление физическим доступом к ТС, СрЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие НСД	0,31±0,05	П	П	П	П	–	–	–	–	–

Условное обозначение	Наименование метрики (защитной меры)	Весовой коэффициент	Связанные деструктивные состояния[1)]								
			HW		*CL*		*SW*		*IA*		
			[*I*]	[*U*]	[*I*]	[*U*]	[*I*]	[*U*]	[*C*]	[*M*]	[*U*]
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	0,17±0,05	–	–	–	–	–	–	П	–	–
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)	0,16±0,02	–	П	–	П	–	–	–	–	–
Защита ИС, ее средств, систем связи и передачи данных (ЗИС)											
ЗИС.1	Разделение в ИС функций по управлению (администрированию) ИС, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций ИС	0,06±0,03	–	–	–	–	П	–	–	–	–
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом	0,04±0,01	–	–	–	–		П	–	–	–
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	0,11±0,04	–	–	П	–	–	–	П	П	–
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности СрЗИ)	0,04±0,01	–	–	П		–	–			–
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств	0,06±0,03	–	–	–	–	–	–	П		–
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с информацией, при обмене ими с иными ИС	0,02±0,02	–	–	–	–	–	–	П	П	
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода	0,05±0,02	–	–	–	–	П	–	–	–	–

Условное обозначение	Наименование метрики (защитной меры)	Весовой коэффициент	Связанные деструктивные состояния[1)]								
			HW		*CL*		*SW*		*IA*		
			[*I*]	[*U*]	[*I*]	[*U*]	[*I*]	[*U*]	[*C*]	[*M*]	[*U*]
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи	0,06±0,05	–	–	–	–	–	–	П	–	–
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации	0,06±0,05	–	–	–	–	–	–	П	–	–
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам	0,04±0,03	–	–	–	–	–	–	–	П	–
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	0,04±0,03	–	–	П	–	–	–	–	–	–
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю	0,03±0,02	–	–	–	–	–	–	–	П	–
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя	0,03±0,02	–	–	–	–	–	–	–	П	–
ЗИС.14	Использование устройств терминального доступа для обработки информации	0,04±0,02	–	–	–	–	–	–	–	–	–
ЗИС.15	Защита архивных файлов, параметров настройки СрЗИ и ПО и иных данных, не подлежащих изменению в процессе обработки информации	0,05±0,03	–	–	–	–	–	–	П	П	–
ЗИС.16	Выявление, анализ и блокирование в ИС скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов	0,06±0,03	–	–	П	–	–	–	–	–	–
ЗИС.17	Разбиение ИС на сегменты (сегментирование ИС) и обеспечение защиты периметров сегментов ИС	0,07±0,04	–	–	П	–	–	–	–	–	–
ЗИС.18	Обеспечение загрузки и исполнения ПО с машинных носителей информации, доступных только для чтения, и контроль целостности данного ПО	0,03±0,02	–	–	–	–	П		–	–	–

Условное обозначение	Наименование метрики (защитной меры)	Весовой коэффициент	Связанные деструктивные состояния[1)]								
			HW		*CL*		*SW*		*IA*		
			[*I*]	[*U*]	[*I*]	[*U*]	[*I*]	[*U*]	[*C*]	[*M*]	[*U*]
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти	0,03±0,02	–	–	–	–	П	П	–	–	–
ЗИС.20	Защита беспроводных соединений, применяемых в ИС	0,08±0,03	–	–	П	–	–	–	–	–	–
Выявление инцидентов и реагирование на них (ИНЦ)											
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них	0,12±0,01	–	–	–	–	–	–	П	П	П
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов	0,24±0,02	–	–	–	–	–	–	П	П	П
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИС пользователями и администраторами	0,12±0,01	–	–	–	–	–	–	П	П	П
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий	0,17±0,04	–	–	–	–	–	–	П	П	П
ИНЦ.5	Принятие мер по устранению последствий инцидентов	0,21±0,03	–	–	–	–	–	–	П	П	П
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов	0,14±0,03	–	–	–	–	–	–	П	П	П
Управление конфигурацией информационной системы и системы защиты информации (УКФ)											
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию ИС и СЗИ	0,09±0,02	–	–	–	–	П	П	–	–	–
УКФ.2	Управление изменениями конфигурации ИС и СЗИ	0,41±0,05	–	–	–	–	П	П	–	–	–
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации ИС и СЗИ на обеспечение защиты информации и согласование изменений в конфигурации ИС с должностным лицом (работником), ответственным за обеспечение безопасности информации	0,38±0,06	–	–	–	–	П	П	–	–	–
УКФ.4	Документирование информации (данных) об изменениях в конфигурации ИС и СЗИ	0,12±0,04	–	–	–	–	П	П	–	–	–
Криптографическая защита информации (КЗИ)											
КЗИ.1	Шифрование конфиденциальной информации, на носителях данных и в каналах связи	0,75±0,05	–	–	–	–	–	–	П	–	–
КЗИ.2	Использование разных криптографических ключей для шифрования информации, принадлежащей различным субъектам доступа	0,25±0,02	–	–	–	–	–	–	П	–	–

[1)] «П» – превентивная мера; «К» – корректирующая мера

Приложение В

(обязательное)

Акты о внедрении результатов

ПАО «ГАЗПРОМ»

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ГАЗПРОМ ТРАНСГАЗ САНКТ-ПЕТЕРБУРГ»

(ООО «Газпром трансгаз Санкт-Петербург»)

УТВЕРЖДАЮ
Заместитель генерального директора
по корпоративной защите
и управлению персоналом
_____ А.В. Круглов
«__» _____ 2016 г.

АКТ
о внедрении результатов диссертационного исследования Нурдинова Руслана Артуровича на тему «Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик»

Настоящим актом удостоверяется, что в компании ООО «Газпром трансгаз Санкт-Петербург» изучены теоретические и практические результаты диссертационного исследования Нурдинова Р.А., а именно:

1. Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик.
2. Метод аппроксимации функции вероятности реализации угроз нарушителем на основе данных об инцидентах информационной безопасности.

По мнению руководства компании и специалистов управления корпоративной защиты данные результаты обладают актуальностью и представляют практический интерес.

Результаты диссертационного исследования Нурдинова Р.А. использованы при разработке программного модуля управления рисками информационной безопасности в составе системы автоматизации процессов управления информационной безопасностью ООО «Газпром трансгаз Санкт-Петербург», находящейся в опытной эксплуатации.

Использование результатов диссертационного исследования Нурдинова Р.А. позволило повысить эффективность и результативность процесса управления рисками информационной безопасности в ООО «Газпром трансгаз Санкт-Петербург».

Заместитель начальника
управления корпоративной защиты: _____ Д.М. Шабанов

Начальник отдела информационной
безопасности: _____ К.И. Люкшин

Рисунок В.1 – Акт о внедрении в производственный процесс ООО «Газпром трансгаз Санкт-Петербург»

Общество с ограниченной ответственностью
«ГАЗИНФОРМСЕРВИС»

«Утверждаю»
Заместитель генерального директора –
технический директор
ООО «Газинформсервис»
_____ Н.В. Нашивочников
«5» мая 2016 г.

АКТ
О практическом применении полученных результатов диссертационного исследования Нурдинова Руслана Артуровича на тему
«Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик»

В компании ООО «Газинформсервис» подробно изучены результаты диссертационного исследования Нурдинова Р.А. По мнению руководства компании предложенные в диссертационной работе Нурдинова Р.А. модели, методы и методики обладают теоретической и практической значимостью.

Настоящим актом подтверждается, что методика формирования рационального комплекса защитных мер, предложенная в диссертационной работе Нурдинова Р.А., используется в компании ООО «Газинформсервис» при проектировании систем защиты для автоматизированных и информационных систем. Стоит отметить, что использование данной методики позволило повысить эффективность проектируемых и внедряемых компанией ООО «Газинформсервис» комплексных решений по обеспечению информационной безопасности.

Компания ООО «Газинформсервис» выражает глубокую признательность Нурдинову Р.А. за практическое применение полученных в его диссертационной работе результатов в проектной деятельности ООО «Газинформсервис» и надеется на активное продолжение Нурдиновым Р.А. исследований в данной области и дальнейшее сотрудничество.

Советник технического директора, к.т.н. И.А. Жуклинец

Ведущий инженер, к.т.н. И.М. Гусев

Рисунок В.2 – Акт о внедрении в производственный процесс ООО «Газинформсервис»

Частное образовательное учреждение дополнительного профессионального образования

«ЦЕНТР ПРЕДПРИНИМАТЕЛЬСКИХ РИСКОВ»

197022, Санкт-Петербург, улица Профессора Попова, 27

тел./факс (812) 234-95-48, 234-95-65, 234-95-66, 346-48-93

Лицензия на право осуществления образовательной деятельности № 1577 от 20.11.2015 г. выдана Комитетом по образованию Правительства Санкт-Петербурга

Исх. № 100-04/16

«21» апреля 2016 года

В Диссертационный совет

АКТ

О внедрении полученных результатов диссертационного исследования Нурдинова Р.А. на тему «Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик»

Настоящим Актом удостоверяется, что результаты диссертационной работы Нурдинова Р.А. внедрены в учебный процесс в ЧОУ ДПО «Центр предпринимательских рисков». В частности, при подготовке материалов курса «Управление информационной безопасностью» были использованы следующие результаты диссертационной работы Нурдинова Р.А.:

1. Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик.
2. Методика формирования рационального комплекса защитных мер для корпоративной информационной системы на основе формализованной модели количественной оценки рисков.
3. Метод аппроксимации функции вероятности реализации угроз нарушителем на основе данных об инцидентах информационной безопасности.

Также в состав материалов курса «Управление информационной безопасностью» вошли результаты сравнительного анализа подходов к оценке рисков информационной безопасности, представленные в первой главе диссертационного исследования Нурдинова Р.А.

Использование результатов диссертационного исследования Нурдинова Р.А. позволило повысить качество и глубину проработки материалов курса «Управление информационной безопасностью» по вопросам управления рисками информационной безопасности, что нашло положительный отклик у слушателей курса.

Благодарим Нурдинова Р.А. за использование результатов его диссертационного исследования в учебном процессе ЧОУ ДПО «Центр предпринимательских рисков» и выражаем заинтересованность в активном продолжении Нурдиновым Р.А. исследований в данной области и дальнейшее сотрудничество.

Директор ЧОУ ДПО «ЦПР» Казанцев В.Г.

Рисунок В.3 – Акт о внедрении в учебный процесс ЧОУ ДПО «Центр предпринимательских рисков»

УТВЕРЖДАЮ
Проректор по учебной деятельности
Санкт-Петербургского Национального
исследовательского университета
информационных технологий,
механики и оптики

_____ Н.В. Михайлов

М.П.

«6» июня 2016 г.

АКТ

о внедрении результатов диссертационной работы Нурдинова Р.А. на тему «Модель количественной оценки рисков безопасности корпоративной информационной системы на основе метрик» по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»

Комиссия в составе:

Председатель комиссии: Птицын Алексей Владимирович, зам. зав. каф. БИТ, к.т.н., доцент,

Комаров Игорь Иванович, доцент каф. БИТ, к.ф.-м.н., доцент

Лебедев Илья Сергеевич, профессор каф. БИТ, д.т.н., доцент,

Левина Алла Борисовна, доцент каф. БИТ, к.ф.-м.н.,

составили настоящий акт о том, что результаты диссертационной работы Нурдинова Р.А. внедрены в учебный процесс кафедры «Безопасные информационные технологии» ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

При подготовке учебных материалов по дисциплинам «Организация и управление службой защиты информации» и «Технологии обеспечения информационной безопасности объекта» были использованы следующие результаты диссертационного исследования Нурдинова Р.А.:

1. Модель количественной оценки рисков безопасности корпоративной информационной системы.
2. Методика формирования рационального комплекса защитных мер для корпоративной информационной системы.

Использование результатов диссертационного исследования Нурдинова Р.А. позволило повысить качество и глубину проработки учебных материалов по вопросам управления рисками информационной безопасности и выбора защитных мер для корпоративных информационных систем.

Председатель: _____ А.В. Птицын

Члены комиссии: _____ И.И. Комаров

_____ И.С. Лебедев

_____ А.Б. Левина

Рисунок В.4 – Акт о внедрении в учебный процесс кафедры безопасных информационных технологий Университета ИМТО

Приложение Г

(обязательное)

Перечень структурных элементов информационной системы «Бухгалтерия и кадры»

Таблица Г.1 – Перечень элементов ИС «Бухгалтерия и кадры»

Наименование элемента	Краткое описание	Место размещения	Коли-чество	Тип
1. Сервер 1С	Сервер БД прикладной системы «1С: Предприятие»	Администрация	1	ТС
2. Корпоративный сервер	Сервер корпоративного портала	Администрация	1	ТС
3. Терминальный сервер	Сервер терминального доступа, предназначенный для пользователей филиала	Администрация	1	ТС
4. Сервер ИБ	Сервер централизованного администрирования СрЗИ	Администрация	1	ТС
5. Файловый сервер	Сервер для хранения и обработки файлов, содержащих информацию ограниченного доступа	Администрация	1	ТС
6. Сервер ИТ-сервисов	Сервер контроллера домена и централизованного обновления ОС	Администрация	1	ТС
7. АРМ пользователей администрации	АРМ пользователей с ограниченными правами доступа к ресурсам КИС	Администрация	75	ТС
8. АРМ администраторов ИТ	АРМ пользователей с административными правами доступа к ресурсам КИС	Администрация	5	ТС
9. АРМ администраторов ИБ	АРМ пользователей с привилегированными правами доступа к ресурсам КИС	Администрация	3	ТС
10. АРМ разработчиков 1С	АРМ пользователей с правами разработчиков 1С	Администрация	3	ТС
11. АРМ пользователей филиала	АРМ удаленных пользователей с ограниченными правами доступа к ресурсам КИС	Филиал	14	ТС
12. Коммутатор Cisco Catalyst 3560	Коммутатор уровня ядра / распределения	Администрация	1	ТС

Наименование элемента	Краткое описание	Место размещения	Коли-чество	Тип
13. Коммутатор HP	Коммутаторы, используемые для подключения АРМ пользователей администрации к ЛВС	Администрация	3	ТС
14. Коммутатор Cisco Catalyst 2960	Коммутатор, используемый для подключения АРМ пользователей филиала к ЛВС	Филиал	1	ТС
15. ЛС сегмента серверов администрации	ЛС Fast Ethernet для подключения серверов к ЛВС	Администрация	6	ЛС
16. ЛС сегмента АРМ администрации	ЛС Fast Ethernet для подключения АРМ администрации к ЛВС	Администрация	86	ЛС
17. ЛС сегмента АСО администрации	ЛС Gigabit Ethernet для коммутации АСО администрации	Администрация	6	ЛС
18. ЛС сегмента АРМ филиала	ЛС Fast Ethernet для подключения АРМ филиала к ЛВС	Филиал	14	ЛС
19. ЛС Интернет администрации	Резервированные ЛС (Gigabit Ethernet) для подключения ЛВС администрации к сети Интернет	За пределами контролируемой зоны	2	ЛС
20. ЛС Интернет филиала	Резервированные ЛС (Gigabit Ethernet) для подключения ЛВС филиала к сети Интернет	За пределами контролируемой зоны	2	ЛС
21. ПО сервера 1С	Включает следующее ПО: – ОС Windows Server 2012; – СУБД SQL Server Standard 2014; – 1С Предприятие	Сервер 1С	1	ПО
22. ПО сервера корпоративного портала	Включает следующее ПО: – ОС Windows Server 2012; – Microsoft Sharepoint; – СУБД SQL Server Standard 2014	Сервер корпоративного портала	1	ПО
23. ПО терминального сервера	ОС Windows Server 2012	Терминальный сервер	1	ПО
24. ПО сервера ИБ	Включает следующее ПО: – ОС Windows Server 2012; – Kaspersky Security Center	Сервер ИБ	1	ПО
25. ПО файлового сервера	ОС Windows Server 2012	Файловый сервер	1	ПО
26. ПО сервера ИТ	Включает следующее ПО: – ОС Windows Server 2012; – Microsoft AD; – WSUS	Сервер ИТ-сервисов	1	ПО

Наименование элемента	Краткое описание	Место размещения	Коли-чество	Тип
27. ПО АРМ пользователей администрации	Включает следующее ПО: – ОС Windows 7; – Microsoft Office; – Kaspersky Endpoint Security	АРМ пользователей администрации	75	ПО
28. ПО АРМ администраторов ИТ	Включает следующее ПО: – ОС Windows 7; – Microsoft Office; – Kaspersky Endpoint Security	АРМ администраторов ИТ	5	ПО
29. ПО АРМ администраторов ИБ	Включает следующее ПО: – ОС Windows 7; – Microsoft Office; – Kaspersky Endpoint Security	АРМ администраторов ИБ	3	ПО
30. ПО АРМ разработчиков 1С	Включает следующее ПО: – ОС Windows 7; – Microsoft Office; – Kaspersky Endpoint Security	АРМ разработчиков 1С	3	ПО
31. ПО АРМ филиала	Включает следующее ПО: – ОС Windows 7; – Microsoft Office; – Kaspersky Endpoint Security	АРМ пользователей филиала	14	ПО
32. ПО коммутатора Cisco Catalyst 3560	ОС Cisco IOS	Коммутатор Cisco Catalyst 3560	1	ПО
33. ПО коммутатора HP ProCurve	YB 15 (HP)	Коммутатор HP ProCurve	3	ПО
34. ПО коммутатора Cisco Catalyst 2960	ОС Cisco IOS	Коммутатор Cisco Catalyst 2960	1	ПО
35. БД 1С	БД прикладной системы «1С: Предприятие»	– сервер 1С; – АСО; – ЛС	1	ИА
36. БД корпоративного портала	Корпоративные документы, новости, справочник сотрудников и прочие сведения	– сервер портала; – АСО; – ЛС	1	ИА
37. БД пользователей	Учетные записи пользователей домена	– сервер ИТ; – АРМ; – АСО; – ЛС	1	ИА
38. Каталог файлов пользователей	Каталог файлов на сетевом диске, содержащих информацию ограниченного доступа	– файловый сервер; – АСО; – ЛС	1	ИА