Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет»

На правах рукописи

Аль Балуши Маджед Пир Бахш

АНАЛИТИЧЕСКОЕ И ПРОЦЕДУРНОЕ ОБЕСПЕЧЕНИЕ ЭКСПЕРТНОЙ СИСТЕМЫ ОЦЕНКИ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ СЕТЕВЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

05.25.05 – Информационные системы и процессы (технические науки)

Диссертация на соискание учёной степени
кандидата технических наук

Научный руководитель: доктор технических наук, профессор
В.Е. Дидрих

Тамбов 2014

СОДЕРЖАНИЕ

ОСНОВНЫЕ УСЛОВНЫЕ ОБОЗНАЧЕНИЯ И СОКРАШЕНИЯ

L– ценность информации;

H – риск от персонала СИС;

O – оценка опасности НВВ;

q – доступность, конфиденциальность и целостность;

W_d^q – оценка надежности d-ого СПНВВ по q;

E_{dj} – величина действующего временного парирования НВВ;

P_{ji}^q - риск от j-ого НВВ, которое направлено на i-й ресурс с целью нарушения q;

V_i^q – оценка важности i-ого ресурса по Д, К и Ц;;

G_i^q – оценка устойчивости функционирования i-ого ресурса СИС q;

T_i^q – требуемый уровень устойчивости функционирования i-ого ресурса по q;

Q_s^q – оценка устойчивости функционирования s-ого объекта по q;

ИС – информационная система;

СИС – сетевая информационная система;

ЭС – экспертная система;

ИИС – интеллектуальная информационная система;

НВВ – негативные внешние воздействия;

СПНВВ – средства парирования негативных внешних воздействия;

МПНВВ – механизм парирования негативных внешних воздействия;

Д, К, Ц –доступность, конфиденциальность, целостность;

И, Ф, Ч – информационный, физический, человеческий ресурс.

ВВЕДЕНИЕ

Актуальность темы исследования. Понятие «сетевые информационные системы (СИС)» уже признано исследователями предметной области информационных систем и технологий. Оно базируется на понятии информационной системы (ИС), которое трактуется как совокупность программно-аппаратных средств объединенных в систему информационными процессами, направленными на достижения конкретной цели в интересах, как правило, эргатического звена.

СИС предполагает обязательное использование информационных процессов связанных с передачей информации и организации распределенной работы пользователей.

На практике имеют место ряд негативных внешних воздействий (НВВ), которые существенно влияют на условия и качество функционирования СИС, снижая устойчивость, и при этом обладают параметрической неопределенностью, недетерминированным характером. Для нейтрализации этих НВВ разрабатываются и применяются средства парирования негативных внешних воздействий (СПНВВ).

Устойчивость функционирования СИС – свойство сохранять набор основных функциональных возможностей системы в различных условиях этого процесса, в том числе в условиях негативных внешних воздействий.

Анализ и оценка показателей этого свойства является актуальной задачей в практике проектирования и эксплуатации СИС, поскольку на их основе возможно обеспечение заданного уровня устойчивости функционирования.

Степень разработанности темы. В работах российских и зарубежных ученых рассматривались различные подходы для оценки различных свойств СИС, в том числе и устойчивости функционирования, влияющих на эффективность и защищенность этих систем, например, в работах: Громов

Ю.Ю., А.А. Малюка, Ж.С. Сарыпбекова, Ю.Е. Мельникова, А.Г. Додонова, В.М. Вишневского, Ю.Е. Малашенко, М.Г. Кузнецова, J.H. Dinitz, B.Hotmann, C.J. Colbourn, S. Tani и др. Предлагаемые ими подходы не учитывают при получении оценки риска и оценки опасности НВВ такие факторы как важность ресурсов и ценность обрабатываемой информации; требуемый уровень устойчивости функционирования, учитывающий эти факторы; то, что тип исследуемой системы влияет на оценку показателя риска.

В настоящее время на практике используется множество похожих интеллектуальных информационных систем (ИИС) предназначенных для оценки защищенности информационных систем, однако не существует ИИС для проведения анализа и оценки устойчивости функционирования СИС при НВВ. Примерами, наиболее известных ИИС, являются: «АванГард» (Россия), Risk Watch (США), CRAMM (Великобритания). Анализ возможностей этих систем показывает, что они обладают следующими недостатками: не обеспечивают многофакторную оценку устойчивости через степень риска, зависящую от важности используемых ресурсов и ценности информации; не решают оптимизационных задач по выбору способов и средств парирования НВВ при построении оценок устойчивости СИС и др.

Таким образом, актуальная практическая задача заключается в построении ЭС, позволяющей оценивать устойчивость функционирования СИС при НВВ с учетом важности ресурсов и ценности информации, а также генерировать рекомендации по ее улучшению.

В свою очередь – решаемая научная задача заключается в синтезе модели информационных процессов экспертной системы, учитывающие многофакторность условий функционирования СИС и оптимизирующие подбор СПНВВ при заданном уровне устойчивости .

Цель работы: обеспечение заданного уровня устойчивости функционирования СИС при НВВ на основе экспертной оценки риска ее нарушения и генерации рекомендаций.

Задачи исследования:

Провести анализ особенностей процесса функционирования СИС в аспекте устойчивости, построить структурную модель знаний для многофакторного оценивания устойчивости функционирования СИС.

Разработать аналитическую и процедурную модели оптимальной оценки рисков нарушения устойчивости функционирования СИС при НВВ.

Синтезировать структуру экспертной системы оптимального выбора СПНВВ, обеспечивающую требуемую устойчивость функционирования СИС. Определить механизм формирования рекомендаций обеспечения устойчивости.

Объект исследования: Процесс функционирования СИС

Предмет исследования: Модели информационных процессов в экспертной системе оценки устойчивости функционирования СИС.

Методы исследования. Для проведения исследований в работе использованы методы: теории вероятностей, нечеткой логики, информационной безопасности, системного анализа, моделирования систем.

Результаты, выносимые на защиту и их научная новизна:

Построена структурная модель знаний для многофакторного оценивания устойчивости функционирования СИС, отличающаяся учетом факторов, которые характеризуют опасность НВВ и надежность защиты применением соответствующих средств и способов защиты, важность главным образом информационных ресурсов СИС, влияющих на устойчивость функционирования СИС.

Предложена аналитическая модель оптимальной оценки уровня устойчивости функционирования СИС при НВВ, отличающаяся использованием показателей ценности информации, важности ресурсов СИС и рисков от НВВ, получаемых экспертным путём.

Предложена процедурная модель оценки факторов устойчивости функционирования СИС при НВВ, отличающаяся использованием продукционных правил определяются ценности информации путем

обработки нечетких характеристик важности ресурсов, опасности НВВ и надежности СПНВВ.

Синтезирована структура экспертной системы оптимального выбора СПНВВ, обеспечивающая требуемую устойчивость функционирования СИС, отличающаяся модулем оптимизации затрат на реализацию СПНВВ в условиях заданных НВВ.

Теоретическая и практическая значимость работы:

1. Разработанные модели являются развитием методологического аппарата исследования сетевых информационных систем функционирующих в условиях негативных воздействий и подбора эффективных средств парирования этих воздействий.

2. Полученные модели позволяют построить экспертную систему многофакторной оценки устойчивости функционирования СИС в условиях различных НВВ, оптимизировать набор СПНВВ и выработать рекомендации по обеспечению заданного уровня устойчивости.

Реализация и внедрение результатов работы. Основные результаты исследований использованы: в учебном процессе по специальности «Информационные системы и технологии» на кафедре «Информационные системы и защита информации» ФГБОУ ВПО «ТГТУ»; в научных исследованиях и разработках по оценке свойств функционирования СИС ООО «КОНУС-ИТ» (Тамбов); в методических разработках регионального учебно-научного центра по безопасности информации и для исследования СИС, функционирующих в ФГБОУ ВПО «ТГТУ».

Степень достоверности и апробация работы. Достоверность научных результатов обеспечивается полнотой системного анализа проблемы синтеза и повышения качества функционирования СИС и подтверждается корректным применением математического аппарата: теории систем, теории принятия решений, математического программирования, нечеткой математики. Для подтверждения достоверности научных выводов в работе проведена сравнительная оценка результатов, полученных с использованием

разработанных моделей, с результатами, представленными в научных исследованиях других авторов.

Основные результаты работы обсуждались на всероссийских и международных научных конференциях: «Техника и безопасность объектов уголовно-исполнительной системы - 2011» (Международная научно-практическая конференция, г. Воронеж, 2011), «Актуальные проблемы деятельности подразделений УИС» (Всероссийская научно-практическая конференция, г. Воронеж, 2013), «Математические методы и информационно-технические средства» (VIII Всероссийская научно-практическая конференция, г. Краснодар, 2012), «Прикладная математика, управление и информатика» (Всероссийская научно-практическая конференция, г. Белгород, 2012), «Наука и образование для устойчивого развития экономики, природы и общества» (Международная научно-практическая конференция, г.Тамбов, 2013), «Информатика: проблемы, методология, технологии" (XIV Международная конференция г. Воронеж, 2014); «Современные информационные технологии» (Международная научно-техническая конференция, .г. Пенза, 2014); на научных семинарах кафедр «Информационные системы и защита информации» ФГБОУ ВПО «ТГТУ», «Прикладная информатика» Тамбовского филиала Московского государственного университета культуры и искусств.

Объем и структура работы: Диссертация, общий объем которой составляет 121 страницу, состоит из введения, трех глав, заключения, списка использованной научной литературы, включающего 132 наименования научных трудов на русском и иностранных языках. Диссертация содержит 24 иллюстрации и 21 таблицу.

Работа соответствует п. 1 «Методы и модели описания, оценки, оптимизации информационных процессов и информационных ресурсов, а также средства анализа и выявления закономерностей в информационных потоках» Паспорта специальности 05.25.05 «Информационные системы и процессы».

Публикации: Результаты диссертационной работы отражены в 20 публикациях, в том числе в 4 статьях в научных журналах, рекомендованных ВАК.

Основное содержание работы.

В главе 1 «Особенности процесса функционирования сетевых информационных систем в аспекте его устойчивости» по информации из доступных научных публикаций проведен анализ состояния и перспектив развития методологического аппарата оценки уровня устойчивости функционирования СИС, путем рассмотрения таких факторов как: НВВ, эргатические (человекомашинные) звенья, ценность обрабатываемой информации в СИС, СПНВВ; обнаружены ключевые слабости методов оценки и анализа устойчивости СИС.

Проделанный анализ дал выявить цель работы и задачи исследования, решение которых даст возможность избавиться от некоторых из перечисленных недостатков.

В главе 2 «Разработка аналитической и процедурной моделей оптимальной многофакторной оценки устойчивости функционирования СИС при НВВ» предложен подход к формализации процедуры оценки устойчивости функционирования СИС при НВВ. Предложенная формализация учитывает возможные факторы, влияющие на исследуемую СИС.

Предлагаемая модель оценки свойства устойчивости, позволила сформулировать две (прямую и обратную) оптимизационные задачи по выбору СПНВВ:

Использование многофакторной оценки устойчивости функционирования СИС в условиях НВВ в качестве целевой функции оптимального выбора СПНВВ, дает основание считать эту оценку оптимальной в смысле возможности выбора лучшего варианта СПНВВ.

В главе 3 «Синтез структуры экспертной системы оптимального выбора СПНВВ и механизма формирования рекомендаций обеспечения требуемой

устойчивости функционирования СИС» представлены структура экспертной системы оптимального выбора СПНВВ, обеспечивающая требуемую устойчивость функционирования СИС, определен механизм формирования рекомендаций обеспечения устойчивости.

Экспериментальные исследования устойчивости проведены на примере СИС кафедры «Информационные системы и защита информации» ФГБОУ ВПО «ТГТУ».

В заключении сформулированы основные результаты работы, имеющие признаки научной новизны и практической значимости.

Полученные результаты могут быть рекомендованы к использованию в системах требующих оптимизации средств защиты от НВВ, обеспечивающих требуемый уровень устойчивости функционирования СИС.

1. Особенности процесса функционирования сетевых информационных систем в аспекте его устойчивости

В современном обществе информационные технологии применяются во всех сферах общественной деятельности, обучении, производстве. Появление и активное развитие средств передачи данных открыло для пользователей цифровых устройств новые возможности оперативного обмена информацией. Устойчивость функционирования информационных систем (ИС) напрямую влияет на развитие страны во всех сферах, поскольку на их основе строится единая информационная среда, объединяющая информационные системы различной степени, автоматизированные и телекоммуникационные системы, сетевые информационные системы и т.д.

В источниках [1-22] отмечается, что задача обеспечения устойчивого функционирования ИС входит в число важнейших задач, так как функционирование ИС непосредственно влияет на состояние экономической, оборонной и политической составляющих безопасности Государств.

Под информационной системой (ИС) понимается программно-аппаратная система, состоящая из человеко-машинных (эргатических) звеньев, технических и аппаратных средств, а также программного обеспечения. Объединяя несколько ИС в локальную вычислительную сеть, образуется сетевая информационная система (СИС), используемая для поиска, сбора, хранения, обработки и передачи информации. СИС объединяют в единую информационную среду территориально удаленных поставщиков и потребителей информации.

СИС могут подвергаться вредным внешним воздействиям, которые оказывают соответствующее влияние и обладают недетерминированностью, неопределенностью и способны снизить устойчивость функционирования СИС. К инфраструктуре СИС относят: персональные компьютеры, серверное и сетевое оборудование, системное и сетевое программное обеспечение,

другие периферийные устройства, необходимые для функционирования ИС, а также средства связи, обслуживающий персонал, служебные помещения.

Устойчивостью функционирования СИС при негативных внешних воздействиях (НВВ) является ее способность исполнять возложенные функции с требуемыми параметрами качества при НВВ. Система будет считаться устойчивой по отношению к ряду НВВ, если её общий уровень устойчивости входит в интервал заданного значения качества.

Задача обеспечения устойчивого функционирования СИС напрямую связана с противодействием различным внешним вредным воздействиям, которые могут оказывать вредное влияние на функционирование СИС. Анализ проблемы отрицательного влияния различных воздействий извне на устойчивость функционирования СИС и обеспечение защиты СИС, а также содержащейся в ней информации от НВВ во многом связны между собой. При этом необходимо отличать понятия устойчивости и информационной безопасности, так как они связаны с задачами синтеза и анализа СИС.

Информационная безопасность – это степень защищенности информации и поддерживающей ее инфраструктуры от любых злонамеренных или случайных воздействий. Задачами информационной безопасности является минимизация ущерба, а также предотвращение и прогнозирование такого рода воздействий [66,79,81,87,88,98,101,103,104]. Информационная безопасностью АС – это такое состояние системы, при котором она противостоит вредным внешним и внутренним воздействиям, но в то же время ее функционирование не создает информационных угроз для элементов самой системы и внешней среды [65].

Согласно [64], под устойчивостью функционирования СИС понимается степень адекватности реализованных в ней механизмов обеспечения защиты существующим в данной среде функционирования рискам, связанным с нанесением вреда вредными внешними воздействиями.

Живучесть СИС – свойство системы сохранять способность выполнения требуемых функций в условиях воздействия внешних дестабилизирующих

факторов, а также способность ликвидировать последствия НВВ и возвращаться работоспособности требуемой степени. Для этого система использует избыточные ресурсы системы. Авторы публикаций, приведенных в [22-43,45-63] определяют надежность и стойкость сетевой структуры или ее отдельных компонентов как главные характеристики живучести системы.

Внедрение информационных технологий во многие сферы общественной деятельности, появление сложного программного и аппаратного обеспечения, усложнение структуры сетевых информационных систем (СИС) и существование неограниченного количества вредных внешних воздействий, способных снизить уровень устойчивости функционирования СИС, - все это может привести к нарушению функционирования СИС при НВВ. Цена такого нарушения, особенно в финансовой деятельности крайне высока и может достигать нескольких сот тысяч долларов. Примеров потерь и даже финансового краха в банках и в корпоративных сетях из-за нарушения функционирования достаточно много. По результатам исследований организации *Infonetics*, в среднем количество сбоев в ЛВС США равно 23,6 в год, среднее время их устранения - около 5 часов, а потери владельца сети составляют до 50 тыс. $ в час.

Хотя компьютерные средства и информационные технологии интенсивно развиваются, рост уровня защиты с помощью программных и аппаратных средств, свести уязвимость современных ИС в СИС к нулю не удается. Поэтому проблемы обеспечения устойчивости функционирования СИС остаются актуальными как среди специалистов в области информационных систем и сетей, так и многочисленных пользователей, в том числе компаний, работающих в разных сферах экономики.

В настоящее время существует неизвестное число НВВ, которые оказывают влияние на устойчивость функционирования СИС. НВВ разделяют на внешние и внутренние в зависимости от их источников относительно системы, на которую они воздействуют. Примером НВВ является несанкционированное проникновение в СИС, *DOS*-атаки (сокр. от

англ. *DenialOfService* - «отказ в обслуживании») [88]. Поэтому при проектировании и разработке любой современной информационной системы невозможно обойтись без реализации некоторых механизмов парирования вредных внешних воздействий (МПНВВ) для обеспечения целостности, доступности и конфиденциальной информации, а также обеспечения устойчивости функционирования самой системы при НВВ.

Основным фактором при принятии решения об обеспечении необходимой степени устойчивости функционирования СИС является ценность обрабатываемой в системе информации. Также существуют другие факторы, влияющие на определение требуемой степени функционирования СИС: важность объектов (и ресурсов) системы, доступность, целостность и конфиденциальной информации, обрабатываемой в системе. Поэтому необходимо точно разграничивать все возможные НВВ в условиях неопределенности.

Стабильное функционирование СИС – неотъемлемая часть современной жизни, а потому требования к стабильному и качественному доступу к информации в обществе чрезвычайно высоки. Например, в условиях рыночной экономики особое значение приобретают достоверность и полнота информации, без которых невозможна маркетинговая, финансовая и инвестиционная деятельность [66].

Согласно [66], проблема обеспечения функционирования СИС при НВВ обусловлена следующими факторами:

– темпы развития информационных систем значительно опережают темпы развития средств парирования вредных внешних воздействий (СПНВВ);

– значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью персональных компьютеров и других средств автоматизации;

– резкое увеличение круга пользователей, имеющих непосредственный доступ к данным и вычислительным ресурсам;

– бурное развитие глобальной сети Интернет, через которую осуществляется передача больших объемов информации, чаще всего без обеспечения требуемой степени обеспечения защиты;

– появление новых способов накопления, обработки и передачи информации, способствующие возникновению новых НВВ, связанных с возможностью потери, искажения и раскрытия данных, адресованных или принадлежащих конечным пользователям.

Проблема обеспечения устойчивости функционирования СИС при вредных внешних воздействиях является многоплановой и комплексной и охватывает ряд важных задач. Тем не менее, она отличается от других проблем этой области тем, что средства борьбы с ними носят наиболее высокотехнологичный и максимально динамичный характер. Это легко объяснимо: от устойчивости функционирования СИС зависит финансовое благополучие физических и юридических лиц, государственные тайны, персональные данные граждан, управляемость и независимость страны в целом.

В этой главе рассматриваются и анализируются основные факторы, влияющие на устойчивость функционирования СИС (вредные внешние воздействия, способы и средства парирования НВВ, необходимые качества обрабатываемой информации в СИС, ее свойства), а также основные существующие интеллектуальные информационные (экспертные) системы, предназначенные для оценки анализа устойчивости функционирования СИС при НВВ.

1.1 Обзор подходов к оценке уровня устойчивости функционирования систем

В настоящее время не существует единого стандарта проведения оценки устойчивости функционирования СИС. Поэтому процессы анализа устойчивости СИС часто существенно отличаются друг от друга в разных странах.

На основе данных источников [67-71] были рассмотрены подходы к определению защищенности СИС. В этих публикациях к основным факторам, влияющим на оценку устойчивости функционирования СИС, авторы относят:

1. Частоту реализации внешнего воздействия, которая зависит от значений параметров «защищенность ресурса» и «потенциал злоумышленника».

2. Качественный показатель ущерба, зависящий от таких параметров, как значимость ресурса и частота реализации вредных внешних воздействий на этот ресурс.

3. Оценку опасности способом экспертных оценок.

4. Вероятность преодоления механизма обеспечения защиты от НВВ.

5. Оценку риска причинения ущерба, зависящего от влияния НВВ (величины ущерба от одной реализации НВВ, их количества, значения вероятности нанесения ущерба от одной реализации НВВ).

К основным недостаткам существующих способов оценки устойчивости функционирования СИС относят:

– значительные различия оценок опасности НВВ для разных систем, в зависимости от типа исследуемой системы, ее значимости, а также ценности обрабатываемой в ней информации;

– отсутствие учета важности ресурсов СИС;

– использование только экспертных оценок при проведении оценки показателей устойчивости и отсутствие учета влияния элементов СИС друг на друга.

Также существует ряд количественных и качественных [71,72] подходов к оценке устойчивости функционирования СИС. Качественная оценка устойчивости функционирования СИС, в отличие от количественной оценки, не позволяет получать точные значения показателей устойчивости функционирования, однако дает возможность разделять СИС по степени устойчивости функционирования и сравнивать их между собой.

1.2 Влияние фактора значимости информации обрабатываемой в СИС

При анализе и проектировании МПНВВ и СПНВВ с целью обеспечения устойчивости функционирования СИС, которые направлены на обеспечение защиты системы и обрабатываемой в ней информации от нарушения ее физической, логической целостности, необходимо иметь представление о характере самой информации и определить ее ценность, для того чтобы определить требуемая степень качества функционирования СИС.

Автор [66] отмечает, что для получения наилучшей эффективности МПНВВ должны обеспечить защищенность информации в соответствии с ее ценностью, а также важностью ресурсов ИС, где она обрабатывается. Поэтому при разработке МПНВВ вне зависимости от типа информации, количественная оценка ценности информации не всегда позволяет оценить и обосновать необходимые затраты на построение МПНВВ.

Ценность информации зависит от того, насколько она актуальна и важна для решения конкретной задачи, а также от того, насколько в дальнейшем она найдет применение в каких-либо видах деятельности человека. В современной теории информации понятие ценности информации, как само понятие информации, не имеет строгого формального определения, что затрудняет определение необходимых и достаточных уровней МПНВВ [75,116].

Поэтому считается целесообразным диссертационной работе рассмотреть возможность построения экспертной системы (ЭС) для проведения оценки ценности информации. При построении такой ЭС, во-первых, необходимо провести классификацию систем обработки, хранения и передачи информации по типу информации, подлежащей защите.

Авторы публикаций, приведенных в [66,72,108] разделяют подлежащую защите информацию по трем характеристикам: по принадлежности, по степени конфиденциальности (степени ограничения доступа) и по содержанию.

Автором в [73] предложены такие основания разделения информации по типам тайны, как:

– области деятельности, в которых может быть информация, являющаяся данным видом тайны;

– владельцы информации (они могут частично пересекаться);

– на кого возложено обеспечение защиты данного вида тайны (по некоторым видам тайны возможно пересечение).

Стоит отметить, что отсутствует единая классификация информации, но нам необходимо выбрать одну систему разделения информации на классы, которая должна охватывать наиболее значимые области человеческой деятельности. В данной работе будем использовать разделение по классам информации по типу ее содержания:

1 – политическая, 2 – научно-техническая, 3 – военная,

4 – технологическая, 5 – коммерческая, 6 – деловая,

7 – экономическая.

Очевидно, что все перечисленные типы информации в большинстве случаев имеют неодинаковые оценки важности.

Методика, предложенная для экспертной системы по оценке важности информации, которая описывается в главе два, учитывает главные аспекты, влияющие на важность информации:

– упорядочение по важности различных типов информации;

– постановка в соответствие каждому типу информации некоторой оценки в виде интервала.

Экспертная система позволяет учесть аспекты существенности информации, вероятности негативного воздействия и экономические расходы на восстановление информации, для оценки важность информации.

В представленной ЭС самой ценной информацией является та, которая наиболее востребована (государством, предприятием, общественной организацией, гражданином и т.д.), и ущербы из-за уничтожения, изменения, неавторизированного доступа.

1.3 Влияние негативных воздействий на устойчивость функционирования СИС

1.3.1. Содержание термина негативные воздействия и их классификация

Негативное внешние воздействие – это неблагоприятные воздействия, оказывающие влияние на систему, которые способны понизить степень устойчивости СИС или нарушить свойств информации, обрабатываемой в системе (целостность, конфиденциальность и доступность), их не стоит путать с теми воздействиями, которые вызваны конфликтами внутри СИС.

К указанным внешним воздействиям относят воздействие компьютерных вирусов, атак хакеров, а также действия пользователей СИС, приводящие к нарушению функционирования и др. Стоит отметить, что в данной работе НВВ разделяются на внешние и внутренние, в зависимости от положения их источников относительно системы, на которую они оказывают воздействие.

При выборе СПНВВ прежде всего необходимо определить и классифицировать возможные НВВ, направленные на систему.

Обеспечение достаточного уровня устойчивости функционирования сетевой информационной системы, а также защиты от возможных видов негативных воздействий и ущерба от них (при нарушении Д, К, Ц информации) любых субъектов – конечная цель создания МПНВВ по мнению многих авторов [76-78,101,108].

Тенденции последнего времени в области обработки, передачи и накопления информации значительно повлияли на рынок услуг по исследованию методов и способов оказания неблагоприятных воздействий, направленных на искажение, раскрытие или уничтожение информации.

Какое-либо возможное деяние (действие/бездействие), направленное на информационный ресурс и приводящее к потере, искажению или раскрытию информации (то есть наносящее ущерб пользователю или собственнику) называется НВВ [66,100].

С момента создания СИС появилась проблема нарушения ее устойчивости и как следствие многие специалисты пытались создать классификацию негативных воздействий. Классифицировали как источники, так и сами НВВ, что послужило бы подспорьем в дальнейшей стандартизации средств и методов противодействия.

Для определения полного набора требований к разрабатываемому МПНВВ важными задачами являются:

– определение и классификация НВВ;

– определение возможных реализаций НВВ и вероятность их реализаций;

– моделирование нарушителя.

Многие авторы, такие как [65,79-86,99,108], отмечают, что есть множество подходов и параметров разделения НВВ на классы, но единая система разделения на классы отсутствует. Делят на классы НВВ по многим параметрам (по природе возникновения, источнику, положению источника, степени воздействия, цели воздействия, способу доступа к ресурсам т.д.) как показано в таблице 1.1 [86], каждый из параметров классификации отражает одно из обобщенных требований к системе защиты.

Во второй главе проводится формализация процесса описания вредных внешних воздействий, поэтому необходимо в первую очередь выбрать несколько параметров классификации НВВ, под которые подходит любое воздействие. При этом должны выполняться следующие утверждения:

1. Любое НВВ должно быть классифицировано как минимум по одному параметру.

2. Классификация НВВ должна позволять оценить устойчивость функционирования СИС в случае внутренних и внешних воздействиях отдельно.

Таблица 1.1 – Общий классификатор негативных внешних воздействий

Классификационный признак	Содержание классификатора
По источнику ВВ	Внешние, внутренние
По цели воздействия	Нарушение конфиденциальности, Нарушение доступности, Нарушение целостности
По принципу воздействия	Использование существующих (штатных)каналов доступа, Использование скрытых существующих каналов доступа, Формирование основных каналов доступа.
По способу воздействия	Нарушение структур данных, Нарушение текстов, объектных и загрузочных кодов программ, Нарушение функций общего программного обеспечения, Нарушения функции системного программного обеспечения.
По характеру воздействия	Активное воздействие (нарушение, искажение, разрушение), Пассивное воздействие (сбор информации, наблюдения ,анализ)
По объектам и субъектам воздействия	Подразделения Предприятия, Внешние абоненты, Обслуживающий персонал.
По средствам воздействия	Несанкционированный доступ(НСД), Воздействие компьютерными вирусами, Специальное программно-техническое воздействие (СПТВ), Проявление недекларированных возможностей, Имитовоздействие на информацию. Сбои и отказы в программах и техническом оборудовании КИС, ошибки оператора(появление дефектов) .
По используемой ошибке	Ошибки в организационно-технических мероприятиях, ошибки в проекте МПНВВ; Ошибки в выборе средств защиты информации; Недостаточное качество средств защиты; Ошибки в работе администратора локальной сети, администратора безопасности информации,; Ошибки в работе автоматизированных рабочих мест (АРМ); Ошибки и/или недекларированные возможности в алгоритмах и программах; Ошибки в структурах данных (использование избыточных, ложных или искаженных данных); Ошибки сертификационных испытаний.
По состоянию нарушаемых технологических процессов	Сбор, прием, передача данных, обмен информацией; Осуществление информационно-вычислительного процесса; Запись, считывание, хранение информации в базе данных.
По типу нарушения (нарушение конфиденциальности информации)	Персональные данные, Коммерческая тайна, Профессиональная тайна.
По типу воздействия	Программное, Програмнно-техническое, Техническое, ПЭМИН (радиоперехват и радиоэлектронное подавление).
По потенциальному ущербу	Низкий ущерб (несущественный, на этапе административных решений); Средний ущерб (требует материальных затрат); Высокий ущерб (значительный материальный ущерб),; Катастрофический ущерб (ущерб на уровне затрат, приводящих к корректировке расходования бюджетных средств государства)

Окончание таблицы 1.1

По соответствию требованиям к средствам защиты информации	Классы защищенности для АС; Классы защищенности для средств вычислительной техники (СВТ); Классы защищенности для межсетевых экранов; Классы защищенности для антивирусных средств; Классы по контролю отсутствия недекларированных возможностей.
По сценариям воздействия субъекта доступа	Внешний злоумышленник, Санкционированный пользователь, Санкционированный абонент удаленного доступа, Зарегистрированный пользователь внешней системы, Администратор АС, Администратор безопасности информации, Программист-разработчик.
По этапам жизненного цикла системы	Технологические угрозы, Эксплуатационные угрозы.
По характеру возникновения	Непреднамеренные воздействия, Преднамеренные воздействия.
По виду совершенного компьютерного преступления.	Неправомерный доступ к компьютерной информации, Создание, использование и распространение вредоносных программ, Нарушение правил эксплуатации СВТ,АС.

3. Выбранный параметр должен описывать человеческие, технологические и стихийные НВВ.

Проведя анализ перечисленных параметров классификации НВВ и рассмотрев требования к описанию процесса исследования оценки устойчивости функционирования СИС, было выбрано несколько параметров классификаций, позволяющих полно описывать любое возможное НВВ как показано на рисунке 1.1. Для описания НВВ необходимо рассматривать все выбранные параметры и важность каждого из них.

В зависимости от положения их источников относительно системы, на которую они влияют, НВВ разделяют на внутренние и внешние.

Поэтому в этой части данной научной работы актуально рассматривать классификацию источников НВВ (внешние и внутренние), цель НВВ с точки зрения нарушения следующих аспектов: доступности, конфиденциальности и целостности и множество антропогенных, техногенных и стихийных источников НВВ для описания любого возможного НВВ.

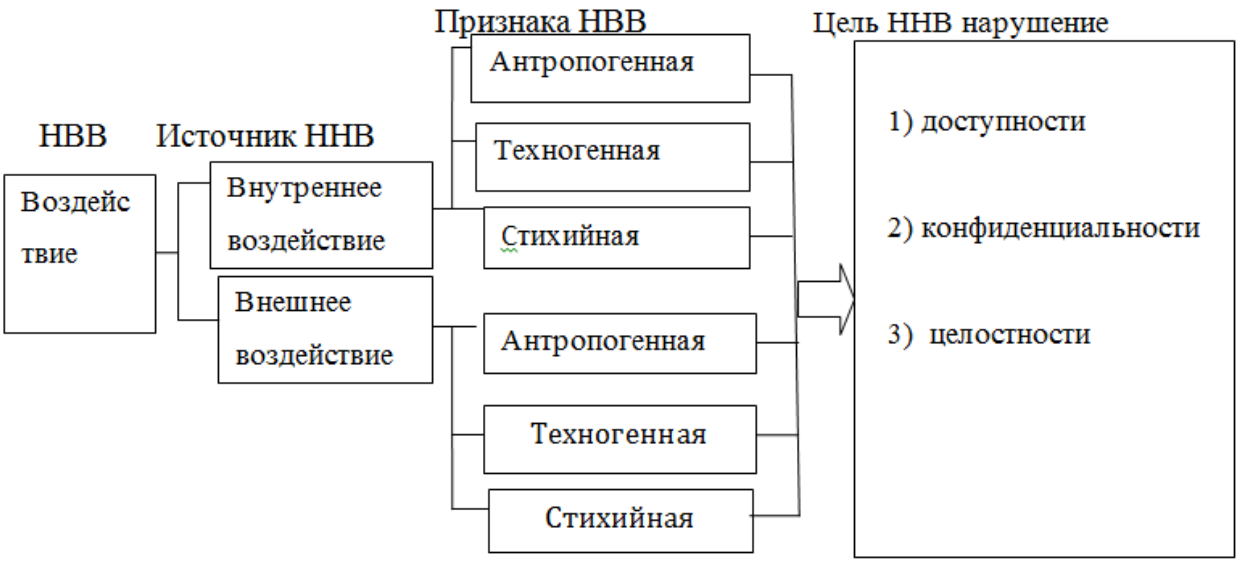

Рисунок 1.1 – Предлагаемая классификация возможных негативных внешних воздействий

1.3.2. Цели нарушения устойчивости функционирования СИС

Считается, что НВВ связано с определенной целью нарушения устойчивости СИС (нарушение доступности, целостности или конфиденциальности), а также иметь одну или несколько целей нарушения. Авторы публикаций, приведенных в [66.86.108] выделяют следующие цели нарушения:

1. Нарушения целостности информации. Под целостностью понимают свойство информации сохранять свою структуру и/или содержание в процессе передачи или хранения [79].

Нарушение целостности – это частичная, а возможно даже и полная потеря целостности, компрометация, дезинформация. Авторы публикаций, приведенных в [66,79] отмечают, что такие НВВ предназначены в основном для информационных систем с сетевой структурой, и информация способна потерять свою ценность или даже быть утрачена при ее несанкционированной модификации или даже удалении, но при это не следует путать это с изменениями, выполняемыми администраторы или полномочные лица.

2. Нарушения конфиденциальности информации. Конфиденциальностью информации является свойство информации, которое указывает на востребованность ограничений на круг людей, обладающих доступом к данной информации, и характеризующее способность системы сохранять указанную информацию втайне от людей, не обладающих правом доступа к ней [65]. НВВ нарушения конфиденциальности – это НВВ, направленные на разглашение информации, которая является в той или иной степени секретной.

3. Нарушения доступности информации. Доступность информации — это характеристика системы, в которой происходит циркуляция информации, характеризующейся возможностью предоставить в приемлемое время доступ к нужной информации и подготовленность соответствующих автоматических служб к обработке поступающих запросов [65,86].

Авторы публикаций, приведенных в [65,66,79,98-101] понимают под нарушением доступа ситуацию, когда НВВ снижают работоспособность системы или блокируют доступ (частично или полно) к некоторым ресурсам компьютерной системы.

1.3.3. Источники возникновения негативных внешних воздействий

Авторы публикаций, приведенных в [65,87-89], указывают на то, что эффективно можно блокировать НВВ, если есть информация об их источниках и цели, для достижения которой они применены к ресурсам информационной системы. Обнаружено, что раскрытие любого преступления, связанного с нарушением целостности, конфиденциальности и доступности, стоит начинать с поиска ответа на вопрос «кому это выгодно?».

Стоит указать, что для нанесения ущерба направленного на ухудшение устойчивости работы СИС, как и для получения выгоды, источники НВВ могут пользоваться слабостями самих систем. Кроме того, возможно незлонамеренные действия со стороны источников НВВ по активации тех или иных уязвимостей, наносящих вред. Поэтому необходимо

классифицировать источники и последствия реализации НВВ, рассмотреть человеческий фактор как источник воздействия, оказывающий влияние на устойчивость функционирования СИС.

1.3.4. Классификация источников негативных внешних воздействий

В качестве источников НВВ могут выступать как субъекты (личность), так и объективные проявления [66,79,86,88,90]. При этом, источники НВВ могут находиться как внутри организации - внутренние источники, так и за ее пределами - внешние источники. Помимо этого, актуально деление источников на субъективные и объективные. Субъективные воздействия зависят от действий пользователей (сотрудников) и чаще всего устраняются программно-аппаратными способами. Объективные уязвимости зависят от нюансов построения и технических характеристик оборудования, применяемого на защищаемом объекте. Влияние таких уязвимостей можно ослабить с помощью технических и инженерно-технических СПНВВ, но полное устранение таких уязвимостей невозможно.

При изучении возможных вредных внешних воздействий на СИС для определения политики МПНВВ, необходимо проводить разделение источников НВВ на внутренние и внешние источники, так как при выборе способов и средств парирования вредных внешних воздействий их можно разделить на СПНВВ от внутренних или от внешних воздействий. Такая классификация позволяет проводить оценку устойчивости функционирования СИС от внутренних НВВ отдельно от остальных воздействий.

Общей классификацией источников НВВ согласно [65,79-81,86,90,101,108] является следующая классификация:

1. Антропогенные источники НВВ (обусловлены действиями субъекта).
2. Техногенные источники НВВ (обусловлены техническими средствами).
3. Стихийные источники НВВ.

Под антропогенными источниками НВВ понимаются субъекты, действия которых могут повлечь за собой умышленное или непреднамеренное воздействие на СИС. В качестве антропогенных источников можно рассматривать весь персонал СИС (имеющий санкционированный доступ) и посторонних лиц (несанкционированный доступ). Необходимо отметить, что источники НВВ (субъекты, действия которых могут быть привести к снижению степени устойчивости функционирования СИС) могут быть как внешние, так и внутренние. Поэтому при рассмотрении антропогенных источников актуально рассматривать модель нарушителя и делить на внутренних и внешних нарушителей.

К техногенным источникам НВВ относят технические средства программно-аппаратного комплекса, в том числе отказы и сбои оборудования, ошибки программного обеспечения, сбои электропитания и др. Нужно уточнить, что данные источники НВВ являются зависимыми от характеристик техники и в большинстве случаев выступают внешними.

Для СИС стихийные источники в большинстве случаев выступают в роли внешних. Можно выделить среди стихийных (естественных) источников НВВ такие как: ураганы, пожары, землетрясения, бури, наводнения.

Сбор информации о противнике является приоритетным при создании МПНВВ, так как дает ключевой первичный материал, необходимый для разработки достаточно эффективной системы противодействия [66,87].

Мнение, что главной опасностью для СИС являются внешние субъекты, действующие снаружи, хоть и широко распространено является неправильным. Как показывает Статистика: внутренние пользователи порождают больше всего опасность. Как показывают исследования: 70-80% из нарушений в корпоративной среде происходят по вине внутренних пользователей. Данные *PricewaterhouseCoopers* показывают, что 33% источников НВВ - работники, 28% - бывшие работники [66,88]. Из этого

следует повышенная актуальность эксплуатации СПНВВ от внутренних пользователей СИС и делает эту задачу центральной для специалистов, относящихся к области информационных технологий и защиты информации.

Автор [88] уделяет внимание внутренним НВВ и отмечает, что в любой организации существуют люди, которые имеют доступ к конфиденциальной информации и могут передать ее другим лицам или исказить ее (случайно или преднамеренно). Также автор отмечает, что проблема внутренних НВВ в крупных компаниях с распределенной информационной инфраструктурой состоит в том, что с ростом количества сотрудников и вычислительной техники вероятность совершения утечки возрастает.

Большинство субъектов СИС нарушают функционирование и правила использования СИС (умышленно или случайно), используя права доступа к ресурсам СИС. Удалить влияние вредных внешних воздействий от субъектов СИС можно через правила разграничения доступа к ее ресурсам.

Авторы публикаций, приведенных в [88,91] отмечают, что чаще всего причинами нарушения устойчивости функционирования СИС являются: любопытство, месть руководству компании, работа на компанию-конкурента, а также автор приводит примерный список персонала типичной корпоративной сети и соответствующих степеней риска от каждого из них таблица 1.2.

Стоит отметить, что способы воздействия субъектов СИС разделяют на внешние и внутренние. Пример такого деления представлен на рисунке 1.2. Чаще всего активные способы воздействия вносят изменения в СИС, поэтому их легче обнаружить.

Также необходимо помнить, что негативно на устойчивость СИС могут воздействовать посторонние лица. Например, посетители, конкуренты, бывшие сотрудники, хакеры и другие. К внешним преднамеренным НВВ можно отнести НВВ, исходящие из сетевого окружения, в том числе глобальной сети Интернет.

Таблица 1.2 – Уровни риска от персонала в типичной корпоративной сети

Наибольший риск	Повышенный риск	Средний риск	Ограниченный риск	Низкий риск
Администратор безопасности; Сетевой администратор;	менеджер обработки; оператор системы; системный программист; оператор ввода подготовки данных;	менеджер программного обеспечения; инженер системы;	инженер по оборудованию; инженер или оператор по связи; оператор периферийного оборудования; пользователь-операционист; прикладной программист; администратор баз данных; библиотекарь системных магнитных носителей; пользователь-программист;	библиотекарь магнитных носителей пользователей; инженер по периферийному оборудованию; пользователь сети.

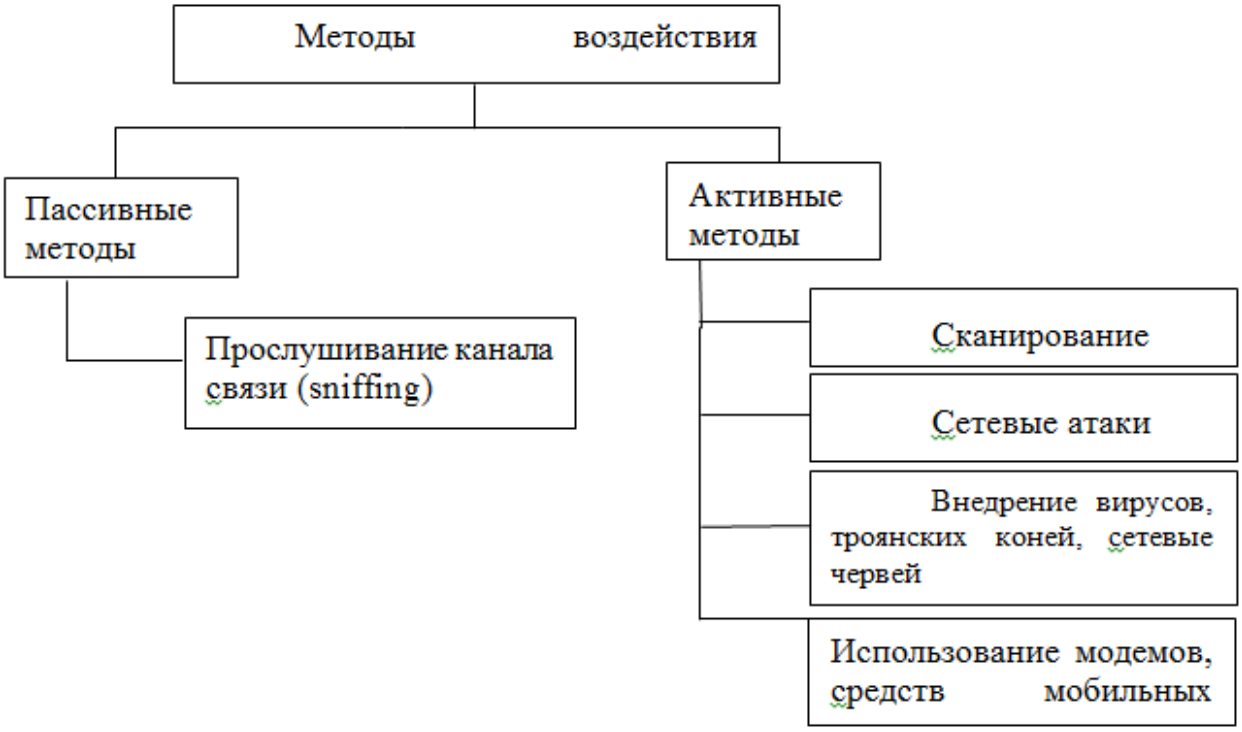

Рисунок 1.2 – Методы негативных воздействий субъектов СИС [88]

При изучении устойчивости функционирования СИС необходимо уделять большое внимание субъектам СИС. Во-первых, они имеют более выгодное положение, чем другие, поскольку уже обладают информацией *о* СИС (о сотрудниках, инфраструктуре и др.). Во-вторых, согласно статистике, большинство случаев нарушения функционирования СИС исходит изнутри системы. Согласно данным национального института стандартов и технологии США (*NIST*), наиболее частые случаи нарушения устойчивости функционирования ИС - 4% - вирусы, ошибки пользователей и персонала (55%),10% - нечестные сотрудники, 6% - обиженные сотрудники, 15% - проблемы физически стабильного функционирования и только 10% случаев - атаки извне [88].

1.4 Средства парирования негативных внешних воздействий

Состояние сетевой информационной системы, в котором ее функционирование не формирует опасность выхода из строя элементов этой системы, а так же в котором система успешно противодействует негативным воздействиям называется устойчивостью функционирования СИС. Устойчивостью функционирования сетевых информационных систем при НВВ является ее способность исполнять возложенные функции с требуемыми параметрами качества при НВВ. Система будет считаться устойчивой по отношению к ряду НВВ, если её общий уровень устойчивости входит в интервал заданного значения качества.

Основная проблема систем типа СИС или АСОИ – обеспечение устойчивости функционирования, так как основной деятельностью этих типов систем является хранение, обработка, выдача, передача и сбор информации. Защита всех компонентов сетевой информационной системы (персонала, данных и программно-аппаратного комплекса), то есть противодействие всем возможным вторжениям в процесс работы СИС есть, не что иное как, процесс обеспечения устойчивости функционирования СИС при НВВ.

Авторы публикаций, приведенных в [66,79,92] отмечают, что есть два подхода для обеспечения устойчивости стабильного функционирования СИС (таблица 1.3): фрагментарный и комплексный

Таблица 1.3 – Подходы обеспечения устойчивости

	Фрагментарный	Комплексный
Описание	направлен на противодействие четко определенным НВВ в заданных условиях	ориентирован на создание защищенной среды обработки информации в СИС, объединяющей в единый комплекс разнородные меры противодействия НВВ.
Достоинства	высокая избирательность к конкретному НВВ.	организация защищенной среды обработки информации позволяет гарантировать определенный степень устойчивости СИС
Недостатки	-отсутствие единой защищенной среды обработки информации, -небольшое видоизменение НВВ ведет к потере эффективности	- ограничения на свободу действий пользователей СИС, -большая чувствительность к ошибкам установки и настройки СПНВВ, -сложность управления.
Пример	указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т.п.	

Многие государственные и коммерческие предприятия строят собственные подходы к обеспечению требуемого уровня устойчивости сетевых информационных систем на основе комплексного подхода, то есть решение в рамках одной программы комплекса частных задач [66]. Подход, в основе которого лежит интеграция множества подсистем обеспечения заданного уровня устойчивости от НВВ (интегральный подход), представляет собой наиболее полную форму комплексного подхода.

Оценка устойчивости функционирования СИС основывается, в том числе, на оценке обеспечения защиты информации, поскольку обработка, сохранение и передача информации является конечной целью АСОИ и СИС.

Для достижения максимальной устойчивости СИС необходимо парировать НВВ, направленные на инфраструктуру СИС и на обрабатываемую в них информацию. Авторы публикаций, приведенных в [82-84,93,108] выделяют следующие основные способы обеспечения устойчивости функционирования СИС при негативных внешних воздействиях:

1.Организационные (административные). Организационные мероприятия охватывают все структурные элементы аппаратуры на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

Организационные меры могут предусматривать:

– Ограничение круга лиц, имеющих доступ в помещения, где происходит обработка конфиденциальной информации.

– Определение списка должностных лиц, которые имеют допуск для выполнения служебных обязанностей по обработке конфиденциальной информации.

– Ограничение физического доступа к архивам и папкам, где хранится ценная информация.

– Исключение просмотра посторонними лицами содержания обрабатываемой информации путем установки дисплея, клавиатуры и принтера соответствующим образом.

– Использование отдельных компьютеров для хранения и обработки информации различной степени конфиденциальности.

– Хранение магнитных и прочих съемных носителей, в том числе содержащих секретную, конфиденциальную информацию, в тщательно закрытых прочных шкафах.

- Уничтожение красящих лент и других материалов, содержащих фрагменты ценной информации. Использование приборов для уничтожения бумаги.

– Обязательное подписание операторами договора о неразглашении информации.

2. Организационно-технические меры предполагают:

– Использование средств контроля доступа к информационным ресурсам.

– Применения средств низкоуровневого форматирования для уничтожения информации с устройств хранения данных.

– Использование стабилизаторов напряжения и источников бесперебойного питания для обеспечения стабильного электрического питания компьютера.

– Отключение от локальной сети или сети удаленного доступа компьютера, обрабатывающего конфиденциальную информацию.

– Уничтожение информации непосредственно после ее использования.

3. Технические средства представляют собой механические, электрические, электромеханические и электронные устройства, предназначенные для предотвращения вредных внешних воздействий, возможных на путях проникновения и доступа потенциального нарушителя к компонентам защиты. Вся совокупность технических средств делится на аппаратные и физические.

4. Программные средства представляют собой специальное программное обеспечение, предназначенное для выполнения функций парирования НВВ. К данному классу СПНВВ относятся: криптографические, антивирусные средства, межсетевые экраны, системы обнаружения вторжений, системы разграничения доступа и т.п.

5. Законодательные (правовые). Законодательные меры определяются законодательными актами государства. Применительно к Российской Федерации к ним относятся: Конституция, законы Российской Федерации, указы Президента Российской Федерации, доктрина информационной безопасности Российской Федерации, кодексы Российской Федерации, постановления Правительства Российской Федерации, государственные стандарты обеспечения защиты информации Российской Федерации и прочие руководящие документы. Они регламентируют правила обработки и

передачи информации с ограниченным доступом и устанавливают меры ответственности за их нарушение.

1.5 Способы оценки вероятного ущерба в сетевых информационных системах

В настоящее время для оценки устойчивости функционирования СИС не существует специальных инструментальных средств, однако широко распространены интеллектуальные системы для оценки риска и защищенности информации, обрабатываемой в СИС. Примерами таких систем, получивших определенную известность, являются *COBRA* (Великобритания), «АванГард» (Россия), ТРИФ (Россия), КОНДОР+ (Россия), *RiskWatch*(США), *CRAMM* (Великобритания), *RASoftwaerTOOL* (Великобритания) и ряд других. Ввиду того, что каждый из перечисленных программных продуктов основываются на собственных способах и подходах к анализу рисков, а также собственных вариантах решения поставленных задач, они имеют как преимущества, так и ряд недостатков. В соответствии с международным стандартом безопасности *IS*O17799:2005 (представлен *ISO* (*the International Organization for Standardization*) и *IE*C (*the International Electro technical* C*ommission*)) представлено большинство инструментальных средств [94,97].

Службой безопасности Соединённого Королевства, по заданию правительства Ее Величества, был разработан и принят в качестве государственного стандарта метод *CRAMM* (*the UK Government Risk Analysis and Management Method*) [95,97].

ПО *CRAMM* сочетает в себе качественные и детерминированные способы оценки возможных негативных воздействий, то есть использует комплексный подход. При этом существует две базы знаний, одна из которых имеет коммерческую направленность и может быть использована, как крупными, так и небольшими предприятиями, вторая – правительственный профиль.

Согласно методике *CRAMM*, для каждого этапа определяется набор исходных данных, последовательность мероприятий, анкеты для проведения интервью, списки проверки и набор отчетных документов. В первый этап исследования входит идентификация и определение ценности защищаемых ресурсов (создается: модель ресурсов; готовится отчет по первому этапу оценки рисков, в котором суммируются полученные результаты этого этапа). На втором этапе производится оценка, анализ возможных вредных внешних воздействий и уязвимостей. На третьем этапе производится выбор адекватных контрмер, готовятся отчеты детальной оценки безопасности; оценка стоимости рекомендуемых контрмер. К недостаткам способа *CRAMM* можно отнести:

– аудит по способу *CRAMM* – процесс достаточно трудоемкий и может потребовать достаточно длительной работы аудитора;

– способ требует от аудитора специальную подготовку и высокую квалификацию;

– программный набор *CRAMM* создает много документации в печатной форме, которая в большинстве случаев неполезна на практике;

– *CRAMM* не поддерживает создание собственных шаблонов отчетов;

–*CRAMM* скорее предназначен для аудита уже существующих ИС, находящихся в эксплуатации, а не для ИС, которые только разрабатываются;

– *CRAMM* пользователи не могут дополнять базу знаний, что осложняет адаптацию к потребностям организации;

–*CRAMM* не локализован, работает на английском языке и обладает существенной стоимостью лицензии - от 2000 до 5000 долл. [94,96].

Достоинствами *CRAMM* являются: применение технологии оценки НВВ и уязвимостей по косвенным факторам с возможностью верификации результатов, удобная система для создания моделей информационной системы с точки зрения безопасности, большой объем базы знаний по контрмерам. Он позволяет весьма детально оценить риски и различные варианты контрмер [97].

Программное обеспечение *RiskWatch* американской компании *Riskwatch International* является мощным средством анализа и управления рисками (*risk assessment solutions*). Компания *RiskWatch* предоставляет программные продукты для проведения различных видов аудита безопасности (*security risk assessments*). Они включают в себя следующие средства аудита и оценки рисков: *RiskWatch for Physical Security* - для физических способов обеспечения защиты ИС; *RiskWatch for Information Systems* - для информационных рисков; *HLPAA-WATCH for Healthcare Industry* - для оценки соответствия требованиям стандарта *HIPAA* (*US Healthcare Insurance Portability and Accountability Act*); *RiskWatch RW*17799 *for IS*O 17799 - для оценки требованиям стандарта *IS*O 17799 [93,97].

Автор [93] отмечает, что в качестве критериев для оценки и управления рисками используются предсказание годовых потерь (*Annual Loss Expectancy, ALE*) и оценка возврата от инвестиций (*Return on Investment, ROI*).

RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств обеспечения защиты. Используемая в программе методика включает в себя 4 фазы [92]. Первая фаза - определение предмета исследования. На данном этапе производится описание параметров организации - тип организации, состав исследуемой системы, базовые требования в области безопасности. Вторая фаза - ввод данных, описывающих конкретные характеристики системы. Третья фаза – оценка рисков. Сначала устанавливаются связи между ресурсами, потерями, НВВ и уязвимостями, выделенными на предыдущих этапах. Четвертая фаза это генерация отчетов. Типы отчетов: краткие итоги.

Достоинством *RiskWatch* является гибкость способа, обеспечиваемая возможностью введения новых категорий, описаний и т.д., на основе чего возможно создание собственных профилей, учитывающих отечественные требования в области информационной безопасности, разработка ведомственных методик оценки и управления рисками.

Недостаткам ПО *RiskWatch* считают:

– полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывают понимание риска с системных позиций - способ не учитывает комплексный подход к информационной безопасности;

– данных способ не учитывает организационные и административные факторы защиты и используется для оценки рисков программно-технической степени защиты;

– ПО *RiskWatch* представлено только на английском языке;

– высокая стоимость лицензии (от 15 000 долл. за одно рабочее место для небольшой компании; от 125 000 долл. за корпоративную лицензию).

В отличие от *CRAMM*, программа *RiskWatch* более ориентирована на точную количественную оценку соотношения потерь от НВВ затрат на создание системы защиты. Стоит также отметить, что в этом продукте не производится разделение рисков на сферы информационной и физической безопасности компьютерной сети [95].

Отечественным ПО оценки риска в информационных системах является система «АванГард», созданная в Лаборатории системного анализа проблем информатизации Института системного анализа РАН. Она является экспертной системой управления информационной безопасностью. ПО «АванГард» предназначено для решения задач управления безопасностью в больших территориально-распределенных автоматизированных информационных системах и призвано облегчить задачи контроля за центральными структурами уровня обеспечения информационной безопасности на местах. Комплекс «АванГард» состоит из нескольких частей:

– «АванГард-Анализ» (позволяет строить структурные модели АИС, в которой проводится выявление критических сегментов и объектов, строить модели угроз и модели рисков, связанных с отдельными составляющими АИС и таким образом выявлять те сегменты и объекты, риск нарушения безопасности которых является критическим);

– «АванГард-Контроль» (позволяет проводить мониторинг-контроль выполнения требований по защите критических сегментов АИС и определять «узкие» места в защите и обеспечении безопасности АИС).

Основными возможностями комплекса являются: гибкая система ввода и редактирования модели предприятия, возможность построения модели рисков, система оценки и сравнения рисков, оценка мер противодействия, построение вариантов комплексов мер обеспечения защиты и оценка остаточного риска [94,97].

Перечисленные инструментальные средства оценки рисков имеют общие принципы работы, которые представлены на рисунке 1.3

Авторы публикаций, приведенных в [92-94,96,97] различают программные обеспечения оценки устойчивости функционирования СИС (рисунок 1.4):

1) ПО стандарта *ISO* 17799 (базового уровня),

2) ПО для полной оценки рисков.

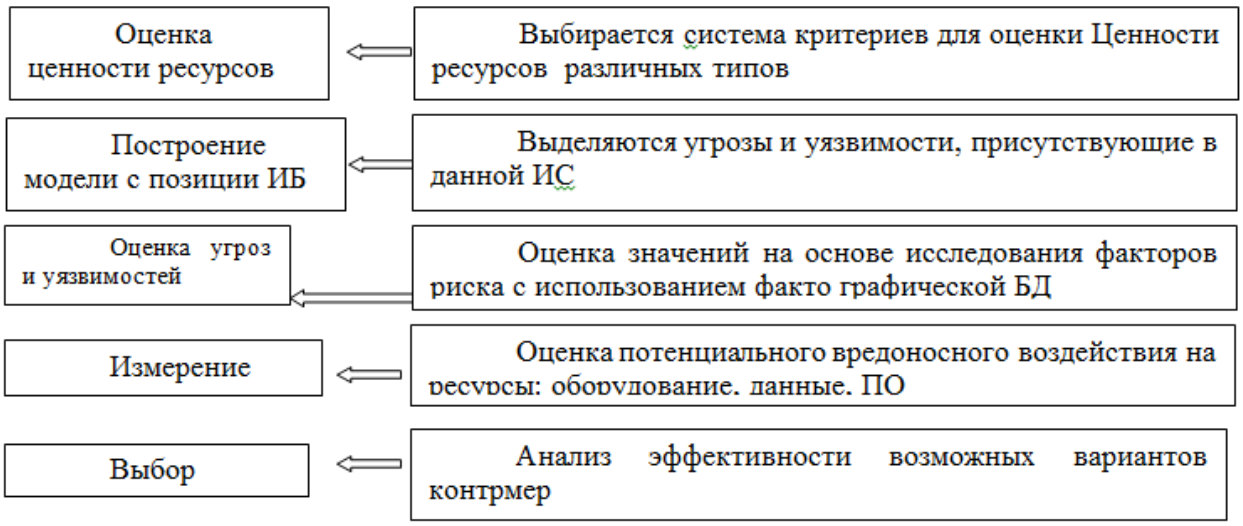

Рисунок 1.3 – Основные функции программных продуктов Авангард, *CRAMM, RiskWatch*

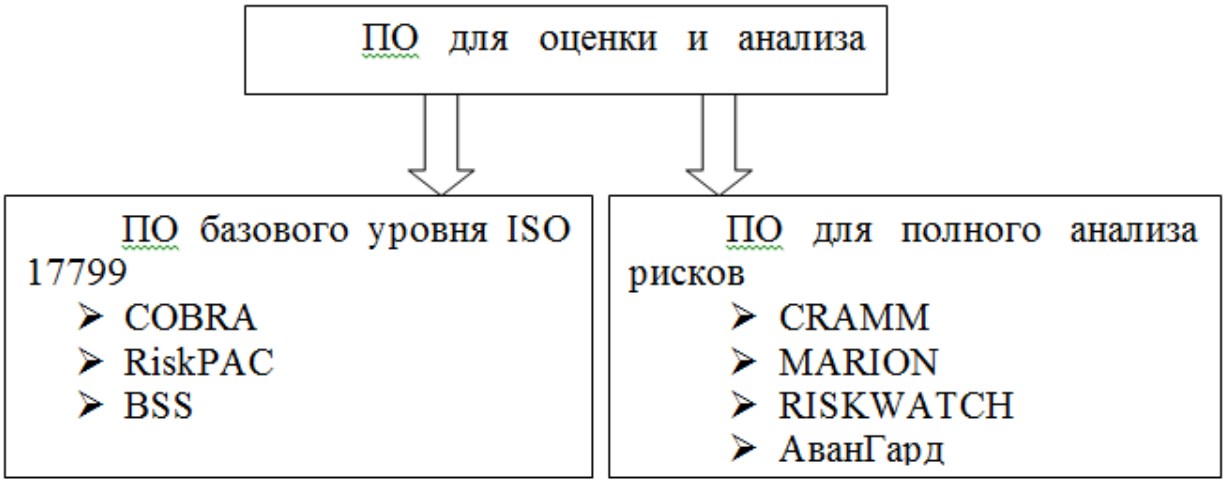

Рисунок 1.4 – Классификация ПО для анализа и оценки рисков

В таблице 1.4 приведено сравнение трех экземпляров ПО по анализу и оценки рисков.

Таблица 1.4 – Сравнительный анализ инструментальных средств оценки рисков [109]

Критерии сравнения	CRAMM, Central Computer and Telecommunications Agency (UK)	RiskWatch, компания RiskWatch(USA)	ГРИФ 2006 Digital Security Office, Компания(Россия)
Поддержка	Обеспечивается	Обеспечивается	Обеспечивается
Легкость в работе конечного пользователя	Использование способа RAMM требует специальной подготовки ивысокой квалификации аудитора.	Использование способа RiskWatch требует специальной подготовки и высокой квалификации аудитора.	Интерфейс программы ориентирован на ИТ-менеджеров руководителей Не требует специальных знаний в области ИБ.
Цена	Стоимость лицензии от 2000 до 5000 долл. за одно рабочее место.	Стоимость лицензии от 10 000 долл. за одно рабочее место.	Стоимость лицензии от 1000 долл. за одно рабочее место.

Окончание таблицы 1.4

Системные требования	- Операционная система: Windows XP / 2000 /NT / Me /98 -Свободное дисковое пространство - 50 MB -Минимальные требования: -Оперативная память - 64 MB ; -Процессор 800 Mhz . -Рекомендуемые требования: Оперативная память - 128 MB; Процессор - 1000 Mhz.	-Оперативная память - 256 MB RAM; Свободное дисковое пространство - 30 MB для инсталляции; -Операционная система -Windows 2000/XP.	-Минимальные системные требования: 1.Оперативная память: 256 Mb. 2.Свободное дисковое пространство (для диска, где расположены данные пользователя): 300 Mb. 3.Операционная система: Windows 2000/XP. -Рекомендуемые системные требования: 1. Оперативная память: 512 Mb. 2. Свободное дисковое пространство (для диска, где расположены данные пользователя): 1 Gb. 3. Операционная система: Windows 2000, Windows XP
Количественный или качественный способ	Качественная оценка	Количественная оценка	Качественная и количественная оценки
Наличие сетевого решения	Отсутствует	Отсутствует	Корпоративная версия

1.6 Постановка задач исследования

В современном мире информационные системы и технологии активно внедряются во все сферы общественной деятельности. Они активно влияют на состояние экономической, политической, оборонной и других составляющих безопасности любой страны. Существенным образом национальная безопасность зависит от устойчивости СИС различной степени.

Появление и развитие современных способов и средств передачи данных, а также интенсивное расширение глобальной сети Интернет, оказывает положительное влияние на эффективность производственных процессов. Но, несмотря на интенсивное развитие, уязвимость современных сетевых информационных систем не уменьшается. Поэтому проблемы

обеспечения устойчивости функционирования СИС привлекают пристальное внимание как специалистов в области компьютерных систем и сетей, так и многочисленных пользователей, включая компании, работающие в сфере электронного бизнеса.

Эксперты, работа которых связна с СИС, нуждаются в средствах, которые смогут облегчить их работу за счет автоматизации некоторых процессов. Поэтому актуальным является построение экспертной системы для проведения оценки устойчивости функционирования СИС при НВВ и повышения ее устойчивости за счет генерации рекомендаций.

При построении экспертной системы оценки устойчивости функционирования СИС при НВВ необходимо уделять внимание следующим аспектам:

1. Ценность информации. Важной задачей при изучении устойчивости функционирования СИС является определение ценности информации, поскольку для получения наибольшей эффективности механизма парирования вредных внешних воздействий необходимо адекватно обеспечивать устойчивость функционирования СИС в соответствии с ценностью обрабатываемой информации. Оценка ценности информации зависит от следующих параметров:

– важность информации по отношению к определенным задачам;

– на сколько опасен ущерб в случае нарушения ее конфиденциальности;

– доступность, целостность и конфиденциальность информации.

Для оценки и обоснования необходимых затрат на построение МПНВВ необходимо сначала провести оценку ценности обрабатываемой информации.

Стоит учитывать, что не существует единой классификации информации. Однако, принято разделять информацию по содержанию на политическую, научно-техническую, военную, технологическую, коммерческую, экономическую, деловую. Такое деление охватывает все

области исследования. Очевидно, что при таком делении оценки важности информации разных типов будут различаться.

2) Оценка и классификация НВВ. Анализ НВВ проводится с целью проведения оценки опасности НВВ и вероятности нарушения доступности, конфиденциальности и целостности информации. Оценка опасности НВВ для различных видов систем может отличаться в зависимости от вид рассматриваемой СИС и ценности информации.

Существуют различные подходы разделения НВВ на классы, но при выборе определенного подхода для ЭС необходимо, чтобы она включала все возможные НВВ. Поскольку основную опасность для СИС представляют внутренние НВВ, чаще всего источники делят на внутренние и внешние. Также в качестве источников могут выступать как субъекты (пользователи, внешние нарушители), так и объективные проявления.

3. Оценка риска, связанного с персоналом СИС зависящего от должности и независимого от цели (причинами тут часто выступают: месть, любопытство и саботаж со стороны компании-конкурента).

4. Оценка ценности ресурсов и объектов СИС. Для достижения наилучшей эффективности средств и способов парирования НВВ надо добиться нужной устойчивости функционирования ресурсов СИС относительно их важности. Также оценки рисков нарушения устойчивости ресурсов зависят от оценок важности ресурсов СИС.

Целью работы является повышение устойчивости функционирования СИС при НВВ за счет генерации рекомендаций с использованием построенной ЭС.

Для получения цели исследования необходимо поставить и решить следующие задачи:

1. Построить интерактивную систему формирования знаний для оценивания объектов, ресурсов СИС и факторов, влияющих на устойчивость функционирования СИС.

2. Разработать методику оценки устойчивости функционирования СИС при НВВ, основанную на опасности НВВ оценке рисков от НВВ, надежности СПНВВ, важности ресурсов и элементов СИС; поставить и решить задачи максимизации критерия оценки устойчивости функционирования СИС, минимизации затрат на применение СПНВВ.

3. Синтезировать структуру экспертной системы для оценки устойчивости функционирования СИС при НВВ, функционирующую в режимах использования пользователем и экспертом и генерирующую рекомендации по повышению устойчивости.

2 Разработка аналитической и процедурной моделей оптимальной многофакторной оценки устойчивости функционирования СИС при НВВ

Разработка и реализация механизмов парирования негативных внешних воздействий (МПНВВ) – неотъемлемая задача при создании практически любой современной информационной системы.

Обеспечение должной степени устойчивости функционирования СИС подразумевает ряд вопросов: адекватно ли работают СПНВВ; соответствует ли требуемый уровень функционирования ценности обрабатываемой в данной системе информации; обеспечивает ли в полной мере существующее МПНВВ стабильное функционирование ресурсов данной системы. Корректное выполнение своих функций специалистами, отвечающими за устойчивость функционирования СИС и за управление автоматизации в данной системе, предполагает наличие средств, облегчающих анализ устойчивости функционирования СИС.

Для этих целей логично разработать единый подход к анализу устойчивости функционирования СИС. Данный подход должен объединять в себе знания и опыт экспертов и вместе с тем охватывать широкий круг задач, быть простым для применения и удовлетворять требованиям пользователей.

Уровень устойчивости функционирования СИС складывается из оценок ценности информации, значимости ресурсов, возможного ущерба (опасности) от НВВ, «слабостей» СПНВВ, уровня надежности защиты используемых средств парирования.

2.1 Аналитическая модель определения ценности обрабатываемой информации

Задача определения ценности информации несколько затруднена в связи с тем, что современная теория информации не дает строгого определения понятия ценность информации. Показатель ценности

информации, задаётся множеством свойств, использующихся для определения требуемого уровня устойчивости функционирования СИС и необходимой степени надежности МПНВВ [66].

Предлагается следующий подход для проведения оценки ценности информации [114]:

На первом этапе необходимо провести классификацию по характеру содержащейся информации (например, военная; коммерческая; политическая и др.) или по видам тайн (семейная, служебная и т.д.) и определить важность информации (таблица 2.1) в виде интервала [*A*-*B*].

Таблица 2.1 – Определение ценности классов информации

А) По характеру содержащейся информации
$1.\begin{Bmatrix}1.Политическая\\2.Военная\end{Bmatrix}(85-100)$
$2.\begin{Bmatrix}3.Научно-техническая\\4.Технологическая\end{Bmatrix}(70-85)$
$3.\{5.экономическая\}(50-80)$
$4.\begin{Bmatrix}3.Научно-техническая\\4.Технологическая\end{Bmatrix}(0-50)$
или
Б) По видам тайн
$1.\{Государственная\}(80-100)$
$2.\{Профессиональная\}(60-85)$
$3.\{Коммерческая\}(50-70)$
$4.\{Служебная\}(30-50)$
$5.\{Семейная\ и\ личная\}(0-30)$

После чего, пользователю требуется ответить на ряд вопросов, характеризующих определенный тип информации.

На втором этапе создается экспертная система, которая на основе исходных фактов об информации и экспертных оценок, проводит процедуру оценки важности выбранного типа информации и определяет класс ценности информации. Предлагается использовать нечеткую логику для продукции правил ЭС, так как, зачастую, нет возможности четко оценить

характеристики информации и сложности полной формализации предметной области.

Выразим принадлежность информации к тому или иному классу ценности с помощью лингвистической переменной «класс ценности информации».

Введем три лингвистические переменные, содержащие четыре терма (критическая, важная, средняя и низкая):

1. важность информации (ВИ),
2. опасность реализации НВВ с точки зрения ущерба (ОУ),
3. экономические расходы на восстановление информации (ЭР).

Итоговая оценка ценности информации определяется с помощью экспертных оценок всех лингвистических переменных и правилу логического вывода «*modusponens*», после определения функций принадлежности информации к классам ценности.

Определим следующие экспертные оценки (таблица 2.2).

Таблица 2.2 – Экспертные оценки

Экспертная оценка	Обозначение
Важность информации (ВИ)	$D \in [0..100]$
Опасность реализации угроз с точки зрения ущерба (ОУ)	$O \in [0..100]$
Экономические расходы на восстановление информации (ЭР)	$P \in [0..100]$

Функция принадлежности имеет множество типовых форм, из них наиболее распространены: треугольная, трапецеидальная и гауссова функции принадлежности.

1) Треугольная функция принадлежности:

$$t(x,a,b,c)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1-\left(\dfrac{x-b}{c-b}\right), b\le x\le c\\ 0, востальныхслучаях\end{cases},$$

2) Трапецеидальная функция принадлежности**:**

$$t(x,a,b,c,d)=\begin{cases}1-\dfrac{b-x}{b-a}, a\le x\le b\\ 1, b\le x\le c\\ 1-\left(\dfrac{x-c}{d-c}\right), c\le x\le d\\ 0, востальныхслучаях\end{cases},$$

3) Гауссова функция принадлежности:

$$t(x)=\exp\left[-(\frac{x-c}{\sigma})^2\right] .$$

Заметим, что трапецеидальные функции являются наиболее подходящими для данной задачи.

Определим функции принадлежности (Z) по всем лингвистическим переменным (таблица 2.3).

Таблица 2.3 – Функции принадлежности

Входные переменные	Функция принадлежности	Обозначения
Важность информации критическая	(Z,90,95,99,100)	ВИ1
Важность информации важная	(Z,80,85,90,95)	ВИ2
Важность информации средняя	(Z,40,50,60,80)	ВИ3
Важность информации низкая	(Z,0,10,30,45)	ВИ4
Опасностьущерба критическая	(Z,90,95,97,100)	ОУ1
Опасность ущерба большая	(Z,85,90,90,95)	ОУ2
Опасность ущерба средняя	(Z,60,75,80,86)	ОУ3
Опасность ущерба низкая	(Z,0,20,50,65)	ОУ4

Окончание таблицы 2.3

Экономические расходы критические	(Z,85,90,95,100)	ЭР1
Экономические расходы большие	(Z,75,80,85,90)	ЭР2
Экономические расходы средние	(Z,50,65,75,85)	ЭР3
Экономические расходы низкие	(Z,0,20,40,55)	ЭР4

Запишем правила для определения ценности информации (таблица.2.4):

Таблица 2.4 – Правила определения ЦИ

Если (((ЭР) очень критические и (ВИ) важная или (ОУ) критическая) или ((ВИ) низкая или (ЭР) критические) или ((ВИ) важный и (ЭР) низкие), то ценность информации критическая.
Если ((ВИ) важная и (ОУ) средняя и (ЭР) низкие) или (ВИ) очень важная) или (ВИ) очень важная и (ЭР) средние), то ценность информации важная.
Если (((ВИ) средняя и (ОУ) средняя и (ЭР) средние) или ((ВИ) низкая и (ОУ) средняя и (ЭР) высокие) или ((ВИ) важная и (ЭР) низкие)), то ценность информации средняя.
Если ((ВИ) средняя и (ОУ) низкая и (ЭР) низкие или ((ЭР) средние и (ОУ)низкая)), то ценность информации низкая.
$f1(ЦИ) = (цЭР1(ЭР)^2 \wedge (цНИ2(ВИ))) \vee цО1(О)) \vee (ВИ4(ВИ)) \vee (ЭР1(ЭР)) \vee (ВИ2(ВИ) \wedge (ЭР4(ЭР)))$ $f2(ЦИ) = (цВИ2(ВИ) \wedge цО3(О)) \wedge (цЭР4(ЭР)) \vee (цВИ2(ВИ)^2) \vee (цВИ2(НИ)^2 \wedge цЭР3(ЭР)))$
$f3(ЦИ) = (цВИ3(ВИ) \wedge цО3(О)) \wedge (цЭР3(ЭР)) \vee (цВИ4(ВИ)^2) \vee (цО3(О) \wedge цЭР2(ЭР)) \vee (цВИ2(ВИ) \wedge цЭР4(Эр))$
. . . . .
$fn(ЦИ) = ((цВИ3(ВИ) \wedge цО4(О) \wedge цЭР4(ЭР)) \vee (цЭР3(ЭР) \wedge цО4(О)))$

На последнем этапе оценим все лингвистические переменные, с помощью группы вопросов, включающих четыре варианта ответа (таблица 2.5). Экспертами определяется важность каждого из вопросов. Заметим, существенную разницу между группами вопросов по каждому типу информации.

Таблица 2.5 – Диапазоны оценок ответов

Категории ответов	Примеры вариантов ответов	Диапазон
1-критический	Критический, очень высокий, очень важный, очень надежный	(90%-100%)
2-важный	Высокий, важный, надежный	(75%-90%)
3-средний	Средний, ниже среднего, выше среднего	(40%-75%)
4-низкий	Очень низкая стоимость, низкая стоимость, низкая надежность	(0%-40%)

Значимость ответа вычисляется произведением важности вопроса (Q_n) на разницу верхней (B) и нижней (A) границы интервала ответа и добавлением значения нижней границы интервала:

$$Y_i = ((B - A)Q_n) + \text{A}, \tag{2.1}$$

Средняя оценка важности ответов (F) есть отношение суммы всех показателей значимости ответов (Y) к их числу (u):

$$F = \frac{\sum_{i=1}^{u} Y}{u} \tag{2.2}$$

Ценность информации (L) получается путем суммирования произведения общей существенности лингвистических переменных (P) на разницу диапазона (K) и нижней границы (A)

$$L = (P * K) + A \tag{2.3}$$

Отметим, что ценность различных информационных систем имеет непосредственную зависимость от ценности обрабатываемой информации. Равно как и оценка рисков, которая также зависит от важности информации, а также оценка опасности НВВ.

2.2 Формализация процесса анализа устойчивости функционирования СИС

Состояние сетевой информационной системы, при котором она способна противодействовать вредным воздействиям (как внешним, так и внутренним) и ее деятельность не создает угроз для узлов самой системы будем называть устойчивостью функционирования СИС. А способность, в полном объеме и с заданным уровнем качества, выполнять возложенные функции при негативных воздействиях будем называть устойчивость функционирования СИС при НВВ. СИС устойчива к воздействию группы НВВ, если её общий уровень устойчивости принадлежит интервалу требуемого значения качества.

Оценка уровня устойчивости функционирования СИС сводится к получению показателей важности следующих факторов:

1) вредные внешние воздействия;

2) объекты и ресурсы СИС;

3) способы и средства парирования НВВ;

4) генерация вариантов рекомендаций для получения требуемой (оптимальной) степени защищенности СИС.

По источнику возникновения НВВ необходимо разделять на внешние и внутренние. Важными свойствами источников НВВ являются тип и положение относительно атакуемой системы.

$$Z = \{Z_S, Z_G, Z_D\}$$

где

Z - Множество источников НВВ.

Z_S , Z_G, Z_D - подмножество антропогенных, техногенных и стихийных источников НВВ соответственно.

$$Z_{in} = \begin{bmatrix} Z_{inG} \\ Z_{inS} \\ Z_{inD} \end{bmatrix} \qquad Z_{out} = \begin{bmatrix} Z_{ouG} \\ Z_{outS} \\ Z_{ouDt} \end{bmatrix}$$

где

Z_{in} - множество внутренних НВВ,

Z_{out} -множество внешних НВВ.

Идентифицировать НВВ будем по степени опасности нарушения Д, К, Ц:

$$Z_{in} = \begin{bmatrix} Z_G^{д} & Z_G^{к} & Z_G^{ц} \\ Z_s^{д} & Z_s^{к} & Z_s^{ц} \\ Z_D^{д} & Z_D^{к} & Z_D^{ц} \end{bmatrix} \Rightarrow Z_{inj}{}^{q} \in Z;$$

$$Z_{out} = \begin{bmatrix} Z_G^{д} & Z_G^{к} & Z_G^{ц} \\ Z_s^{д} & Z_s^{к} & Z_s^{ц} \\ Z_D^{д} & Z_D^{к} & Z_D^{ц} \end{bmatrix} \Rightarrow Z_{inj}{}^{q} \in Z;$$

Ресурсы системы принято делить на человеческие, информационные и физические.

Обозначим O - множество объектов сетевой информационной системы, тогда $O = \{O_1, O_2, O_3, ...O_n\}$, U – множество ресурсов СИС разделенных на группы:

$$U = \begin{bmatrix} U_{и} \\ U_{ч} \\ U_{ф} \end{bmatrix}$$

Оценивать каждый ресурс будем по доступности, целостности и конфиденциальности, так как тип ресурса не влияет на показатель значимости по Д, К, Ц:

$$U = \begin{bmatrix} U_{и}^{д} & U_{и}^{к} & U_{и}^{ц} \\ U_{ч}^{д} & U_{ч}^{к} & U_{ч}^{ц} \\ U_{ф}^{д} & U_{ф}^{к} & U_{ф}^{ц} \end{bmatrix} \Rightarrow U = U_{gi}^{q},$$

Где $U_{и}^{д}, U_{и}^{к}, U_{и}^{ц}$- множество показателей значимости информационных ресурсов; $U_{ф}^{д}, U_{ф}^{к}, U_{ф}^{ц}$- множество показателей значимости физических ресурсов; $U_{ч}^{д}, U_{ч}^{к}, U_{ч}^{ц}$- множество показателей значимости человеческих ресурсов.

Так как негативное воздействие (*Z*) не привязано к конкретному ресурсу (*U*) СИС, то:

Внутренние:

$$Z_{in}U = \left\{Z_j^q U_g^q \mid Z_j^q \in Z, U_g^q \in U\right\};$$

Внешние:

$$Z_{out}\,U = \left\{Z_j^q U_g^q \mid Z_j^q \in Z,\, U_g^q \in U\right\}$$

Для каждого типа НВВ есть определенные источники (внутренние и внешние), направленные на определенный ресурс с определенной целью нарушения:

а) $Z_{inj}U = (Z_{inj},\ \ Z_g^q),$ $\quad b)\ Z_{outj}U=(Z_{outj}\ ,\ Z_g^q)$

Для каждого НВВ существует один или несколько средств парирования негативных внешних воздействий (СПНВВ). Одним из отличий методов и средств парирования НВВ является уровень надежности парирования конкретного вида НВВ по Д, К и Ц.

Пусть N - множество средств парирования НВВ,

$$N_{in} = \left\{N_{in1}, N_{in,2}, N_{in,3}, \ldots\ldots, N_{in,d}\right\},$$

$$N_{out} = \left\{N_{out1}, N_{out,2}, N_{out,3}, \ldots\ldots, N_{out,d}\right\}.$$

Обозначаем:

N^{∂}-совокупность СПНВВ с целью нарушения доступности;

$N^{ц}$- совокупность СПНВВ с целью нарушения целостности;

$N^{к}$ - совокупность СПНВВ с целью нарушения конфиденциальности.

Тогда внутренние и внешние СПНВВ:

$$N_{in} = \left\{N_{ind}^q\right\}, N_{out} = \left\{N_{outd}^q\right\},$$

Все элементы СИС рассматриваем как объекты, подвергаемые негативным воздействиям. Тогда объект может соответствовать одному или нескольким ресурсам. Кроме того, оцениваем уровень устойчивости функционирования различных ресурсов с учетом типа, а именно физического, человеческого.

Влияние уровня профессиональной компетенции пользователей (персонала) на устойчивость функционирования СИС как в целом, так и по отдельным ресурсам определяется должностными полномочиями и квалификацией этих лиц.

2.3 Аналитическая модель влияния уровня профессиональной компетенции и должностных полномочий персонала СИС на устойчивость ее функционирования

Основополагающим фактором оценки риска каждой группы персонала является должность. При этом его цель не столь существенна.

Оценка вероятности негативного воздействия со стороны персонала в зависимости от должностью требует:

1) Синтеза перечня персонала по вероятности негативного воздействия с учетом уровня доступа к сетевой информационной системе [88]:

Таблица 2.6 – Обобщенный перечень персонала типичной СИС

Степень риска (категории)	Должность	В процентах
Наибольший риск	1-сетевой администратор; 2-администратор безопасности;	(95%-100%)
Повышенный риск	3-оператор системы; 4-оператор ввода подготовки данных; 5-менеджер обработки; 6-системный программист;	(85%-95%)
Средний риск	7-инженер системы; 8-менеджер программного обеспечения;	(60%-85%)
Низкий риск	17-инженер по периферийному оборудованию; 18-библиотекарь магнитных носителей пользователей; 19-пользователь сети.	(0-25%)

Окончание таблицы 2.6

Ограниченный риск	9-прикладной программист; 10-инженер или оператор по связи; 11-администратор баз данных; 12- инженер по оборудованию; 13-библиотекарь системных магнитных носителей; 14-операторпериферийного оборудования; 15-пользователь-программист; 16- пользователь-операционист;	(25%-60%)

2) Проведения регулярного тестирования, для выявления уровня квалификации и знаний по требованиям эксплуатации СИС.

Общие требования к такого рода тестированиям предполагают наличие множества вопросов с заранее определённой ценностью верного ответа. Желательно формулировать вопросы таким образом, чтобы предполагались однозначные ответы (да/нет). Оценивать результаты теста будем следующим образом:

$$П = \frac{\sum Q_d}{n} \quad , \tag{2.4}$$

где П - Уровень квалификации персонала;

Q_d - верный ответ на *d*-тый вопрос;

n - число вопросов

$$H = ((1-П)(B-A))+A, \tag{2.5}$$

где H – оценка негативного воздействия на СИС со стороны персонала; A, B - минимальное и максимальное значение интервала степени риска, в зависимости от должности персонала.

Типовое тестирование, с показателями важности представлено в таблице 2.7.

Таблица 2.7 – Типовое тестирование

Вопрос	Важность	Ответ
1.Знаете ли Вы программирование?	56%	Да/ Нет
2.Знакомы ли Вы с работой механизма защиты в Вашей системе?	68%	Да/ Нет
3.Любите ли Вы Вашу работу?	78%	Да/ Нет
4.Любите ли Вы Ваше руководство?	40%	Да/ Нет
5.Знакомы ли Вы с принципами противодействия НВВ?	90%	Да/ Нет
6.Знакомы ли Вы с возможными НВВ?	95%	Да/ Нет
7.Знаете ли Вы важность обрабатываемой информации в Вашей системе?	85%	Да/ Нет
8.Выполняете ли Вы условия безопасности?	30%	Да/ Нет
9.Проходили ли Вы курсы повышения квалификации?	20%	Да/ Нет
10. Дипломированный ли Вы специалист?	85%	Да/ Нет
11.Довольны ли Вы Вашей зарплатой?	65%	Да/ Нет

Для получения реальной оценки уровня устойчивости функционирования СИС, следует учитывать оценку возможного негативного воздействия каждого пользователя сетевой информационной системы. Для повышения уровня устойчивости функционирования сетевой информационной системы следует повышать уровень квалификации пользователей, так как это снижает риски связанные с НВВ обусловленными человеческим фактором.

2.4. Процедурная модель формирования входных данных

Одной из приоритетных задач при построении ЭС оценки устойчивости функционирования СИС считается изучение предметной области с точки зрения поиска подходов к формированию знаний и оцениванию объектов. В данной ЭС предметная область характеризуется неопределенностью и многокритериальностью, что говорит *о* необходимости поиска разнообразных подходов к решению возникающих задач (ценность ресурсов СИС, надежность СПНВВ, опасность НВВ по (Д, Ц и К)). Для снижения затрат на улучшение качества ожидаемого результата, а так же

исследование предметной области и для формирования знаний, используемых как входные данные ЭС, предлагается построить интерактивную систему.

Интерактивная система формирования знаний, для каждого типа исследуемой системы, будет иметь отличия проявляющиеся в уровне влияния в зависимости от типа исследуемой системы. Такая система включает в себя множество документов, содержащих вопросы, отражавшие факторы об исследуемой задаче. Каждый вопрос, в зависимости от того, насколько этот фактор влияет на оценку исследуемой задачи, имеет свою ценность в соответствии с типом системы и варианты ответа, которые, в свою очередь, имеют оценку в диапазоне [0-100%].

Существенность ответа на каждый вопрос получается путем суммирования произведения важности каждого вопроса на разницу диапазона ответа и нижней границы диапазона ответа по формуле:

$$Y_i = (Q_i M_i) + A \ , (2.1)$$

где Y – существенность ответа; Q – ценность вопроса;

M – интервал ответа (B – A);

A – минимальное значение ответа;

i – номер вопроса.

Оценка влияния этих факторов на систему есть отношение суммы важностей всех ответов к их числу по формуле:

$$F = \frac{\sum_{i=1}^{u} Y_i}{u}, \quad (2.6)$$

где F – общая оценка влияния фактора;

Y – существенность ответа;

u – количество вопросов.

Приведём несколько примеров работы интерактивной системы при оценке надежности СПНВВ, важности ресурсов СИС и опасности НВВ. Данные примеры будут иметь незначительные отличия, в то время как основные принципы интерактивной системы останутся неизменными.

2.5 Распознавание и оценка опасности негативных внешних воздействий

Проведём идентификацию и оценку опасности НВВ с целью выявления всех возможных НВВ и определения опасности каждого из них. С помощью идентификации станет возможно подробно описать НВВ: наименование НВВ, характеристики, цели НВВ нарушения аспектов, возможные уязвимости МПНВВ, тип ресурса, на который оно воздействует (человеческий, информационный и физический). Также идентификация должна дать возможность добавлять новые НВВ.

В процессе идентификации НВВ, каждое НВВ представляется в виде класса, содержащего поля с информацией об имени, характеристиках и объектах класса, а также несколько свойств НВВ (рисунок 2.1).

Рисунок 2.1 – Структурная схема идентификации НВВ

Имя класса имеет уникальный идентификатор и включает информацию, необходимую для определения данного класса. Характеристика класса – общее описание НВВ и обобщает участие объектов в нём (наименование НВВ, источники НВВ, объекты НВВ, СПНВВ).

Отметим, что любое НВВ имеет собственные показатели возможности нарушения целостности, конфиденциальности и доступности, поэтому интерактивная система формирования знаний необходима для проведения оценки опасности НВВ по аспектам Ц, К и Д.

1. Оценить потенциальный вред НВВ по Д, К и Ц (таблица 2.8) таким образом:

Таблица 2.8 – Проведение оценки потенциального вреда НВВ по Д, К и Ц

Аспекты	Важность вопроса	Варианты ответа			
		первый	второй	третий	четвертый
Опасность нарушения доступности ресурса от осуществления этого НВВ	100%	Низкая	Средняя	Высокая	Критическая
Опасность нарушения конфиденциальности ресурса от осуществления этого НВВ	100%	Низкая	Средняя	Высокая	Критическая
Опасность нарушения целостности ресурса от осуществления этого НВВ	100%	Низкая	Средняя	Высокая	Критическая

2.Оценить обобщенный потенциальный вред НВВ в целом, при помощи вопросов, через которые можно определить все свойства НВВ и

вероятности его появления, а также влияние НВВ на оценку устойчивости функционирования ресурсов СИС и на систему в целом (таблица 2.9).

Таблица 2.9 - Пример проведения обобщенной оценки потенциального вреда НВВ

Вопрос	Важность вопроса	Первый вариант ответа	Второй вариант ответа	Третий вариант ответа	Четвертый вариант ответа
1.Затраты на реализацию НВВ	70%	Низкие	Средние	Высокие	Очень высокие
2.Уровень уязвимости, через которую реализуется НВВ	50%	Низкая	Средняя	Высокая	Очень высокая
3.Нужное время для реализации НВВ	20%	Мало	Средне	Много	Очень много
4.Возможность предотвращения НВВ	90%	Легко	Трудно	Очень трудно	Невозможно
5.Возможность обнаружения реализации НВВ	80%	Легко	Трудно	Очень трудно	Невозможно
6.Частота появления НВВ	100%	Неизвестно	Низкая	Высокая	Очень высокая
7.Опасность реализации НВВ	65%	Низкая	Средняя	Высокая	Критическая
8.Простота реализации НВВ	70%	Относительно Легко	Легко	Сложно	Очень сложно
9.возможность восстановления ресурса после реализации НВВ?	85%	Легко	Трудно	Очень трудно	Невозможно

При этом любой из вопросов имеет свою ценность и свои варианты ответа, как показано в таблицах 2.8 и 2.9. Диапазоны оценки ответов показаны в таблице 2.10.

Таблица 2.10 – Примеры диапазонов ответов на предлагаемые вопросы

Варианты ответов	Примеры каждого варианта	Диапазон
Первый вариант	Критический, очень высокий, очень важный, очень надежный	(90%-100%)
Второй вариант	Высокий, важная, надежная	(75%-90%)
Третий вариант	Средний, ниже среднего, выше среднего	(50%-75%)
Четвертый вариант	Очень низкая стоимость, низкая стоимость, низкая надежность	(0-50%)

3. Выполним оценку ответа каждого вопроса по формуле (2.1), после чего вычислим общую опасность НВВ по формуле (2.6), используя ответы из таблицы 2.10:

$$Y_i = (Q_i M_i) + A ,$$

где Y – существенность ответа;

Q – ценность вопроса;

M – интервал ответа;

A – минимальное значение ответа;

i – номер вопроса.

$$O_o = \frac{\sum_{i=1}^{u} Y_i}{u} , \qquad (2.6)$$

где *O*- обобщенная оценка потенциального вреда НВВ; Y_i - существенность ответа; *u* - число вопросов.

4. Определим опасность НВВ, влияющую на ресурсы с определенной целью по формуле:

$$O_q = \frac{\sum_{i=1}^{u} Y + Y_q}{u+1} \qquad (2.7)$$

где O_q – оценка опасности НВВ с определенной целью Д, К, Ц;

Y_q – существенность ответа по Д, К, Ц;

$u + 1$ – количество вопросов (u) увеличенное на еденицу.

Проведение данной идентификации дает возможность адекватно описать любое НВВ, а также добавить новое в случае его отсутствия в БД. Данный подход к оценке опасности НВВ (общая опасность и опасность по определенному аспекту) дает возможность более четкой оценки риска от каждого НВВ (по Д, К и Ц). Влияние на уровень опасности НВВ, определяемое главными факторами, определяют вопросы, а силу влияния каждого фактора на опасность НВВ отражает ценность каждого вопроса. Стоит отметить, что одинаковые вопросы для различных типов систем могут иметь разную ценность.

2.6. Распознавание и оценка уровня защиты средствами парирования негативных воздействий

Для системного анализа устойчивости функционирования СИС требуется сопоставить степень опасности НВВ, влияющих на объекты и ресурсы СИС, с оценками надежности средств парирования НВВ. Механизм парирования НВВ содержит непустое множество средств и методов парирования НВВ. СПНВВ, предназначенные для обеспечения устойчивости функционирования СИС, могут иметь разные цели назначения (обеспечение того или иного аспекта безопасности информации), разную степень надёжности обеспечения устойчивости функционирования и быть направленными на разные типы ресурсов (физические, информационные и человеческие). Идентификация и оценка надежности СПНВВ проводится с целью определения списка всех возможных СПНВВ и их эффективности. Это позволяет с одной стороны описать каждое СПНВВ, НВВ, с другой стороны подобрать рациональным образом новые СПНВВ (рисунок 2.2).

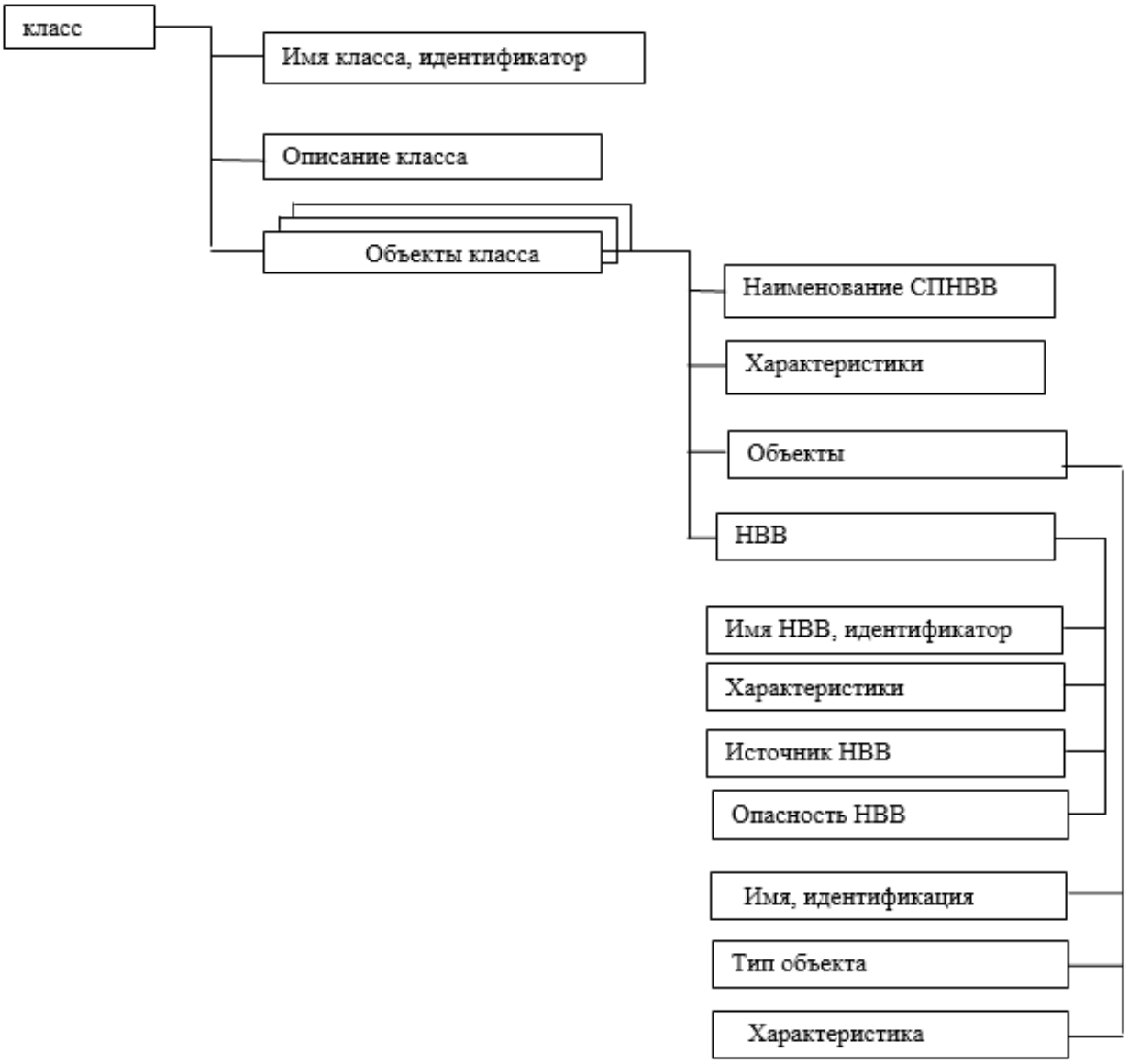

Рисунок 2.2 – Структурная схема идентификации СПНВВ

Методы и средства парирования НВВ любого МПНВВ разделяются на программные, аппаратные и программно-аппаратные.

Следует заметить, что в разных обстоятельствах эксплуатации, надёжности СПВВ отличаются. Этот факт следует учитывать при оценке надежности СПВВ по конкретному аспекту. Например, когда на операционную систему не устанавливаются обновления, это снижает показатели ее надежности и повышает вероятность негативного воздействия.

Внесем необходимые изменения в интерактивную систему формирования знаний с целью получения оценки надежности СПНВВ, для решения поставленной задачи.

Приведём пример оценки надежности СПНВВ.

1) Оцениваем уровень защищенности для конкретных СПНВВ по Д, К и Ц (таблица 2.11).

Таблица 2.11- Результаты оценки уровня защищенности СПНВВ по Д, К и Ц

Аспекты	Важность вопроса	Варианты ответа			
		Первый	Второй	Третий	Четвертый
Надежность защиты по доступности от возможных НВВ	100%	Низкая	Средняя	Высокая	Идеальная
Надежность защиты по конфиденциальности от возможных НВВ	100%	Низкая	Средняя	Высокая	Идеальная
Надежность защиты по целостности от возможных НВВ	100%	Низкая	Средняя	Высокая	Идеальная

2) Оценить надежность СПНВВ в целом с помощью группы, определяющей все факторы, которые оказывают влияние на надежность СПНВВ (таблица 2.12).

Таблица 2.12 - Пример проведения общей оценки надежности СПНВВ

Вопрос	Важность вопроса	Первый вариант ответа	Второй вариант ответа	Третий вариант ответа	Четвертый вариант ответа
1.доступ посторонним людям к нему.	100%	Просто	Легко	Трудно	Невозможно
2.надежно защищает объект от возможных СПНВВ	100%	Слабо	Средне	Надежно	Очень надежно
3.уровень уязвимости	100%	Низкий	Средний	Высокий	Очень высокой
4.простота настройки	90%	Легко	Средне	Трудно	Очень трудно
5.вероятность отказа в работе	80%	Небольшая	Средняя	Большая	Очень большая

Окончание таблицы 2.12

6.время ремонта/восстановления в случае его частичного разрушения	100%	0 минут до 30минут	От 30 минут до 1 часа	От 1 часа до 12 часов	Больше 12 часов
7. Стоимость в случае его полного разрушения	65%	Низкая	Средняя	Высокая	Критическая
8. стоимость в случае его частичного разрушения	70%	Низкая	Средняя	Высокая	Критическая
9.частота появления ошибок в его работе	85%	Незначимо	Редко	Средне	Очень часто
10.простота обнаружения ошибок в его работе	85%	Легко	Средне	Трудно	Невозможно
11.частота появления конфликтов в его работе с другими СПНВВ или программами.	85%	Незначимо	Редко	Средне	Очень часто

Как показано в таблицах 2.13 и 2.14, каждый вопрос обладает своей важностью и своими вариантами ответа (таблица 2.13).

Таблица 2.13 – Варианты формализованных ответов

Варианты ответов	Примеры каждого варианта	Диапазон
Первый вариант	Критический, очень высокий, очень важный, очень надежный, очень часто.	(90%-100%)
Второй вариант	Высокий, важная, надежная.	(75%-90%)
Третий вариант	Средний, ниже среднего, выше среднего	(50%-75%)
Четвертый вариант	Очень низкий, низкий, редко, незначимый	(20%-50%)

3) Вычисляем существенность каждого ответа (2.1) и оценку обобщенного уровня защиты для конкретного СПНВВ:

$$Y_i = (Q_i M_i) + A \ ,$$

где Y – существенность ответа;

Q – ценность вопроса;

M – интервал ответа;

A – минимальное значение ответа;

i – номер вопроса.

$$W_o = \frac{\sum_{i=1}^{u} Y_i}{u}, \quad (2.8)$$

где W_o – обобщенный уровень защиты для конкретного СПНВВ;

Y – существенность ответа;

u – число вопросов.

4) Отношение суммы по всем оценкам ответов из таблицы 2.12 и оценкам ответов на вопросы с конкретной целью из таблицы 2.11 к числу вопросов, выразит оценку надежности СПНВВ по Д, К и Ц, формула 2.9:

$$W_q = \frac{\sum_{i=1}^{u} Y_i + Y_q}{u+1}, \quad (2.9)$$

где W_q – оценка надежности СПНВВ с определенной целью обеспечения доступности, конфеденциальности и целостности;

Y_q – существенность ответа по Д, К, Ц;

u + 1 – количество вопросов таблицы 2.12 увеличесннное на еденицу

Необходимо учесть, что уровень надежности СПНВВ зависит и от других факторов. В связи с этим необходимо оценить, влияние этих факторов на итоговую оценку. А с помощью группы вопросов, для проведения оценки при эксплуатации, будут учтены эксплуатационные условия СПНВВ (таблица 2.14).

Оценка уровня защищенности (надежности) СПНВВ по Д, К и Ц в период эксплуатации, получается умножением показателя надежности средства парирования (по требуемому фактору – Д, К, Ц) на значение этого показателя из таблицы 2.14.

Таблица 2.14. Оценки уровня защищенности СНПВВ во время эксплуатации

Аспекты	Ценность вопроса	Варианты ответа			
		Первый	Второй	Третий	Четвертый
1.Кто настраивает	85%	Пользова-тель	С небольшим опытом	Специалист с опытом	Специалист с большим опытом
2.Частота обновления	100%	Низкая	Средняя	Высокая	Идеальная
3.Частота ремонта	100%	Низкая	Средняя	Высокая	Идеальная

Обобщенная и частные (по Д, К, Ц) оценки уровня защищенности средства парирования (общая надежность и надежность по Д, К, Ц) позволяют определить, способность примененных средств обеспечить заданный уровень устойчивости функционирования СИС при негативных воздействиях. Кроме того, обобщенная оценка в период эксплуатации соответствует реальному уровню защищенности обеспеченному этим средством, то есть реальной надежности этого средства.

2.7. Распознавание и оценка значимости ресурсов СИС

Максимальная эффективность средств и методов парирования НВВ, достигается путем обеспечения устойчивости функционирования ресурсов СИС.

Все компоненты СИС являются ресурсами и делятся на человеческие, информационные и физические. Ресурсы СИС – это совокупность обрабатываемой, передаваемой, принимаемой или хранимой информации и элементы системы. К элементам относятся пользователи и аппаратно-программные средства).

В процессе оценки уровня устойчивости функционирования СИС следует оценить отдельные ресурсы на К, Д, Ц без учета их типов.

Все элементы СИС рассматриваем как объекты, подвергаемые негативным воздействиям. Тогда объект может соответствовать одному или нескольким ресурсам. Кроме того, оцениваем уровень устойчивости функционирования различных ресурсов с учетом типа, а именно физического, человеческого.

Перечень ресурсов СИС и значимость каждого из них определяются путем распознавания ресурсов. Такой механизм позволяет описать ресурсы, а именно задать для них: имя, степень уязвимости и др. (рисунок 2.3). Кроме того, распознавание позволяет добавить новый ресурс.

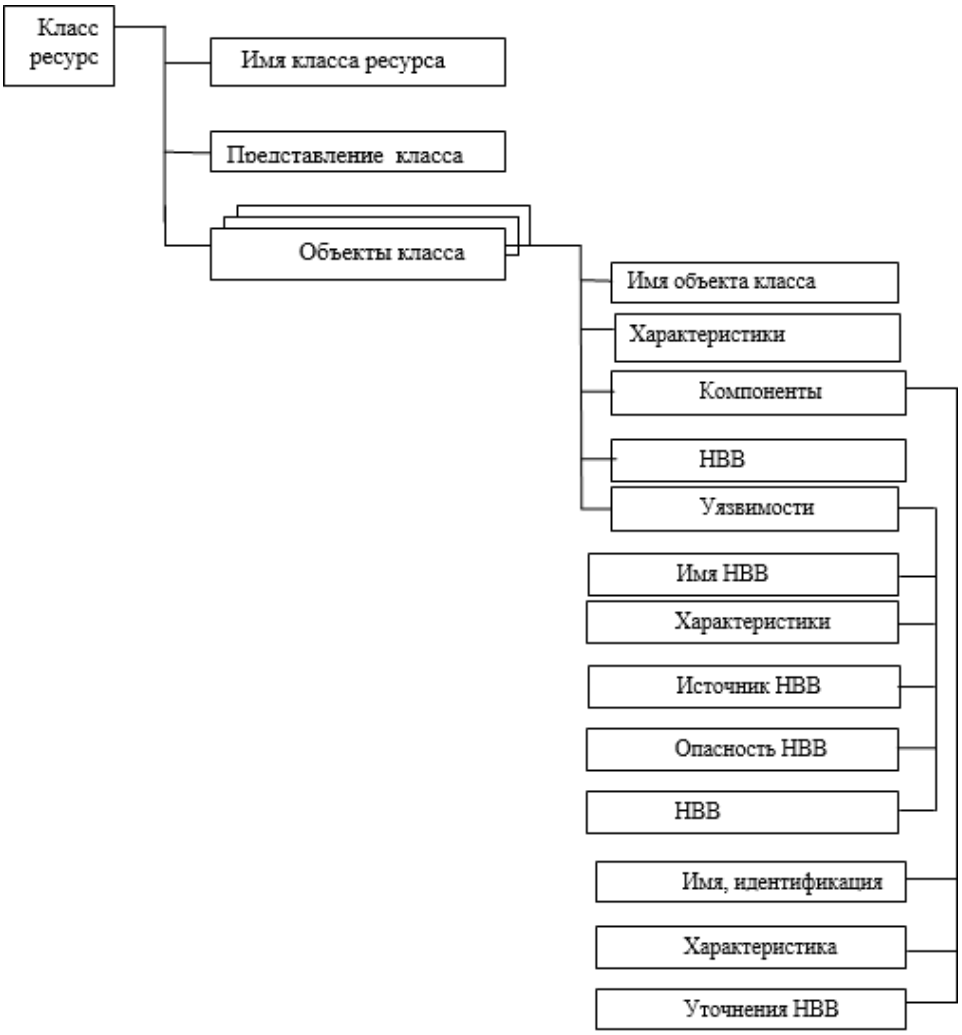

Рисунок 2.3 – Описание ресурсов СИС в механизме распознавания

Для оценки значимости определенного ресурса требуется задать четыре типа вопросов. Один из этих типов отвечает за определение обобщенной значимости ресурса, а остальные – за Д, К и Ц.

Вопросы отражают основные аспекты, влияющие на значимость ресурса, а значимость каждого вопроса задает значение влияния аспекта на значимость ресурса (ПРИЛОЖЕНИЕ А).

Каждый тип вопросов имеет свое формализованное множество ответов с диапазоном важности от нуля до ста процентов (таблица 2.16).

Таблица 2.16 – Множество формализованных ответов

Варианты ответов	Примеры каждого варианта	Диапазон
Первый вариант	Критический, очень высокий, очень важный, очень надежный	(90%-100%)
Второй вариант	Высокий, важный, надежный	(75%-90%)
Третий вариант	Средний, ниже среднего, выше среднего	(50%-75%)
Четвертый вариант	Очень низкая стоимость, низкая стоимость, низкая надежность	(20%-50%)

Для получения обобщенной оценки значимости ответов и обобщенной оценки значимости ресурса используем формулы (2.1) и (2.2).

Полагаем:

$\sum_{i=1}^{u} Y_{il}^{q}$ - обобщенная значимость ответов одного типа по (Д, К и Ц) для *l*-ого ресурса;

$\sum_{i=1}^{u} Y_{il}^{o}$ - обобщенная значимость ответов для *l*-ого ресурса, по всем типам.

Важности ресурса по доступности, целостности и конфиденциальности определяем выражением:

$$V_l^q = \frac{\sum_{i=1}^{u} Y_{il}^{q} + \sum_{i=1}^{u} Y_{il}^{o}}{z}, \quad (2.10)$$

где V_l^q– важность *l*-ого ресурса по Д, К, Д; z - число вопросов двух групп.

Обобщенную важность ресурса определяем выражением:

$$V_l^o = \frac{\sum_{i=1}^{u} Y_{li}^{o} + \sum_{i=1}^{u} Y_{li}^{k} + \sum_{i=1}^{u} Y_{li}^{d} + \sum_{i=1}^{u} Y_{li}^{t}}{s}, \quad (2.11)$$

где V_l^o - обобщенная важность ресурса; $\sum_{i=1}^{u} Y_l^o$ - обобщенная ценность ответов общей группы; $\sum_{i=1}^{u} Y_l^d$ - сумма значимости ответов группы для определения

доступности; $\sum_{i=1}^{u} Y_l^t$ - сумма значимости ответов группы для определения целостности; $\sum_{i=1}^{u} Y_l^k$ - сумма значимости ответов группы для определения конфиденциальности.

Если ресурсы СИС будут отличаться уровнем важности, то возможно определить частную важность ресурса по Д, К и Ц и использовать ее для последующего определения риска и формирования предложений с целью повышения уровня устойчивости функционирования СИС.

2.8 Процедурная модель оценки уровня устойчивости функционирования СИС при негативных воздействиях

Из практики известно, что основным фактором определяющим устойчивость функционирования СИС в условиях негативных воздействий является наличие механизмов защиты от влияния воздействий через существующие в системе уязвимости. Кроме того, целесообразно учитывать фактор связанный с надежностью механизмов парирования, то есть уровнем защищенности путем применения выбранных средств парирования.

В процессе оценки уровня устойчивости функционирования СИС требуется анализировать риски с целью оценки возможного ущерба от негативных воздействий. Значит, одно или несколько негативных воздействий направлены одновременно на нарушение не менее одного аспекта ресурса (рисунок 2.4). Также важно учесть, что средства парирования, как правило, противодействуют одному или нескольким воздействиям и обеспечивают соответствующий уровень устойчивого функционирования прикрываемых ресурсов СИС по одному или нескольким аспектам одновременно.

Очевидно, что негативные воздействия аналогично средствам парирования одновременно влияют на работу нескольких ресурсов.

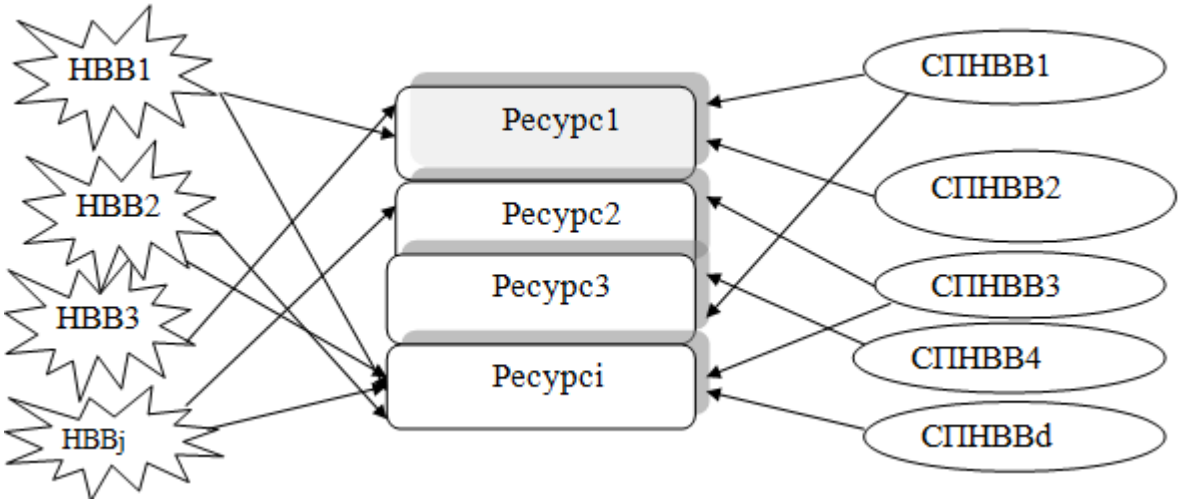

Рисунок 2.4 – Схема влияния НВВ и СПНВВ

В условиях конкретного негативного воздействия направленного на соответствующий ресурс определяем риск причиненный в рамках конкретного аспекта:

$$\mathrm{P}_{ji}^{q} = O_j^q V_i^q (1 - W_{1i}^q E_{1j}) ... (1 - W_{di}^q E_{dj}), \tag{2.12}$$

$$E_{dj} = \begin{cases} 1, \textit{если } d-\textit{ое СПНВВ включен для } j-\textit{ого НВВ} \\ 0, \qquad\qquad \textit{в противном случае} \end{cases},$$

где P_{ji}^{q} - риск возможного ущерба от j-ого НВВ на i-й ресурс с целью нарушения ; O_j^q – оценка опасности (ущерб с определенной вероятностью) j-ого НВВ; W_d^q - оценка надежности (вероятность преодоления) d-ого СПНВВ; V_i^q - оценка важности i-ого ресурса по Д, К и Ц; E_{dj} - индикатор включения конкретного средства парирования.

Риск нарушения устойчивости (W^q) функционирования ресурса по Д, К, Ц, вследствие негативных воздействий определяем выражением:

$$w^{q} = \frac{\sum_{j=1}^{x} \mathrm{P}_{ji}^{q}}{x} . \tag{2.13}$$

Уровень устойчивости (G_i^q) функционирования ресурса по Д, К, Ц с заданным значением (T_i^q) определяем выражениями:

$$G_i^q = \min\left\{1, \frac{\left|1 - W_i^q\right|}{T_i^q}\right\}, \tag{2.14}$$

$$T_i^q = V_i^q L, \tag{2.15}$$

Тогда, в целом для объекта системы оценка уровня устойчивости (Q_s^q) имеет вид:

$$Q_s^q = \frac{\sum_{i=1}^{n} V_{is}^q G_{is}^q}{\sum_{i=1}^{n} V_{is}^q}. \tag{2.16}$$

Обобщение оценки уровня устойчивости для всей системы (W^q) без учета человеческого фактора получим в виде:

$$W^q = \frac{\sum_{i=1}^{n} V_i^q G_i^q}{\sum_{i=1}^{n} V_i^q}, \tag{2.17}$$

Остается учесть взаимодействие между объектами (аппаратно-программными) системы и ее пользователями, то есть учесть человеческий фактор.

Влияние уровня профессиональной компетенции пользователей (персонала) на устойчивость функционирования СИС как в целом, так и по отдельным ресурсам определяется должностными полномочиями и квалификацией этих лиц. Например, системный администратор с низким уровнем профессиональной компетенции не способен обеспечить заданный уровень устойчивости функционирования системы.

Обозначим:

G_i^q и GH_i^q - уровень устойчивости функционирования ресурса до и после влияния персонала соответственно на *i*-тый ресурс;

H_p - оценка риска нанесения ущерба в СИС от влияния персонала;

GH_{ip}^{q} - индекс должностных полномочий персонала.

Тогда

$$GH_{ip}^{q} = GH_{i}^{q} - (GH_{i}^{q} H_{P}) \quad (2.18)$$

Обобщенная по всем ресурсам оценка (GH^{q}) уровня устойчивости функционирования СИС, с учетом влияния человеческого фактора, определяется по формуле:

$$GH^{q} = \frac{\sum_{i=1}^{n} GH_{ip}^{P}}{n}, \quad (2.19)$$

На основании оценок важности ресурсов системы, уровня устойчивости каждого ресурса и заданного его значения, опасности негативных воздействий и надежности средств парирования получаем рекомендации, сгенерированные ЭС, позволяющие обеспечить уровень устойчивости функционирования СИС в целом не ниже заданного.

Механизм выработки рекомендаций в первую очередь предполагает выявление ресурсов с низким уровнем устойчивости функционирования. Для этого оценку уровня устойчивости ресурса дополняем его важностью и ценностью обрабатываемой информации по Д, К и Ц, после чего сравниваем оценку уровня устойчивости ресурса с требуемым по Д, К и Ц.

Такой подход обеспечивает гибкость при определении рекомендаций с учетом важности ресурса и ценности информации.

Следующим шагом в процедуре генерации рекомендаций для обеспечения заданного уровня устойчивости функционирования СИС является решение задачи оптимизации, которая формулируется в прямом и двойственном (обратном) аспектах:

Прямая оптимизационная задача имеет вид:

Для каждого объекта СИС выбрать СПНВВ (E_{ds}), так чтобы обеспечить максимальный уровень устойчивости (Q_s^q) функционирования системы при заданном уровне затрат на реализацию (C_z) средств парирования:

$$\left.\begin{array}{l} Q_s^q = \dfrac{\sum_{i=1}^{n} V_{is}^q G_{is}^q}{\sum_{i=1}^{n} V_{is}^q} \to \max; \\ \text{при ограничении } \sum_{d=1}^{k} CN_s \le C_z. \end{array}\right\}$$

V_{is}^q и G_{is}^q - оценка важности и уровня устойчивости соответственно, для *s*-го ресурса *i*-го объекта по (Д, Ц, К); CN_s - стоимость всех СПНВВ для *s*-объекта.

Обратная задача оптимизации с учетом ограничения по заданному уровню устойчивости функционирования T_s^q СИС имеет вид:

Для каждого объекта СИС выбрать СПНВВ (E_{ds}), так чтобы обеспечить минимальные затраты (CN_s) на реализацию средств парирования при заданном уровне устойчивости (T_s^q) функционирования системы.

$$\left.\begin{array}{l} CN_s \to \min; \\ \text{при ограничении } Q_s^q = \dfrac{\sum_{i=1}^{n} V_{is}^q G_{is}^q}{\sum_{i=1}^{n} V_{is}^q} \ge Tp_s. \end{array}\right\}$$

Суммарные затраты на реализацию (CN_s) всех СПНВВ для *s*-ого объекта:

$$CN_s = \sum_{d=1}^{k} CN_d . E_{ds}, \qquad (2.20)$$

$$E_{ds} = \begin{cases} 1, & если\ d-ое\ СПНВВ\ включен\ для\ s-огообъекта \\ 0, & в\ противномслучае \end{cases},$$

CN_d - затраты на реализацию *d*-ого СПНВВ.

Тогда общие затраты (CN_c) на реализацию всех СПНВВ применительно ко всей системе равны:

$$CN_c = \sum_{s=1}^{S} CN_s. \quad (2.21)$$

Таким образом, решение приведенных оптимизационных задач обеспечивает выбор такого набора средств парирования негативных воздействий при котором уровень устойчивости функционирования СИС не ниже заданного, а затраты на реализацию оптимального набора средств парирования минимальны.

2.9. Аналитическая модель базы нечетких правил

2.9.1 Способы обеспечения непротиворечивости нечетких правил

Создание продукционной модели системы в условиях неопределенности (нечеткой модели) предполагает использование как результатов непосредственных измерений детерминированных параметров и характеристик, так и экспертных оценок качественных параметров.

Если предположить, что проблема отсутствия противоречий в базе нечетких правил решена заблаговременно, то проверка согласования мнений экспертов не является обязательной. А при использовании только результатов непосредственных измерений задачу моделирования можно отнести к задачам распознавания системы. Более сложная ситуация возникает в случае комплексного использования количественных и качественных оценок, при этом база нечетких правил должна синтезироваться на основе эвристических предположений с уточнением по детерминированным данным. В каждом из этих случаев моделирование предполагает использование соответствующих процедур.

Процедурные модели для детерминированного случая (использование экспериментальных данных, в качестве обучающей выборки) формирования базы нечетких правил с заданной структурой поясним на примере:

пусть, требуется синтезировать базу нечетких правил со структурой *MISO* (x_1, x_2 - входные переменные, y – выходная переменная). Обучающая выборка задана множеством $x_1^{(k)}, x_2^{(k)}, y^{(k)}, \kappa = 1,...,K$ (2.22), где k – количество вариантов обучающей выборки.

Шаг 1. Определение нечетких множеств на входе и выходе.

Если известны границы изменения переменных $x_1 \in \left[x_1^{(\min)}, x_1^{(\max)} \right], x_2 \in \left[x_2^{(\min)}, x_2^{(\max)} \right], y \in \left[y^{(\min)}, y^{(\max)} \right].$, то возможно выделить некоторые отрезки в рамках этих границ. Причем, количество отрезков и их длина выбираются для каждой переменной.

На рисунке 2.5 показан вариант отрезков с заданными функциями принадлежности соответствующих переменных.

Для x_1 определены нечеткие множества с лингвистическими значениями $\{ L_1$ - низкое, M_1 - среднее, H_1 - высокое$\}$, для x_2 - $\{ L_2$, LM_2 - между низким и средним, M_2, HM_2 - между высоким и средним, $H_2 \}$, для y - $\{ L_y, LM_y, HM_y, H_y \}$.

Хотя применимы другие способы разбиения и виды функций принадлежности соответствующие задаваемым отрезкам.

Шаг 2. Разработка базы нечетких правил. Для этого используем два подхода.

Первый вариант заключается в том, что на основе возможных сочетаний нечетких высказываний, формируем множество нечетких правил, общее количество которых определяется соотношением:

$$l = l_1 \cdot l_2 ... l_m \cdot l_y , \qquad (2.23)$$

где $_1$, $_2$, ..., , - число функций принадлежности переменных $x_1, x_2, ..., x_m$; .

Для примера (рисунок 2.5), база нечетких правил имеет вид:

П1: ЕСЛИ x_1 есть L_1 И ... И X_2 есть L_2, ТО y есть L_y ,

П: ЕСЛИ x_1 есть M_1 И...И x_2 есть HM_2, ТО y есть LM_y,

П: ЕСЛИ x_1, есть H_1 И ... И x_2 есть LM_2, ТО y есть HM_y,

П60: ЕСЛИ x_1 есть H_1, И ... И x_2 есть H_2, ТО y есть H_y,

Второй вариант заключается в том, что каждое правило формируется в соответствии с заданной выборкой. При этом для всех переменных необходимо определить соответствующие функции принадлежности на заданных нечетких множествах (рисунок 2.5):

для $x_1^{(1)}: \mu_{L_1}(x_1^{(1)}) = 0.1; \mu_{M_1}\left(x_1^{(1)}\right) = 0.9; \mu_{H_1}\left(x_1^{(1)}\right) = 0.1;$

для $x_2^{(1)}: \mu_{L2}\ (x_2^{(1)}) = 0; \mu_{LM_2}\left(x_2^{(1)}\right) = 0; \mu_{M_2}\left(x_2^{(1)}\right) = 0.2; \mu_{HM_2}\left(x_2^{(1)}\right) = 0.9; \mu_{H_2}\left(x_2^{(1)}\right) = 0$

для $y^{(1)}: \mu_{L_y}(y^{(1)}) = 0; \mu_{LM_y}\left(y^{(1)}\right) = 0.7; \mu_{HM_y}\left(y^{(1)}\right) = 0.3; \mu_{H_y}\left(y^{(1)}\right) = 0$

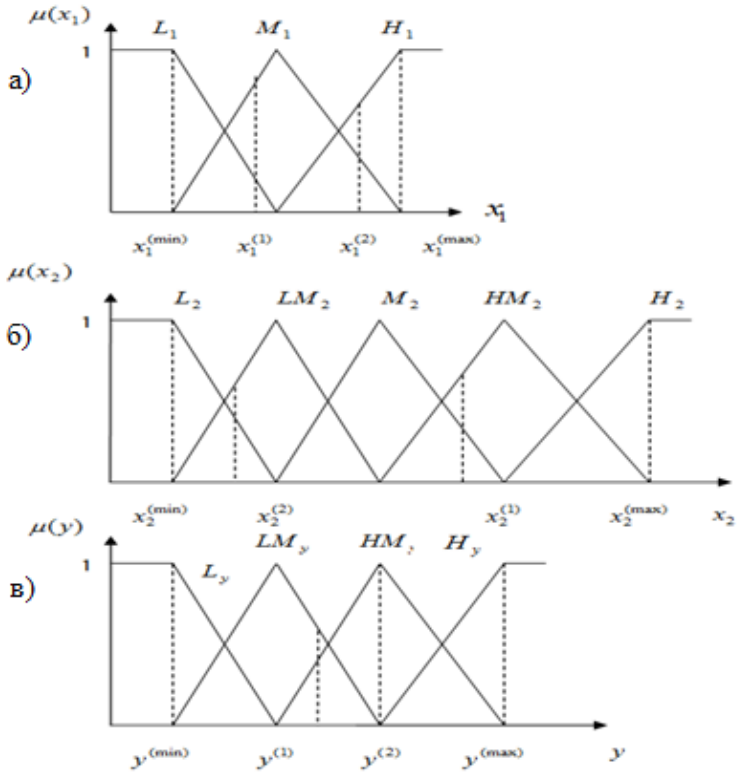

Рисунок 2.5 – Вариант задания функций принадлежности для нечетких переменных: а) $\mu(x_1)$; б) $\mu(x_2)$; в) $\mu(y)$.

Затем, выбирая максимальные значения принадлежности, различных переменной задаем соответствие их нечетких множеств каждой обучающей выборке.

На пример, для $x_1^{(1)}$ таким соответствием будет нечеткое множество $M_1, x_2^{(1)} - HM_{2,} y^{(1)} - LM_y$.

Тогда, варианту обучающей выборки состоящей из переменных $(x_1^{(1)}, x_2^{(1)}, y^{(1)})$ будет соответствовать правило:

ЕСЛИ x_1 есть M_1, И ... И x_2 есть HM_2, ТО y есть LM_y.

Аналогично для обучающей выборки $(x_1^{(2)}, x_2^{(2)}, y^{(2)})$ правило имеет вид:

ЕСЛИ x_1 есть H_1, И ... И x_2 есть LM_2, TO y есть HM_y.

Совокупность подобных нечетких правил образует начальную базу.

Очевидно, что при значительном количестве переменных заданных функциями принадлежности, целесообразно использовать второй вариант процедуры формирования базы нечетких правил.

Шаг 3. Определение значимости правил.

На практике, множество правил может включать и противоречивые, в которых одинаковые предпосылки приводят к разным заключениям, то есть это множество является избыточным. Устранить этот недостаток возможно путем увязки качественных оценок экспертов (эмпирических гипотез) с характером обучающей выборки (экспериментальные данные, результаты детерминированных измерений). Что снизит общее количество правил и возможных противоречий.

Пусть множество переменных в обучающей выборке достаточно полно характеризует особенности моделируемой системы.

Тогда, анализируя правило соответствующее каждой выборке определяем его значимость:

$$r_i = \sum_{k=1}^{K} \mu_{A_{i1}}(x_1^{(k)}) \cdot \mu_{A_{i2}}(x_2^{()k}) ... \mu_{Aim}(x_m^{(k)}) \cdot \mu_{Bi}(y^{(k)}), i = 1, ..., n. \quad (2.24)$$

Шаг 4. Уменьшение объема базы правил. Анализируя полученные значимости правил необходимо исключить из базы, в первую очередь,

противоречащие правила заменив их единственным правилом, имеющим максимальную значимость. Если объем базы требует дальнейшего сокращения количества правил, то из нее удаляются правила с наименьшей значимостью.

Шаг 5. Параметрическая настройка правил в базе. Настройка параметров правил предполагает подбор наиболее подходящих параметров функций принадлежности при которых обеспечивается максимальная «степень активности» соответствующих правил на всех вариантах обучающей выборки.

В случае использования функции принадлежности треугольного вида (рисунок 2.5) процедуре настройки подвергается единственный параметр – мода.

2.9.2 Настройка параметров нечетких правил

Задача настройки параметров нечетких правил, для случая построения нечеткой продукционной модели в виде нечеткой нейронной продукционной сети (*fuzzy-neuralnetwork*/*system*) решается на этапе обучения.

Допустим, что сформирована окончательная безызбыточная и непротиворечивая база нечетких правил типа с *MISO*-структурой.

Тогда для обучающей выборки вида

$$(x_1^{(k)}, x_2^{(k)}, ..., x_m^{(k)}, y^{(k)}), k = 1, ..., K, \qquad (2.25)$$

Процедура настройки заключается в следующем:

Этап 1. Определяем значение переменной $y'^{(k)}$ на выходе в соответствие с принятой нечеткой продукционной моделью на входе которой наблюдаем переменные $x_1^{(k)}, x_2^{(k)}, ..., x_m^{(k)}$, для каждого варианта обучающей выборки.

Этап 2. Вычисляем ошибки $(E^{(k)})$ по всем вариантам обучающей выборки:

$$E^{(k)} = \frac{1}{2}(y'^{(k)} - y^{(k)})^2, k = 1, ..., K. \qquad (2.26)$$

Этап 3. Подстраиваем параметры функций принадлежности нечетких продукционных правил. Используем для подстройки параметров градиентный метод с применением полученной ошибки выходных переменных (2.26).

Тогда, значения $y'^{(k)}$ настраиваем, следующим образом:

$$y'^{(k)} := y'^{(k)} - \eta \frac{\partial E^{(k)}}{\partial y'^{(k)}}, k = 1,..., K, \quad (2.27)$$

где $\eta \in [0,1]$ - коэффициент, определяющий скорость подстройки (обучения).

Настройка $y'^{(k)}$ подразумевает изменение параметров функций принадлежности переменных входящих в продукционное правило, минимизирующие ошибки всех вариантов обучающей выборки (например, моды – рисунок 2.5).

Итерационная процедура (этапы 1-3) настройки параметров считается завершенной и успешной, когда ошибки по каждому варианту обучающей выборки меньше заданного порогового значения (ε).

$$E^{(k)} < \varepsilon, k = 1,..., K. \quad (2.28)$$

Второй вариант окончания процедуры настройки может определяться средней суммарной погрешностью нечеткой продукционной модели на всех вариантах обучающей выборки:

$$E = \frac{1}{K} \sum_{k=1}^{K} (y'^{(k)} - y^{(k)})^2 < \varepsilon. \quad (2.29)$$

Заметим, что применение градиентного метода настройки параметров требует значительных вычислительных ресурсов, поэтому для их снижения часто используют для этих же целей генетические алгоритмы.

2.10 Выводы по главе 2

1. Разработаны основные модели определяющие особенности экспертной системы для определения ценности информации с использованием нечеткой

логики. Обоснован механизм оценки уровня устойчивости и функционирования ресурса СИС и степени надежности защиты СПНВВ на основе анализа основных свойств информации (значимость, расходы на восстановление, ущерб от НВВ), определяющих ее ценность.

2. В результате исследования установлено, что формирование базы знаний для оценки уровня устойчивости СИС необходимо проводить индивидуально для каждой исходной исследуемой системы. При этом обязательно учитывать тот факт, что факторы устойчивого функционирования по-разному проявляются в различных типах систем. Поэтому эти факторы в явном виде отражаются в содержании множества вопросов экспертной анкеты, при этом значимость вопроса определяется степенью влияния фактора на условия устойчивого функционирования СИС (важность ресурсов СИС, степень возможного ущерба от негативных воздействий, уровень надежности защиты средствами парирования).

3. Формализация процесса анализа устойчивости функционирования СИС при НВВ заключается: в оценке ценности информации, значимости ресурсов, возможного ущерба (опасности) от НВВ, уровня надежности защиты используемых средств парирования, уровня устойчивости функционирования СИС; в определении «слабостей» средств парирования негативных воздействий; в синтезе рекомендаций для повышения уровня устойчивости функционирования СИС на основе определения оптимального набора СПНВВ.

4. Разработанные модели экспертной системы обеспечивают исследование риска (ущерба с определенной вероятностью) от негативных воздействий в условиях многофакторного подхода, учитывающего ценность обрабатываемой информации и значимость используемых ресурсов. В тоже время полученные частные оценки устойчивости функционирования отдельных ресурсов в аспектах Д, К, Ц позволяют выявлять уязвимости в используемых СПНВВ для каждого ресурса.

5. Полученная процедура оценки уровня устойчивости функционирования СИС учитывает влияние человеческого фактора через

должностные полномочия и уровень профессиональных компетенций персонала, что очевидно делает оценку устойчивости более полной.

6. Практическое применение экспертной системы позволяет вырабатывать рекомендации по выбору средств парирования негативных воздействий обеспечивающие уровень устойчивости функционирования системы не ниже заданного и минимальные расходы на реализацию варианта СПНВВ.

3 Синтез структуры экспертной системы оптимального выбора СПНВВ и механизма формирования рекомендаций обеспечения требуемой устойчивости функционирования СИС

3.1 Пользовательские требования к системе

Задача оценки устойчивости функционирования СИС при НВВ имеет некоторые сложности. К ним можно отнести: неопределенность и неполноту исходной информации об объектах (ресурсах), подлежащих исследованию, *о* степени риска каждого из возможных НВВ, *о* других существующих факторах, влияющих на уровень устойчивости и усложняющих ситуацию.

Необходимо, чтобы ЭС для оценки устойчивости удовлетворяла следующим требованиям:

1) Простота в использовании. ЭС должна быть рассчитана на широкий круг лиц, которые могут с ней работать.

2) Выполнение следующих функций: оценка угроз НВВ, оценка важности ресурсов СИС (информационных, человеческих, физических).

3) Должна обладать свойствами комплексности, самообучаемости, практической направленности.

4) Использование сгенерированных системой рекомендаций для повышения устойчивости функционирования исследуемой системы.

В таблице 3.1. представлены функциональные требования, необходимые пользователю, которые представлены в виде описанных на естественном языке функций, которые должна выполнять экспертная система. В таблице также перечислены действия, которые должна выполнять система в зависимости от действий пользователя.

Таблица 3.1 – Функциональные пользовательские требования

Описание	Действие	
Инициация процесса	Пользователь должен иметь возможность запуска процесса анализа и оценки устойчивости функционирования СИС.	Система находится в ожидании до того момента, когда пользователь выполнит функцию <создать процесс>
Идентификация ресурсов	Пользователь должен иметь возможность редактировать используемые ресурсы (выбирать из предложенного множества и добавлять новые)	Система отображает списки ресурсов из БД
Определение возможных негативных внешних воздействий	Пользователь должен иметь возможность выбирать из предложенного множества возможных НВВ те, которые воздействуют на ресурс; необходимо учитывать тип ресурса.	Система отображает списки возможных НВВ из БД
Введение структуры СИС.	Система выводит модель каждого объекта, который состоит из разных ресурсов. Пользователь должен иметь возможность уточнять, изменять и вносить новые данные в модель объекта.	Система отображает форму с моделью объектов СИС, предлагает пользователю редактировать и уточнять данную модель.
Оценка ресурсов	Пользователь должен иметь возможность ответить на предлагаемые вопросы для оценки важности ресурсов.	Система отображает список вопросов в соответствии с типом ресурса и системы.
Оценка важности информации, обрабатываемой и передаваемой в СИС.	Пользователь должен иметь возможность ответить на предлагаемые вопросы для оценки важности информации.	Система отображает список вопросов для оценки важности информации в соответствии с типом системы (политической, экономической и т.д.).

Окончание таблицы 3.1

Инициация процесса оценки устойчивости функционирования СИС.	Пользователь имеет возможность инициировать запуск процесса оценки.	Система выводит результат, где отображена оценка устойчивости функционирования каждого ресурса/объекта и системы в целом по Д, К, Ц.
Прерывание	На каждом этапе пользователь может прервать процесс исследования и выйти из программы, не сохраняя записи.	В случае экстренного выхода система предлагает сохранять или не сохранять данные.
Оптимизация	Пользователь должен иметь возможность указывать критерии оптимальности для повышения устойчивости функционирования СИС.	Система предлагает пользователю выбирать критерии оптимизации. После выбора задаются значения критериев оптимизации.
Рекомендации	Пользователь имеет возможность просмотреть отчет (рекомендации) по повышению уровня устойчивости функционирования СИС.	Система генерирует рекомендации и другие отчеты

3.2 Структурная модель ЭС оценки уровня устойчивости функционирования СИС

ЭС предназначенная для проведения оценки уровня устойчивости функционирования СИС при НВВ, многофакторного анализа условий функционирования и выбора оптимального набора СПНВВ, обеспечивающего заданный уровень устойчивости с учетом значимости ресурсов и ценности информации [110, 111].

Решение этой задачи проводится в условиях неопределенности исходной информации и нечеткости экспертных знаний. Подход к решению анализа устойчивости и генерации вариантов по повышению уровня функционирования, основанный на теории нечетких множеств, позволяет формализовать эти нечеткости в базе данных и использовать аппарат нечеткого вывода.

Более подробное описание структуры данной ЭС с указанием всех компонентов и их взаимосвязей представлено на рисунке 3.1 ЭС состоит из следующих главных компонентов: интерфейс эксперта, интерфейс пользователя, база данных, интерактивная система формирования знаний, база знаний, модель приобретения знаний, блок принятия решения и генерации рекомендаций.

Пользовательский интерфейс позволяет вводить данные исследуемой СИС и включает в себя следующие компоненты [111]:

1. Интерфейс, обеспечивающий задание ценности информации и типа исследуемой СИС (блок 2.1).

2. Интерфейс ввода структуры СИС (блок 2.2). Позволяет указать структуру СИС путем добавления объектов и их описаний, а также выбирать ресурсы этого объекта из предложенного списка и добавлять новые.

3. Интерфейс позволяющий задавать негативные воздействия (блок 2.3) из числа возможных.

4. Интерфейс определения существующих СПНВВ (блок 2.4). Пользователю предоставляется возможность ввода СПНВВ и их описаний (путем выбора из предложенного множества), также предлагает добавить новые.

5. Интерфейс определения критериев рекомендаций (блок 2.5), который позволяет пользователю вводить необходимые параметры для генерации рекомендаций по повышению устойчивости функционирования СИС.

6. Интерфейс вывода (блок 2.6). Система отображает перечень объектов, а также набор параметров для каждого из них: значимость, оценки текущего и заданного уровня устойчивости функционирования для каждого ресурса (по Д, К и Ц). Помимо этого, отображаются рекомендации по обеспечению заданного уровня устойчивости функционирования объектов СИС.

Интерфейс эксперта позволяет проводить интерактивный многофакторный анализ свойств системы и состоит из нескольких компонентов:

1. Интерфейс определения ценности информации. Данный интерфейс ЭС позволяет эксперту выбрать тип системы и указать оценки важности вопросов и возможные ответы на них.

2. Интерфейс оценивания значимости ресурсов СИС. Эксперт настраивает систему в зависимости от выбранного типа ресурса: он определяет оценки важности указанных вопросов.

3. Интерфейс синтеза характеристик возможных НВВ. ЭС позволяет эксперту вносить в систему НВВ и проводить оценку возможного ущерба (опасности) от каждого их них.

4. Интерфейс выбора варианта реализации СПНВВ и оценки уровня защиты средствами парирования по Ц, Д и К. ЭС позволяет эксперту вносить в систему дополнительные СПНВВ и оценивать их надежность.

База данных, в которой хранятся текущие данные решаемой задачи.

База знаний, в которой хранятся долгосрочные данные, описывающие рассматриваемую область, и правила преобразования данных этой области. Правила используются в базе данных для определения отношений между событиями, объектами и др. В дальнейшем на их основе делаются логические выводы.

Заполнение экспертной системы знаниями реализуется на основе использования моделей приобретения в интерактивной системе и формирования базы знаний.

Блок принятия решений и генерации рекомендаций (блок 8) реализует механизм рассуждений, позволяющий оперировать со знаниями с целью получения новых знаний.

Весь набор функций экспертной системы можно сгруппировать в четыре группы, которые назовем базовыми функциями, а именно это

подготовка исходных данных, многофакторное оценивание, оптимальный выбор средств парирования для объектов системы и представление отчета.

Рассмотрим взаимодействие компонентов ЭС (рис. 3.1). Из блока 5, формирующего тип и параметры исследуемого объекта, эти данные передаются в блок 6, где интерактивными процедурами блока 7 собственно формируется объект с учетом данных и знаний пополняемых через пользовательский интерфейс. Затем производится оценка рисков (вероятного ущерба) и уровня устойчивости функционирования СИС в условиях заданных негативных воздействий (блок 8).

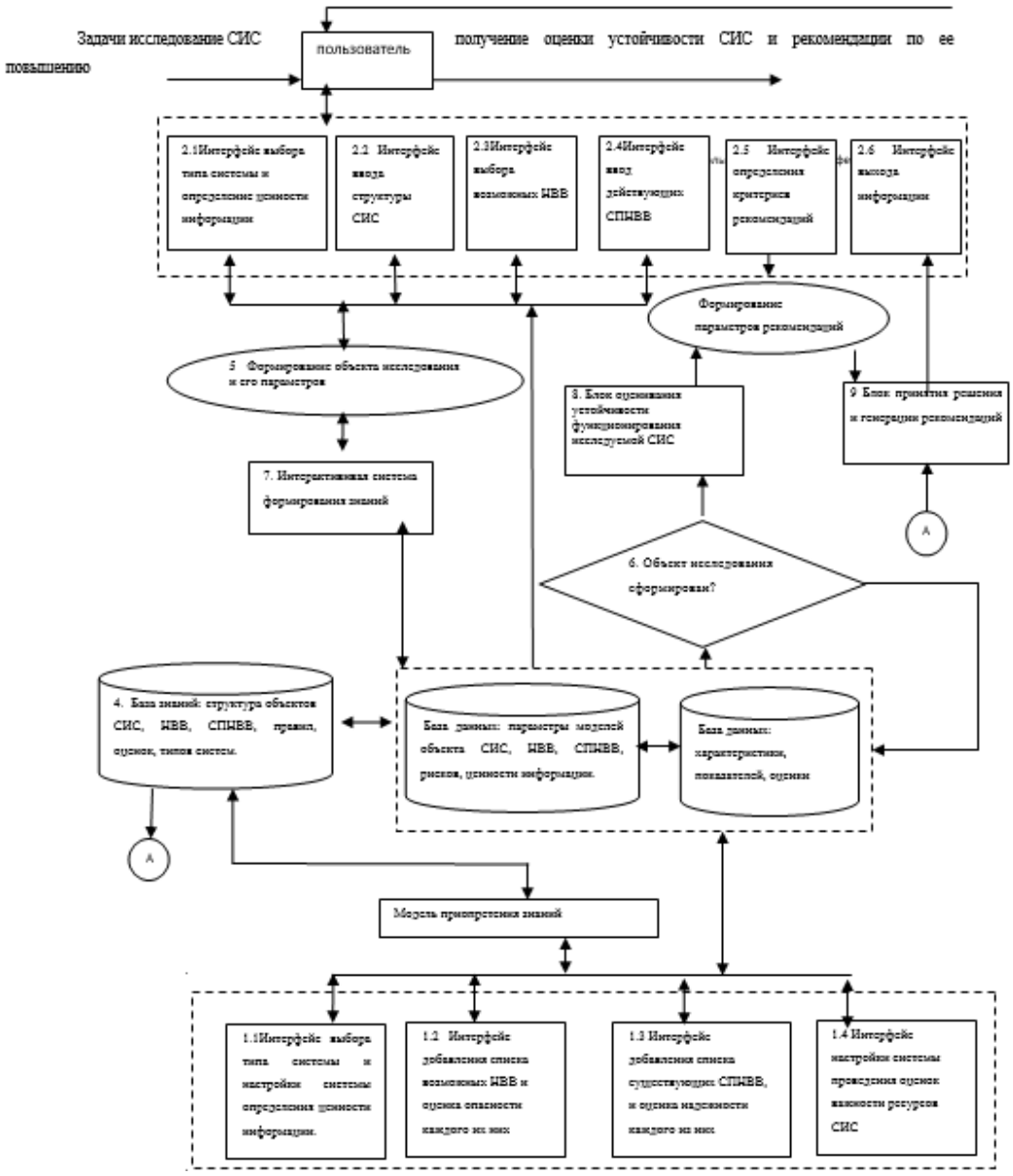

Рисунок 3.1 – ЭС оценки устойчивости функционирования СИС при НВВ

В блоке 9 определяются сведения для выработки рекомендаций на основе данных блока 2.5 (критерии и ограничения оптимизационной задачи) с целью обеспечения уровня устойчивости функционирования СИС не ниже заданного.

3.3 Процедурная модель функционирования экспертной системы

Для прогнозирования поведения системы в конкретных ситуациях необходимо описать ее реакции в ответ на действия эксперта/пользователя. Отражение реакции или поведения системы на определенные действия в определенных ситуациях называется прецедентом.

Прецедент отображает возможный набор реакций системы при взаимодействии с пользователем/экспертом.

Для представления процессов функционирования ЭС необходимо отобразить поведение системы до получения ожидаемого результата в двух режимах работы (режимы работы эксперта и пользователя).

Разработку моделей, описывающих взаимодействие между персоналом и ЭС, будем выполнять при помощи языка *UML* (*UnifiedModelingLanguage* – унифицированный язык моделирования) [123,124].

Диаграммы прецедентов позволяют визуализировать поведение системы с точки зрения взаимодействия с пользователем или экспертом (рисунок 3.2) и (рисунок 3.3). На диаграммах прецедентов представлены функции, которые могут выполнять пользователи (рисунок 3.2) и эксперты (рисунок 3.3) при взаимодействии с ЭС. На рисунке 3.4 представлен интерфейс программы – работа ЭС в режиме пользователя.

Рисунок 3.2 – Диаграмма прецедентов ЭС (режим работы пользователя)

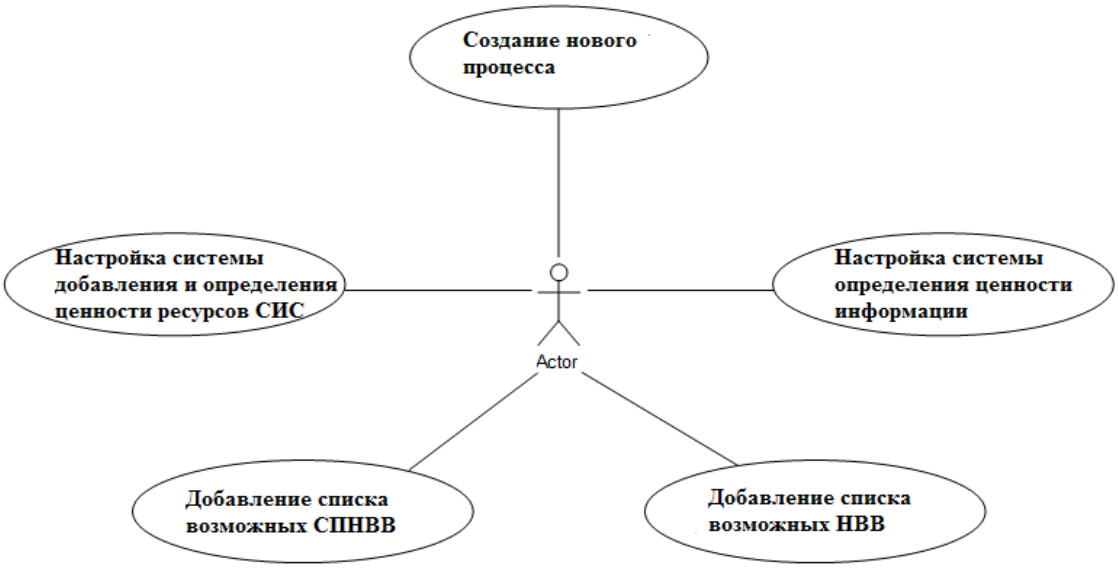

Рисунок 3.3 – Диаграмма прецедентов ЭС (режим работы эксперта)

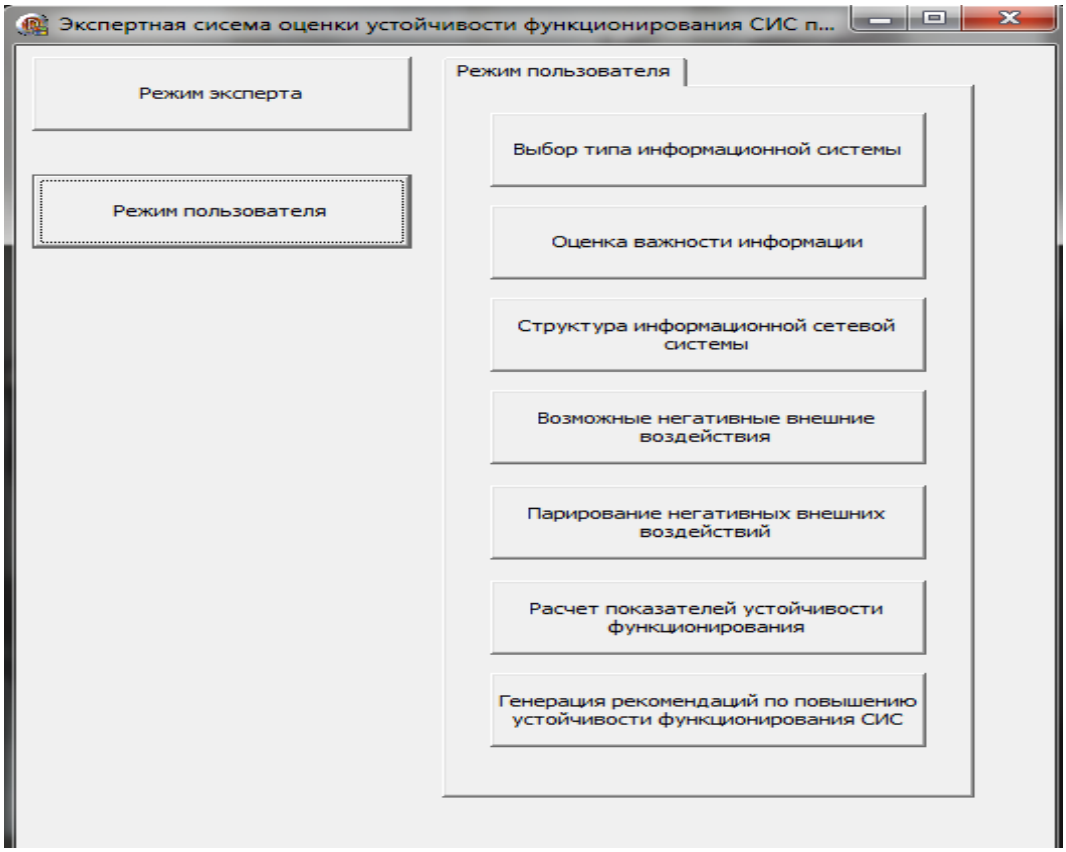

Рисунок 3.4 – Интерфейс пользователя

На рисунке 3.5 представлен алгоритм аутентификации пользователей, по которому ЭС предоставляет уровень доступа согласно типу учетной записи или ограничивает доступ к системе, ели аутентификация не пройдена.

Рисунок 3.5 – процедура авторизации в ЭС

Реализация прецендетов может быть организована как последовательным так и параллельным образом, например, генерация вариантов средств парирования в режиме пользователя выполняется только после задания экспертом критерия и ограничений оптимизационной задачи. В ПРИЛОЖЕНИИ Б проведено описание прецедентов ЭС режима работы пользователя (рисунок 3.2).

На рисунке 3.6 отображена диаграмма деятельности ЭС, выполнена в нотации языка *UML*. Она описывает поведение ЭС в зависимости от действий пользователя. Для полного представления всех видов деятельности системы необходимо описать ее поведение до получения ожидаемого результата.

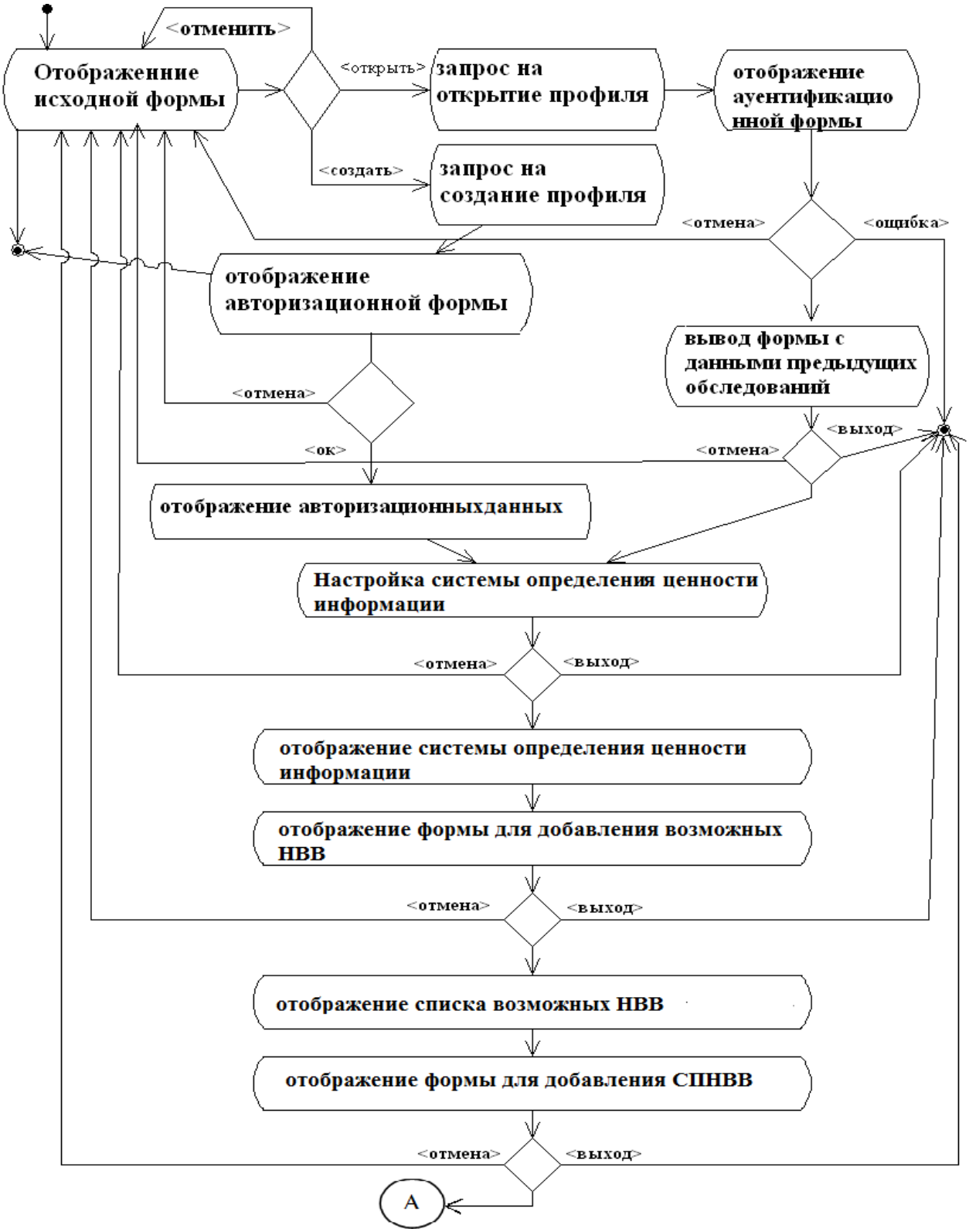

Рисунок 3.6а – Диаграмма деятельности ЭС (режим работы пользователя)

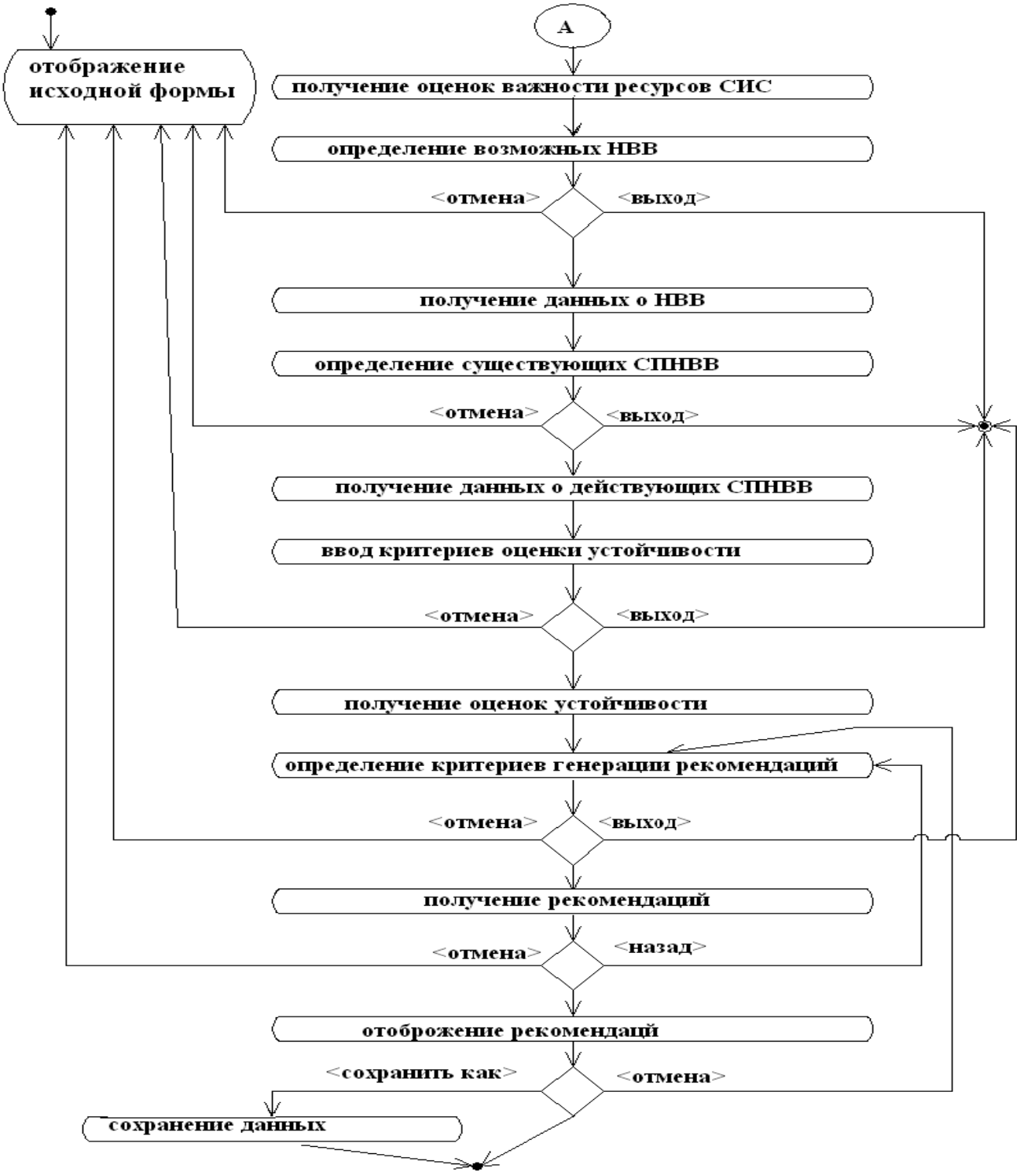

Рисунок 3.6б – Диаграмма деятельности ЭС (режим работы пользователя)

В ПРИЛОЖЕНИИ В проведено описание прецедентов режима ЭС работы эксперта.

Диаграмма деятельности ЭС построенная по прецедентам режима работа эксперта ПРИЛОЖЕНИЕ В приведена на рисунке 3.7.

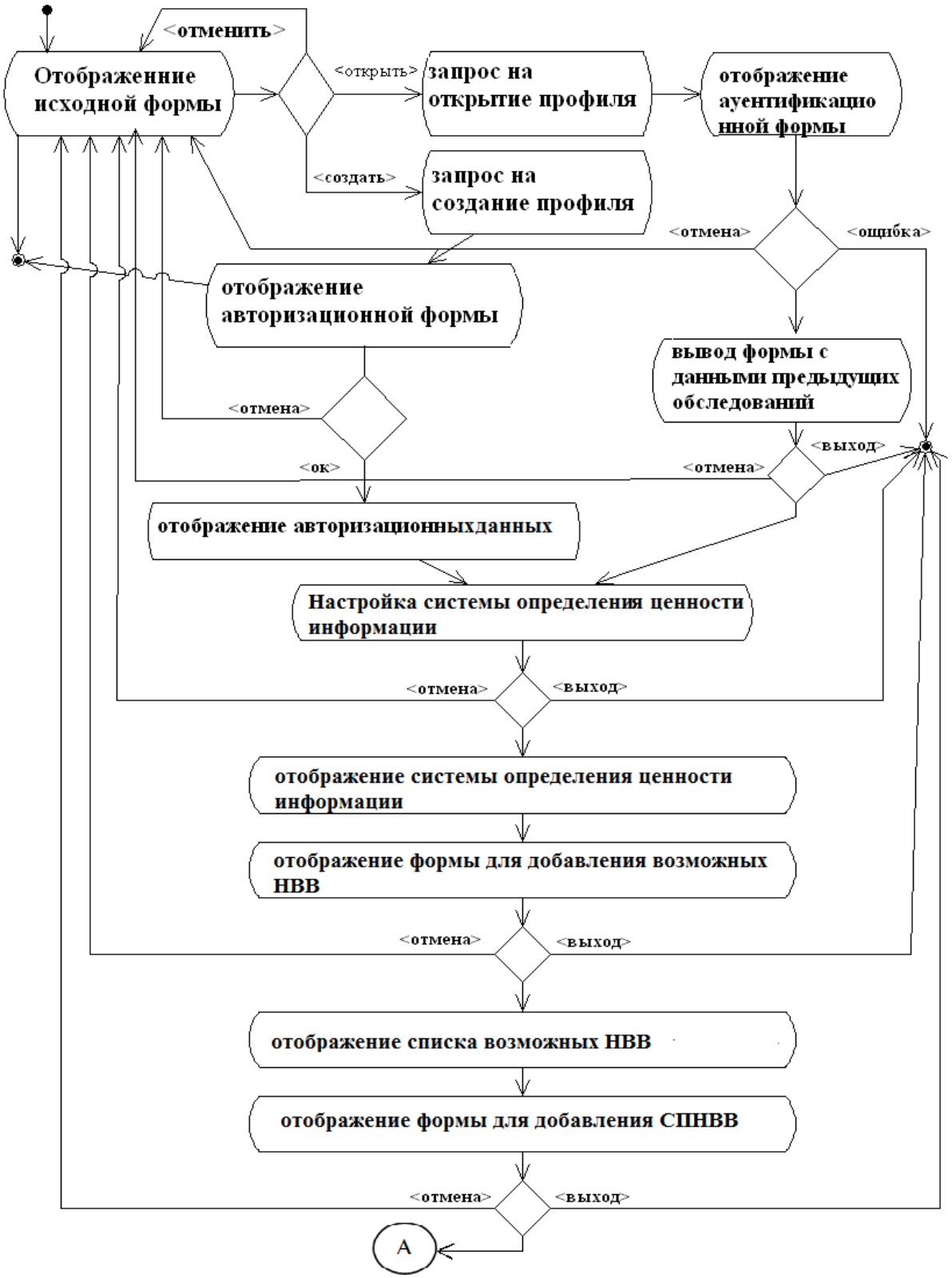

Рисунок 3.7а – Диаграмма деятельности ЭС (режим работы эксперта)

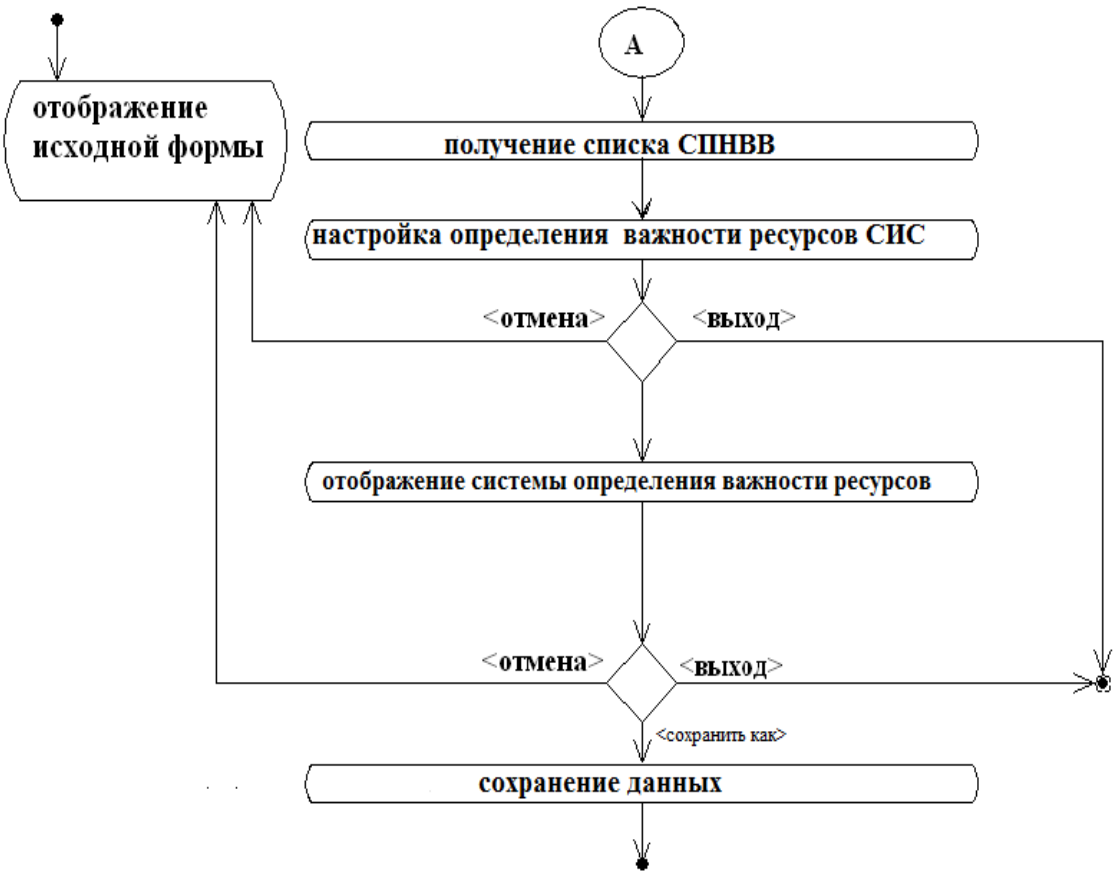

Рисунок 3.7б – Диаграмма деятельности ЭС (режим работы эксперта)

Внутреннее состояние построенной ЭС можно определить с помощью классов и отобразить соответствующей диаграммой. В нотации языка *UML* [117, 123, 124] разработана диаграмма классов, (рис.3.8), которая дает возможность визуального представления всех элементов ЭС, принимающих участие в данной модели.

Для реализации генерации вариантов по обеспечению стабильного функционирования СИС необходимо с вязать классы «*Recommendation*» с классами (*Meansofcounteringthenegativeexternaleffectsdirectory*, *Riskmodel*) отношением зависимости реализации (вызов) и зависимости абстракции (вывод).

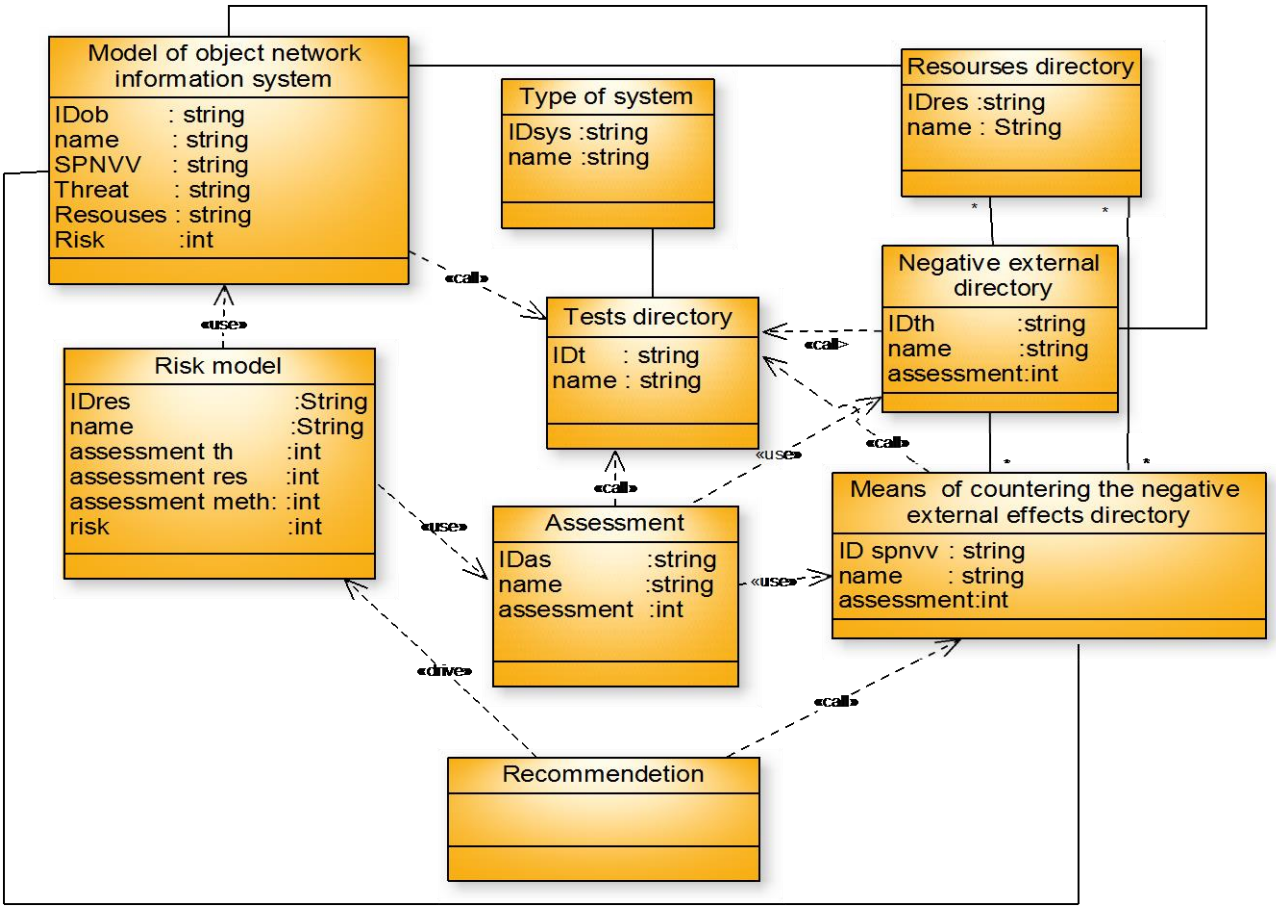

Рисунок 3.8 – Классы созданной ЭС оценки устойчивости функционирования СИС

Таким образом, синтезированные элементы отображающие классы ЭС в рамках модели базы знаний и базы данных определяющие внутреннее состояние системы.

Для реализации генерации вариантов по обеспечению стабильного функционирования СИС необходимо связать классы «*Recommendation*» с классами (*Meansofcounteringthenegativeexternaleffectsdirectory*, *Riskmodel*) отношением зависимости реализации (вызов) и зависимости абстракции (вывод).

3.4 Общие рекомендации оценки уровня устойчивости функционирования СИС при НВВ с помощью разработанной экспертной системы

Рассмотрим работу ЭС по оценке уровня устойчивости функционирования СИС при негативных воздействиях и подбору средств парирования.

Начальным этапом применения ЭС являются:

1) определение типа исследуемой системы. Оценка устойчивости, зависящей от типа исследуемой системы, дает более конкретные результаты, так как факторы, которые влияют на уровень устойчивости СИС, отличаются своим уровнем влияния.

2) оценка ценности информации. Для того, чтобы выявить требуемый уровень качества функционирования СИС, необходимо изучить эту информацию и определить ее ценность.

3) ввод структуры СИС и определение ресурсов каждого объекта.

4) выбор потенциальных негативных воздействий.

5) определение действующих средств парирования НВВ.

На рисунке 3.9 представлена структура СИС кафедры «Информационные системы и защита информации» ФГБОУ ВПО «Тамбовский государственный технический университет», на примере которой проведена оценка уровня устойчивости функционирования в условиях негативных воздействий с выбором оптимального набора средств парирования.

СИС состоит из трех сегментов (каждый из них выделен пунктиром) и 54 рабочих станций. Каждый сегмент СИС включает в себя определенное число рабочих станций, связанных с сервером, аккумулирующим информацию СИС. Каждому сегменту, как и для СИС в целом, с помощью ЭС оценки устойчивости функционирования СИС можно выделить устойчивость функционирования и предложить определенные рекомендации по улучшению устойчивости функционирования при НВВ. Для примера

возьмем один из сегментов СИС (сегмент №1), изображенный на рисунке 4.1, который состоит из сервера и 10-ти рабочих станций.

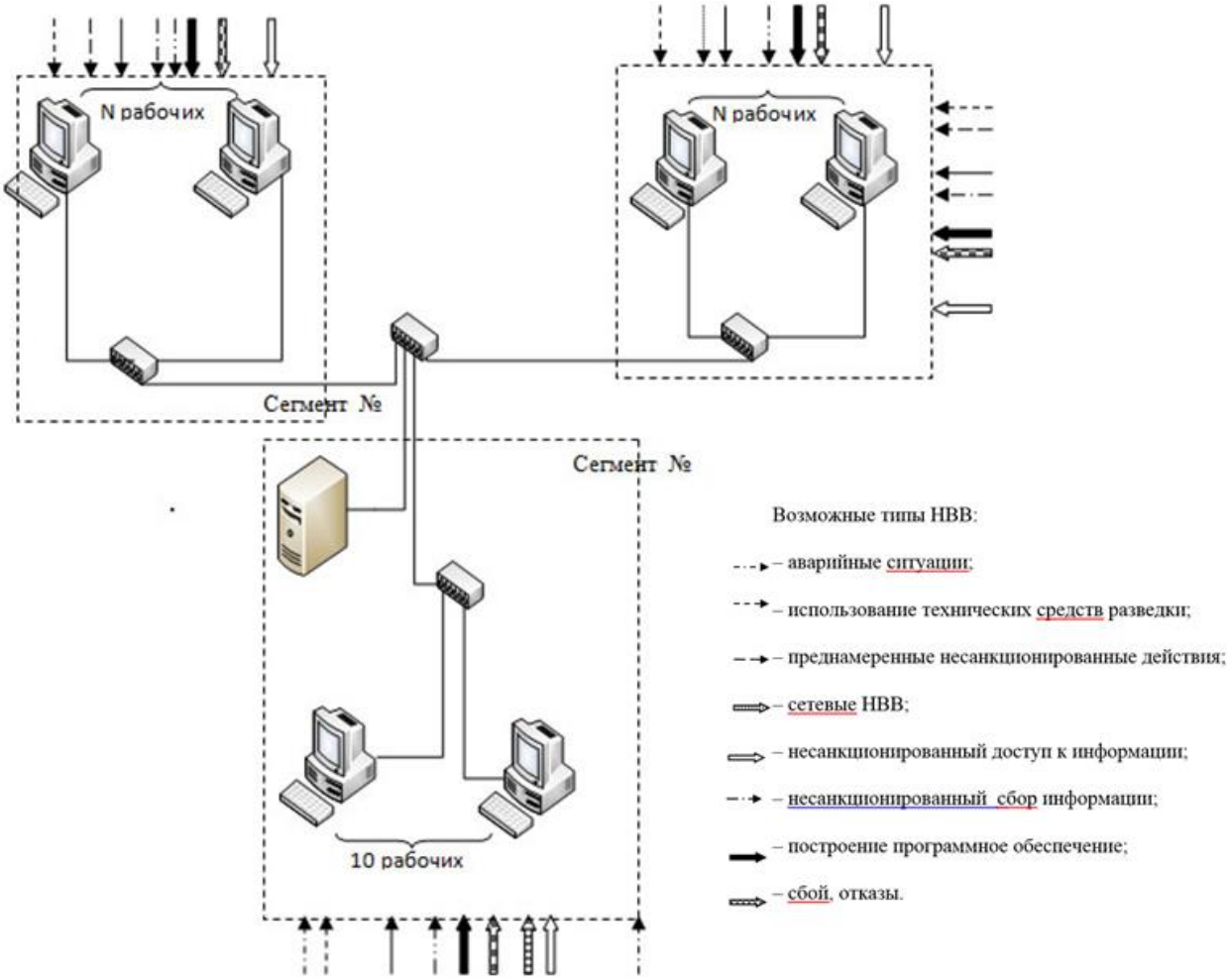

Рисунок 3.9 - Структура исследуемой СИС

Каждый тип НВВ соответствует определенному классу уязвимости. Например, тип «Несанкционированный доступ» (НСД) объединяет воздействия направленные на нарушение устойчивости функционирования по фактору доступность:

1. Несанкционированный доступ к функция операционной системы.
2. Несанкционированный доступ к данным с нарушением конфиденциальности.
3. Несанкционированный доступ к данным с нарушением целостности.
4. Использование вредоносного ПО.

5. Несанкционированный доступ к ресурсу из-за особенности его размещения.

6. И прочее.

Для анализа устойчивости функционирования данного сегмента следует указать перечень ресурсов всех серверов, рабочих станций и информационной сети в целом. Список ресурсов двух серверов и рабочих станций приведен в ПРИЛОЖЕНИИ Г.

На рисунке 3.10 отображаются процедуры выбора типа системы и последующего анализа ценности информации.

Для выбранного типа исследуемой системы предлагается задать необходимость информации, опасность нарушения, стоимость восстановления (рисунок 3.11), с целью определения ее ценности.

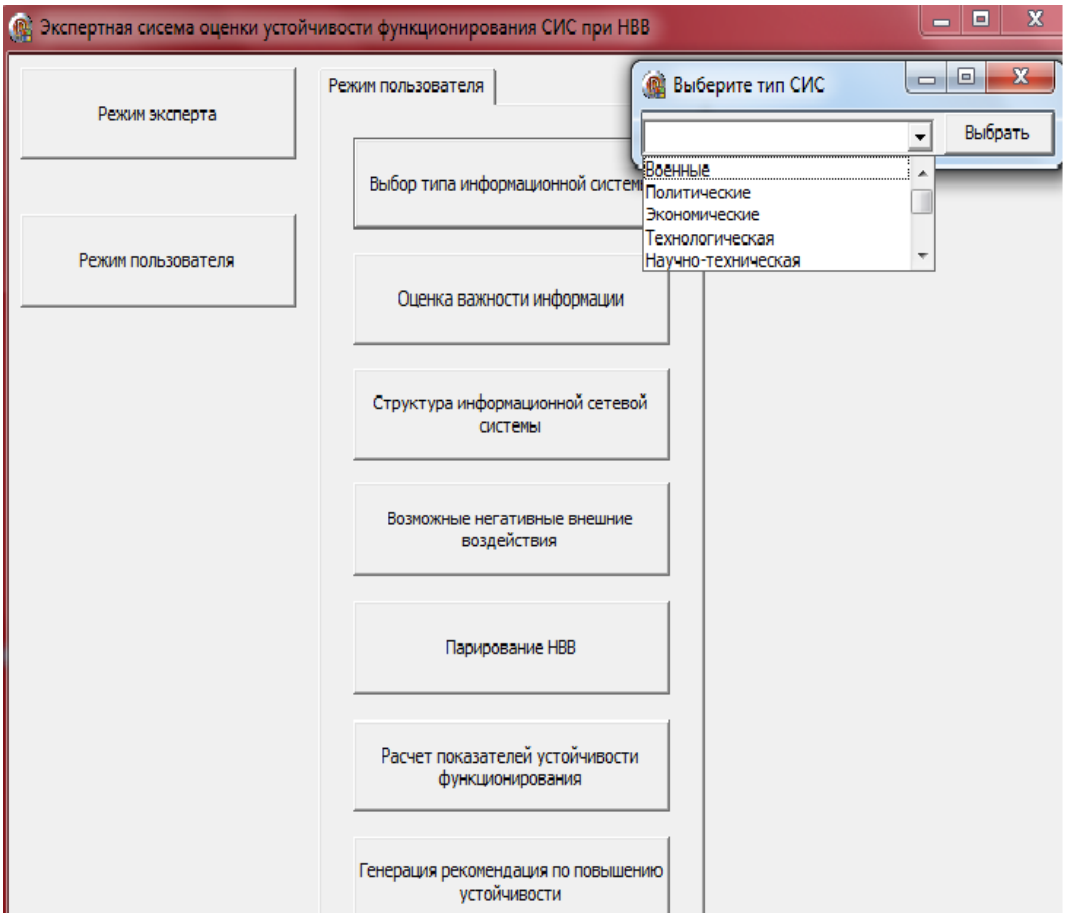

Рисунок 3.10 – Окно выбора типа исследуемой СИС

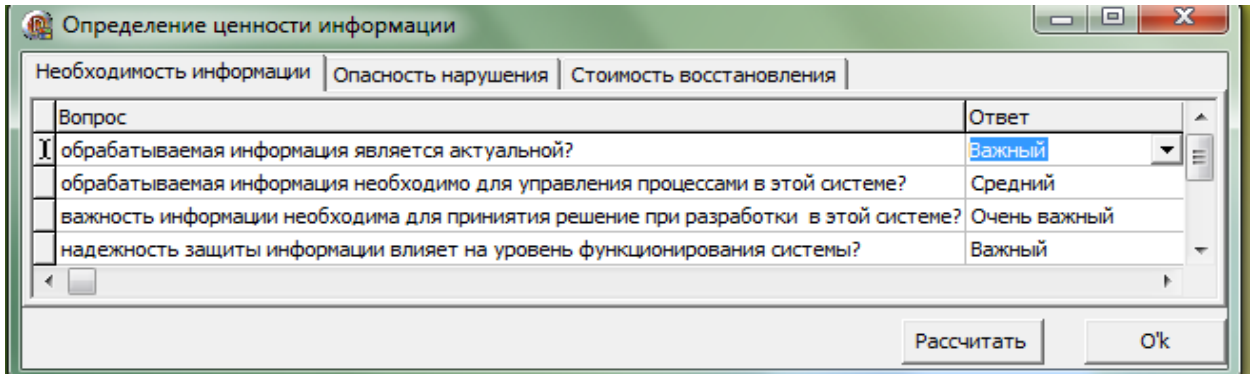

Рисунок 3.11 – Окно определения ценности информации

На втором этапе требуется добавить объекты СИС с соответствующими ресурсами, чем определяется структура исследуемой СИС (рисунок 3.12).

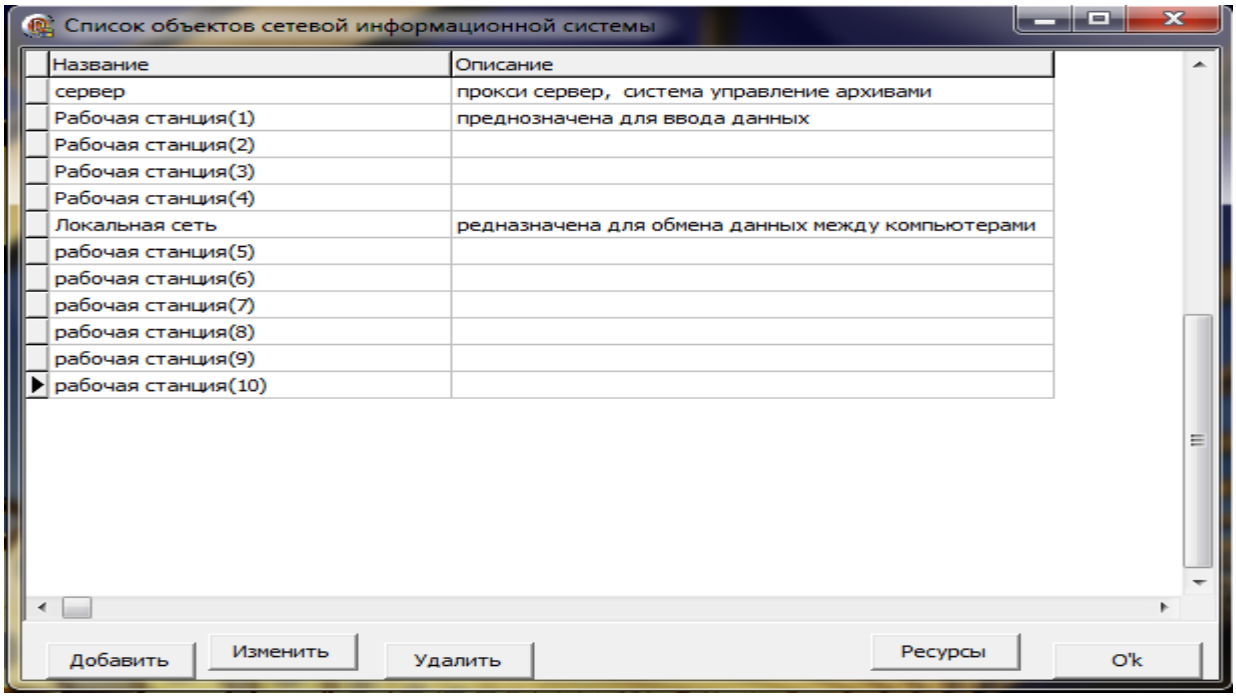

Рисунок 3.12 – Окно задания структуры СИС

В окне «Список ресурсов» следующим после задания структуры задается необходимые ресурсы соответствующего объекта исследуемой СИС (рисунок 3.13).

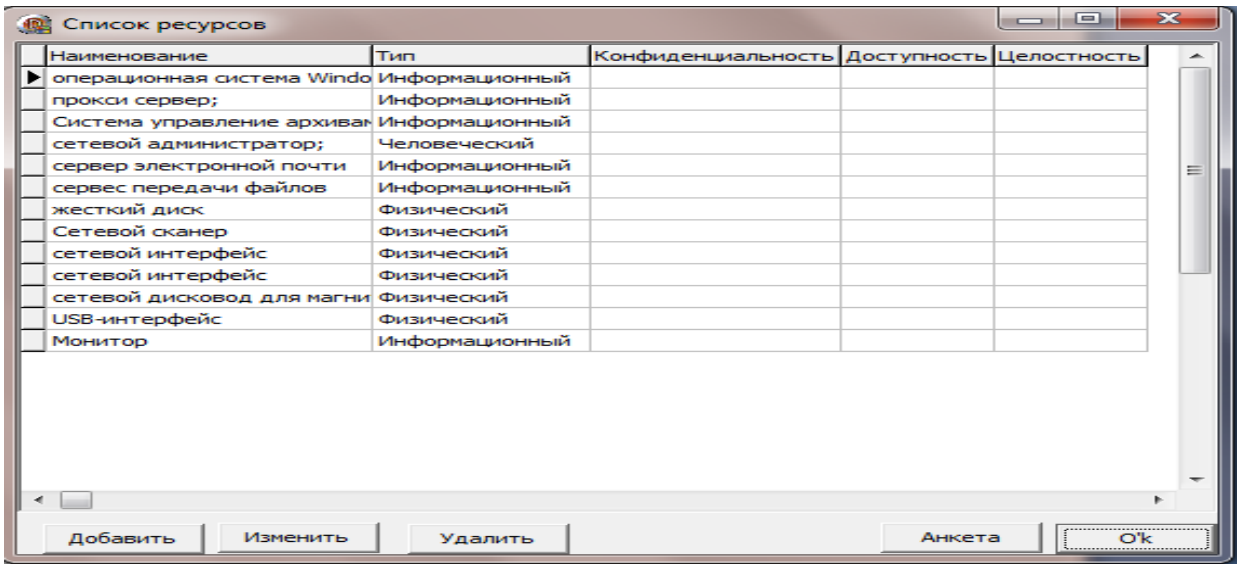

Рисунок 3.13 – Окно добавления ресурсов выбранного объекта

Для анализа важности ресурса требуется указать исследуемый ресурс и нажать кнопку «Анкета». ЭС отображает анкету в зависимости от типа ресурса (рисунок 3.14), которая содержит вопросы для выявления значимости ресурса по К, Д и Ц (рисунок 3.15).

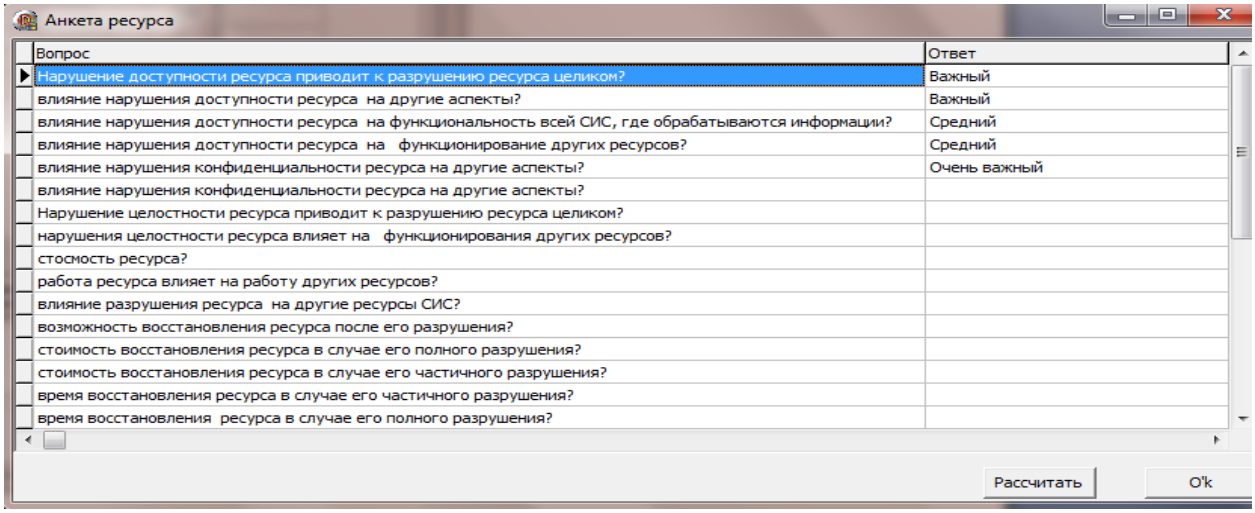

Рисунок 3.14 – Окно задания значимости ресурсов по Д, К и Ц

После выделения всех объектов и их ресурсов исследуемой СИС важно обозначить список возможных НВВ для каждого ресурса. Процесс проведения анализа опасности НВВ совершается в режиме эксперта. Этот процесс описан подробно в главе 2 и 3. И необходимо отметить, что каждое НВВ обладает своей оценкой опасности по Д, К и Ц.

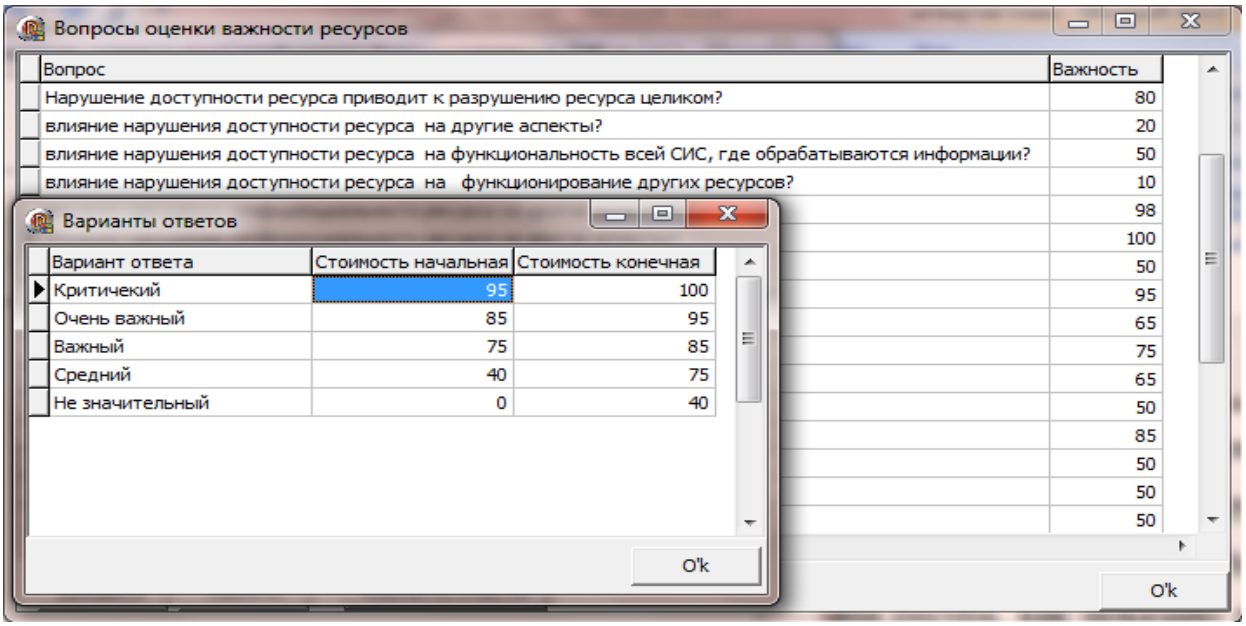

Рисунок 3.15 – Окно добавления вопросов и вариантов ответов

В результате проведения вычислительного эксперимента на примере СИС кафедры добились улучшения показателей (оценки) устойчивости функционирования СИС на 23,5% и снижения затрат на реализацию оптимального набора СПНВВ на 17,4% .

3.5 Выводы по главе 3

1. Определены функциональные требования, необходимые пользователю, которые представлены в виде описанных на естественном языке функций для реализации в экспертной системе.
2. На основе требований к функционалу синтезирована структура экспертной системы и описаны ее основные элементы и их особенности.
3. Поведение системы в конкретных ситуациях как реакция в ответ на действия эксперта/пользователя описано объектно-ориентированными моделями в нотации *UML* (диаграммами прецедентов, деятельности и классов).
4. На основе моделей разработан макет программного обеспечения экспертной системы и проведен вычислительный эксперимент по оценке уровня устойчивости фрагмента СИС кафедры «Информационные системы и

защита информации» ФГБОУ ВПО «ТГТУ» и подбора оптимального состава способов, и средств парирования негативных воздействий.

5. В результате эксперимента добились улучшения показателей (оценки) устойчивости функционирования СИС на 23,5% и снижения затрат на реализацию оптимального набора СПНВВ на 17,4% .

ЗАКЛЮЧЕНИЕ

1. Построена структурная модель знаний для многофакторного оценивания устойчивости функционирования СИС, отличающаяся учетом факторов, которые характеризуют опасность НВВ и надежность защиты применением соответствующих средств и способов защиты, важность главным образом информационных ресурсов СИС, влияющих на устойчивость функционирования СИС и позволяющая разработать программный модуль формирования базы знаний с учетом различных факторов

2. Предложена аналитическая модель оптимальной оценки рисков нарушения устойчивости функционирования СИС при НВВ, отличающаяся использованием показателей ценности информации, важности ресурсов СИС и рисков от НВВ, получаемых экспертным путём и позволяющая оптимизировать рекомендуемый набор СПНВВ по заданному уровню устойчивости функционирования или по минимальным затратам на их реализацию в данных условиях.

3. Предложена процедурная модель оптимальной оценки рисков нарушения устойчивости функционирования СИС при НВВ, отличающаяся использованием продукционных правил определяются ценности информации путем обработки нечетких характеристик важности ресурсов, опасности НВВ и надежности СПНВВ и позволяющая построить экспертную систему многофакторной оценки устойчивости функционирования СИС в условиях различных НВВ.

4. Синтезирована структура экспертной системы оптимального выбора СПНВВ, обеспечивающая требуемую устойчивость функционирования СИС, на основе многофакторной структурой знаний и модулем оптимизации затрат на реализацию СПНВВ в условиях заданных НВВ.

5. Вычислительный эксперимент показал возможность улучшения показателей (оценки) устойчивости функционирования СИС на 23,5% и снижения затрат на реализацию оптимального набора СПНВВ на 17,4% .

Таким образом в диссертационной работе решена научная задача системы моделей информационных процессов экспертной системы, учитываемых многофакторность условий функционирования СИС и оптимизирующие подбор СПНВВ при заданном уровне устойчивости.

Полученные результаты могут быть рекомендованы к использованию в системах требующих оптимизации средств защиты от НВВ, обеспечивающих требуемый уровень устойчивости функционирования СИС.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Петров, В.П. Система обеспечения национальной безопасности России: проблемы формирования и совершенствования: (философ.-политолог. анализ) :дисс. канд. философ. наук / В.П. Петров. - М.,1997. 220с.

2. Проблемы информационно-психологической безопасность: сб.ст. и материалов конф. РАН.-М.:Институт психологии,1996.-65с.

3. Прохожев, А.А. Национальная безопасность : основы теории, сущность , проблемы : учеб. Пособие /А.А.Прохожев .-М.:РАГС,1995.-530с.

4. Сухов, А.Н. О теоретических аспектах национальной безопасности / А.Н.Сухов //Безопасность .-1996.№ 7-12.-С.312-35.

5. Маркоменко, В.И. Роль и место ФАПСИ в системе информационной безопасности России / В.И.Маркоменко // Сборник материалов международной конференции «Безопасность информации». – М.: Автоном. некоммер. организации Рос. Инженерной акад. ,1997.- С.45-50.

6. Гареев,М.А. Нациальная безопасность России как теория и практика/ М.А.Гареев // Безопасность. -1993.-№8.-С.75-80.

7. Безопасность России: системный подход: постановка проблемы // Безопасность.1993.-№5. – С. 15-16.

8. Ницевич, В.Ф. Информационное обеспечение национальной безопасности России: дисс.канд.философ.наук / В.Ф.Ницвич. – М.,1996.-197с.

9. Юсупов, Р.М. Информационная безопасность – основа национальной безопасности / Р.М.Юсупов // Сборник материалов международной конференции «Безопасность информации». – М.: Автоном. некоммер. организации Рос. Инженерной акад. ,1997.- С.110-115.

10. Носков, Ю.Г. Опасность и безопасность с позиции деятельностного подхода / Ю.Г.Носков// Безопасность. – 1998.-№1-2.С.170-179.

11. Концепция национальной безопасности // Рос.газ.-2000.-18 янв.

12. Доктрина информационной безопасности Российской Федерации // Рос.газ.-2000.-10 сент.

13. Закон Российской федерации «О безопасности» Рос.газ.-1992.-6 мая.

14. Андреев, Н.Н. О некоторых направлениях исследований в области безопасности информации / Н.Н.Андреев // Сборник материалов международной конференции «Безопасность информации». – М.: Автоном. некоммер. организации Рос. Инженерной акад. ,1997.- С.94-97.

15. Райх, В.В. Информационное оружие – основное средство обеспечения национальных интересов / В.В.Райх, В.А.Тихонов, В.В.Прудник, А.М. Подкауро, под ред.проф. В.М.Тютюнника,. Тамбов: Изд-во МИНЦ, 2001.

16. Безопасность России: правовые, соц.-экон. и науч.техн. аспекты: основополагающие гос.док.- М.:МГ «Фзнание»,1998.Ч.1.-512с.

17. Белов, П.Г. О семантике, объектах и методах обеспечения национальной безопасности России / П.Г.Белов // Безопасность. – 1998. -№5-6. –С.40.

18. Гацко, М.Ф. угрозы интересам национальной безопасности России и проблемы предотвращения: дис.канд.философ.наук/ М.Ф.Гацко.- М.,1996.-207с.

19. Зегжда. Д.П. основы безопасности информационных систем / Д.П.Зегжда, А.М.Ивашко.- М.: Горячая линия – Телеком, 2000.-452с.

20. Манилов, В.Л. Угрозы национальной безопасность / В.Л.Манилов // Воен.мысль. -1996. - №1.С.7-17.

21. Манилов, В.Л. Национальная безопасность: ценности, интересы, целы/ В.Л.Манилов // Воен.мысль. -1995. - №6.С.29-40.

22. Ballou, R.H. Commercial Software for Locating Warehouses an Other Facilities / R.H. Ballou and J. Masters // Journal of Business Logistics. 1993. - 14:2.

23. Chu, P.C. Induced System Restrictiveness: An Experimental Demonstration / P.C. Chu and J.J. Elam // IEEE Transactions on Systems, Man and Cybernetics. 1990. - 20. - P.195-201.

24. Locating Tax Facilities : A graphics Based Microcomputer Optimization Model, Management Science / P.D. Domich, K. L. Hoffman, R. H. F. Jackson and M. A. McClain. 1991. - 37:8. - P. 960-979.

25. Hwang. Steiner, F.K. Tree Problems / F.K. Hwang and D.S. Richards // Networks. 1992. - Vol. 22. - P. 55-89.

26. Kawatra, R. A Multicommodity Network Flow Application For The Capacitated Minimal Spanning Tree Problem / R. Kawatra // Opsearch. 1994. - 31,4.-P. 296-308.

27. Pirkul, H. Locating Concentrators in Centralized Computer Networks / H. Pirkul and V. NAGARAJAN // Annals of Operations Research. 1992. - 36. -P. 247-262.

28. Вишневский, В.М. / В.М. Вишневский, Д.Л. Белоцерковский // Автоматика и телемеханика. — 1997. -№ 1.-С. 108-120.

29. Вишневский, В.М. Принципы построения единой системы продажи и бронирования билетов на транспорте / В.М. Вишневский, А.В. Ризов, Е.В. Федотов // ВКСС connect. 2001. - № 1. - С.80-85.

30. Назаров, А.Н. Модели и методы расчета структурно-сетевых параметров сетей АТМ / А.Н. Назаров. М. : Изд-во «Горячая линия - Телеком», 2002. - 256 с.

31. Requirements for Traffic Engineering Over MPLS / D.O. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, J. McManus // IETF Draft, draft-ietf-mpls-traffic-eng-00.txt. October 1998.

32. Gail, H.R. Spectral analysis of M|G|1 and G|M|1 type Markov chains / H.R. Gail, S.L. Hantler, B.A. Taylor // Advances in Applied Probability. 1996. - Vol. 28.-P. 114-165.

33. Gelenbe, E. (Ed.) Feature issue on G-networks / E. Gelenbe (Ed.) // European J. of Oper. Res. 2000. - Vol. 126P.

34. Gelenbe, E. G-networks with multiple class of signals and positive customers / E. Gelenbe, A. Labed // European J. of Oper. Res. 1997. - Vol. 10. — P. 1-13.

35. Gelenbe, E. Introduction to queueing networks / E. Gelenbe, G. Pujolle. -N.Y. : John Wiley, 1998.- 244P.

36. Grassmann, W.K. Matrix analytic methods / W.K. Grassmann, D.A. Stanford // Computational Probability. Boston : Kluwer Academic, 2000. -P. 153 - 203.

37. Trivedi Queueing Networks and Markov Chains / Gunter Bolch, Stefan Greiner, Hermann de Meer and Kishor S. // John Wiley & Sons, Inc. -1998.- 726 p.

38. He, L. Connection Admission Control Design for GlobeView 2000 ATM Core Switches / L. He, A.K. Wong // Bell Labs Tech. J. - January - March 1998-P. 94-110.

39. Kawamura, R. Implementation of self-healing function in ATM networks based on virtual path concept / R. Kawamura, K. Sato, I. Tokizawa // IEEE. 1995. — P. 303-311.

40. Kulkarni, V.G. Retrial queues revisited / V.G. Kulkarni, H.M. Liang // Frontiers in Queueing. Boca Raton : CRC Press, 1997. - P. 19-34.

41. On the self-similar nature of Ethernet traffic (extended version) / W.E. Leland, M.S. Taggu, W. Willinger, D.V. Wilson // IEEE/ACM Trans, on Networking. 1994. - Vol. 2, N 1. - P. 1-15.

42. Mitrani, I. The spectral expansion solution method for Markov processes on lattice strips / I. Mitrani // Advances in Queueing. Boca Raton : CRC Press, 1995.-P. 337-352.

43. Murakami, K. Comparative study on restoration schemes of survivable ATM networks / K. Murakami, H.-S. Kim // IEEE INFOCOM . 1997. - N 5.- P. 1-8.

44. Ng Chee. Hock Queueing Modeling Fundamentals. John Wiley & Sons, Inc. 1997.- 222 P.

45. Orda, A. Routing with End-to-End QoS Guarantees in Broadband Networks / A. Orda // IEEE/ACM Transactions on Networking. 1999. - Vol. 7, N3.-P. 365-374.

46. Porotsky, S. Discrete Markov model of the ATM network node / S. Porotsky, V. Vishnevsky // Proceedings of the conference «Distributed Computer Communication Networks. Theory and Applications». Israel, 1996. - P. 223-227.

47. Reilly, J. Scheduled Connections: Managing Temporal Constraints on Broadband Network Resources / J. Reilly, M. Abate // Proceedings of IS& N'98. May 1998. Lecture Notes in Computer Science. — Springer.

48. Rubinstein, R.Y. Discrete Event Systems : Sensitivity Analysis and Stochastic Optimization via Score Function Method / R.Y. Rubinstein, A. Shapiro., -John Wile & Sons,- 1993.

49. Salama, H. A. Distributed Algorithm for Delay- Constrained Routing / H. Salama, D. Reeves, Y. Viniotis // Proc. INFOCOM'97 1997.

50. Syski, R. A personal view of queuing theory / R. Syski // In : Frontiers in Queueing- Boca Raton-New York-London-Tokyo : CRC, 1997. -P. 3-18.

51. Vishnevsky, V. Architecture of Moscow scientific society backbone and employment of radio spread spectrum technology / V. Vishnevsky, V. Vorobjev // Proceedings IV Russian-German Seminar on Integrated Networks and Flow Control. Moscow, 1994.

52. Vishnevsky, V. Combinatoric Algorithm of the Synthesis of the Data Transmission Network Topological Structure / V. Vishnevsky // Proceedings Conference INFO-94. Tel-Aviv (Israel), 1994.

53. Vishnevsky, V. On an algorithm of topological optimization of data networks / V. Vishnevsky, D. Belotserkovski // in: Proceedings of the conference «Distributed Computer Communication Networks. Theory and Applications». - Israel, 1996.-P. 131-138.

54. Wu, T.-H. Fiber Network Service Survivability / T.-H. Wu. Artech House, 1992.

55. Xiong, Y. Restoration strategies and spare capacity requirements in self-healing ATM networks / Y. Xiong, L. Mason // IEEE. 1997. - N 5.

56. Gupta, R. Problems in Communication Network Design and Location: Planning; New Solution Procedures / R. Gupta. Ph. D. dis. - The Ohio State University, 1996.

57. Мельников, Ю.Е. Критерии и модели оценки живучести систем телеобработки / Ю.Е. Мельников, В.А. Мясников. М. : МЭИ, 1988. - 60с.

58. Мельников, Ю.Е. Модель комплексной оценки и обеспечения живучести распределенных информационно-вычислительных систем / Ю.Е. Мельников, Ж.С. Сарыпбеков // Материалы II Всесоюзной науч.-техн. конф.- М. : 1988.

59. Березюк, Н.Т. Живучесть микропроцессорных систем управления / Н Н.Т. Березюк, А.Я. Гапунин, Н.И. Подлесный. Киев : Техника, 1989. - 143 с.

60. Васильев, О.П. Об одном подходе к оценке живучести многофункциональных территориально-распределенных информационно-вычислительных систем / О.П. Васильев, Ю.Н. Мельников // Автоматика и телемеханика- 1981 .-№ 12.-С. 133-137.

61. Boer, J.L. A survey of some theoretical aspects of multiprocessing / J.L.Boer//ACM Comput. Surv. 1993.-Vol. 5, N 1. - P. 31-80.

62. Диллон, Б. Инженерные методы обеспечения надежности систем / Б. Диллон, Ч. Сингх. М. : Мир, 1984. - 320с.

63. Димитриев, Ю.К. Вычислительные системы из мини-ЭВМ / Ю.К. Димитриев, В.Г. Хорошевский. М. : Радио и связь, 1982. - 304с.

64. Сидак, А.А. Формирование требований безопасности современных информационных технологий / А.А. Сидак. – М. : Изд-во Моск. гос. ун-та леса, 2001. – 412 с.

65. Громов, Ю.Ю. Информационная безопасность и защита информации / Ю.Ю.Громов,В.О.Драчев,О.Г.Иванова,Н.Г.Шахов. – М. :Изд-во" Нобелистика", 2008. – 126 с.

66. Биячуев, Т.А. Безопасность корпоративных сетей / Т.А Биячуев, // под ред. Л.Г.Освецкого. – СПб: СПб ГУ ИТМО, 2004.- 161 с.

67. Исаева, В. Как обосновать затраты на информационную безопасность? [Электронный ресурс] / В. Исаева. – Режим доступа :http://www.networkdoc.ru. – Загл. с экрана.

68. Остапенко, Г.А. Методика оценки защищенности для пуассоновского дискретного распределения вероятностей ущерба от компьютерных атак / Г.А. Остапенко, О.А. Казьмин, Е.В. Субботина, Л.В. Пентюхин // Информция & безопасность. – 2006. – № 1. – С. 100–103.

69. Остапенко, Г.А. Оценка рисков и защищенности атакуемых кибернетических систем на основе дискретных распределений случайных величин / Г.А. Остапенко // Информация & безопасность. – 2005. – № 2. – С. 70–76.

70. Остапенко, Г.А. Методика оценки параметров риска с применением непрерывных распределений вероятностей ущерба / Г.А. Остапенко // Информация и безопасность. – 2006. – № 1. – С. 55–58.

71. Малюк, А.А. Информационная безопасность. Концептуальные и методологический основы защиты информации / А.А. Малюк. – М. : Новое издание, 2003. – 386 с.

72. Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел / под ред. А.А. Чекалина. – М. : Горячая линия–Телеком, 2006. – 452 с.

73. Алексенцев, А.И, Издательство: Журнал "Управление персоналом" Издательство: Журнал "Управление персоналом", 2003г. 200с ,ISBN: 5-95630-004-3.

74. Фатьянов, А. А. Тайна и право (Основные системы ограничений на доступ к информации в российском праве): Моногр. / А. А. Фатьянов. - М. : Изд-во МИФИ, 1998. - 288с. - ISBN 5-7262-0271-6

75. Духин, А.А. Теория информации**:** учебное пособие / А.А. Духин. М.: Гелиос АРВ.2007. – 248с.

76. Остапенко, Г.А. Опасность, ущерб, и риски систем / Остапенко Г.А, Батищев Р.В. учебное пособие: Воронеж, 2007.

77. Федеральный закон (О государственной регистрации прав на недвижимое имущество и сделок с ними) № 85 122-Ф3 от21 июля 1997 г.//собрание законодательства РФ:офиц.изд.-1997.-№30.-Ст.3594.

78. Иванов, А.А. Чрезвычайные ситуации в системе защиты информации /А.А.Иванов, В.В.Шарлот//Конфидент.-2000.-№4-5.-С.10-22.

79. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин.//учеб.пособие. – М. : ИД «ФОРУМ»:ИНФОРА-М, 2008.- 416 с.

80. Девянин, П.Н. Теоретические основы компьютерной безопасности :учебное пособие для вузов /П.Н. Девянин, О.О. Михальский, Д.И. Правиков и др. - М.:Радио и связ,2000.-192с.

81. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защита информации / А.А. Малюк // учеб. пособие.- М. : Горячая линия-Телеком, 2004.-280с.

82. Гераситенко, В.А. Защита информации в автоматизированных системах обработки данных / В.А. Гераситенко.М .: Энергоатомиздат, кн. 1 и 2, 1994.- 400с.

83. Хоффман Л.ДЖ Современые методы защита информации . Ппр. С ангиз. –М.:советское радио 1980.

84. Расторгуев, С.П. Программные методы защиты информации в компьютерах и сетях./ С.П. Расторгуев. – М.: «Агентства Яхтсмен». 1993.

85. Гайкович С.П, Ершов Д.В, Основы безопасности информационной технологии, учебное пособие М.:МИФИ. 1995.

86. Белов, Е.Б. Основы информационной безопасности. / Е.Б. Белов, В.П. Лось // Москва, Горячая линия – Телеком, 2006.-544с.

87. Малюк, А.А. Введение в защиту информации в автоматизированных системах / А.А Маюк, С.В. Пазизин, Н.С. Погожи. - М: Горячая линия-Телеком, 2001.-148с.

88. Скиба, В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов - М. : Питер, 2008. -320с.

89. Торокин, А.А. инженерно-техническая защита информации / А.А. Торокин - М. : Гелиос АРВ,2005. - 960с

90. http://www.elvis.msk.su/files/class.pdf. Вихорев Сергей Викторивич. М

91. Демин В.С. Автоматизированные банковские системы. — М. : Москва: Менатеп-Информ, 2001г. – 325 с.

92. Гайкович, В., Першин А. Безопасность электронных банковских систем / В. Гайкович, А. Першин //Под ред. Ю.В. Гайковича. — М.: Единая Европа, 1994.

93. Остерлох, Х. TCP/IP. Семейство протоколов передачи данных в сетях компьютеров. / Х. Остерлох. – М. : ДиаСофтЮП, 2002г.- 576 с.

94. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования .изд.офиц.-Введ.1996-01-01.-[электронный ресурс].-Электрон. Дан.-Режим доступа:http://www.nist.ru/hr/doc/gost/5073-95.htm.-Загл.с экр.

95. «Современные методы и средства анализа и контроля рисков информационных систем компаний CRAMM, RiskWatch и ГРИФ» <http://www.ixbt.com/cm/informationsystem-risks012004.shtml>.

96. «Затраты на ИТ-защиту: ищем золотую середину», <http://www.cnews.ru/reviews/free/consulting/practics/risks.shtml>.

97. «Обзор существующих методов оценки рисков и управления информационной безопасностью», <http://ocenkariskov.narod.ru/PolikOtc.html>

98. Ярочкин, В.И. Система безопасности фирмы / В.И. Ярочкин. – 2-е изд. – М. : Ось-89, 2003. – 352 с.

99. Щеглов, А.Ю. Защита компьютерной информации от несанкционированного доступа / А.Ю. Щеглов. – СПб. : Наука и техника, 2004. – 384 с.

100. Фленов, М. Компьютер глазами хакера / М. Фленов. – СПб. : БХВ-Петербург, 2005. – 300 с.

101. Куприянов, А.И. Основы защиты информации / А.И. Куприянов – М. : Академия, 2008. – 256 с.

102. Устинов, Г.Н. Основы информационной безопасности / Г.Н. Устинов. – М. : Синтег, 2000. – 248 с.

103. Бармен Скотт. Разработка правил информационной безопасности / Скотт Бармен. – М. : Вильямс, 2002. – 208 с.

104. Бузов, Г.А. Защита от утечки информации по техническим каналам: Учебное пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – М. : Горячая линия–Телеком, 2005. – 416 с.

105. Романцов, А.П. Криптография и стеганография / А.П. Романцов ; под ред. А.В. Петракова. – М. : РИО МТУСИ, 2002. – 320 с.

106. Баутов, А. Стандарты и оценка эффективности защиты информации / А. Баутов // Стандарты в проектах современных информационных систем : докл. на III Всерос. практ. конф., Москва, 23–24 апреля 2003 г. / Президиум РАН. – М., 2003.

107. Баутов, А. Экономический взгляд на проблемы информационной безопасности / А. Баутов // Открытые системы. – 2002. – № 2. – С. 7–9.

108. Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 г. № 149-ФЗ // Рос.газ. – 2006. – 29 июля. – С. 2.

109. «Актуальность задачи обеспечения информационной безопасности для бизнеса», <http://www.dsec.ru/about/articles/ar_compare/>.

110. Аль-Балуши, Интеллектуальная информационная система оценки устойчивости функционирования сетевых информационных систем. Техника и безопасность /Аль-Тамими Н.Ю., Аль-Балуши М.П., Ауад М., Лыонг Хак Д., Минин Ю.В //объектов уголовно-исполнительной системы-2011: сборник материалов Международной научно-практической конференции: в 2

т./ФКОУ ВПО Воронежский институт ФСИН России. – Воронеж: ИПЦ «Научная книга». – Т.1. – 2011. – С.382-388

111. Аль-Балуши, Некоторые аспекты интеллектуальной информационной системы оценки функционирования сетевых информационных систем. Техника и безопасность /Аль-Балуши М.П., Аль-Тамими Н.Ю., Ауад М., Лыонг Хак Д., Минин Ю.В// объектов уголовно-исполнительной системы-2011: сборник материалов Международной научно-практической конференции: в 2 т./ФКОУ ВПО Воронежский институт ФСИН России. – Воронеж: ИПЦ «Научная книга». – Т.1. – 2011. – С.388-394

112. Аль-Балуши, Оценка надежности средств парирования внешних воздействий. Техника и безопасность / Аль-Балуши М.П., Аль-Тамими Н.Ю., Ауад М., Лыонг Хак Д., Минин Ю.В// объектов уголовно-исполнительной системы-2011: сборник материалов Международной научно-практической конференции: в 2 т./ФКОУ ВПО Воронежский институт ФСИН России. – Воронеж: ИПЦ «Научная книга». – Т.1. – 2011. – С.394-399

113. Аль-Балуши, Применение цепных дробей для оценки живучести сетевых информационных систем в условиях неопределенности /А.И. Елисеев, М.П. Аль-Балуши, М. Ауад, Хак Д. Лыонг// Математические методы и информационно-технические средства: Труды VIII Всероссийской научно-практической конференции, 22-23 июня 2012 г. – Краснодар: Краснодарский университет МВД России, 2012. – 278 с. – С.71 (1 с.)

114. Аль-Балуши , Система формирования знаний в интелектуальнои информационной системе оценки функционирования сетевых информационных систем,/ М. Аль-Балуши, Н.А. Овчинников, В.В. Паладьев, В.Е. Дидрих// Конференция Воронежского института ФСИН,2013

115. 8. Аль-Балуши , Процедура оценки надежности средств парирования внешних воздействий / М. Аль-Балуши, , В. Е. Дидрих // Международная конференция , «Актуальные проблемы прикладной математики, информатики и механики»,Конференция Воронежского института ФСИН,2013.

116. Аль-Балуши, Использование математического аппарата нечеткой логики для определения пертинентности результатов поиска текстовых сведений. /Д.В. Поляков, М.П. Аль-Балуши, М. Ауад, Хак Д. Лыонг// Математические методы и информационно-технические средства: Труды VIII Всероссийской научно-практической конференции, 22-23 июня 2012 г. – Краснодар: Краснодарский университет МВД России, 2012. – 278 с. – С.163 (1 с.)

117. Подход к генерацииT, S – норм на основе рядов Фурье. /Д.В. Поляков, Л.В. Пучков, М.П. Аль-Балуши, М. Ауад //Математические методы и информационно-технические средства: Труды VIII Всероссийской научно-практической конференции, 22-23 июня 2012 г. – Краснодар: Краснодарский университет МВД России, 2012. – 278 с. – С.165 (1 с.)

118. Аль-Балуши, К вопросу проектирования вопросно-ответных информационными системами / Долгов А.А., Хорохорин М.А., Минин Ю.В., Сила М.К., Аль-Балуши М// Актуальные проблемы деятельности подразделений УИС: сборник материалов Всероссийской научно-практической конференции: в 2 т. – Воронеж: ИПЦ «Научная книга». – Т. 1. – 2013. - С.59-63

119. Аль-Балуши, Процедура принятия решений в информационной тренажерной системе при условии ограниченного времени прохождения / Моисеев А.С., Лыонг Хак Д., Аль-Балуши М., Минин Ю.В// Актуальные проблемы деятельности подразделений УИС: сборник материалов Всероссийской научно-практической конференции: в 2 т. – Воронеж: ИПЦ «Научная книга». – Т. 1. – 2013. - С.106-109

120. Аль-Балуши, Метрики оценки уязвимости сетевых систем / Наука и образование для устойчивого развития экономики, природы и общества/ Проскуряков С.В., Аль-Балуши М//: сборник докладов Международной научно-практической конференции. – в 4 т. – Тамбов: Тамб. гос. техн. ун-т. – 2013. – Т.3. – С. 357-364

121. Аль-Балуши, Механизм оценки устойчивости функционирования сетевых информационных систем,/ М. Аль-Балуши, Н.А. Овчинников, В.В. Паладьев, В.Е. Дидрих // : Воронежского института ФСИН,2013

122. Аль-Балуши ,Модель информационной системе оценки устойчивости функционирования сетевых информационных систем,/М. Аль-Балуши, Н.А. Овчинников, В.В. Паладьев, В.Е. Дидрих//: Воронежского института ФСИН,2013

123. Аль-Балуши М,Распознавание негативных внешних воздействий на сетевую информационную систему /Гречушкина А.Ю., Дидрих В.Е., , Аль-Балуши М., Ауад М //Московский автомобильно-дорожный государственный технический университет (МАДИ).

124. Wang L. X. Generating fuzzy rules by learning from examples / L. X.Wang, J.M. Mendel // IEEE Transaction on systems, Man and Cybernecics.- 1992. V.22. - №6.P.1414-1427/

125. Громов, Ю.Ю. Представление знаний в информационных системах / Ю.Ю.Громов, О.Г. Иванова, Н.Г.Мосягина, Г.А. Соседов, В.Н. Точка. – М. : Изд-во Нобелистека, 2008. – 140 с.

126. Джим Арлоу. UML 2 и Унифицированный процесс. Практический объектно-ориентированный анализ и проектирование / Джим Арлоу, Айла Нейштадт // - Пер. с англ. – СПб: Символ_Плюс, 2007. – 624 с.

127. Эдвард Йордон. Объектно-ориентированный анализ и проектирование систем./ Эдвард Йордон, Карл Аргила //- Пер. с англ. – Изд.-ЛОРИ, 2007. – 264 с.

128. Аль-Балуши М, Распознавание негативных внешних воздействий на сетевую информационную систему / Аль-Балуши М., Гречушкина А.Ю., Дидрих В.Е., Зайцев Д.В. //Приборы и системы. Управление, контроль, диагностика". – 2014. - №1. - С.50-54. (ВАК)

129. Аль-Балуши Задача оценки надежности средств парирования внешних воздействий / Аль-Балуши М.П., Зайцев С.В., Копылов С.А., Дидрих В.Е. // "Информатика: проблемы, методология, технологии" : материалы XIV Международная конференция (6-8 февраля 2014 года): в 3-х т. -Воронеж: Издательско-полиграфический центр Воронежского государственного университета, 2014. – Т.3. – С.68-71

130. Аль-Балуши Применение аппарата нечеткой логики для оценки функционирования сетевых информационных систем / Аль-Балуши М.П., Зайцев С.В., Копылов С.А., Дидрих В.Е. // "Информатика: проблемы, методология, технологии" : материалы XIV Международная конференция (6-8 февраля 2014 года): в 3-х т. -Воронеж: Издательско-полиграфический центр Воронежского государственного университета, 2014. – Т.3. – С.71-75

131. Аль-Балуши Задача определения оценки устойчивости функционирования сетевых информационных систем / Аль-Балуши М.П., Зайцев С.В., Копылов С.А., Дидрих В.Е. // "Информатика: проблемы, методология, технологии" : материалы XIV Международная конференция (6-8 февраля 2014 года): в 3-х т. -Воронеж: Издательско-полиграфический центр Воронежского государственного университета, 2014. – Т.3. – С.75-78

132. Аль-Балуши, Применение аппарата нечеткой логики для оценки функционирования сетевых информационных систем / Аль-Балуши М.П., Костерин Е.В., Елисеев А.И., Дидрих В.Е. // Современные информационные технологии: Труды международной научно-технической конференции. -Пенза: Пензенский государственный технологический университет, 2014,вып. 19.- С.24-27

ПРИЛОЖЕНИЕ А

Список вопросов для определения важности ресурсов

Вопросы	Важность Вопроса	Первый вариант	Второй вариант	Третий вариант	Четвертый вариант
Группа вопросов по доступности					
-Приводит ли нарушение доступности ресурса к разрушению ресурса целиком?	95%	Незначимо	Значимо	Важно	Очень важно
-Влияют ли нарушения доступности ресурса на другие аспекты?	30%	Незначимо	Значимо	Важно	Очень важно
-Влияют ли нарушения доступности ресурса на функциональность всей СИС, где обрабатывается информация?	95%	Незначимо	Значимо	Важно	Очень важно
-Влияют ли нарушения доступности ресурса на функционирование других ресурсов?	99%	Незначимо	Значимо	Важно	Очень важно
Группа вопросов по конфиденциальности					
-Приводит ли нарушение конфиденциальности ресурса к разрушению ресурса целиком?	95%	Незначимо	Значимо	Важно	Очень важно
-Влияют ли нарушения конфиденциальности ресурса на функционирование других ресурсов?	8%	Незначимо	Значимо	Важно	Очень важно
-Влияют ли нарушения конфиденциальности ресурса на другие аспекты?	95%	Незначимо	Значимо	Важно	Очень важно
-Влияют ли нарушения конфиденциальности ресурса на функциональность всей СИС, где обрабатывается информация?	87%	Незначимо	Значимо	Важно	Очень важно

Группа вопросов по целостности					
-Приводит ли нарушение целостности ресурса к разрушению ресурса целиком?	95%	Незначимо	Значимо	Важно	Очень важно
-Влияют ли нарушения целостности ресурса на другие аспекты?	40%	Незначимо	Значимо	Важно	Очень важно
-Влияют ли нарушения целостности ресурса на функциональность всей СИС, где обрабатывается информация?	95%	Незначимо	Значимо	Важно	Очень важно
-Влияют линарушения целостности ресурса на функционирование других ресурсов?	99%	Незначимо	Значимо	Важно	Очень важно

Список вопросов для определения важности ресурсов

Общая группа вопросов для определения важности ресурсов					
1-Какова стоимость ресурса?	80%	Низкая	Средняя	Высокая	Очень высокая
2-Влияет ли работа ресурса на работу других ресурсов?	95%	Не влияет	Влияет	Средне	Очень влияет
3-Влияют ли разрушения ресурса на другие ресурсы СИС?	90%	Незначимо	Значимо	Влияют	Очень влияют
4-Возможно ли восстановление ресурса после его разрушения?	85%	Легко	Сложно	Очень сложно	Невозможно
5-Какова стоимость восстановления ресурса в случае его полного разрушения?	80%	Низкая	Средняя	Высокая	Критическая
6-Какова стоимость восстановления ресурса в случае его частичного разрушения?	80%	Низкая	Средняя	Высокая	Критическая
7-Каково время восстановления ресурса в случае его частичного разрушения?	85%	Меньше 30 минут	Нескольк о часов	Нескольк о дней	Несколько месяцев
8-Каково время восстановления ресурса в случае его полного разрушения?	94%	Меньше 30 минут	Нескольк о часов	Нескольк о дней	Несколько месяцев

ПРИЛОЖЕНИЕ Б

Описание прецедентов

1.Прецеденты. Создание нового процесса.	
Описание	Прецедент дает возможность пользователю создать новый процесс по анализу и оценке устойчивости функционирования СИС.
Предусловия	Система отображает начальную форму с альтернативными функциями <открыть>,<создать>,<закрыть>. Пользователь инициирует новый процесс с помощью функции <создать>.
Основной поток	1) Согласие прецедента с решением пользователя начать анализ оценки устойчивости функционирования СИС с помощью функции <создать>. 2)Отражается форма, которая просит у пользователя пройти авторизацию, если пользователь не зарегистрирован системе .Для этого пользователю предлагается ввести данные: Ф,И,О, наименование проекта, адрес проекта , должность пользователя ,логин и пароль. 3) Заполнение всех полей формы авторизации активизирует функцию <ОК>. Успешная авторизация запускает процесс введение структуры СИС.
Альтернативные потоки	1) Пользователь имеет возможность выбирать функцию<Отмена>, находясь в режиме авторизации, после чего происходит возврат к исходной форме. Система дает возможность начать заново.

	2) Система дает возможность пользователю открыть существующие процессы с помощью функции<Открыть>. Для получения доступа к уже существующему процессу пользователь должен пройти аутентификацию. При неудачной аутентификации система дает пользователю возможность пройти аутентификацию 3 раза, после чего происходит возврат к исходной форме. 3) В любой момент пользователь может выйти из системы, выбрав функцию <Выход>.
Постусловия	Если прецедент успешен, система сохраняет данные о проекте и о пользователе.
2. Прецедент. Выбор и Оценка ценности информации, обрабатываемой в СИС.	
Описание	Прецедент позволит пользователю выбирать тип исследуемой системы из множества предлагаемых типов систем и в соответствии с этим типом оценить важность информации, обрабатываемой в СИС.
Предусловия	Авторизация пройдена успешно, данные сохранены
Основной поток	1) Система отображает форму, в которой пользователю предлагается выбрать тип исследуемой системы: 1- Политическая, 2- Военная, 3- Научно-техническая, 4- Технологическая, 5- Экономическая. 2) Выбрав тип информации, система отображает форму, где показано три списка вопросов,

	определяющих: 1- Необходимость информации, 2- Опасность нарушения конфиденциальности информации,
	3- Стоимость восстановления информации или ресурсов, которые с ней связны. 3) Нажав <далее>-переход из одного списка вопросов в другой. Пользователь получает ценность информации, нажав <расчет>.
Альтернативные Потоки	Пользователь имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена>- выход в исходную форму 3) <Выход>- выход из системы, запрос подтверждения сохранения данных. Сохранение данных обследования 4) < сохранить > 5)<печать> - печать отчёт о ценности информации.
Постусловия	Данные о ценности информации сохранены.
3.Прецедент. Ввод структуры сети.	
Описание	Прецедент позволит пользователю вводить объекты системы и ресурсы каждого объекта (из чего состоит объект (информационные, физические и человеческие ресурсы))
Предусловия	Авторизация пройдена успешно, данные сохранены.
Основной поток	1) Система отображает форму, в которой пользователю предлагается вводить наименование

	всех объектов. 2) После завершения ввода наименований всех объектов активизируется функция<Далее>. 3) Отображается форма, где показан список всех объектов и список предлагаемых физических, информационных и человеческих ресурсов. 4) Пользователь выбирает ресурсы каждого объекта (из чего
	состоит объект). 5) Нажимая кнопку<Далее> система переходит к выбору ресурсов следующего объекта. 6) В случае, если в списке нет нужного ресурса, Пользователь нажимает кнопку<Добавить >. 7) При вводе всех объектов Пользователь нажимает кнопку <Готово>. Система отображает исходную форму.
Альтернативные потоки	Пользователь имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена>- выход в исходную форму. 3) <Выход> - выход из системы, запрос подтверждения сохранения данных. Сохранение данных обследования. 4) < сохранить >
Постусловия	По данным сгенерирована структура СИС. Данные обследования содержат сведения об объектах СИС, и из чего состоит каждый объект (человеческие, информационные и физические ресурсы).
4. Прецедент. Оценка важности ресурсов.	
Описание	Прецедент дает возможность оценить важность каждого

	ресурса по аспектам: 1- Доступность, 2- Целостность, 3- Конфиденциальность. В соответствии с его типом (физический, информационный и человеческий).
Предусловия	Имеется список объектов, имеются данные о ресурсах каждого объекта системы.
Основной поток	1) Система отображает форму, в которой отображается список идентифицированных ресурсов СИС. 2) Выбрав ресурс, активизируется функция<Далее>. 3) Выбор функции<Далее>система отображает список вопросов для определения важности выбранного ресурса. 4) После ответа на вопросы активизируется функция <ОК>. 5) Выбор функции <ОК> система возвращается в список ресурсов системы. 6) Функция <Отчет> активизируется в конце.
Альтернативные Потоки	Пользователь имеет возможность выбирать функции: 1) <Назад> - переход к предыдущей форме. 2) <Отмена>- выход в исходную форму. 3) <Выход> - выход из системы, запрос подтверждения сохранения данных. - сохранение данных 4) <Сохранить > 5)<Печать> - печать отчёта о важности каждого ресурса.

Постусловия	Сохраняются данные о важности ресурсов СИС по определенным аспектам.
5. Прецедент. Определение возможных НВВ.	
Описание	Имеются данные об объектах СИС, список возможных НВВ, уязвимость каждого объекта. Прецедент дает возможность пользователю определить возможные НВВ. НВВ классифицированы по признаку источника возникновения (внутренний, внешний) и расположения относительно системы, и разделены на множество антропогенных, техногенных и стихийных источников НВВ.
Предусловия	Структура объектов (ресурсов) СИС определена
Основной поток	1) Система отображает форму, в которой отображен список всех объектов СИС, список предлагаемых НВВ. 2) Пользователь определяет все возможные НВВ к каждому объекту. 3) Нажав кнопку<Далее> система переходит к следующему объекту. 4) Если отсутствует какое-то НВВ в списке предлагаемых НВВ, то можно его добавить с помощью функции<Добавить>. 5) При определении всех возможных НВВ ко всем объектам активизируется функция <Готово> 6) Нажав <Готово> система вернется в исходную форму.
Альтернативные Потоки	Пользователь имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена>- выход в исходную форму.

	3) <Выход> - выход из системы, запрос подтверждения сохранения данных. Сохранение данных. 4) < Сохранить> 5)<Печать> - печать отчёта, где отображено наименование объекта и все возможные НВВ, которые на него направлены.
Постусловия	Сохраняются данные об угрозах каждого объекта.
6. Прецедент. Определение действующих СПНВВ и оценка факторов, влияющих на их уровень надежности.	
Описание	Прецедент дает возможность пользователю определить, какие СПНВВ направлены на защиту объектов системы.
Предусловия	Модель структуры СИС сгенерирована, имеются данные о МПНВВ системы от внешних и внутренних НВВ.
Основной поток	1) Система отправляет пользователю форму, отображающую список всех объектов СИС, а также список предлагаемых СПНВВ. 2) Пользователь определяет все существующие СПНВВ, направленные на защиту каждого объекта. 3) При нажатии кнопки<Далее>, система переходит к определению СПНВВ следующего объекта. 4) При выборе программных СПНВВсистема отправляет пользователю список вопросов для определения влияния условий эксплуатации на его надежность(например, часто ли обновляется антивирус). 5) Можно добавить какое-нибудь СПНВВ с помощью функции<Добавить>, если оно отсутствует в списке предлагаемых средств. 6) При определении всех СПНВВ активизируется функция <Готово>. 7) После нажатия кнопки<Готово>, система вернется в

	исходную форму.
Альтернативные Потоки	Пользователь имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена>- выход в исходную форму. 3) <Выход> - выход из системы, запрос подтверждения сохранения данных. 4) <Сохранить > Сохранение данных . 5)<Печать>- печать отчёта, где отображено наименование объекта и всех существующих СПНВВ, которые направлены на него.
Постусловия	Сохраняются данные о связи между СПНВВ и объектами СИС, и данные о надежности программных продуктов, предназначенных для обеспечения стабильного функционирования системы при НВВ.ёё1ё
7. Прецедент. Оценки устойчивости функционирования СИС	
Описание	Прецедент дает возможность пользователю выбирать критерии, по которым система будет оценивать устойчивость функционирования СИС.
Предусловия	Риск от каждого НВВ рассчитан.
Основной поток	1) Система отображает форму, в которой предлагается выбирать критерии оценки устойчивости: 1- Учитывать человеческие факторы, которые оказывают влияние на уровень устойчивости системы (уровень персонала, который связан с ресурсами СИС в зависимости от должности). 2- Оценить устойчивость системы при внешних и внутренних НВВ по отдельности или совместно. 3- Возможность оценить устойчивость функционирования определенного ресурса по отдельности. 4- Возможность оценить устойчивость функционирования определенного объекта по отдельности,с учётом всех связанных с ним ресурсов. 5- Оценить устойчивость системы в целом.

	6- Отображать требуемый уровень обеспечения устойчивости функционирования каждого ресурса по отдельности. 2) При нажатии кнопки<Оценить> система оценивает устойчивость системы,с учётом критериев, выбранных пользователем.
Альтернативные Потоки	Пользователь имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена>- выход в исходную форму. 3) <Выход> - выход из системы, запрос подтверждения сохранения данных. 4) <Сохранить> Сохранение данных . 5)<Печать> - печать отчёта, где отображена оценка устойчивости функционирования СИС.
Постусловия	Оценка устойчивости функционирования СИСопределена.
8. Прецедент. Определение критериев оптимальности для генерации рекомендации.	
Описание	Прецедент дает возможность пользователю выбирать критерии, определяющие, какие ресурсы системы нуждаются в повышении устойчивости,а также возможность генерации рекомендаций по повышению устойчивости СИС.
Предусловия	Проведена оценка устойчивости функционирования и сохранена, НВВ определены, СПНВВ определены, риски оценены.
Основной поток	1) Система отправляет пользователю форму, позволяющую задать критерии, по которым определяются какие ресурсы нуждаются в защите. 2) После выбора критериев активизируется функция<<Определить>>. 3) Система отображает форму, где показаны ресурсы, которые нуждаются в повышении устойчивости их функционирования. 4) При нажатии кнопки<<Генерация >>, система отображает форму, где показаны рекомендации.

Альтернативные Потоки	Пользователь имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена> - выход в исходную форму. 3) <Выход> - выход из системы, запрос подтверждения сохранения данных. 4) <Закрыть > - выход из системы, запрос подтверждения сохранения данных. 5) <Сохранить > Сохранение данных . 6)<Печать>- печать отчёта о рекомендациях.

ПРИЛОЖЕНИЕ В

Описание прецедентов - Эксперт

1.Прецеденты. Создание нового процесса.	
Описание	Прецедент дает возможность эксперту создать новый процесс обучения системы анализа и оценки устойчивости функционирования СИС.
Предусловия	Система отображает начальную форму с альтернативными функциями<Открыть>,<Создать>,<Закрыть>. Эксперт инициирует новый процесс с помощью функции<Создать>.
Основной поток	1) Согласие прецедента с решением эксперта начать новый процесс обучения системы с помощью функции<Создать>. 2) Отражается форма, которая предоставляет эксперту возможность пройти авторизацию, если эксперт не зарегистрирован в системе. Для этого эксперту предлагается ввести данные: Ф.И.О., наименование проекта, адрес проекта, должность пользователя,логин и пароль. 3) Заполнение всех полей формы авторизации активизирует функцию <ОК>. Успешная авторизация запускает процесс обучения.
Альтернативные Потоки	1) При нажатии кнопки<Отмена>, находясь в режиме авторизации, происходит возврат к исходной форме. Система дает возможность начать заново. 2) Система дает возможность эксперту открыть существующие
	процессы с помощью функции<Открыть>. Для получения доступа к уже существующему процессу пользователь должен пройти аутентификацию. При неудачной аутентификации система дает эксперту возможность пройти аутентификацию 3 раза, после чего происходит возврат к исходной форме. 3) В любой момент эксперт может выйти из системы, выбрав функцию <Выход>.
Постусловия	Если прецедент успешен, система сохраняет данные о проекте и об эксперте.
2. Прецедент. Настройка системы определения ценности информации, обрабатываемой в СИС.	
Описание	Прецедент позволяет экспертуиз множества предлагаемых типов систем выбирать тип исследуемой системыи в соответствии с этим типом оценить факторы, которые влияют на ценность

	информации, обрабатываемой в СИС.
Предусловия	Авторизация пройдена успешно, данные сохранены, выбран тип системы.
Основной поток	Система отображает форму, в которой эксперту предлагается выбрать тип исследуемой системы: 1- Политическая, 2- Военная, 3- Научно-техническая, 4- Технологическая, 5- Экономическая. После выбора типа содержащейся в системе информации, отображается форма, где эксперту нужно определить вопросы (факторы) и их важность для проведения оценки ценности информации. Эксперт относит вопросы в три списка: - Список вопросов для определения необходимости
	- Список вопросов для определения опасности нарушения конфиденциальности информации, - Список вопросов для определения стоимости восстановления информации или связанных с ней ресурсов. Нажав<Далее>-переход из одного списка вопросов в другой.
Альтернативные Потоки	Эксперт имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена>- выход в исходную форму. 3) <Выход> - выход из системы, запрос подтверждения сохранения данных. 4) <Сохранить > - сохранение данных обследования 5)<Печать> - печать отчёта о ценности информации.
Постусловия	Вопросы и их важности о ценности информации сохранены.
3.Прецедент. Добавление списка возможных НВВ.	

Описание	Прецедент позволит эксперту вводить все возможные НВВ и данные о каждом из них.
Предусловия	Авторизация пройдена успешно, данные сохранены,выбран тип системы.
Основной поток	Прецедент дает возможность определить источник НВВ и методы воздействия. Система отображает форму, в которой эксперту предлагается ввести наименование всех НВВ и определить, на какие объекты (ресурсы) они воздействуют. После завершения ввода наименований всех НВВ активизируется функция<Далее>. Отображается форма, где показан список всех НВВ и список
	предлагаемых вопросов для определения опасности осуществления НВВ. После завершения проведения оценки опасности для каждого НВВ активизируется функция<Далее>. Нажимая кнопку<Далее> система переходит к оценке следующего НВВ. При оценке всех НВВ эксперт нажимает кнопку <Готово>. Система отображает исходную форму.
Альтернативные Потоки	Эксперт имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена>- выход в исходную форму. 3) <Выход> - выход из системы, запрос подтверждения сохранения данных. 4) <Сохранить> - Сохранение данных обследования
Постусловия	По данным сгенерирован список НВВ. Данный список содержит сведения о возможных НВВ и оценках опасности каждого из них.
4. Прецедент. Добавление всех возможных СПНВВ.	
Описание	Прецедент позволит эксперту вводить все возможные СПНВВ и данные о каждом из них, а также оценить надежности средств парирования по: 1- Доступности, 2- Целостности,

	3- Конфиденциальности.
Предусловия	Авторизация пройдена успешно, данные сохранены, выбран тип системы.
Основной поток	1) Система отображает форму, в которой эксперту предлагается ввести наименование всех СПНВВ, и определить, для каких НВВ они предназначены. 2) После завершения ввода наименований всех СПНВВ активизируется функция<Далее>. 3) Отображается форма, где показан список всех СПНВВ и список предлагаемых вопросов для определения надежности средств парирования НВВ. 4) После завершения проведения оценки надежности для каждого СПНВВ активизируется функция<Далее>. 5) При нажатии кнопки<Далее> система переходит к оценке следующего СПНВВ. 6) После оценки всех СПНВВ эксперт нажимает кнопку <Готово>. Система отображает исходную форму.
Альтернативные Потоки	Пользователь имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена>- выход в исходную форму. 3) <Выход> - выход из системы, запрос подтверждения сохранения данных. 4) <Сохранить > Сохранение данных . 5)<Печать> - печать отчёта о важности каждого ресурса.
Постусловия	Сохраняются данные о СПНВВ.
5. Прецедент.Настройка системы добавления и определения важности ресурсов СИС.	
Описание	Прецедент позволит эксперту вводить возможные ресурсы СИС и данные о каждом из них, а также настраивать систему для оценки важности ресурсов в зависимости от типа ресурса (информационные, физические, человеческие) по: 1- Доступности,

	2- Целостности, 3- Конфиденциальности.
Предусловия	Авторизация пройдена успешно, данные сохранены, выбран тип системы.
Основной поток	1- Система отображает форму, позволяющую добавить список предлагаемых ресурсов. 2- При нажатии кнопки<Далее> происходит переход к системе настойки определения важности ресурсов СИС. 3- Отображается форма для внесения вопросов, которыеотражаютфакты о ресурсах в зависимости от их типа. Важность каждого ресурса, отражающая уровень влияния факта на систему,задаётся с помощью функции<Добавить>. 4- После ввода всех ответов, активизируется функция <Готово>. 5- После нажатия кнопки<Готово>, система вернется в исходную форму.
Альтернативные Потоки	Пользователь имеет возможность выбирать функции: 1) <Назад>- переход к предыдущей форме. 2) <Отмена> - выход в исходную форму 3) <Выход> - выход из системы, запрос подтверждения сохранения данных. 4) <Сохранить > Сохранение данных . 5) <Печать> - печать отчёта, где отображено наименование объекта и все направленные на него НВВ.
Постусловия	Сохраняется система настройки определения важности ресурсов СИС.

ПРИЛОЖЕНИЕ Г

Список ресурсов исследуемой СИС

Объект	Ресурс	Тип ресурса
Сервер	1-операционная система Windowsserver 2003; 2-прокси сервер; 3-система управления архивами; 4- сетевой сервер базы данных; 5-сетевой администратор;	Информационный Информационный Информационный Информационный Человеческий
	6-сервер электронной почты; 7-сервис передачи файлов; 8-жесткий диск; 9-сетевой сканер; 10- сетевой интерфейс; 11-сетевой дисковод для магнитооптических дисков DVD-RW; 12- сетевой принтер; 13-USB-интерфейс; 14-монитор.	Информационный Информационный Физический Физический Физический Физический Физический Физический Физический
Рабочая станция (1)	1- операционная система Windows XP; 2- сервис электронной почты; 3- программы сканирования и распознавания знаний; 4- сервер электронной почты; 5- сервис передачи файлов; 6- оператор периферийного оборудования;	Информационный Информационный Информационный Информационный Информационный Человеческий

	7- сетевой интерфейс; 8- жесткий диск; 9- монитор;	Физический Физический Физический
Рабочая станция(2)	1- операционная система Windows XP;	Информационный
	2- сервис электронной почты; 3- программы сканирования и распознавания знаний; 4- сервер электронной почты; 5- сервис передачи файлов; 6- оператор периферийного оборудования; 7- сетевой интерфейс; 8- жесткий диск; 9- монитор.	Информационный Информационный Информационный Информационный Человеческий Физический Физический Физический
Рабочая станция(3)	1- операционная система Windows XP; 2- сервис электронной почты; 3- система базы данных; 4- пользователь-программист; 5- монитор; 6- USB-интерфейс; 7- сетевой интерфейс.	Информационный Информационный Информационный Человеческий Физический Физический Физический
Рабочая станция(4)	1- операционная система Windows XP; 2- сервис электронной почты; 3- пользователь; 4- монитор; 5- USB-интерфейс;	Информационный Информационный Человеческий Физический Физический

	6- сетевой интерфейс.	Физический
Рабочая станция(5)	1- операционная система Windows XP, 2- сервис электронной почты; 3- пользователь; 4- монитор; 5- USB-интерфейс; 6- сетевой интерфейс.	Информационный Информационный Человеческий Физический Физический Физический
Рабочая станция(6)	1- операционная система Windows XP; 2- сервис электронной почты; 3- система базы данных; 4- пользователь; 5- монитор; 6- USB-интерфейс; 7- сетевой интерфейс.	Информационный Информационный Информационный Человеческий Физический Физический Физический
Рабочая станция(7)	1- операционная система Windows XP; 2- сервис электронной почты; 3- система базы данных; 4- пользователь; 5- монитор; 6- USB-интерфейс; 7- сетевой интерфейс.	Информационный Информационный Информационный Человеческий Физический Физический Физический
Рабочая станция(8)	1- операционная система Windows XP;	Информационный

	2- сервис электронной почты; 3- система базы данных; 4- пользователь; 5- монитор; 6- USB-интерфейс; 7- сетевой интерфейс.	Информационный Информационный Человеческий Физический Физический Физический
Рабочая станция(9)	1- операционная система Windows XP; 2- сервис электронной почты; 3- система базы данных; 4- пользователь-программист; 5- монитор; 6- USB-интерфейс; 7- сетевой интерфейс.	Информационный Информационный Информационный Человеческий Физический Физический Физический
Рабочая станция(10)	1- операционная система Windows XP; 2- сервис электронной почты; 3- система базы данных; 4- пользователь-программист; 5- монитор; 6- USB-интерфейс; 7- сетевой интерфейс.	Информационный Информационный Информационный Человеческий Физический Физический Физический
Локальная сеть	1- коммутатор; 2- линии связи.	Физический Физический

ПРИЛОЖЕНИЕ Д

Акты о внедрении и использовании результатов диссертационного исследования

Утверждаю
Врио генерального директора
ООО «Агентство консалтинговых,
образовательных и научных услуг в области
инновационных технологий»
доктор технических наук, профессор
Громов Ю.Ю.
«30» января 2014 года

АКТ
использования результатов диссертационной работы
АЛЬ БАЛУШИ МАДЖЕД ПИР БАХШ
на тему: «Аналитическое и процедурное обеспечение экспертной системы оценки устойчивости функционирования сетевых информационных систем»

Комиссия в составе: председателя – члена совета директоров Ивановой Ольги Геннадьевны, кандидата технических наук, доцента; и члена – инженера-программиста Паладьева Виктора Валерьевича составила настоящий Акт о том, что результаты диссертационной работы АЛЬ БАЛУШИ МАДЖЕД ПИР БАХШ на соискание ученой степени кандидата технических наук, а именно:

процедурная модель оптимальной оценки рисков нарушения устойчивости функционирования СИС при НВВ, позволяющая построить экспертную систему многофакторной оценки устойчивости функционирования СИС в условиях различных НВВ;

структура экспертной системы оптимального выбора СПНВВ, обеспечивающая требуемую устойчивость функционирования СИС, на основе многофакторной структурой знаний и модулем оптимизации затрат на реализацию СПНВВ в условиях заданных НВВ,

использованы в НИР и ОКР выполняемых по тематике разработки и исследования экспертных систем и сетевых информационных систем различного предметного назначения.

Использование результатов позволило обосновать архитектуру экспертной системы на концептуальном уровне, определить стратегию и механизмы обеспечения защиты сетевых информационных систем, рациональным образом подбирать способы и средства парирования негативных воздействий в проектируемой системе.

Результаты в виде задач оптимального выбора средств парирования негативных внешних воздействий использованы при разработке программ профессиональной переподготовки и повышения квалификации специалистов в области проектирования и обеспечения защиты сетевых информационных систем.

Председатель комиссии: О.Г. Иванова
член комиссии: В.В. Паладьев
30 января 2014 года

Утверждаю
директор Центрально-черноземного
регионального учебно-научного центра по
проблемам защиты информации
кандидат технических наук, профессор
Мартемьянов Ю.Ф.
«20» января 2014 года

АКТ
использования результатов диссертационной работы
АЛЬ БАЛУШИ МАДЖЕД ПИР БАХШ
на тему: «Аналитическое и процедурное обеспечение экспертной системы оценки устойчивости функционирования сетевых информационных систем»

Комиссия кафедры «Информационные системы и защита информации» в составе: председателя – ведущего специалиста по защите информации Щербинина Павла Алексеевича и членов комиссии – ведущего инженера Минаева Александра Сергеевича; инженера Перфильева Владимира Александровича составила настоящий Акт о том, что результаты диссертационной работы АЛЬ БАЛУШИ МАДЖЕД ПИР БАХШ на соискание ученой степени кандидата технических наук используются в разработках учебных материалов по тематике оценки показателей функционирования сетевых информационных систем и способов парирования негативных внешних воздействий, а так же при проведении научных исследований по проблемам защиты информации, модернизации способов и средств защиты. А именно:

аналитическая модель оптимальной оценки уровня устойчивости функционирования СИС при НВВ, отличающаяся использованием показателей ценности информации, важности ресурсов СИС и рисков от НВВ, получаемых экспертным путём, которая позволяет оптимизировать рекомендуемый набор СПНВВ по заданному уровню устойчивости функционирования или по минимальным затратам на их реализацию в данных условиях;

процедурная модель оценки факторов устойчивости функционирования СИС при НВВ, отличающаяся использованием продукционных правил определяются ценности информации путем обработки нечетких характеристик важности ресурсов, опасности НВВ и надежности СПНВВ, которая позволяет построить экспертную систему многофакторной оценки устойчивости функционирования СИС в условиях различных НВВ.

Председатель комиссии: Щербинин П.А.

члены комиссии: Минаев А.С.

Перфильев В.А.

20 января 2014 года

Утверждаю
Помощник ректора ФГБОУ ВПО «Тамбовский государственный технический университет»
доктор педагогических наук, профессор
Ракитина Е.А..
«25» января 2014 года

АКТ
использования результатов диссертационной работы
АЛЬ БАЛУШИ МАДЖЕД ПИР БАХШ
на тему: «Аналитическое и процедурное обеспечение экспертной системы оценки устойчивости функционирования сетевых информационных систем»

Комиссия кафедры «Информационные системы и защита информации» в составе: председателя – профессора кафедры Алексеева Владимира Витальевича, доктора технических наук, профессора и членов комиссии – доцента кафедры Гриднева Виктора Алексеевича, кандидата технических наук, доцента; доцента кафедры Яковлева Алексея Вячеславовича, кандидата технических наук, доцента составила настоящий Акт о том, что результаты диссертационной работы АЛЬ БАЛУШИ МАДЖЕД ПИР БАХШ на соискание ученой степени кандидата технических наук используются в учебном процессе на кафедре «Информационные системы и защита информации» ФГБОУ ВПО «Тамбовский государственный технический университет» при непосредственном участии автора диссертационных исследований в разработке учебно-методических материалов лекций, лабораторных работ и обучающих программных комплексов по следующим дисциплинам кафедры: «Моделирование опасности в автоматизированных системах», «Программно-аппаратные средства обеспечения информационной безопасности», «Разработка и эксплуатация защищенных автоматизированных систем», «Надежность аппаратно-программных комплексов».

Результаты диссертационного исследования используются для обучения студентов по следующим направлениям и специальностям: 230400 «Информационные системы и технологии», 090303 «Информационная безопасность автоматизированных систем», что дает возможность повысить качество и эффективность учебного процесса.

Председатель комиссии: д.т.н., профессор Алексеев В.В.

члены комиссии: к.т.н., доцент Гриднев В.А.

к.т.н., доцент Яковлев А.В.

25 января 2014 года