На правах рукописи

Нурдинов Руслан Артурович

МОДЕЛЬ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКОВ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ МЕТРИК

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2016

Работа выполнена в Федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

Научный руководитель: доктор военных наук, профессор
Каторин Юрий Федорович

Официальные оппоненты: доктор технических наук, доцент
Беззатеев Сергей Валентинович
ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения», заведующий кафедрой технологий защиты информации и техносферной безопасности

кандидат технических наук, доцент
Гончаренко Владимир Анатольевич
ФГБВОУ ВО «Военно-космическая академия имени А.Ф. Можайского», профессор кафедры информационно-вычислительных систем и сетей

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный технологический институт (технический университет)»

Защита состоится «27» декабря 2016 г. в 14:00 на заседании диссертационного совета Д.002.199.01 при Федеральном государственном бюджетном учреждении науки Санкт-Петербургском институте информатики и автоматизации Российской академии наук по адресу: 199178, Россия, Санкт-Петербург, 14 линия В. О., дом 39.

С диссертацией можно ознакомиться в библиотеке и на сайте Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

Автореферат разослан « ____ » _____ 2016 г.

Ученый секретарь
диссертационного совета Д.002.199.01
кандидат технических наук Фаткиева Р.Р.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

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

Во многих стандартах по информационной безопасности (ИБ) (ISO/IEC 27000 серии, NIST SP 800 серии, СТО БР ИББС и прочих) предлагается использовать риск-ориентированный подход к обеспечению ИБ, в соответствии с которым защитные меры выбираются для снижения неприемлемых рисков.

Риски могут оцениваться качественно и количественно (в стоимостных величинах). Количественная оценка позволяет обосновать затраты на реализацию защитных мер путем их сопоставления с выгодами от снижения рисков. Вместе с тем, существует 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);
- неопределенность правил использования статистических данных для оценки вероятности событий риска.

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 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 математических моделей для оценки рисков безопасности КИС.

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

Степень разработанности темы исследования

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 методики оценки рисков, основанные на нечеткой логике, линейном программировании, статистическом анализе, байесовских сетях, нейронных сетях, логико-вероятностном моделировании, моделировании с использованием когнитивных карт и имитационном моделировании.

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. Для повышения качества выбора защитных мер необходимо разработать формализованную модель количественной оценки рисков, учитывающую взаимосвязи между событиями риска 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 ИБ;
- 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 разработки методики количественной оценки вероятности реализации угроз нарушителем применяются методы математической статистики, теории вероятностей, теории нейронных сетей и метод анализа иерархий.

Положения, выносимые на защиту:

1. Модель оценки рисков безопасности корпоративной информационной системы на основе определения деструктивных состояний ее элементов обеспечивает переоценку рисков при изменении исходных данных без повторного привлечения экспертов.
2. Методика формирования рационального комплекса защитных мер для корпоративной информационной системы на основе минимизации значения показателя затратоемкости активов позволяет повысить качество выбора защитных мер.
3. Методика количественной оценки вероятности реализации угроз нарушителем на основе экспертно-нейросетевого определения метрик позволяет повысить точность прогнозирования вероятности событий риска.

Научная новизна результатов исследования заключается в следующем:

1. Предложена оригинальная формализованная модель количественной оценки рисков безопасности КИС, отличающаяся набором связанных переходов ее элементов в деструктивные состояния, рассматриваемых в качестве событий риска.
2. Разработана методика, позволяющая повысить качество выбора защитных мер для корпоративной информационной системы, отличающаяся применением предложенного в работе показателя затратоемкости активов.
3. Выполнен синтез уникальной методики количественной оценки вероятности реализации угроз на основе определения метрик нарушителя и защитных мер, отличающейся использованием комбинации экспертных и нейросетевых методов. Для повышения точности прогнозирования вероятности реализации угроз 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 ИБ.

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

Практическую значимость исследования составляют предложенные модели и методики, которые позволяют повысить качество выбора защитных мер для корпоративных информационных систем и могут быть использованы при проектировании и внедрении систем защиты информации.

Предложенные модели и методики **внедрены** в практику деятельности ООО «Газинформсервис» и ООО «Газпром трансгаз Санкт-Петербург». Основные результаты исследования используются в учебном процессе ЧОУ ДПО «Центр предпринимательских рисков» и в учебном процессе кафедры безопасных информационных технологий Университета ИТМО.

Основные результаты диссертационной работы прошли **апробацию** и были одобрены 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;
- III Международная научно-практическая конференция «Информационные управляющие системы и технологии», Украина, г. Одесса, сентябрь 2014.

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

Личный вклад автора в публикациях, написанных в соавторстве, состоит в следующем: в статьях [1, 6-10] представлены модель оценки рисков безопасности КИС и методика количественной оценки вероятности реализации угроз нарушителем; в работе [2] приведены результаты сравнительного анализа стандартов и методик оценки рисков ИБ; в публикациях [3, 5, 11, 12] раскрыты основные положения методики формирования рационального комплекса защитных мер.

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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность выбранной темы исследования; сформулированы цель, предмет и объект, научная задача и частные задачи исследования; раскрыты принципы используемых методов исследования; определены положения, выносимые на защиту; показана научная новизна, теоретическая и практическая значимость полученных результатов исследования, приведены сведения об их внедрении и апробации.

В первой главе проведен анализ предметной области оценки рисков безопасности информационных систем. Приводится подробная характеристика таких понятий, как информационная система (ИС), риск ИБ, угроза, источник угроз, уязвимость, ущерб, защитная мера.

В классическом представлении процесс оценки рисков состоит из трех последовательных процедур: идентификации рисков, анализа рисков и сравнительной оценки рисков. В части реализации данных процедур проведен сравнительный анализ стандартов и методик, подразделяемых на:

- международные и национальные стандарты (ISO/IEC 27000 и 31000 серий, NIST SP 800 серии, BSI-Standard 100-3, MAGERIT, EBIOS);
- отраслевые стандарты и стандарты организаций (РС БР ИББС-2.2-2009, СТО Газпром 4.2-3-003-2009, PCI DSS Risk Assessment Guidelines);
- методологии научных групп (CRAMM, RiskWatch, OCTAVE, ГРИФ, руководство Microsoft).

Проведенный анализ показал, что чаще всего оценка параметров риска (вероятности реализации угрозы, величины ущерба и прочих) выполняется экспертами по некоторым качественным шкалам, что затрудняет формализацию

правил и процедур оценки рисков. Как следствие, динамическая переоценка рисков при изменении входных данных невозможна без повторного привлечения экспертов.

Одна из главных проблем существующих подходов к оценке рисков ИБ заключается в сложности получения объективных количественных оценок. Прогнозирование вероятности события риска с приемлемой точностью является весьма трудоемкой и трудновыполнимой задачей ввиду отсутствия четких требований к составу исходных данных, правил оценки (математической модели) и недостатка статистики реализации угроз.

Рассмотрены методы, используемые для прогнозирования вероятности случайного события, подразделяемые на экспертные (индивидуальные и групповые) и формализованные (статистические, структурные и моделирование), определены их преимущества и недостатки. Установлено, что для прогнозирования вероятности реализации угроз нарушителем необходимо использовать комбинированный подход, согласно которому группой экспертов определяется аппроксимирующая функция на основе взвешенных метрик нарушителя и защитных мер, а ее дальнейшая настройка осуществляется с применением методов обучения нейронной сети.

Сделан вывод, что для повышения качества выбора защитных мер необходимо разработать формализованную модель количественной оценки рисков. В качестве события риска предложено рассматривать не реализацию отдельной угрозы, а переход элемента КИС в деструктивное состояние в результате реализации одной или нескольких угроз. Это позволяет однозначно определить причинно-следственные связи между событиями риска.

Во второй главе проведен структурный анализ корпоративных информационных систем. Приводится обоснование набора типов элементов КИС, представленных на рисунке 1: технические средства, линии связи (ЛС), программное обеспечение, информационные активы.

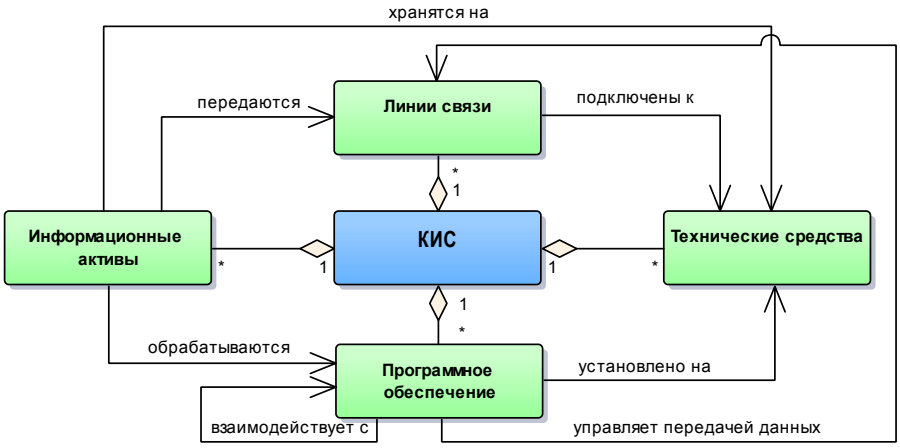


Рисунок 1 – Типы элементов КИС

Рассмотрена возможность детализации элементов КИС на подтипы. Например, технические средства могут подразделяться на серверы, активное сетевое оборудование (АСО), автоматизированные рабочие места (АРМ) и прочие.

Модель оценки рисков безопасности КИС, предложенная в работе, формируется на основе двух частных моделей: инфраструктурной модели КИС и модели сценариев реализации угроз.

Инфраструктурная модель КИС представляет собой неориентированный граф $G^{IS} = \{O^{IS}, L^{IS}\}$, в котором O^{IS} – множество элементов КИС, L^{IS} – множество связей между элементами, определяемое матрицей смежности $A^{IS} = [a_{ij}^{IS}]$.

Множество источников угроз безопасности КИС представлено кортежем $ST^{IS} = \{V^{NS}, V^{AS}\}$, в котором V^{NS} – класс естественных источников угроз, V^{AS} – класс антропогенных источников угроз (нарушителей).

Для учета связей между источниками угроз и элементами КИС задается матрица $A^{ST} = [a_{ij}^{ST}]$, в которой $a_{ij}^{ST} = 1$, если источник угроз ST_i^{IS} может реализовать угрозу в отношении элемента КИС O_j^{IS}, а иначе $a_{ij}^{ST} = 0$.

Модель сценариев реализации угроз определена как ориентированный граф $G^{TM} = \{V^{TM}, H^{TM}\}$ с вершинами $v'_i \in V^{TM}$ двух типов и дугами $h'_{ji} \in H^{TM}$. Вершины первого типа $v'_i \in ST^{IS}$ соответствуют классам источников угроз, а вершины второго типа $v'_i \in DS^{IS}$ – деструктивным состояниям элементов КИС.

В ходе анализа документов по моделированию угроз, оценке рисков и теории надежности, а также опроса специалистов определены следующие деструктивные состояния элементов КИС:

- нарушение конфиденциальности ($IA^{[C]}$), целостности ($IA^{[M]}$) и доступности ($IA^{[U]}$) информационного актива;
- несанкционированный доступ ($HW^{[I]}$, $CL^{[I]}$, $SW^{[I]}$) и нарушение доступности ($HW^{[U]}$, $CL^{[U]}$, $SW^{[U]}$) технического средства, линии связи и программного обеспечения соответственно.

Определено множество переходов, содержащих причину $v'_i \in V^{TM}$ и результат $v'_j \in DS^{IS}$. Вершины v'_i и v'_j соединяются дугой h'_{ji}, либо несколькими дугами через промежуточные вершины $v'_r \in DS^{IS}$, называемые условиями перехода. Множество дуг H^{TM} определяется матрицей смежности $A^{TM} = [a_{ij}^{TM}]$.

Переходы $v'_j \in DS^{IS}$, возникающие в результате связанных переходов $v'_i \in DS^{IS}$, называются зависимыми, а веса соответствующих им дуг равны 1. Примером зависимого перехода является отказ программного обеспечения при отказе технического средства, на которое оно установлено.

Для переходов, возникающих в результате реализации угроз естественными или антропогенными источниками, определяется два типа весовых функций.

Для прогнозирования частоты редких независимых событий в теории надежности и в теории рисков используется распределение Пуассона. Отмечается, что угрозы, реализуемые естественными источниками, возникают, как правило, редко и независимо друг от друга. Весовая функция перехода $v'_j \in DS^{IS}$ с причиной $v'_i \in ST^{NS}$ определяется как вероятность возникновения опасного события за период оценки:

$$f_{ji}^{NS} = 1 - e^{-\lambda_i}, \qquad (1)$$

где λ_i – среднее число опасных событий (отказов, аварий) для $v'_i \in V^{NS}$.

При оценке λ_i необходимо удостовериться, что в потоке учитываемых опасных событий отсутствует последействие. В противном случае, зависимые события должны быть объединены или исключены.

Точное определение функции распределения вероятности реализации угроз нарушителем является нетривиальной и трудноразрешимой задачей. В качестве весовой функции перехода $v'_j \in DS^{IS}$ с причиной $v'_i \in ST^{AS}$ предлагается использовать аппроксимирующую функцию f_{ji}^{AS} вида:

$$f_{ji}^{AS} = \left(1 + e^{-z(d_i - \psi_j)}\right)^{-1}, \qquad (2)$$

где z – неотрицательный множитель;

d_i – степень опасности нарушителя $v'_i \in V^{AS}$;

ψ_j – степень реализации превентивных защитных мер для $v'_j \in DS^{IS}$.

Выбор логистической функции в формуле (2) обусловлен ее нелинейностью, непрерывной дифференцируемостью и подходящей областью значений [0; 1].

Для оценки показателей степени опасности нарушителей и степени реализации защитных мер определены наборы взвешенных метрик, принимающих значения в интервале [0; 1]. Каждая метрика характеризует степень соответствия некоторого признака нарушителя или защитной меры заданному целевому значению.

Для оценки степени опасности нарушителя предлагается использовать следующие метрики, сформированные с учетом положений ГОСТ Р ИСО/МЭК 18045-2013: 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 *i*-го нарушителя определяется по формуле:

$$d_i = \prod_h \left(M_{ih}^V\right)^{w_{ih}^V}, \qquad (3)$$

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

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

Основываясь на положениях нормативных документов ФСТЭК России, в частности, Приказов № 17 и № 21, для КИС сформированы метрики защитных мер, сгруппированные в 15 категорий (управление доступом, антивирусная защита и прочие). Метрики характеризуют степень реализации защитных мер, подразделяемых на превентивные (предотвращающие переход элемента КИС в деструктивное состояние) и корректирующие (снижающие величину ущерба от перехода). Степень реализации превентивных защитных мер ψ_j определяется по формуле:

$$\psi_j = \prod_g \left(\sum_l w_{gl}^C \cdot M_{gl}^C \right)^{w_{jg}^K}, \qquad (4)$$

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

w_{gl}^C – весовой коэффициент *l*-ой защитной меры *g*-ой категории, $\sum_l w_{gl}^C = 1$;

w_{jg}^K – весовой коэффициент *g*-ой категории, $\sum_g w_{jg}^K = 1$.

Степень реализации корректирующих защитных мер ψ'_j по аналогии с ψ_j определяется по формуле (4).

В диссертационной работе приведено теоретическое обоснование формул (3) и (4). Кроме того, использование данных формул позволяет провести оценку начальных значений весовых коэффициентов категорий и метрик методом анализа иерархий, преимуществами которого являются простота вычислений, интерпретируемость и возможность проверки качества полученных оценок. Последовательность этапов начальной оценки весовых коэффициентов приведена на рисунке 2.

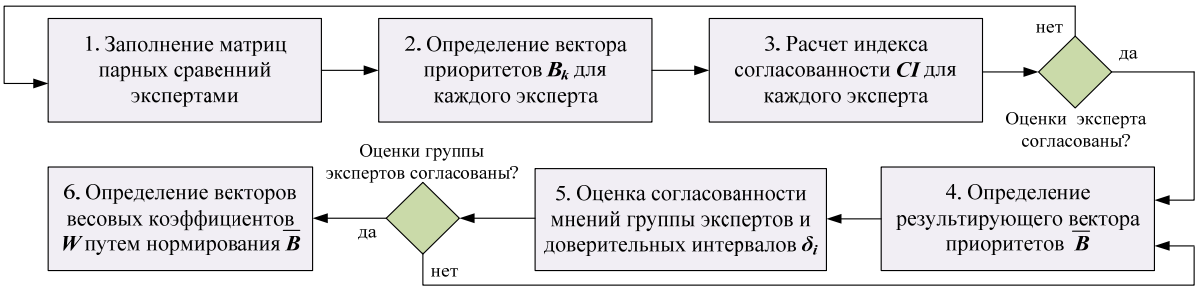


Рисунок 2 – Последовательность этапов начальной оценки весовых коэффициентов

Согласованность полученных оценок определяется дважды. Сначала оценивается индекс согласованности оценок каждого эксперта:

$$CI = \frac{\lambda_{k\max} - m}{m-1}, \quad (5)$$

где $\lambda_{k\max}$ – максимальное собственное число матрицы парных сравнений k-го эксперта;

m – размерность матрицы парных сравнений.

Оценки эксперта считаются согласованными, если отношение согласованности $CR = CI / CIS$, где CIS – среднее значение индекса согласованности, входит в допустимые диапазоны, приведенные в таблице 1. Согласованность мнений группы экспертов определяется по правилу трех сигм. Несогласованные оценки не учитываются при расчете результирующего вектора приоритетов $\overline{B}$:

$$\overline{B} = \left(\overline{b_1}, \overline{b_2}, \ldots, \overline{b_m}\right)^T, \overline{b_i} = \sqrt[K_E]{\prod_k b_{ik}}, \quad (6)$$

где $\overline{b_i}$ – результирующий приоритет i-го элемента;

b_{ik} – приоритет i-го элемента, оцененный k-ым экспертом;

K_E – число экспертов.

Таблица 1 – 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]							

Доверительный интервал δ_i определяется по формуле:

$$\delta_i = t_{cm} \cdot \sigma_{gi} \Big/ \sqrt{K_E}, \quad (7)$$

где $t_{cm} = 0{,}95$ – критерий Стьюдента;

σ_{gi} – геометрическое стандартное отклонение.

Вектор весовых коэффициентов W определяется путем нормирования результирующего вектора приоритетов:

$$w_i = \overline{b_i} \Big/ \sum_{i=1}^{m} \overline{b_i}, \ \forall i \in [1; m]. \quad (8)$$

Оценка начальных значений весовых коэффициентов осуществлялась группой квалифицированных экспертов из 18 человек. При выборе экспертов были выполнены требования, предъявляемые стандартами ГОСТ Р ИСО/МЭК 27006-2008 и РС БР ИББС-2.2-2009, в том числе требования к образованию, опыту работы и прочие.

Модель оценки рисков безопасности КИС представляет собой ориентированный граф $G^{RM} = \{V^{RM}, H^{RM}\}$, формируемый 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;
2) определяются вершины $v_i \in V^{AS} \subset V^{RM}$, соответствующие нарушителям, и вершины $v_i \in V^{NS} \subset V^{RM}$, соответствующие естественным источникам угроз.
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 $ST_x^{IS} \to v_i$ и $O_y^{IS} \to v_j$ справедливо: $a_{xy}^{ST} = 1$;
   - в матрице A^{TM} для $ST_x^{IS} \to v_i$ и $DS_y^{IS} \to v_{ji}$ 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 $O_x^{IS} \to v_i$ и $O_y^{IS} \to v_j$ справедливо: $a_{xy}^{IS} = 1$;
   - в матрице A^{TM} для $DS_x^{IS} \to v_i$ 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 $v_j \in V^{DS}$ определяются значения ψ_j и ψ'_j.

Величина полного риска для КИС R_{IS} определяется как:

$$R_{IS} = \sum_{v_j \in V^{DS}} p(v_j) \cdot q(v_j), \tag{9}$$

где $p(v_j)$ – безусловная вероятность события риска;
$q(v_j)$ – величина ущерба от события риска.

Безусловная вероятность события риска $v_j \in V^{DS}$ определяется как:

$$p(v_j) = 1 - (1 - p^{NS}(v_j)) \cdot (1 - p^{AS}(v_j)), \tag{10}$$

где $p^{NS}(v_j)$ и $p^{AS}(v_j)$ – значения вероятности события риска $v_j \in V^{DS}$ в результате реализации угроз естественными источниками и нарушителями соответственно.

Для оценки значений $p^{NS}(v_j)$ на основе графа G^{RM} строится граф отказов $G^F = \{V^F, H^F\}$, в котором $V^F = V^{RM} \setminus (V^{AS} \cup HW^{[I]} \cup CL^{[I]} \cup SW^{[I]} \cup IA^{[C]})$ и $H^F = H^{RM} \setminus H^{AS}$. Предварительно из графа G^F удаляются циклы путем слияния образующих их вершин, после чего выполняется топологическая сортировка поиском в глубину. Для каждой вершины $v_j \in V^{DS}$ в порядке увеличения j значение $p^{NS}(v_j)$ определяется по формуле:

$$p^{NS}(v_j) = 1 - \prod_{\forall i:\, a_{ij}^F = 1} \left(1 - p^{NS}(v_j \mid v_i)\right), \tag{11}$$

где $p^{NS}(v_j \mid v_i)$ – условная вероятность перехода $v_j \in V^{DS}$ по причине $v_i \in V^{NS}$, определяемая функцией f_{ji}^{NS} по формуле (1);

$A_F = [a_{ij}^F]$ – матрица смежности графа G^F.

Для оценки значений $p^{AS}(v_j)$ на основе графа G^{RM} строится граф атак $G^A = \{V^A, H^A\}$, в котором $V^A = V^{RM} \setminus V^{NS}$ и $H^A = H^{RM} \setminus H^{NS}$. В соответствии с принципом гарантированного результата значение $p^{AS}(v_j)$ определяется наибольшим значением вероятности реализации сценария, приводящего к переходу $v_j \in V^{DS}$. Если определить длины дуг h_{ji} как $l_{ji} = -\ln(f_{ji}^{AS})$, задача сводится к известной задаче нахождения кратчайшего пути.

В соответствии с алгоритмом Дейкстры кратчайший путь из вершины $v_i \in V^{AS}$ до каждой вершины $v_j \in V^{DS}$ графа G^A должен удовлетворять условию:

$$L_{ji} = \sum_{x,y} l_{xy} \cdot \chi_{xy} \to \min, \tag{12}$$

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

Для каждого нарушителя $v_i \in V^{AS}$ определяются кратчайшие пути L_{ji} до вершин $v_j \in V^{DS}$, после чего выполняется обратное преобразование: $p^{AS}(v_j \mid v_i) = e^{-L_{ji}}$. Значение $p^{AS}(v_j)$ определяется для каждой вершины $v_j \in V^{DS}$ по формуле:

$$p^{AS}(v_j) = \underset{v_i \in V^{AS}}{MAX}\left(p^{AS}(v_j \mid v_i)\right). \tag{13}$$

Величина ущерба $q(v_j)$ от перехода $v_j \in V^{DS}$ определяется суммой последствий, выраженных в стоимостных величинах, с учетом степени реализации корректирующих защитных мер:

$$q(v_j) = \left(1 - \psi'_j\right) \cdot \sum_b J_{jb}, \qquad (14)$$

где J_{jb} – b-ый показатель последствий.

Для каждого деструктивного состояния сформированы наборы показателей последствий, характеризующих финансовые, репутационные, производственные, экологические и иные потери, и определены правила их оценки.

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

$$S_{IS} = \sum_i \sum_b J_{ib}, \forall v_i \in V^{DS}. \qquad (15)$$

Показано, что вычислительная сложность алгоритмов, используемых в модели оценки рисков, имеет вид: $T = O(N_O^2)$, где N_O – количество элементов КИС.

Предложена методика формирования рационального комплекса защитных мер для КИС, процедуры которой представлены на рисунке 3. Прежде всего, на основе типового перечня защитных мер, включающего средства защиты и организационные меры, формируется множество альтернативных комплексов $Z_A = \{z_1, z_2, \ldots, z_x\}$, каждый из которых содержит уникальный набор защитных мер $z_x = \{c_{x1}, c_{x2}, \ldots, c_{xy}\}$. При формировании альтернативных комплексов учитываются следующие ограничения:

– совместимость и взаимозависимость защитных мер в составе комплекса;
– требования нормативных документов к формируемой СЗИ;
– ограниченность выделенного бюджета на СЗИ S_B.

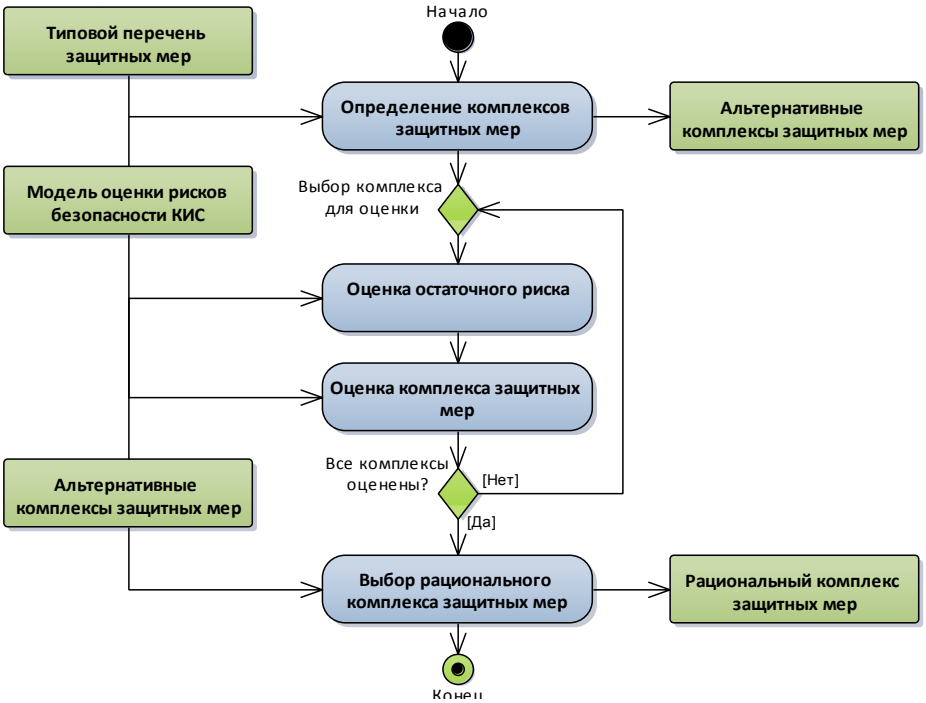


Рисунок 3 – Методика формирования рационального комплекса защитных мер

Для каждого альтернативного комплекса определяется величина остаточного риска R_z по формуле (9). В работе предложен показатель затратоемкости активов ω_z, определяемый отношением суммы реальных затрат на защитные меры и предполагаемых затрат (остаточного риска) к стоимости защищаемых активов КИС:

$$\omega_z = \left(S_z + R_z\right) / S_{IS}, \qquad (16)$$

где S_z – затраты на реализацию комплекса защитных мер.

Показатель затратоемкости активов принимает минимальное значение при оптимальном сочетании величины остаточного риска и затрат на реализацию комплекса защитных мер, как представлено на рисунке 4.

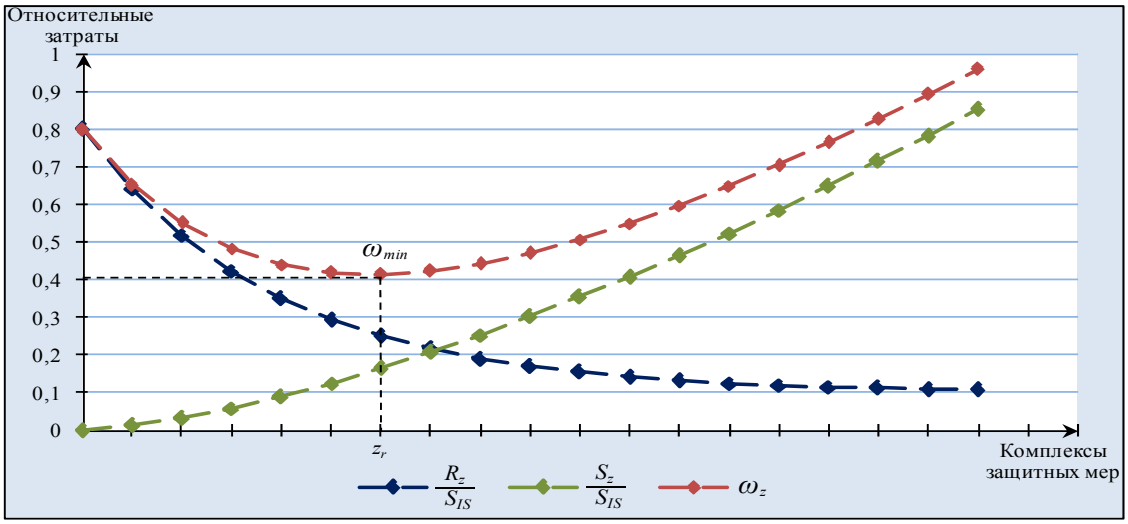


Рисунок 4 – Выбор рационального комплекса защитных мер на основе минимизации показателя затратоемкости активов

Выбор рационального комплекса защитных мер $z_r \in Z_A$ происходит путем решения следующей задачи дискретной оптимизации:

$$\omega_z \to \min_{z_x \in Z_A}, \qquad 0 \le S_z \le S_{IS}\,. \tag{17}$$

При равенстве показателей затратоемкости активов для нескольких альтернативных комплексов защитных мер выбирается тот из них, величина остаточного риска R_z при котором минимальна.

В третьей главе рассмотрен вопрос настройки весовых коэффициентов метрик с использованием методов обучения нейронной сети для повышения точности прогнозирования вероятности реализации угроз нарушителем.

Объектами обучающей выборки служат структурированные сведения об инцидентах ИБ, представленные кортежем:

$$I = [v_i, v_j, \{M_{ih}^V\}, \{M_{gl}^C\}, y_{ji}], \tag{18}$$

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

$\{M_{ih}^V\}$ – множество значений метрик нарушителя;

$\{M_{gl}^C\}$ – множество значений метрик защитных мер;

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

Рассмотрены вопросы сбора исходных данных, в том числе, использование данных из открытых источников и выполнение тестирования на проникновение.

Определены требования, предъявляемые к методу обучения, среди которых: отбор значимых признаков в процессе обучения, возможность обучения на неполных данных, а также выполнение алгоритма обучения за полиномиальное время. Сделан вывод, что для решения поставленной задачи обучения целесообразно использовать методы, основанные на коррекции ошибок или минимизации целевой функции вида:

$$E^{(t)} = 0{,}5 \cdot \left(\varepsilon^{(t)}\right)^2 \to \min\,, \tag{19}$$

где $\varepsilon^{(t)}$ – величина ошибки на t-ом шаге обучения, определяемая по формуле:

$$\varepsilon^{(t)} = f_{ji}^{AS(t)} - y_{ji}^{(t)}\,. \tag{20}$$

Исходя из формул (2)-(4) значение функции f_{ji}^{AS} на t-ом шаге определяется как:

$$f_{ji}^{AS(t)} = \left(1+\exp\left(-z\left(\prod_h \left(M_{ih}^{V(t)}\right)^{w_{ih}^{V(t)}} - \prod_g \left(\sum_l w_{gl}^{C(t)} \cdot M_{gl}^{C(t)}\right)^{w_{jg}^{K(t)}}\right)\right)\right)^{-1}. \quad (21)$$

Показано, что задача обучения функции f_{ji}^{AS} равносильна задаче обучения многослойного персептрона, структура которого представлена на рисунке 5.

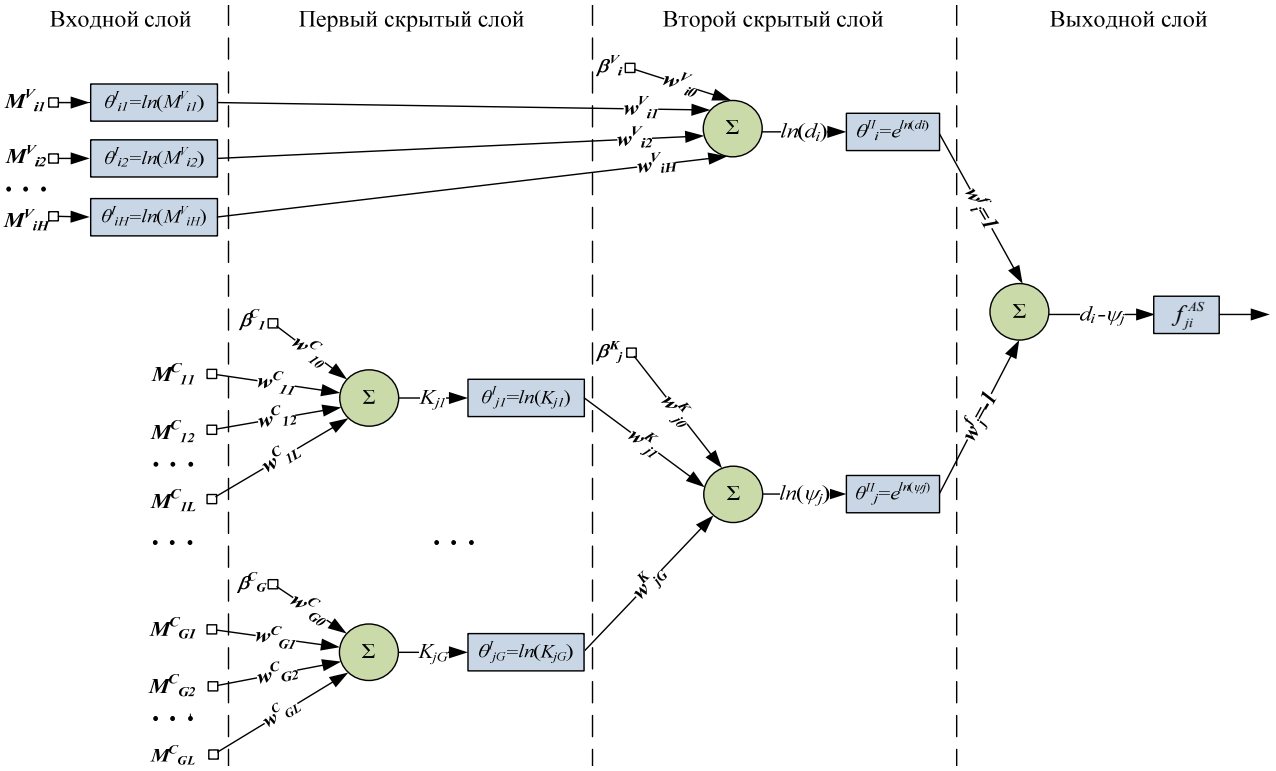


Рисунок 5 – Многослойный персептрон, соответствующий функции f_{ji}^{AS}

В представленной модели многослойного персептрона используются пороговые элементы для метрик нарушителей β_i^V, метрик защитных мер β_g^C 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.

На каждом шаге обучения последовательно выполняются две фазы, представленные на рисунке 6: фаза прямого прохода и фаза обратного прохода.

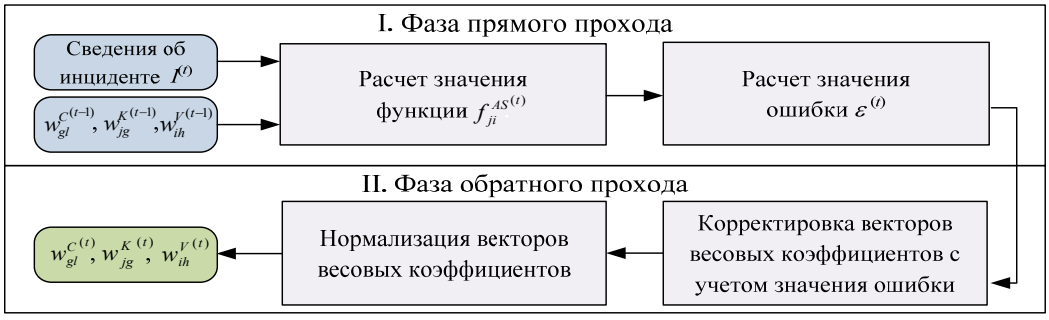


Рисунок 6 – Схема шага обучения

Проведено экспериментальное исследование, основная цель которого заключалась в определении наиболее подходящих параметров обучения: направления минимизации целевой функции, темпа обучения η и прочих.

В ходе экспериментов осуществлялась настройка весовых коэффициентов функции f_{ji}^{AS}, определяющей вероятность реализации угроз НСД к ПО веб-сервера нарушителем через сеть Интернет. Эксперименты проводились путем моделирования процедуры обучения многослойного персептрона, представленного на рисунке 5, с использованием программного кода, написанного на языке C++. Результаты усреднялись по 1000 циклам обучения.

Начальные векторы весовых коэффициентов определялись на основе результатов экспертных оценок методом анализа иерархий. Определение целевых значений весовых коэффициентов осуществлялось путем усреднения данных по инцидентам ИБ, представленных в открытых источниках и аналитических отчетах. Начальные и целевые значения весовых коэффициентов категорий защитных мер представлены в таблице 2.

Таблица 2 – Весовые коэффициенты категорий защитных мер

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

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

$$Q_f^{(t)} = \frac{\sum_h \left| w_{ih}^{V(t)} - \overline{w}_{ih}^{V} \right| + \sum_g \left| w_{jg}^{K(t)} - \overline{w}_{jg}^{K} \right| + \sum_g \sum_l \left| w_{gl}^{C(t)} - \overline{w}_{gl}^{C} \right|}{H + G + \sum_g L_g}, \qquad (22)$$

где H – число метрик нарушителя;

G – число категорий защитных мер;

L_g – число метрик g-ой категории защитных мер.

Поскольку значение ошибки $\varepsilon^{(t)}$, определяемое выражением (20), зависит от объекта обучающей выборки, величина остаточной ошибки определялась в ходе экспериментального исследования как средняя ошибка $\overline{\varepsilon^{(t)}}$ для 10^6 объектов обучающей выборки при фиксированных значениях весовых коэффициентов. Перед началом процедуры обучения значения данных показателей составляли $Q_f^{(0)} = 1057 \cdot 10^{-4}$ и $\overline{\varepsilon^{(0)}} = 0{,}2167$ соответственно.

Для корректировки весовых коэффициентов в ходе экспериментального исследования использовались метод градиентного спуска, метод градиентного спуска с моментом и диагональный метод Левенберга-Марквардта.

При использовании метода градиентного спуска на каждом шаге обучения корректировка весовых коэффициентов задается выражением:

$$\Delta w_l^{(t)} = -\eta \cdot \frac{\partial E}{\partial w_l^{(t)}}, \qquad (23)$$

где η – коэффициент, называемый темпом обучения.

Различают постоянный и адаптивный темп обучения. При адаптивном темпе обучения значение η определяется некоторой зависимостью от порядкового номера шага обучения t, значения ошибки $\varepsilon^{(t)}$ либо другого параметра.

При использовании метода градиентного спуска с моментом корректировка весовых коэффициентов выполняется по правилу:

$$\Delta w_l^{(t)} = -\eta \cdot \frac{\partial E}{\partial w_l^{(t)}} + \alpha \cdot \Delta w_l^{(t-1)}, \tag{24}$$

где α – коэффициент момента, принимающий значения в интервале [0; 1].

Корректировка весовых коэффициентов при использовании диагонального метода Левенберга-Марквардта осуществляется по правилу:

$$\Delta w_l^{(t)} = -\frac{\eta}{\dfrac{\partial^2 E}{(\partial w_l^{(t)})^2} + \mu} \cdot \frac{\partial E}{\partial w_l^{(t)}}, \tag{25}$$

где μ – неотрицательная переменная.

Полученные результаты обучения функции f_{ji}^{AS} с использованием данных методов представлены на рисунке 7.

Наименьшие значения среднего модуля отклонения были получены при использовании диагонального метода Левенберга-Марквардта с $\mu = 0{,}25$ и составили $Q_f^{(100)} = 294 \cdot 10^{-4}$ и $Q_f^{(1000)} = 77 \cdot 10^{-4}$. При выборке из 100 инцидентов ИБ средняя ошибка была снижена 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.

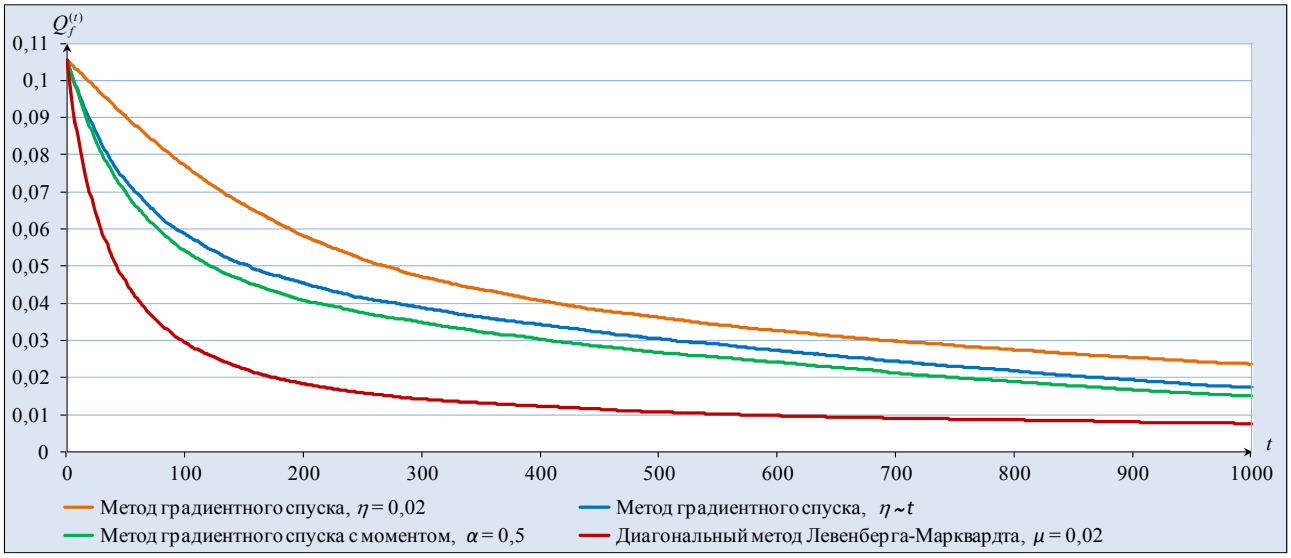
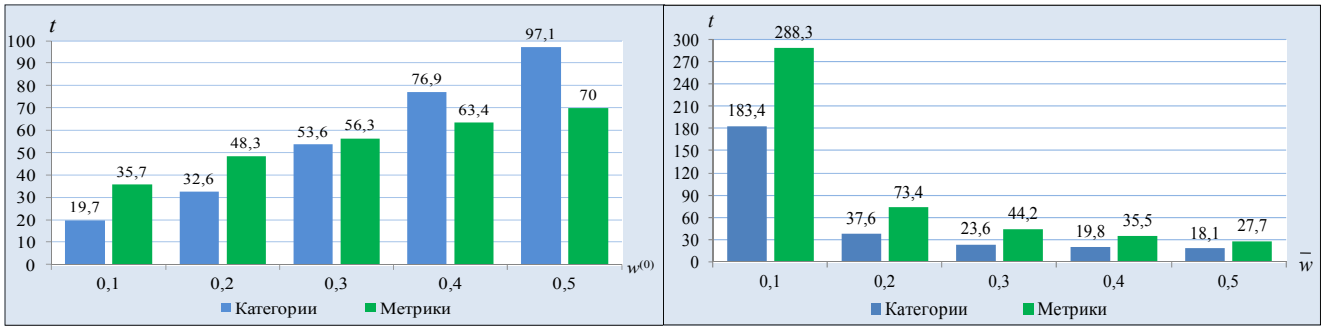


Рисунок 7 – Результаты обучения функции f_{ji}^{AS}

Предложенный метод обучения позволяет осуществлять отбор значимых признаков, подразумевающий как исключение (рисунок 8а), так и определение необходимости добавления (рисунок 8б) категорий и метрик в зависимости от значений их весовых коэффициентов.

Также проведен ряд экспериментов, доказывающих устойчивость предложенного метода обучения к изменению числа категорий и метрик, выбору типов признаков (бинарные, качественные, количественные), а также неполноте данных об инцидентах ИБ (отсутствию значений части метрик).



а) б)

Рисунок 8 – Среднее число шагов обучения, необходимых для: а) исключения незначимых категорий и метрик; б) добавления значимых категорий и метрик

В четвертой главе приведена характеристика использования результатов диссертационного исследования в производственной деятельности предприятий, в том числе при разработке модуля управления рисками безопасности КИС, а также при проектировании и внедрении СЗИ.

Предложенные в диссертационной работе модели и методики использованы при разработке модуля управления рисками в составе системы автоматизации процессов управления ИБ, внедренной в ООО «Газпром трансгаз Санкт-Петербург». Архитектура модуля управления рисками, реализованного на базе интеграционной платформы RSA Archer GRC, представлена на рисунке 9.

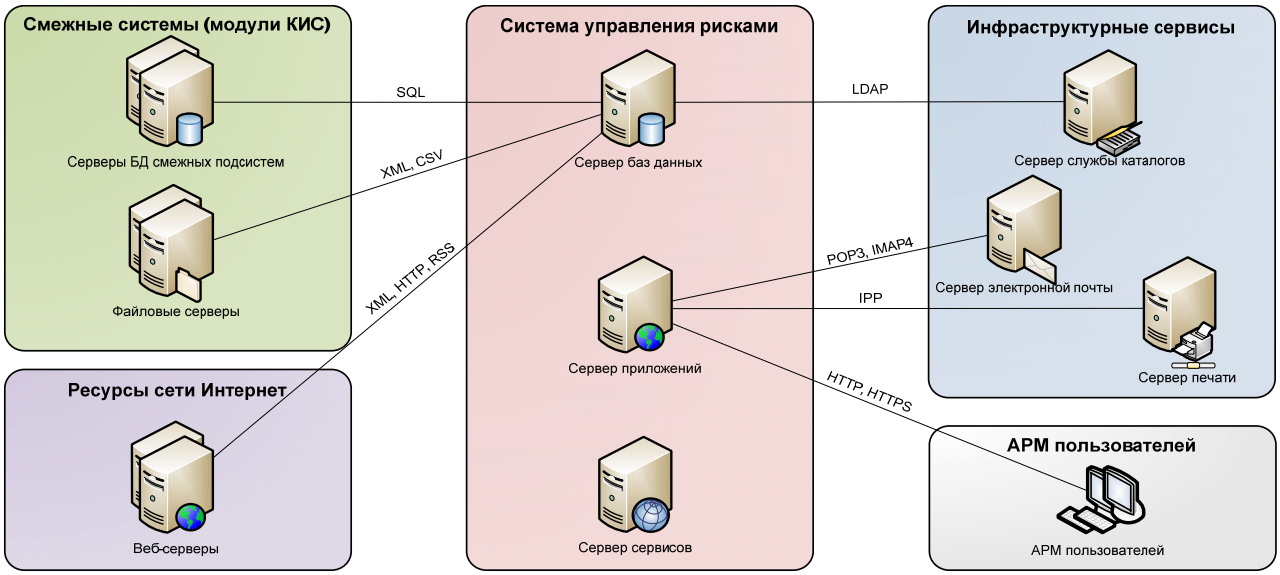


Рисунок 9 – Архитектура модуля управления рисками

Данные, необходимые для оценки рисков безопасности КИС, импортируются из смежных систем, таких как система управления ИТ-активами (ITSM), система контроля защищенности, система мониторинга событий ИБ (SIEM), система предотвращения утечки информации (DLP), а также веб-ресурсов сети Интернет, содержащих базы данных угроз, уязвимостей и инцидентов ИБ. Интеграция модуля управления рисками безопасности КИС со смежными системами осуществляется с использованием SQL-запросов к базам данных, а также механизмов экспорта-импорта файлов в форматах XML и CSV.

Предложенная методика формирования рационального комплекса защитных мер используется в ООО «Газинформсервис» при проектировании СЗИ для автоматизированных и информационных систем. Приведены основные результаты использования данной методики при проектировании и внедрении СЗИ ИС

«Бухгалтерия и кадры», являющейся сегментом КИС предприятия нефтегазовой отрасли. Структурная схема ИС «Бухгалтерия и кадры» представлена на рисунке 10.

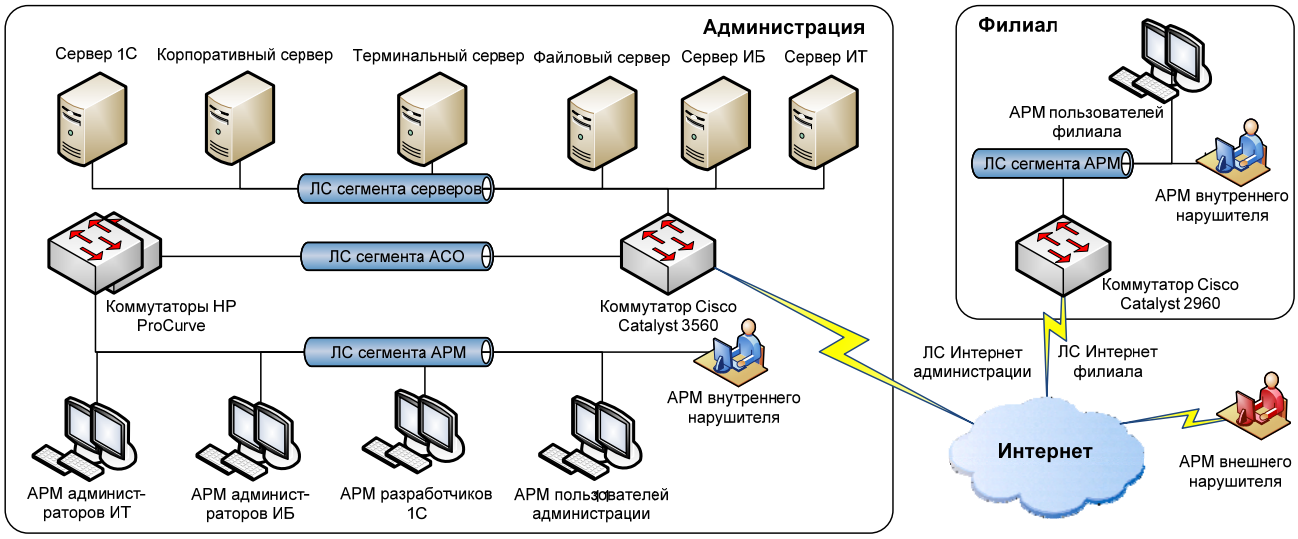


Рисунок 10 – Структурная схема ИС «Бухгалтерия и кадры»

Формирование рационального комплекса дополнительных защитных мер для ИС «Бухгалтерия и кадры» осуществлялось на основе типового перечня, включающего 72 средства защиты, имеющих сертификаты соответствия ФСТЭК России, и 40 организационных мер.

Стоимость активов ИС «Бухгалтерия и кадры» составила $S_{IS} = 12\ 840\ 300$ рублей. В таблице 3 приведены результаты оценки:

– начального комплекса защитных мер, реализованного до внедрения СЗИ ИС «Бухгалтерия и кадры»;
– рационального комплекса дополнительных защитных мер;
– альтернативного комплекса дополнительных защитных мер, предложенного в техническом проекте на СЗИ ИС «Бухгалтерия и кадры».

Таблица 3 – 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**
Начальный	1441,5	3971,6	0,423
Рациональный	425, 6 (1867,1)[1)]	(683,4)	(0,199)
Альтернативный	3007,5 (4449)	(342,3)	(0,360)
[1)] В скобках указаны значения показателей с учетом начального комплекса защитных мер			

На рисунке 11 приведен график снижения показателя затратоемкости активов при пошаговом выборе рациональных защитных мер.

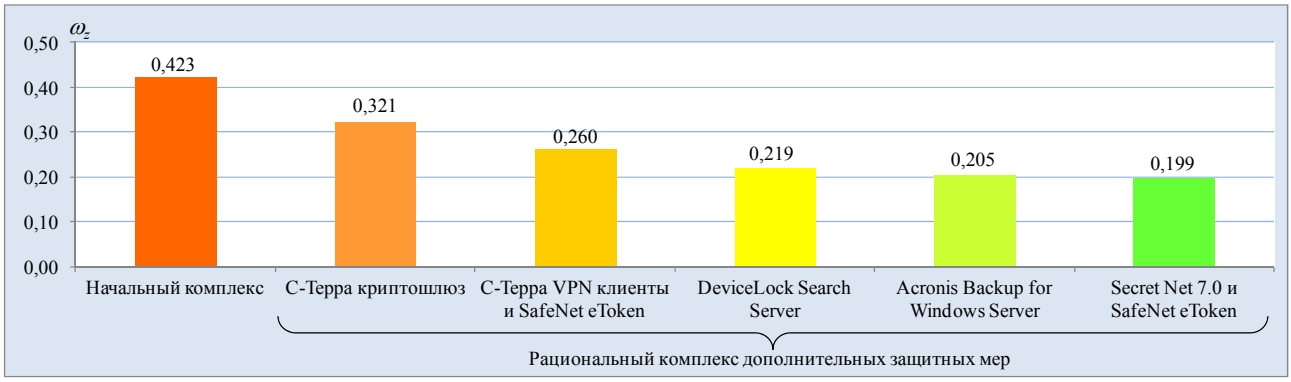


Рисунок 11 – График снижения показателя затратоемкости активов

Таким образом, использование методики формирования рационального комплекса защитных мер позволило:

- выбрать для ИС «Бухгалтерия и кадры» наиболее подходящий комплекс дополнительных защитных мер, обеспечивающий четвертый уровень защищенности персональных данных;
- снизить затраты в 7 раз по сравнению с альтернативным комплексом защитных мер, предложенным в техническом проекте;
- снизить величину остаточного риска в 5,8 раз по сравнению с начальным комплексом защитных мер.

В заключении приведены основные научные и практические результаты, полученные в ходе исследования.

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 были 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 событиями риска, 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 значения 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 ОСНОВНЫХ ПУБЛИКАЦИЙ

Статьи в журналах, входящих в перечень ВАК:

1. Нурдинов Р.А., Каторин Ю.Ф., 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.
2. Нурдинов Р.А., Лившиц И.И. Обеспечение комплексной безопасности сложных промышленных объектов на базе риск-ориентированных стандартов // Информатизация и Связь. 2016. № 1. С. 49-55.
3. Нурдинов Р.А., Вихров Н.М., Ныркov А.П., Каторин Ю.Ф., Шнуренко А.А., Башмаков А.В., Соколов С.С. Анализ информационных рисков // Морской вестник. 2015. № 3 (55). С.81-85.
4. 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.
5. 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.

Статьи в прочих изданиях:

6. Нурдинов Р.А., Каторин Ю.Ф., Зайцева Н.М. Модель количественной оценки рисков безопасности информационной системы // Новый университет. Серия: Технические науки. 2016. № 3 (49). С. 42-47.
7. Нурдинов Р.А., Зайцева Н.М. Оценка ущерба от правонарушений в информационной сфере. Вестник полиции. 2015. № 4. С. 124-132.
8. Nurdinov R.A., Katorin Y.F., Zaitseva N.M. The Quantitative Assessment Model of the Information System Security Risks // Materials of the 3rd International Conference «Technical sciences: modern issues and development prospects». Sheffield, 2015. P. 11-19.
9. Nurdinov R.A., Kanev A.N. The Quantitative Assessment Model of Information System Risk Based on Metrics // First Information Security and Protection of Information Technologies conference. St. Peterburg, 2015. P. 37-41.
10. Нурдинов Р.А. Оценка рисков безопасности информационной системы на основе модели деструктивных состояний и переходов // Материалы конференции «Информационная безопасность регионов России (ИБРР-2015)». СПб., 2015. С. 372-373.
11. Нурдинов Р.А., Каторин Ю.Ф. Определение уровня защиты объекта на основании анализа информационных рисков // Вестник КИГИТ. 2014. № 7 (48). С. 31-40.
12. Нурдинов Р.А. Обоснование целесообразности выбора средств защиты информации // Современные наукоемкие технологии. 2014. № 5-1. С. 81-82.