МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.04.03 ПРИКЛАДНАЯ ИНФОРМАТИКА
(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

Студент Д.А. Палагин _____
И.О. Фамилия (личная подпись)

Научный руководитель кандидат технических наук, доцент А.В. Очеповский
(ученая степень, звание, И.О. Фамилия)

Тольятти 2020

Оглавление

ВВЕДЕНИЕ

В данном диссертационном исследовании рассматриваются вопросы построения комплексной системы защиты информации корпоративной информационной системы на основе интеллектуальных технологий. Безопасность информационных систем - одна из самых больших проблем, стоящих перед технологическим веком общества. Высокая степень автоматизации процессов в современном обществе ставит его в зависимость от уровня безопасности применяемых информационных технологий.

Актуальность работы. Текущий этап развития в области обмена информацией представляет собой интенсивное внедрение современных информационных технологий, массовым распространением сетей различного уровня охвата – локального, корпоративного, глобального, создающего огромный потенциал применения информационного обмена в разнообразных сферах бизнеса. Технологии управления бизнесом, возможности его масштаба в различных сферах деятельности определяются корпоративными информационными системами (КИС), охватывающие в себе инфраструктуру и различные информационные сервисы. Инфраструктура КИС включает сети, серверы, рабочие станции, охватывая подразделения, которые могут быть развернуты по всему миру. Сегмент (СГ КИС) служит структурной единицей КИС.

Массовое использование IT-технологии в КИС вынуждает серьезно относиться к информационной безопасности из-за наличия угроз по защите информации.

Современные теоретические и практические разработки, гарантирующие защиту информации (ЗИ) обладают некоторыми противоречиями: обостренным вниманием к безопасности информационных объектов, значительно повышенными требованиями, которые предъявляются к ЗИ, внедрением принятых международных стандартов по гарантиям информационной безопасности (ИБ), все возрастающими расходами для

обеспечения ЗИ, а с другой стороны ущерб, наносимый владельцам информационных ресурсов компьютерными атаками, увеличивается.

Современные подходы к организации информационной безопасности не обеспечивают должного соответствия требованиям ИБ. Основные недостатки используемых систем (СЗИ) обычно обусловлены сложными технологиями построения архитектуры СЗИ и использованием стратегий от уже известных угроз, как правило, оборонительного характера.

Поэтому, результативное использование информационных технологий в деятельности корпораций требует эффективно управляемых системы ЗИ, поскольку система, которая реализует процессы управления событиями ИБ, планированием модульной структуры системы ЗИ и аудит информационной безопасности, должны проводиться автономно на уровне сегмента КИС.

Объект управления системой информационной безопасности представляет собой сложную организационно-техническую систему, работающую в условиях неопределенности и неполного знания состояния информационной среды. Таким образом, система должна управляться с применением системного анализа и требуемой интеллектуальной поддержкой

Проблемы обеспечения ИБ отражены в работах многих российских и зарубежных ученых. Однако до настоящего времени недостаточно проработанными являются методы обеспечения адаптивной защиты информации, направленные на автоматизацию управления безопасностью информационных систем, которое обеспечивает требуемый уровень ЗИ на протяжении всего времени функционирования системы.

Способом разрешения отмеченной выше проблемы может являться интеллектуальная поддержка в управлении ЗИ в сегменте КИС, подходящих моделей, методов, алгоритмов и программного обеспечения.

Выдвигаемые гипотезы:

- наиболее рациональным подходом к эффективной ЗИ в сегменте КИС является использование интеллектуальных средств для поддержки принятия решений при управлении ЗИ;

- малоисследованными для решения задачи оценки неизвестных атак остаются такие перспективные методы, как метод нейронных сетей, метод нечеткой логики и генетические алгоритмы;

- перспективными на сегодня являются технологии, которые позволяют в реальном времени оценить риск нарушения ИБ с малым привлечением экспертов на базе информации, характеризующей информационную ценность требующих защиты ресурсов, технических характеристик средств защиты, и учета особенностей реальных угроз для конкретного объекта защиты.

Объектом исследования в работе являются обеспечение необходимого уровня ЗИ.

Предмет магистерской диссертации – гибкие методы управления ЗИ в сегменте КИС на основе использования интеллектуальных технологий.

Цель магистерской диссертации состоит в разработке адаптивных методов управления защитой информации в сегменте КИС для обеспечения необходимой защищенности информации в условиях неопределенности информационных атак на основе интеллектуальных технологий.

Для достижения вышеуказанной цели в работе необходимо решить следующий круг **задач**:

- провести анализ КИС как объекта информационной защиты и разработать системную модель ее противодействия информационным угрозам;

- на основе анализа основных подходов к решению проблемы обеспечения информационной безопасности в сегменте КИС, обосновать необходимость развития адаптивных методов достижения заданного уровня защищенности информации с использование интеллектуальных технологий;

- предложить модель для борьбы с угрозами ИБ в сегменте КИС, основанную на выборе рационального варианта реагирования на угрозы ИБ с учетом оперативной информации о состоянии информационной среды;

- создать схему построения системы управления информационной безопасности с применением методов интеллектуальной поддержки при принятии решений.

Теоретической основой выполнения работы явилось изучение и использование научных трудов отечественных и зарубежных авторов по вопросам обеспечения защищенности информационных систем, освещающие вопросы применения интеллектуальных методов принятия решений.

Методологической основой исследования является построение системы управления защитой информации в СГ КИС, базирующейся на формировании управляющей информации, полученной с использованием интеллектуальных технологий.

Для выполнения работы были использованы такие **методы, как** системный анализ, методы теории управления, теории множеств, методы нечеткой логики, теории вероятностей, теории принятия решений, теории защиты информации.

Научная новизна исследования состоит в построении комплексной системы защиты информации корпоративной информационной системы с применением интеллектуальных технологий принятия решений на основании критерия «коэффициент уверенности».

Теоретическая значимость исследования заключается в рассмотрении системы защиты информации как комплексной структуры, анализе факторов, влияющих на эффективность обеспечиваемой защиты информации.

Практическая значимость состоит в возможности использования разработанной в ходе исследования структуры системы защиты информации для построения системы защиты информации корпоративной системы.

Основные положения, выносимые на защиту:

- разработана модель противодействия угрозам информационной безопасности в условиях неопределенности;

- предложено применение «коэффициента уверенности» для принятия решения об отнесении аномальных событий информационной системы к классу атак;

- разработана структура системы интеллектуальной поддержки принятия решений по оперативному управлению защитой информации на основе интеллектуальных технологий.

Магистерская диссертация **включает**: введение, четыре главы, заключение и список литературы.

ГЛАВА 1 АНАЛИЗ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СЕГМЕНТЕ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

1.1Сущность проблемы управления защищенностью информации

Современные корпорации имеют сложную распределенную структуру, которая предопределена многопрофильной деятельностью, территориальным размещением подразделений, многочисленными корпоративными связями с партнерами. Корпоративными, обычно, называют системы управления предприятием, имеющим развитую структуру и отдельные органы управления. Среди корпоративных систем выделяют организационные, информационные и т.п. Большинство бизнес-функций и управленческих процессов предприятий и организаций охватывают корпоративные информационные системы (КИС), являясь важным инструментальным средством ведения бизнеса.

Внедрение новых информационных технологий для предприятий всегда связано с возникновением новых рисков. Чем сложнее является структура корпоративной информационной системы, тем выше степень риска угроз для нее: проникновение извне или несанкционированный доступ изнутри предприятия, в частности с целью финансового мошенничества или раскрытия коммерческой тайны, изменения или уничтожения информации и т.п. [15] Такие риски могут нанести предприятию значительный урон. Создание развитой и защищенной информационной среды является непременным условием развития как отдельных корпораций, так и экономики, общества и государства в целом. Поэтому вопросы обеспечения защищенности информации в сегменте КИС стали в настоящее время очень злободневными.

КИС является сложной человеко-машинной или социо-техничной системой, которая включает в свой состав информационную систему предприятия. Для исследования таких систем используются разные типы

моделей. Процесс функционирования КИС предприятия осуществляется в условиях противоборства предприятия, как социо-техничной системы с одной стороны, и конкурентов, злоумышленников, негативных явлений природы и других объектов и явлений, с другой стороны.

Усложнение и расширение современных КИС приводит к увеличение количества сетевых устройств и различных средств защиты информации (СрЗИ), приводит к большому количеству событий безопасности.

Необходимо отметить, что современные технологические процессы значительно обгоняют теоретические осмысления практических разработок и применений в области информационных технологий, а также в области новых коммуникационных возможностей. Поэтому, имеются основания предполагать неполную адекватность существующим теоретических достижений стоящим задачам защиты информации как в практическом, так и в теоретическом ключе [37].

Основными недостатками широко использующихся СЗИ являются их черты, связанные со строгими архитектурными принципами [9] и использованием в основном оборонительных или наступательных стратегий защиты от наиболее известных и опасных угроз.

Решение обозначенных проблем и эффективное использование современных КИС требует средств и методов равного и надежного управления не только сетями, а также и системой ЗИ, всеми мерами, обеспечивающими безопасность сети [10]. Нам нужны методы, которые позволили бы нам быстро отслеживать изменения в операционной среде системы и предотвращать своевременные нарушения информационной безопасности, управляя как сетевым оборудованием, так и оборудованием безопасности.

Современным подходом обеспечения эффективной защищенности информации в КИС является использование интеллектуальных инструментов поддержки принятия решений (ППР) для управления информационной безопасностью.

В настоящее время разрабатывается интегрированная система управления ЗИ, которая будет охватывать всю инфраструктуру организации и позволяла бы управлять информационной инфраструктурой, независимо от масштаба КИС.

Структурированное представление всего многообразия аспектов управления защитой информации приведено наглядно на рис. 1.1.

Рисунок 1.1— Структурирование проблемы управления ЗИ

В настоящее время практически нельзя найти производителей, которые бы представляли потребителю полный спектр средств, как аппаратных, так и программных, необходимых для построения систем ЗИ, удовлетворяющей современным требованиям. Большинство систем ЗИ строится на основе программно-аппаратных средств, выпущенных различными производителями. Для гарантирования гетерогенной КИС надежности ЗИ необходима система управления информационной безопасностью (СУЗИ), которая может обеспечить правильную конфигурацию каждого из ее компонентов и обеспечить автоматическую поддержку принятия решений по ЗИ, постоянно отслеживая происходящие изменения, контролируя работу пользователей сети.

Такой комплексный подход решения проблемы позволяет создавать действительно безопасную среду функционирования КИС предприятия.

Выполненный нами анализ позволяет утверждать, что на уровне сегмента КИС система управления, которая реализует ряд функций управления, должна функционировать автономно:

- получать и оценивать объективные данные о текущем состоянии безопасности КИС*(аудит);*

- управлять событиями, по которым ведутся протоколирования;

- определять модульный состав системы ЗИ и точки создания средств защиты информации в компьютерной сети предприятия.

Международный стандарт ISO/IEC 27001 [2] описывает модели, используемые для создания, внедрения, эксплуатации, постоянного мониторинга и анализа, обслуживания и улучшения систем управления информационной безопасностью (СМЗИ).

Особенности проектирования и реализации СМЗИ компании определяются ее потребностями и целями, требованиями защиты, размерами и структурой организации. Для эффективного функционирования необходимо идентифицировать различные виды деятельности и управлять ими.

Процессный подход к управлению ЗИ в этом стандарте помогает выделить следующие моменты:

- Определение принципов, целей, процессов и процедур, которые имеют отношение к управлению рисками и совершенствованию ЗИ для достижения результатов, соответствующих целям компании;

- внедрение и функционирование правил, средств контроля, процессов и процедур СМЗИ;

- оценка и измерения показателей процессов, относящихся к политике, цели и практическому опыту менеджмента защиты информации, а также проведение их анализа;

- выполнение корректирующих и предупреждающих процедур, которые основаны на результатах проведения внутреннего аудита и анализа с целью постоянного улучшения управления ЗИ.

Состав СМЗИ включает:

- организационную структуру;

- политику, мероприятия планирования;

- набор процедур, процессов, ресурсов.

Целью СМЗИ является проектирование СЗИ, внедрение, эксплуатация, постоянный контроль, анализ, улучшение ЗИ.

Для создания СМЗИ предприятию необходимо выполнение следующего:

- определение границ системы;

- выработать принцип действия относительно защиты информации с учетом законодательных норм и установленных целей защиты;

- выработать критерии оценки значимости рисков;

- выбрать методологию оценки риска, соответствующую системе управления ЗИ и отвечающую нормативным требованиям; и способные обеспечить, чтобы оценки риска давали конкретные результаты;

- определить приемлемый уровень риска;

- выполнять идентификацию рисков (активы, угрозы и негативные влияния, которые способствуют потере конфиденциальности, целостности и доступности активов и критических уязвимостей системы определения местоположения);

- оценить значимость рисков (оценить вероятность нарушений информационной безопасности в свете существующих угроз и уязвимостей, оценить уровни риска, определить, являются ли риски приемлемыми или требуют ответа);

- найти возможность управления рисками (применение приемлемых средств снижения или принятия риска);

- выбрать методы управления и обработки рисков, которые учитывали бы критерии для принятия рисков;

- согласовать с руководством внедрение системы ЗИ и выполнить подготовку заявления о степени применимости (включая цель управления, средство управления, обоснование выбора).

Этап реализация и эксплуатация СМЗИ предприятия включает следующие действия:

- формулирование плана обработки риска, определяющего подходящие действия по менеджменту, необходимые ресурсы, ответственность;

- реализация этого плана, включая финансирование;

- реализация средства управления, имеющего цель достижения цели управления;

- внедрение процедур и прочих средств управления, которые способны обеспечить быстро обнаружить события в системе ЗИ и реакции на инцидент в системе ЗИ;

- быстрое выявление предпринимаемых и свершившиеся нарушений ЗИ и инцидентов;

- обнаружение событий в системе ЗИ и предотвращение инцидентов с помощью использования индикаторов;

- измерение результативности средств управления для проверки того, что требования были выполнены;

- обновление планов защиты информации с целью учета данных, полученных в процессе деятельности, связанной как с постоянным контролем, так и анализом.

Документацию СМЗИ необходимо подготовить таким образом, чтобы она включала описания методик оценивания риска, планы обработки риска, описание процедур, необходимых предприятию для гарантии результативного планирования.

Стандарт ISO/IEC 17799 дает руководящие указания, которые рекомендуется использовать в процессе проектировании системы защиты. В

стандарте приводятся цель управления и перечень средств управления. Целью политик защиты является обеспечение направлений и поддержки руководством ЗИ в соответствии с бизнес-требованиями, законодательными нормами. Политику в области ЗИ необходимо анализироваться с запланированной периодичностью, чтобы гарантировать ее адекватную пригодность и адекватность.

В отношении управления активами цель состоит в том, чтобы обеспечить и поддерживать необходимые средства защиты активов организации в условиях труда, которые требуют четкой определенности. Необходимо составить и поддерживать реестры важных активов, а также активов, которые каким-либо образом связаны со средствами обработки информации. Информация должна быть классифицирована по значимости и критичности для компании.

Роль и ответственность сотрудников, пользователей в отношении информации и их защиты должны быть задокументированы в соответствии с политикой ЗИ в компании.

Целью управления сетевой безопасностью является защита ЗИ в сетях и защита сетевой инфраструктуры. Адекватное управление сетью требуется для защиты от рисков. Целью постоянного мониторинга является выявление действий, связанных с обработкой информации. Необходимо создать процедуру для постоянного мониторинга использования инструментов, используемых для обработки информации, и результаты должны регулярно проверяться.

Целью управления доступом пользователей является гарантированный доступ для зарегистрированных пользователей и предотвращение несанкционированного доступа в КИС. Назначение и использование разрешений должны контролироваться и должны быть ограничены, установка паролей должна контролироваться формальным процессом администратора. Необходимо установить формальную процедуру регистрации пользователей.

Цель менеджмента инцидентов в СЗИ состоит в гарантировании того, что о событиях и слабостях в системе ЗИ, которые связаны с КИС, сообщается способом, который позволяет проводить своевременно корректирующие процессы. Необходимо установка ответственности руководства и процедур быстрого, результатного и регламентированного реагирования на все инциденты в системе ЗИ. Необходимо предусмотреть механизм, предоставляющий возможности определения количества типов, объемов инцидентов в системе ЗИ и выполнять их постоянный контроль.

В [34] приведены модель зрелости процессов управления информационной безопасностью, в которой наиболее высоким уровнем являются «управляемый» и «оптимизированный». Управляемый уровень характеризуется мониторингом на объекте защиты и оценкой процесса управления, выполняется их оптимизация, частичное использование средств автоматизации. Оптимизационный уровень характеризует проработанность процесса управления информационной безопасностью, способности к выполнению быстрой адаптации в случае возникновения изменений в бизнес-процессе, комплексное использование мер защиты, которые обеспечивают основу для улучшения процессов управления.

Основные шаги, которые необходимо выполнить, включают процесс управления информационной безопасностью [15]:

- планирование — анализ и оценка риска информационной безопасности, определение политик систем управления ЗИ, выбор мер защиты и их обновление для минимизации рисков, принятие решений о внедрении системы управления ЗИ;

- внедрение и эксплуатация системы управления ЗИ, включая разработку планов по обработке рисков информационной безопасности, реализацию мер по ее защите, управление работой, обнаружение и реагирование на возникающие инциденты безопасности;

- проверка (мониторинг и анализ), в том числе анализ производительности, в том числе анализ уровней остаточного риска

информационной безопасности, анализ внутренних аудитов системы управления ЗИ;

- совершенствования системы управления ЗИ, в т. ч. внедрение тактических и стратегических улучшений в системе, требующих принятия решения на уровне планирования, оценки достижения цели.

Стандарт ИСО/МЭК 15408-2002 содержит этапы управления безопасностью; это руководство по управлению безопасностью в информационно-коммуникационной системе [4]. Стандарт раскрывает общие проблемы управления, которые важны для эффективного планирования, внедрения и поддержки безопасности системы.

Анализ существующих стандартов управления безопасностью позволил сделать вывод, что они стремятся создать общие концепции и общие модели управления безопасностью; однако, эти стандарты не включают конкретные подходы к управлению информационной безопасностью в СГ КИС.

1.2 Инфраструктура распределенной корпоративной информационной системы и модель защищенности информации в ней

КИС современные компании являются важным инструментом управления бизнесом и значимым средством производства. Структура КИС состоит из двух больших блоков:

- информационная *инфраструктура;*

- информационные *сервисы.*

Блок информационной инфраструктуры представляет собой материальную базу и среду для функционирования информационной службы.

Инфраструктура современной компании и современного общества может быть представлена таким образом, чтобы она состояла из пространственно-распределенных подразделений этого общества и его

партнеров, клиентов и поставщиков. Основные взаимодействия между объектами компании осуществляются в рамках распределенной КИС с использованием устройств связи и каналов связи, назначаемых оператором связи с использованием различных сетевых программ и сервисы.

Основным принципом структуры распределенного КИС является сегментация сети по территориальной производственной принадлежности. Структурными единицами КИС является распределенный сегмент КИС. Сегмент КИС, в свою очередь, может быть сложной информационной системой, которая распространяется на региональном уровне.

Сегмент КИС представляет собой сеть, состоящую из сегментов сети второго уровня иерархии. В каждом сегменте есть рабочие станции, серверы, сеть, построенная на маршрутизаторах, набор коммутаторов, цифровые модемы, телефонные линии, оптоволоконные каналы FastEthernet, E1 и беспроводные каналы связи.

На рис. 1.2 показывает результат структурного разложения КИС [21].

Внедрение Интернета в технологии корпоративных коммуникаций привело к резкому увеличению числа пользователей внешних сетей, увеличению разнообразия типов каналов связи и использованию новых сетевых и информационных технологий. Это повысило требования безопасности для транзакций электронных сетей: серверов, маршрутизаторов, серверов удаленного доступа, каналов связи, операционных систем, баз данных и приложений. Опасности в каждом элементе системы защиты быстро растут, и эта тенденция сохранится и в будущем [18].

Острой является также проблема возможности внутренних угроз защищенности информации, особенно это касается крупных корпораций, имеющих территориально распределенные подразделения. Чем больше сотрудников и единиц вычислительной техники в корпорации, тем больше вероятность совершения серьезных инцидентов, результатом которых может стать похищение конфиденциальной информации, корпоративной базы

данных, содержащей важную для конкурентоспособности корпорации информацию.

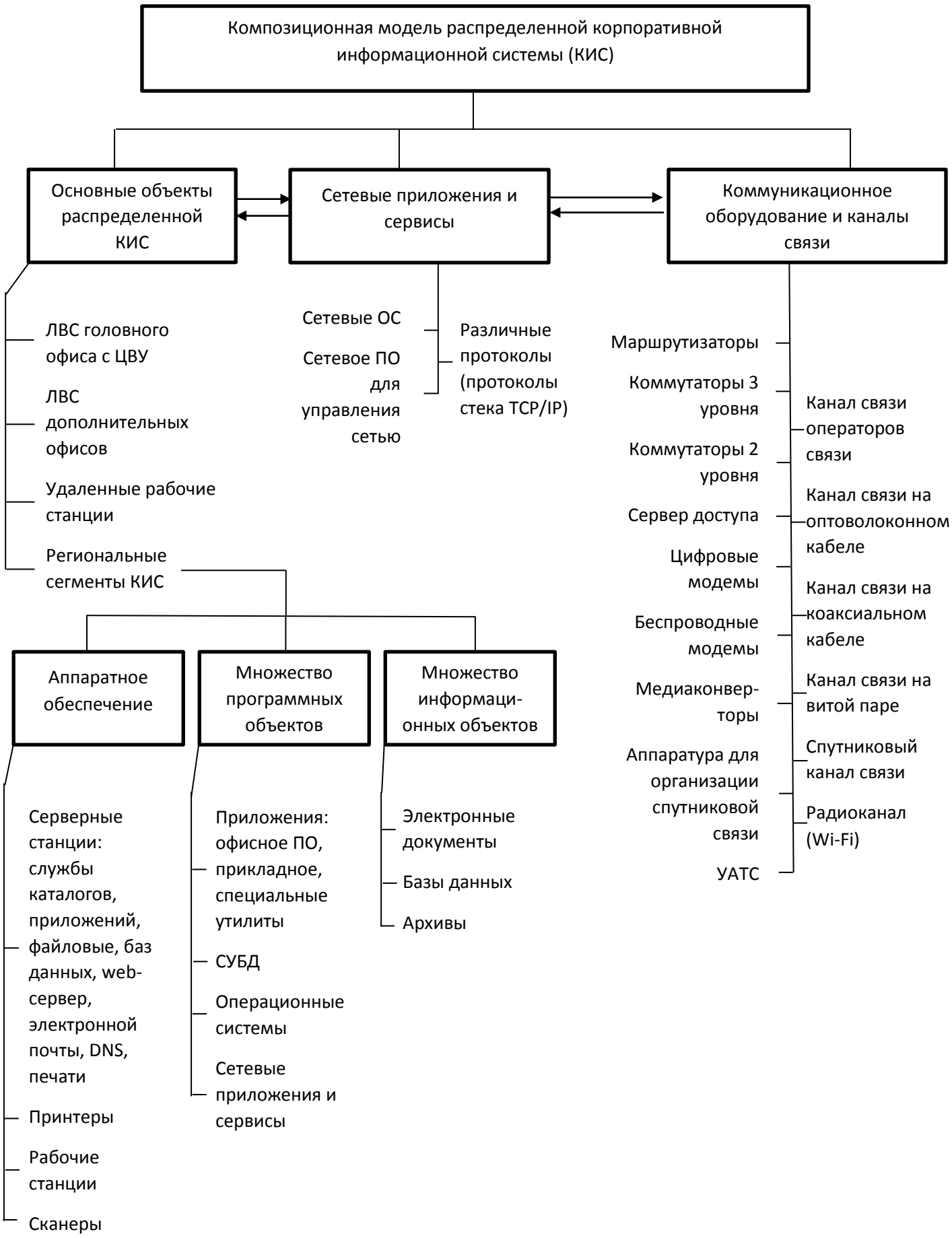

Рисунок 1.2 - Модель распределенной КИС с детализацией СГ КИС

Чем крупнее компания, тем больше объем средств, которыми она управляет, тем более агрессивными и профессиональными могут быть атаки с участием внутренних злоумышленников. По мнению экспертов, развитие и интеграция информационных технологий в корпоративные бизнес-процессы увеличивает опасность внутренних угроз информационной безопасности [30].

Современные средства взлома компьютерных сетей и кражи информации претерпевают быстрое развитие, наряду с другими высоко технологичными информационными отраслями. Поэтому обеспечение информационной безопасности КИС становится одной из первоочередных задач менеджмента компаний. Сохранение конфиденциальности, целостности и доступности информационных ресурсов компании во многом определяет качество и скорость принятия стратегических решений руководством компании.

Задача обеспечения информационной безопасности в КИС можно решить путем построения эффективной *системы ЗИ.*

На рис. 1.3 наглядно продемонстрирована модель состава системы защиты информации СГ КИС [19].

К системе ЗИ выдвигается требование абсолютной прозрачности для уже существующих в рамках КИС приложений и, кроме того, требование совместимости с используемыми корпорацией сетевыми технологиями.

Поэтому, с целью обеспечения надежной защищенности ресурсов КИС, системы ЗИ должны реализовываться на базе наиболее прогрессивных и наиболее перспективных технологий в области информационной защиты.

Рисунок 1.3 - Модель состава системы защиты информации СГ КИС

Поэтому, чтобы обеспечить эффективность компьютеризации в корпорации, необходимо обеспечить такие параметры безопасности информационных ресурсов, как целостность, конфиденциальность, подлинность соответствующей деловой информации, которая циркулирует в локальных и глобальных информационных сетях.

1.3 Современные концепции защищенности информации в корпоративных информационных системах

Развитие и совершенствование вредоносного ПО не стоит на месте, как и развитие систем защиты. Злоумышленники используют современные достижения информационных технологий (облачные технологии, новые алгоритмы шифрования и т.д.). Согласно одиннадцатому отчету Cisco по

кибербезопасности, «чтобы сократить время обнаружения злоумышленников, специалисты по кибербезопасности начинают все больше применять (и закупать) средства, использующие искусственный интеллект (ИИ) и машинное самообучение (МС)» [45]. С одной стороны, шифрование помогает усилить защиту, а с другой - рост как легитимного, так и вредоносного зашифрованного трафика (50% с октября 2017 года) умножает проблемы тех, кто защищается в процессе выявления потенциальных угроз и мониторинга их действий. «За прошедшие 12 месяцев специалисты Cisco по информационной безопасности зафиксировали более чем трехкратный рост шифрованного сетевого трафика от инспектируемых образцов вредоносного ПО» [45].

Использование интеллектуальных технологий и машинного обучения показывает хорошие результаты в области информационной безопасности, и со временем автоматически обнаружит нестандартные шаблоны в зашифрованном веб-трафике, в облачных средах и средах IoT. «Некоторые из 3600 директоров по информационной безопасности, опрошенных в ходе подготовки отчета Cisco 2018 Security Capabilities Benchmark Study, заявили, что доверяют таким инструментам, как МС и ИИ, и хотели бы их использовать, но они разочарованы большим количеством ложных срабатываний»[45].Постепенное совершенствование технологий МС и ИИ со временем позволит снизить количество «ложных тревог», и корректно определять «нормальную» активность сетей, отличая ее от реальных атак.

Как указывают современные эксперты, «эволюция вредоносного ПО за прошедший год показала, что злоумышленники с большей изобретательностью стали использовать незащищенные бреши в системах безопасности, — отметил Джон Стюарт (JohnStewart), старший вице-президент Cisco, директор по информационной безопасности. — Для отражения нападений и уменьшения подверженности нарастающим рискам как никогда ранее важно стратегически совершенствовать защиту, инвестировать в технологии и внедрять передовые методики» [45]

Некоторые результаты отчета Cisco 2018 Annual Cybersecurity Report показывает, что:

- финансовый ущерб от атак становится все более реальным;

- более половины всех атак нанесли финансовый ущерб на сумму более 500 млн. долларов, включая упущенную выгоду, оставление клиентов, упущенную выгоду и прямые расходы;

- атаки на цепочки поставок становятся все более сложными и набирают скорость. [45]

Такие атаки могут повлиять на компьютеры в больших масштабах, и их последствия могут длиться месяцами или даже годами. Необходимо помнить о потенциальных рисках использования программного и аппаратного обеспечения от организаций, которые не воспринимают проблемы информационной безопасности всерьез.

Чтобы снизить риск атаки на цепочку поставок, необходимо пересмотреть сторонние процедуры для проверки эффективности технологий информационной безопасности. В то же время защита информационных систем становится все труднее, уязвимости становятся все более разнообразными.

Чтобы защитить себя, организации используют сложные комбинации продуктов разных производителей. Это осложнение с растущим разнообразием уязвимостей негативно влияет на способность организаций отражать атаки и приводит, среди прочего, к увеличению рисков финансовых потерь.

Согласно отчету Cisco:

- «В 2017 г. 25% специалистов по информационной безопасности сообщили, что используют продукты от 11—20 вендоров, в 2016 г. так ответили 18%;
- Специалисты по информационной безопасности сообщили, что 32% уязвимостей затронули более половины систем, в 2016 г. так ответили 15%;

- Специалисты по информационной безопасности оценили пользу средств поведенческого анализа для выявления вредоносных объектов: 92% специалистов считают, что средства поведенческого анализа хорошо справляются с поставленной задачей; 2/3 представителей сектора здравоохранения и представители индустрии финансовых услуг считают поведенческую аналитику полезной для выявления вредоносных объектов;
- Растет использование облачных технологий; атакующие пользуются отсутствием продвинутых средств обеспечения безопасности;
- В этом году 27% специалистов по информационной безопасности сообщили об использовании внешних частных облаков (показатель 2016 г. — 20%); из них 57% размещают сеть в облаке ради лучшей защиты данных, 48% — ради масштабируемости, 46% — ради удобства эксплуатации»[45].

Хотя облако обеспечивает повышенную безопасность данных, злоумышленники пользуются тем, что компании не очень хорошо защищают развивающиеся и расширяющиеся облачные конфигурации. Эффективность защиты таких конфигураций повышается за счет использования комбинации передовых технологий, таких как передовые технологии безопасности, такие как машинное обучение, и инструментов безопасности мирового класса, таких как облачные платформы информационной безопасности.

В последние годы также наблюдается тенденция к росту вредоносных программ и времени обнаружения. «Продемонстрированное Cisco медианное время обнаружения (timetodetection, TTD) за период с ноября 2016 по октябрь 2017 г. составило около 4,6 часов. В ноябре 2015 г. этот показатель составил 39 часов, а по данным Отчета Cisco по кибербезопасности за 2017 г., медианное время обнаружения за период с ноября 2015 по октябрь 2016 г. составило 14 часов» [45].

Ключевым фактором для Cisco в процессе сокращения времени обнаружения и поддержания его на низком уровне стала технология информационной безопасности. Чем короче время обнаружения, тем быстрее атака будет отражена.

Относительно описанных тенденций, дополнительные рекомендации для подразделений информационной безопасности, являются:

- контроль за соблюдением политик и практик компании по обновлению приложений, систем и устройств;

- своевременное получение точных данных об угрозах и наличие процессов использования этих данных для мониторинга безопасности;

- проведение углубленного и углубленного анализа;

- регулярное резервное копирование данных и проверка процедур восстановления — критические действия в контексте быстрого развития сетевых вымогателей и вредоносных программ;

- выполнять проверки безопасности на микро сервисах, облачных сервисах и системах администрирования приложений.

Галицкий А.В. отмечает существование «различных подходов к формированию архитектур управления информационной безопасностью КИС:

- использование технологии управления всеми устройствами безопасности КИС из центрального узла нереализуемо, так как первичных устройств большое количество, и контроль за ними может вызвать слишком большую загрузку центрального узла управления; затруднительно получение детализированной информации, которая необходима для управления; локальные методы управления в ряде случаев являются технически необходимыми;

- по опыту ведущих производителей средств обеспечения сетевой безопасности известно, что организация может успешно реализовывать свою *политику безопасности* в распределенных КИС при централизованном управлении безопасностью» [10, с.286].

Многие компании (CiscoSystems, ComputerAssociates, PLATINUM) используют механизмы для интеграции управления СрЗИ в традиционные системы управления сетью [8]. Однако этот тип интегрированной системы

управления являются дорогостоящими, а некоторые вопросы управления информационной безопасностью не решаются таких системами.

Эффективная система управления ИБ сетевой КИС должна сопровождаться системой иерархического управления, состоящей из:

- *централизованного* управления на уровне глобальной политики по информационной безопасности, соответствующей бизнес-процессам предприятия и определяющей набор правил безопасности для всех взаимодействий объектов КИС, а также объектов КИС и внешними объектами;

- системы протоколирования событий в сети, мониторинга и аудита, которые не всегда имеют вертикальную структуру, а часто работают автономно в конкретной подсистеме КИС.

Для того, чтобы обеспечить информационную безопасность в сегменте КИС в современных условиях компании начали использовать все больше автоматизированных систем управления информационной безопасностью на основе систем SIEM.

Астахова Л.В. отмечает, что в настоящее время «наиболее широкое распространение на рынке SIEM-систем получили системы, использующие сигнатурные методы корреляции событий информационной безопасности, что обусловлено, в первую очередь, простотой реализации данных систем, а также гибкостью при настройке и дальнейшей эксплуатации» [6, с. 165]. К таким системам SIEM (Security information and event management – управление информацией и событиями безопасности) относятся: HP ArcSight; IBM

QRadar; Symantec SIM; RSA Envision и другие. Недостатком является то, что системы, построенные по этому принципу, не адаптируются к условиям быстро меняющегося состава КИС из-за заранее определенных случаев информационной безопасности, встроенных в систему. К недостаткам таких систем также относится большое количество ложных срабатываний и относительная сложность конфигурации и реализации.

Анализ российского рынка SIEM-систем [24] показывает, что в современных условиях рынок SIEM развивается медленнее, чем за рубежом. Не все зарубежные производители представлены в нашей стране. Но в тоже время наблюдается развитие отечественных SIEM-систем. SIEM-системы чутко реагируют на новые достижения в области обработки данных. Улучшенная аналитика на больших данных BigData играет важную роль в SIEM-системах, используемых в сегменте КИС. Большой интерес представляет новая технология UEBA (User and Entity Behavior Analytics - поведенческая аналитика пользователей и сущностей) для интеграции в SIEM-системы [13]. Один из наиболее полезных вариантов применения модуля UEBA – это выявление инсайдеров путем детектирования статистических аномалий. Если обладающие легитимным доступом к информации сотрудники начинают нестандартно действовать, делать больше запросов или получать информацию по тем блокам данным, по которым ранее не получали, то самообучающиеся системы безопасности подают об этом сигнал.

По прогнозам Gartner ссылка, к 2020 году модули UEBA будут в каждой четвертой SIEM-системе.

Можно констатировать тенденцию развития автоматизированных систем управления защитой информации для сегмента КИС. Однако существующая методология информационного риск-менеджмента не предусматривает комплексный подход к управлению информационным риском. Использование экономико-математических моделей управления защитой информации не всегда ориентировано на достижение конечного

результата бизнес-процессов, что приводит к снижению эффективности управления рисками всего предприятия.

Выводы по первой главе

Успешное использование современных информационных технологий невозможно без эффективного управления не только компьютерной сетью, но и процессом ЗИ. Улучшение управления информационной безопасностью возможно за счет повышения качества эффекта управления как за счет использования новых методов решения проблемы управления, так и за счет сокращения продолжительности циклов этого контроля. Следовательно, обоснованным подходом к улучшению эффективности мер защиты информации могут стать разработки интеллектуальных средств принятия решений, касающихся вопросов *управления ЗИ.*

Хотя в настоящее время проводятся активные исследования по разработке методов и систем ЗИ, остается достаточно непроработанных вопросов, касающихся создания методов создания интеллектуальных средств ПНР в отношении управления ЗИ, что указывает на необходимость комплексных решений совокупности научных задач, которые направлены на выработку не только научно обоснованных, но и практически применимых моделей и методов интеллектуального обеспечения управлением процессов ЗИ.

Реализация упреждающих стратегий защиты информации требует сложных решений, которые включают разработку метода *оценки подозрительной активности* и различных сетевых *событий*, *подготовку информации* для принятия решений об управлении службами безопасности и сетевыми устройствами и реагирование в режиме реального времени на изменения условий операционной среды. *Проблема выбора рационального ответа* на нападение не была решена на практике из-за вероятности ответных действий, которые могли бы повлиять на нормальную работу защищенной КИС. Недостаточно исследованы для решения задач оценки

неизвестных вмешательств остаются методы нейронных сетей, генетический алгоритм и *методы нечеткой логики.*

Сущность управления защитой информации состоит в принятии решений относительно выработки стратегий защиты информации для всех этапов жизненного цикла системы ЗИ. Возрастающие требования к разработкам и мероприятиям внедрения технологий управления защитой информации не соответствуют существующим на данный момент состояниям нормативной базы, которая не позволяет адекватно решить проблему выбора рациональной модульной структуры СЗИ. Существующие руководящие документы и стандарты задают ряд *функциональных требований* к средствам защиты информации и не дают никакой методики проведения сравнительного анализа разных наборов средств ЗИ, которые сертифицированы по одному и тому же классу, преследуя цель выявить более рациональный целостный вариант системы защиты информации.

Исследования и разработки технологий, методов и инструментов, позволяющих в реальном времени оценить риск нарушения ИБ, являются многообещающими, а также направлены на прогнозирование уровня информационной безопасности в процессе проектирования систем информационной безопасности. Следует отметить, что показатели уровня информационной безопасности должны формироваться с минимальным привлечением экспертов на основе информации, характеризующей информационную ценность ресурсов, требующих защиты, данных о технических характеристиках, применяемых или планируемых мерах безопасности, с учетом учет большого количества реальных угроз специфического функционирования конкретных объектов защиты.

Анализируя зарубежные и национальные публикации, связанные с этой проблемой, можно выявить растущую тенденцию популярности инструментов оценки рисков, а также программных инструментов для их анализа и управления рисками.

Анализ представленных на современном рынке программные приложений, для автоматизации управления рисками нарушений ИБ, показал, что основными недостатками таких систем являются:

- наличие высококвалифицированных специалистов;

- трудности, возникающие при адаптации методов к потребностям конкретной организации;

- невозможность оценки эффективности конкретного комплекса защиты информации, используемого в компании;

- необходимость иметь достоверную статистику по корпоративным инцидентам информационной безопасности.

Одной из основных проблем по созданию систем управления ЗИ является проблема обеспечения *автоматизированной поддержкой принятия решений* относительно управления ЗИ в течение всего периода работы КИС и в условиях изменяющихся условий информационной среды. Для этого требуется инфраструктурное программное обеспечение, поддерживающее математические модели и *методы принятия научных решений*. Создание инструментальных программных комплексов, использующих все возможности компьютера, позволит принимать научно обоснованные решения, так как процесс принятия решений будет основан на анализе и прогнозе, выполненном с применением математических методов.

ГЛАВА 2 МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

2.1 Основные научно-теоретические подходы к разработке систем управления защитой информации.

Защита информации, методы и методики защиты уже около тридцати лет являются предметом активного обсуждения как за рубежом, так и в России. Постоянно разрабатываются новые методы, способы и средства защиты информации, выпускаются новые защитные системы, ведутся научно-исследовательские работы по разработке методик управления защитой информации.

Анализ результатов научно-исследовательских работ в области ЗИ показывает, что значительным достижением в теории защиты информации стали работы, посвященные проблемам создания новых средств защиты информации различного характера, осуществляющие защиту информации на различных уровнях (технические средства, программные и аппаратные комплексы, криптографические средства защиты и т.д.), а также интегрированные системы защиты информации [11]. Анализ результатов таких изменений и исследований был представлен в работах российских [7, 8, 11, 14, 23, 33] и зарубежных авторов [23, 37, 44-51]. Ключевым итогом такого рода работ является формирование основ теории защиты информации.

Массовое использование информационных технологий коммерческими корпорациями, колоссальный рост объема критически важной информации, хранящейся и передаваемой в цифровом виде, повышение значимости защиты информации – факторы, повлиявшие на активизацию теоретических исследований, связанных с защитой информации.

В работах [10, 18, 33] рассматриваются вопросы и проблемы компьютерной безопасности. Актуальными являются также вопросы

применения криптографических методов и средств в сфере защиты информации [22], а также вопросы обнаружения нежелательных вторжений [24].

В ряде работ [19, 20, 41] особый акцент сделан на необходимость применения системного подхода для разработки эффективных средств ЗИ, разработки моделей угроз, декомпозиции разрабатываемых СЗИ (систем защиты информации), разбиения их на функциональные подсистемы для определения воздействующих на них факторов и выявления возможных угроз, а также для разработки системы индикаторов, характеризующих эффективность СЗИ.

По мнению многих авторов, разрабатывающих проблемы ЗИ, для эффективного решения данной проблемы обязательными условиями является формирование методологического базиса рассматриваемого вопроса, исследование адаптивной организации систем ЗИ, а также рассмотрение вопросов автоматизации ЗИ [12].

По мнению В.А.Герасименко [11] базой для формирования СЗИ должны служить платы обработки информации, которые устанавливаются на защищаемый объект, и благодаря которой проводится анализ критичности, в соответствии с чем далее проводится обоснование требований к СЗИ. На основании сформулированных требований формируется набор средств защиты информации, применение которых даст возможность обеспечения требуемого уровня защиты. Аргументированное обоснование состава (набора средств) ЗИ – это общая задача всего механизма управления ЗИ.

Особенности проектирования систем ЗИ рассматриваются авторами в [42]. Анализ работ позволяет выделить два основных подхода в отношении построения системы ЗИ:

- продуктный подход;
- проектный подход.

Продуктный подход подразумевает, что первичным является формирование набора средств ЗИ, а далее, на основе функций, выполняемых этими средствами, формулируется политика безопасности. Соответственно, проектный подход предусматривает, в первую очередь, формирование политики безопасности, после чего на основании определенных требований выбираются необходимые для ее реализации средства ЗИ.

Как отмечается в [9], системы на основе проектного подхода лучше оптимизированы и являются более эффективными, что делает их более подходящими для использования в гетерогенных сетях. Кроме того, следует отметить, что решения, спроектированные с помощью проектного подхода, являются более долговременными.

Общие принципы и методика выбора средств защиты информации на основе критерия оптимальности (подразумевающего минимизацию затрат при обеспечении заданного уровня защищенности информации), приведена в [14]. Основой данной методики является оценка эффективности выполнения разных функций с помощью средств ЗИ.

По мнению некоторых авторов, например [34], управление операциями и стратегическое *планирование* использования защитного оборудования рассматриваются как наиболее важные процессы макроуправления. В этом контексте оперативное управление подразумевает динамическое управление информационной безопасностью при ее автоматизированной обработке. В рамках оперативного управления должно быть постоянное признание состояния системы защиты информации, а также принятие и реализация решений, касающихся необходимости оперативных вмешательств в работу системы для обеспечения ЗИ. Для принятия решений правильное решение должно быть выбрано из регистра решений, который создается заранее [44].

Планирование ЗИ относится к процессу формирования в течении запланированного периода программ, обеспечивающих оптимальное использование средств ЗИ. Оптимальность подразумевает обеспечение

необходимого уровня защиты запланированной суммы расходов либо при минимизации данной суммы.

Многие из вышеуказанных авторов отмечают при этом, что задача принятия решений является одной из наиболее сложных и в то же время наиболее важных задач в области автоматизации управления защитой информации.

Особенности и основные понятия организационного управления информационной безопасностью учтены в работе [40]. Автор отмечает, что ограничение для обеспечения возрастающих требований к уровню информационной безопасности является недостаточность имеющегося научно-технического обеспечения (НТО). Для обеспечения необходимого уровня защищенности, НТО должно соответствовать как динамике информационной среды, так и динамике управления стратегиями информационного противостояния. В данной работе отмечается, что многие из предлагаемых на сегодняшний день концептуальных подходов к ЗИ носят не конкретный, общий характер, соответственно, для обеспечения возможности их применения в сложных распределенных КИС они должны быть уточнены и указаны в с учетом процессов, происходящих в реальной среде информационного противостояния. Автор указывает на отсутствие систематических научно-методических исследований в этой области в качестве еще одного ограничивающего фактора становления и развития теории организационного управления ЗИ.

В работе [46] приведено формализованное описание методов синтеза идеальных стратегий организации управления информационной безопасностью в моделях игр для принятия решений и, кроме того, способ управления квантованием пакетов при передаче категорированной информации, управление восстановление целостности информации (алгоритм выбора идеальной стратегии резервного копирования) и метод оценки информационной безопасности в условиях вирусных программ.

Исследование [9] управления информационной безопасностью рассматривается в основном как организационный процесс. В связи с этим, по мнению автора, задачи управления защитой информации могут быть решены административной группой (менеджеры и администраторы безопасности, а также операторы). Автор рассматривает управление защитой информации, как осуществление контроля за распределением информации в корпоративной сети, обеспечение функциональной работоспособности средств ЗИ, фиксация событий, связанных с нарушениями ЗИ и реализуемых при этом функций, а также периодическое обновление БД информационной защиты.

Работы [17, 49] посвящены анализу основных научно-теоретических проблем синтеза адаптированных систем по обеспечению информационной безопасности, а также вопросам применения этих систем в КИС. В данных работах особо подчеркивается невозможность обеспечения абсолютной безопасности как отдельных компонентов системы, так и ее в целом, так как любая защита может быть преодолена при отсутствии ограничения во времени. Целесообразно рассматривать лишь некоторый достаточный уровень защищенности, в состоянии которого стоимость ее преодоления превышает стоимость получаемой при этом информации. До настоящего времени ввиду большой сложности и трудной формализуемости не удается сформировать показатели количественной оценки уровня защищенности информационной системы.

В то же время степень риска зависит от показателей ценности информационных ресурсов, вероятности угроз и простоты уязвимости, а также от *эффективности* применяемых *мер защиты*. Единственным *контролируемым фактором* среди вышеперечисленных является мера защиты. В результате, *оптимальный выбор* защитного снаряжения может снизить риск до приемлемого уровня. Результаты оценки риска служат основанием для обоснования выбора набора мер защиты системы.

Эффективность системы ЗИ зависит не только применяемыми продуктами и методами, обязательным ее условием является также регулярный аудит системы на наличие уязвимостей и мониторинг трафика с целью выявления потенциальных угроз и формирования рекомендаций для их устранения.

Перечисленные средства должны функционировать, взаимодействуя с персоналом службы безопасности КИС, но создают значительные проблемы для проведения анализа и оперативного реагирования на разные нештатные ситуации со стороны администратора безопасности. Соответственно, можно с уверенностью говорить о необходимости автоматизации процесса реагирования на возникающие информационные угрозы. Поэтому перед разработчиками стоит задача разработки и формализации моделей принятия решений о классификации информационных угроз по степени их активности и опасности для системы и о реализации противодействия этим угрозам.

В работе [16] рассматриваются многокритериальная модель оценки безопасности и *метод выбора межсетевых экранов* с использованием метода нечетких множеств, синтез подсистем анализа безопасности и обнаружения угроз, а также метод решения игры для борьбы с информационными угрозами.

Работа [18, 39] посвящена проблемам адаптивного управления ЗИ безопасностью в области защиты от несанкционированного доступа. В данных работах рассмотрены разработки подсистем управления ЗИ, которые реализуют парадигму адаптивного управления и используют неявную *пользовательскую модель* объекта управления в главном цикле. Также рассмотрен метод, позволяющий на этапе проектирования определить рациональный состав и структуру системы защиты информации, основанный на методе минимакса, с применением показателя достижимости характеристик «эталонной» системы. Также рассматривается способ изменения структур и модификаций системы ЗИ во время работы, в котором

используется критерий максимального увеличения показателя безопасности при ограничениях по стоимости.

Следует отметить высокую сложность формирования «эталонной» системы защиты на различных этапах жизненного цикла СЗИ.

2.2 Методы анализа информации по идентификации атак

Методы анализа информации, идентификации атак и принятия решений, используемые в системе защиты информации, в конечном итоге определяют эффективность системы ЗИ.

Основными методами идентификации атак, используемыми в таких системах, являются статистическая система экспертных систем [24] и метод нейронной сети [17].

Статистический метод основан на статистическом устройстве, которое адаптируется к поведению соответствующего лица. Для каждого информационного субъекта формируется его профиль в рамках информационной системы, далее проводится анализ на наличие отклонений (путем сравнения с эталонным) и при выявлении таковых фиксируется наличие несанкционированной информационной деятельности. Преимуществом данного метода является универсальность статистических методов и отсутствие необходимости знаний о возможных атаках для проведения анализа. При этом сложностью является неопределенность при задании граничных характеристик параметров, которые отслеживаются, что вызывает трудности для адекватной идентификации производимой деятельности как аномальной. Такие методы оказываются неприменимыми для реагирования на неизвестные ранее атаки.

Набор правил, охватывающих знания эксперта, составляют экспертную систему. Таким образом, все знания об информационных атаках представляются в виде правил, которые, в свою очередь, записываются в виде порядка (последовательности) действий, применяемых при наличии или реализации информационной угрозы. Экспертная база данных такой

системы должна содержать знания (сценарии) всех или большей части известных информационных угроз и видов атак, кроме того, необходимо постоянное ее обновление. Преимуществом данного метода является очень малое количество ложных тревог, а его ключевым недостатком – неспособность реагировать на появление неизвестной атаки, кроме того, известная атака, реализованная с небольшими изменениями, может привести к неэффективному срабатыванию системы.

Несмотря на имеющиеся недостатки, статистический подход и анализ информационного пространства на основе правил используется в большинстве современных методов обнаружения атак. Однако, растущее количественно и качественно числа атак и их видов приводит к тому, что даже при постоянном обновлении базы данных экспертной системы, такая система не гарантирует покрытие всего диапазона атак.

Нейросетевой подход, в отличие от экспертных систем, позволяет проводить аналитическую работу и определить соответствие имеющихся характеристик работы системы и тех, что сеть научена распознавать, оценив наличие либо отсутствие потенциальной угрозы. Нейронные сети проходят обучение идентификации объектов предметной области на предварительно сформированной выборке, в процессе которого происходит настройка нейросети для достижения удовлетворительных результатов распознавания. По мере работы проведения анализа, нейросеть набирает опыт, что делает результат распознавания более корректным. При этом нейросеть способна по результатам изучения характеристик идентифицировать атаки и угрозы, отличные от тех, что ей встречались ранее.

Технология адаптивного профилирования, разработанная на основе исследований иммунной системы человека, используется для решения проблемы защиты важнейших информационных ресурсов. Такая система показывает высокие результаты в точности определения сетевых атак или несанкционированных действий [37]. Технология адаптивного профилирования работает подобно иммунной системе человека,

предварительно изучая нормальное поведение приложений (наблюдая процесс исполнения кода в штатном режиме в нормально работающих программах). Далее обученная система анализирует работающую ИС и любые отклонения в конфигурации, ошибки ПО и другие уязвимости идентифицируются данной технологией, и происходит их блокировка (прекращение их работы посредством блокировки системных вызовов). Такая технология оказывается эффективна для защиты серверных приложений.

Продолжая процесс обучения, система учится распознавать допустимые изменения приложений, что в конечном итоге приводит к минимизации ложных срабатываний. Данная технология оказывается, таким образом, эффективной для защиты как от известных ранее, так и от неизвестных атак, и даже в случае зашифрованной информации.

Как статистический, так и нейросетевой методы имеют как достоинства, так и недостатки. Кроме того, многие системы защиты информации и разработки в данной области являются запатентованными продуктами иностранных компаний, с закрытым кодом и неизвестными методами, применяемыми в данных системах.

По словам автора [20], методологические и технологические основы создания интеллектуальных средств предотвращения компьютерных атак в КИС все еще находятся на ранней стадии разработки. На современном этапе информационного развития стоит острая необходимость в разработке комплексных решений по реализации средств оценки и противодействия потенциально опасных событий, происходящих в информационной сети, а также по управлению средствами и сетевым оборудованием.

2.3 Методы оценки защищенности информационной системы

Вопрос адекватной оценки степени защищенности ИС неизбежно при создании информационной структуры ИС. Оценка степени защищенности

должна также учитывать такие параметры, как соответствие использованных средств и механизмов защиты и уровня существующих рисков и угроз; определение необходимого и достаточного уровня защищенности в зависимости от среды функционирования ИС, состав критериев для оценки защищенности информационной системы. Данные вопросы рассматриваются в большом количестве работ, в частности [17, 21, 33].

Одной из концептуальных задач создания систем ЗИ является выбор критериев (формализованных мер оценки) для определения уровня защищенности системы. Обычно под формализованными мерами подразумевают способ оценки «силы» определенной характеристики, либо основанные на применении цифровой шкалы оценки реальных характеристик системы [33]. Идея оценки уровня защищенности с помощью ряда критериев была впервые предложена в Оранжевой книге для применения к СУБД и операционным системам.

Если шкала критериев оценки степени защищенности ИС сформирована, то сравнение различных систем защиты осуществляется путем простого сравнения соответствующих числовых показателей для каждой из систем. Такие шкалы критериев сформированы для оценки криптографических механизмов и для систем радиоэлектронной защиты, однако, в области защиты от несанкционированного доступа такая шкала отсутствует.

В качестве критериев оценки защищенности от несанкционированного доступа можно было бы использовать показатели интенсивности атак на систему и вероятности их реализации, рассчитанной в определенный промежуток времени, но проблемой таких показателей является их апостериорность, что снижает их практическую ценность. Для оценки реальной угрозы реализации атак необходимо применять иные критерии, учитывающие такие параметры, как условия использования ИС, квалификация пользователей, применяемые технологии обработки и хранения данных и др. Сложным вопросом является фактически, не только

категоризация, но и полный перечень возможных факторов, которые могут быть причастны к реализации возможных угроз в системе ЗИ.

Наиболее эффективным для практической оценки уровня безопасности системы ЗИ является использование критериев не апостериорных, а априорных критериев. Эти критерии могут быть предоставлены путем сравнения системы и ее состояния с набором эталонных профилей для служб защиты. Профили, которые обеспечивают определенный уровень безопасности, требуемый при определенных условиях, используются в качестве эталонных профилей. Таким образом, мы можем сказать, что две системы имеют одинаковый уровень безопасности, если они реализуют один и тот же набор защитных механизмов, которые имеют одинаковую «силу». Следовательно, система 1 имеет более высокий уровень безопасности, если «сила» хотя бы одного из реализованных механизмов защиты выше, чем у механизмов системы 2, или если система 1 реализовала механизмы защиты, отсутствующие в системе 2 [33].

В работе [11] автором была предложена следующая формула, с помощью которой может быть определен интегрированный показатель безопасности для ИС:

$$Z(T) = \Phi[K, R(T)], \qquad (2.1)$$

где K - показатель целостности учета возможных стратегий атаки;

R - показатель эффективности применения оборонительных стратегий, конструктивно заложенных в СЗИ во временном интервале $[0,T]$.

В вышеуказанной работе на основании формулы 2.1 рассмотрены различные варианты формирования функции Φ для различных информационных сред и ситуаций. Однако, следует отметить, что в работе не рассматривается вопрос реального определения значения показателей K и R. При этом очевидно, что определение этих показателей является нетривиальной задачей. Часть необходимой информации, очевидно, может

быть определена из частных вероятностей реализации, рассчитанных для различных угроз.

Таким образом, можно констатировать, что в рассматриваемой работе не раскрыт вопрос методики и критериев определения уровня защищенности ИС. Фактически, работа не раскрывает вопрос, а только формулирует общую постановку задачи, требующей решения.

В последнее время подходы к анализу рисков, где риски органически связаны с уровнем безопасности, т.е. затем уровень безопасности системы можно определить исходя из анализа возможных рисков и наоборот.

В соответствии с фундаментальными работами в сфере управления рисками [14, 23], анализ рисков рекомендовано проводить в следующих случаях:

- существенное изменение в структуре информационной системы или ее обновление;
- изменение технологий построения корпоративной системы;
- реализация новых/дополнительных подключений в компании;
- реализация подключения к глобальным сетям, которое ранее не было доступно;
- фундаментальные изменения в стратегии и тактике ведения бизнеса в компании;
- плановая или внеплановая проверка эффективности СЗИ.

В соответствии с вышеуказанной работой управление рисками состоит из следующих этапов.

В данных работах предлагаются следующие этапы управления рисками:

- оценка возможных потерь при реализации рисков;
- анализ возможных (потенциальных угроз) в данной информационной среде;
- анализ уязвимостей информационной системы;

- подбор мер и средств защиты, обеспечивающих сокращение риска до приемлемого уровня при заданных ценовых ограничениях.

Автор работы [14] «управление рисками» расценивает как процесс выбора и реализации комплекса контрмер, способных обеспечить требуемый уровень защищенности системы соответственно предварительно проведенному анализу рисков. Согласно данной работе, на каждой стадии жизненного цикла ИС должны быть реализованы соответствующие контрмеры по различным аспектам безопасности, а именно:

- формирование политики ИБ и внесение в нее изменений;

- формирование и корректировки регламентов работы, обслуживания систем и в должностных инструкциях;

- применение для обеспечения информационной безопасности *дополнительных* программно-технических средств защиты.

Согласно работе [23], при проведении оценки рисков информационной системы должны быть учтены такие факторы, как:

- ценность защищаемых информационных ресурсов;

- оценка величины значимости потенциальных угроз и имеющихся уязвимостей;

- эффективность разработанных ранее (существующих) и *планируемых средств защиты информации*.

Анализ рисков важен для дальнейшей сравнительной оценки различных возможных вариантов реализации системы защиты, что особенно важно в связи с повышенными требованиями к СЗИ.

В международном стандарте ИСО/МЭК 15408 [4] «Общие критерии оценки безопасности ИТ» четко структурированы и сформулированы требования по информационной безопасности для различных классов информационных систем. Однако, в то же время, этот документ не содержит методологию оценки этих критериев.

Анализ различных стандартов, принятых в области управления рисками информационной безопасности (как иностранных, так и

отечественных), показывает, что эти стандарты не содержат некоторых важных деталей методологии оценки рисков; для их успешного применения на практике их необходимо указать; требуются также дополнительные методы оценки, учитывающие существенные качественные и количественные показатели.

Важность и актуальность формирования научно-методологической основы проблемы оценки защищенности информации подчеркивается в работе [7]

Процесс решения проблемы обеспечения заданного уровня защищенности можно разбить на две задачи, которые должны быть решены последовательно:

- *оценка в количественном выражении уровня защищенности информации в системе;*

- *анализ данных и* принятие решений о необходимости *настройки параметров и свойств системы защиты для поддержания необходимого* уровня безопасности.

Очевидно, что для определения количественных показателей критериев уровня безопасности необходимо принять решение о необходимости корректировки состава свойств СЗИ, кроме того, необходимо следить за динамикой изменений во времени индикаторы уровня безопасности, основанные на изменениях внешних и внутренних условий ИС.

Инструменты для оценки параметров уровня безопасности, а также для оценки существующих рисков нарушения ИБ, должны позволять строить объектно-ориентированные структурные модели интеллектуальной собственности, а также модели рисков отдельных сегментов КИС.

Таким образом, можно сказать, что создание и развитие интеллектуальных систем защиты информации является серьезной научной проблемой, требующей разработки ряда методов и методологий, научно обоснованных и применимых в рамках создания теории. интеллектуальная безопасность.

Выводы по второй главе

Как показывает проведенный анализ, работы по проблемам создания новых средств защиты информации различного характера, стали значимым достижением в теории защиты информации и являются базисом разработки новых способов создания комплексных систем защиты информации.

Для построения систем информационной безопасности применяются, преимущественно, два подхода: продуктный и проектный. Продуктный подход отталкивается от выбора средств Зи и уже на основании реализованных этим набором функций вырабатывается политика безопасности. Проектный подход подразумевает первоначально формирование политики безопасности, а уже на основании нее – выбор подходящих средств ЗИ.

ГЛАВА 3 МОДЕЛЬ ОЦЕНКИ УРОВНЯ ИНФОРМАЦИОННЫХ РИСКОВ В СЕГМЕНТЕ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

3.1 Обзор методологической базы исследования информационных рисков

Научная литература, национальные и международные стандарты уделяют значительное внимание проблеме управления защитой информации, что связано с широким использованием информации в деятельности современных корпораций.

Анализ существующих стандартов в области менеджмента информационной безопасности [18] показывает, что целью стандартов является формулировка общих концепций, а также этапов управления. Однако стандарты не определяют конкретные подходы к процессам управления безопасностью систем; они устанавливают функциональные требования к защитным средствам, но не представляют методы сравнительного анализа различных комплексов защитных средств для выбора рационального варианта системы ЗИ.

Ученые Бернстайн П., Бланк И.А., Витлинский В.В., Луман Н., Марковиц Г., Найт Ф.Х., Самуельсон П. и другие разработали общие принципы и инструментарий управления экономическими рисками. Математические методы и инструментарий экономико-математичного моделирования представлены в работах Клейнера Г.Б., Кульби В.В., Матвийчука А.В. [44], Сигала А.В. и других специалистов. Статистические методы моделирования могут использоваться для изучения информационных рисков в сочетании с неформальными методами исследований [24]. Управление информационными рисками в условиях неопределенности может осуществляться с использованием гибких методов, таких как интервальный метод, нейронные сети, генетические алгоритмы, а также нечеткие множества и нечеткая логика.

Наиболее соответствующим сути понятием "информационного риска" является понятие "угроза безопасности информации". Липаев В.В. вкладывает в понятие "информационный риск" следующего содержания: это потенциальное событие, которое разрушает несанкционированную информацию, искажает информацию, нарушает ее конфиденциальность или доступность [18].

Проблемы оценивания качества информации, а также надежности аппаратных и программных средств информационных систем рассматривали в своих работах Байхельт Ф., Зегжда П.Д., Стенг Д.И., Франкен П. и др. Стенг Д.И. дополнительно ограничивает понятие информационного риска [37] и учитывает только угрозы информационной безопасности в компьютерных системах. Сторонники такого подхода к определению «информационный риск», как правило, являются экспертами в области ЗИ.

Другая группа специалистов под информационным риском понимает возможности получения убытков, недополучения прибыли и прочие негативные последствия для компании. Примером такого подхода является следующее определение М. Мура: "Информационные риски – это опасность возникновения убытков или вреда в результате применения компанией информационных технологий. Другими словами, информационные риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и других средств связи" [23].

Недостатком вышеприведенного определения является размытый контур объектов, повреждение или изменение свойств, которые приведут к потерям в результате рискованного события. Приведенное выше определение исключает из рассмотрения информационные риски, которые могут быть связаны с оформлением документов, влиянием киберпреступников на информационные ресурсы в результате шпионской или диверсионной деятельности и т. п.

Авторы многих работ, в частности М. Мур [23] и Дж. Джонс [47], для подробного анализа источников риска впервые предлагают создание своей

модели. В зависимости от цели исследования и источников риска выбирается метод моделирования и уровень детализации объектов и процессов.

Одним из разделов математики, нашедшим широкое приложение в моделировании сложных систем, каковой является КИС, является теория множеств. Расширить возможности классической теории множеств позволяет теория нечетких множеств [34]. При моделировании сложных систем целесообразно использовать аппарат нечетких множеств для распределения объектов по подмножествам в условиях недостаточности информации и случайности процессов. При исследовании информационных рисков такое задание стоит, например, при решении задачи отнесения произвольного риска к множеству значимых рисков в конкретной корпоративной системе. Методы нечетких множеств и нечеткой логики позволяют использовать как количественные, так и качественные оценки, получать интегральные показатели. Они в наибольшей степени подходят для работы с экспертными оценками.

В работе предлагается разработать механизм получения оценок риска, который заменил бы метод приблизительной табличной оценки риска современными математическими инструментами.

Формирование системы математических моделей и методов управления информационными рисками основывается на следующих концептуальных положениях:

- разработка и применение методов идентификации информационных ресурсов (активов) корпорации, которые могут стать объектами информационных рисков и угроз этим ресурсам;

- разработка и применение моделей количественного анализа и оценивания факторов (уязвимость, действенность средств защиты и т.п.) и общего уровня информационных рисков с применением инструментария нечеткой логики;

- разработка математических моделей относительно экономического обоснования эффективности использования механизмов (средств) снижения

степени информационных рисков, обеспечения соответствия функциональным критериям защищенности информации (конфиденциальности, целостности, доступности) и снижения связанных с этих потерь (убытков, вреда) предприятию.

В иностранных методиках анализа информационных рисков часто используют модели оценки риска, основанные на трех факторах: угроза, уязвимость, возможные убытки [48].

Выделяют четыре основных этапа анализа информационных рисков:

I. Идентификация компонент: информационных ресурсов и возможных угроз;

II. Оценка частоты событий возможных угроз из-за подверженности риску.

III. Оценка величины возможных убытков.

IV. Результат анализа информационных рисков КИС сводится к оценке общего уровня информационных рисков в корпоративной системе по шкале: C – "критический", H – "высокий", M – "средний", L – "низкий".

Предлагается применить лингвистический подход к моделированию анализа факторов информационного риска. Такой подход обеспечивает количественные описания отдельных элементов модели при условии нечеткой информации о значении критериев оценки факторов риска, их последствий в условиях действия агента угрозы, альтернативных путей для избегания негативного влияния информационных рисков. В соответствии с лингвистическим подходом, в качестве значений критериев и характеристики отношений между ними допускается не только количественное оценивание, но и лингвистическое.

Предлагается использовать интеллектуальные методы в системах интеллектуальной поддержки для оперативного управления информационной безопасностью в КИС: нечеткий вывод численной оценки вероятности информационных атак; организована классификация информации о событиях в базе знаний; модель нейтрализации угроз; принять решение о выборе

оптимального варианта реагирования на события в системе информационной безопасности.

Окончательный выбор состава комплекса средств защиты для системы ЗИ может быть сделан итеративно, шаг за шагом приближаясь к рациональному составу, который отвечал бы требованиям приемлемого уровня затрат на реализацию системы.

3.2 Постановка задачи оценивания риска информационной системы

Система корпорации является сложной человеко-машинной или технической социосистемой, которая включает в свой состав информационную систему предприятия. Для исследования таких систем используются разные типы моделей. Процесс функционирования КИС предприятия осуществляется в условиях противоборства предприятия как технической и социосистемы, с одной стороны, и конкурентов, злоумышленников, негативных влияний природы и других объектов и явлений, с другой стороны.

Одним из разделов математики, которые нашли широкое приложение в моделировании сложных систем, является теория множеств. Расширить возможности классической теории множеств позволяет теория нечетких множеств [14].

При моделировании сложных систем целесообразно использовать аппарат нечетких множеств для распределения объектов за подмножествами в условиях недостаточной информации и случайности процессов. При исследовании информационных рисков такое задание стоит, например, при решении задачи отнесения произвольного риска к множеству значимых рисков в конкретной корпоративной системе. Методы нечетких множеств и нечеткой логики позволяют использовать как количественные, так и качественные оценки, получать интегральные показатели. Они в наибольшей степени подходят для работы с экспертными оценками.

Предлагается разработать механизм получения оценок риска, который заменил бы приблизительный табличный метод приблизительной оценки риска современными математическими инструментами..

Формирование системы математических моделей и методов управления информационными рисками основывается на следующих концептуальных положениях:

- разработка и применение методов идентификации информационных ресурсов(активов) предприятия, которые могут стать объектами информационных рисков и угроз этим ресурсам;

- разработка и применение моделей количественного анализа и оценки факторов (уязвимости, действенности средств защиты и т.п.) и общего уровня информационных рисков с применением инструментария нечеткой логики;

- разработка математических моделей экономического обоснования эффективности использования механизмов способов снижения информационных рисков, обеспечения соответствия функциональным критериям защищенности информации (конфиденциальности, целостности, доступности, наблюдаемости) и снижения связанных с этих потерь (убытков, вреда) предприятию.

В иностранных методиках анализа информационных рисков используется модель оценивания риска по трем факторам: угроза, уязвимость, величина возможных убытков.

Выделяют четыре основных шага анализа информационных рисков [14]:

I. Идентификация компонент:

1. Информационные ресурсы (активы) компании, которые могут быть объектом риска. Согласно стандарту безопасности ISO/IEC 27001: 2013 информационный актив представляет собой материальный или нематериальный объект, который представляет собой информацию или содержит информацию, используется для хранения или обработки информации и является ценным для предприятия (организации);

2. Возможные угрозы (комбинации угроз) актива. Для управления рисками необходимо идентифицировать возможные опасности, которые угрожают КИС. Такими могут быть, например, стихийное бедствие, отключения электропитания, атака злоумышленника с разными степенями сложности последствий.

II. Оценка частоты событий возможных потерь в результате действия риска:

1. Возможный уровень силы (Threatcapability), с которой агенты угрозы будут действовать на актив. Допускается, что некоторая часть популяции агентов угрозы является более способной к влиянию на актив, другая - менее способной [44]. Проводится экспертное оценивание уровня угроз по набору показателей, которые характеризуют возможность доступа нарушителя соответствующего класса к информационным ресурсам по следующей шкале:

TC_VH – "очень высокий";

TC_H – "высокий";

TC_M – "средний";

TC_L – "низкий";

TC_VL – "очень низкий".

2. Ожидаемая действенность средств контроля (Controlstrength) на протяжении отведенного часового интервала. Взяв за основу ориентацию на среднюю способности агентов угрозы, принимается базовый уровень эффективности контроля [44].

Для оценивания уровня защиты используется следующая шкала:

CS_VH – "очень высокий";

CS_H – "высокий";

CS_M – "средний";

CS_L – "низкий";

CS_VL – "очень низкий".

Уязвимость рассматривается как результат влияния факторов возможного уровня силы угрозы и действенности средств контроля [44] и оценивается по шкале:

V_VH – "очень высокий";

V_H – "высокий";

V_M – "средний";

V_L – "низкий";

V_VL – "очень низкий".

Пример базы знаний для оценки уровня чувствительности приведен в табл. 3.1.

Реализации факторов риска (агентов угрозы) в пределах определенного часового интервала.

Таблица 3.1. Оценка уровня чувствительности корпоративной системы

		Чувствительность				
Возможный уровень силы угрозы	TC_VH	V_VH	V_VH	V_VH	V_H	V_M
	TC_H	V_VH	V_VH	V_M	V_M	V_ L
	TC_M	V_VH	V_H	V_M	V_ L	V_VL
	TC_L	V_H	V_M	V_ L	V_VL	V_VL
	TC_VL	V_M	V_ L	V_VL	V_VL	V_VL
		CS_VL	CS_L	CS_M	CS_H	CS_VH
		Действенность средств контроля				

Под факторами следует понимать описание типов злоумышленников, которые преднамеренно или случайно, действиями или бездеятельностью способны нанести убытки корпоративной системе [16].

Оценка частоты реализации факторов риска может проводиться по шкале:

TEF_VH – "очень высокая";

TEF_H – "высокая";

TEF_M –"средняя";

TEF_L – "низкая";

TEF_VL – "очень низкая".

Частота возникновения событий потерь - возможная частота в течение определенного часового интервала, с которой агент угрозы наносит вред активу, рассматривается как результат влияния факторов частоты возникновения угрозы и уязвимости [16].

Используются следующие оценки уровня частоты событий потерь информационных активов:

LEF_VH – "очень высокий";

LEF_H – "высокий";

LEF_M – "средний";

LEF_L – "низкий";

LEF_VL – "очень низкий".

Пример базы знаний для оценивания уровня частоты возникновения событий потерь приводится в табл. 3.2.

Таблица 3.2. Оценивание уровня частоты событий потерь вследствие информационных рисков

		Частота событий потерь				
Частота возникновения угроз	TC_VH	V_VH	V_VH	V_VH	V_H	V_M
	TC_H	V_VH	V_VH	V_H	V_M	V_ L
	TC_M	V_VH	V_H	V_M	V_ L	V_VL
	TC_L	V_H	V_M	V_ L	V_VL	V_VL
	TC_VL	V_M	V_ L	V_VL	V_VL	V_VL
		CS_VL	CS_L	CS_M	CS_H	CS_VH
		Действенность средств контроля				

III. Оценивание величины возможных убытков:

- определение возможного действия каждого из агентов угрозы информационному активу;

- оценивание величины каждой из возможных форм убытков, которые связаны с действием определенного агенту угрозы;

- оценивание величины всех возможных форм убытков по шкале:

PL_VH – "очень большие";

PL_H – "большие";

PL_Sg– "существенные";

PL_M – "средние";

PL_L – "малые";

PL_VL – "очень малые" убытки в соответствующих денежных единицах.

Определение величины возможных убытков может проводиться относительно бюджета корпоративной системы с учетом стоимости информационных активов, стоимости репутации предприятия, и тому подобное.

IV. Результат анализа информационных рисков корпоративной системы сводится к оценке общего уровня информационного риска в КИС по приведенной ниже шкале:

C – "критический";

H – "высокий";

M – "средний";

L – "низкий" уровень информационных рисков.

Пример базы знаний, которая может быть использована для оценивания общего уровня информационного риска, приводится в табл. 3.3.

Таблица 3.3. Оценивание общего уровня

		Уровень информационных рисков				
Величины возможных убытков	PL_VH	H	H	C	C	C
	PL_H	M	H	H	C	C
	PL _Sg	M	M	H	H	C
	PL _M	L	M	M	H	H

	PL_L	L	L	M	M	H
	PL _VL	L	L	L	M	M
		LEF_VL	LEF_L	LEF_M	LEF_H	LEF_VH
		Частота событий потерь				

3.3 Моделирование анализа факторов информационного риска на основе лингвистического подхода

Предлагается применить лингвистический подход к моделированию анализа факторов информационного риска [44]. Такой подход обеспечивает количественные описания отдельных элементов модели при условии нечеткой информации о значении критерия оценки фактора риска, их последствий в условиях действия агента угрозы, альтернативные пути для избегания негативного влияния информационных рисков. В соответствии с лингвистическим подходом, в качестве значений критериев и характеристики отношений между ними допускается не только количественное оценивание, но и предложение на естественном языке. На основании рассчитанных значений групп показателей уровня частоты событий потерь информационных активов и величины возможных убытков в результате информационных рисков проводится оценивание общего уровня информационных рисков в КИС:

$$\Delta = f(\gamma, P), \qquad (3.1)$$

где γ - оценка уровня частоты событий потерь информационных активов;

P – предварительно оцененная величина возможных убытков.

Терм-множество входной переменной *v*, являющейся множеством степеней частоты возникновения возможных потерь, имеет вид:

$$LEF = \{LEF\_VH, LEF\_H, LEF\_M, LEF\_L, LEF\_VL\}, \qquad (3.2)$$

где LEF_VH – "очень высокая" частота;

LEF_H – "высокая частота";

LEF_M – "средняя частота";

LEF_L – "низкая частота";

LEF_VL – "очень низкая".

Терм-множество входной переменной *P*, которая описывает величину потери относительно бюджета КИС, записывается в виде:

$$LD = \{PL\_VH, PL\_H, PL\_Sg, PL\_M, PL\_L, PL\_VL\}, \quad (3.3)$$

где PL_VH – "очень большая";

PL_H – "большая";

PL_Sg – "существенная";

PL_M – "средняя";

PL_L – "малая";

PL_VL – "очень малая".

Для оценивания и проработки лингвистической переменной *B* рекомендовано воспользоваться шкалой из четырех качественных термов:

C - "критический";

H - "высокий";

M - "средний";

L - "низкий" уровень риска.

Терм-множество исходной переменной *B* представляется в виде:

$$IR = \{C, H, M, L\}. \quad (3.4)$$

Следующим этапом анализа является формирование системы нечетких знаний для определения каждого из уровней информационных рисков.

Используя [40, 42], сформирован набор решающих правил, которые реализуют соотношение (1). В табл. 3.4 приведен такой набор.

Таблица 3.4. База знаний для определения уровня информационных рисков

Номер исходящей комбинации	Обобщенные значения групп показателей		Значимость m_{ij}	Выходная переменная Δ
	Уровень частоты возникновения возможных потерь	Величина возможных убытков P		
11	PL_VH	LEF_M	m_{11}	C
12	PL_VH	LEF_H	m_{12}	
13	PL_VH	LEF_VH	m_{13}	
14	PL_H	LEF_H	m_{14}	
15	PL_H	LEF_VH	m_{15}	
16	PL _Sg	LEF_VH	m_{16}	
21	PL_VH	LEF_VL	m_{21}	H
22	PL_VH	LEF_L	m_{22}	
23	PL_H	LEF_L	m_{23}	
24	PL_H	LEF_M	m_{24}	
25	PL _Sg	LEF_M	m_{25}	
26	PL _Sg	LEF_H	m_{26}	
27	PL_M	LEF_H	m_{27}	
28	PL_M	LEF_VH	m_{28}	
29	PL_L	LEF_VH	m_{29}	
31	PL_H	LEF_VL	m_{31}	M
32	PL _Sg	LEF_VL	m_{32}	
33	PL _Sg	LEF_L	m_{33}	
34	PL_M	LEF_L	m_{34}	
35	PL_M	LEF_M	m_{35}	
36	PL_L	LEF_M	m_{36}	
37	PL_L	LEF_H	m_{37}	
38	PL_VL	LEF_H	m_{38}	
39	PL_VL	LEF_VH	m_{39}	
41	PL_M	LEF_VL	m_{41}	L
42	PL_L	LEF_VL	m_{42}	
43	PL_L	LEF_L	m_{43}	
44	PL_VL	LEF_VL	m_{44}	
45	PL_VL	LEF_L	m_{45}	
46	PL_VL	LEF_M	m_{46}	

Следующим шагом является определение математической формы записи решающих правил с помощью функций принадлежности для определения уровней информационных рисков. Например, решающее правило для определения информационных рисков уровня M может быть записано таким образом:

$$\mu^{M}(?, \mathrm{P}) = m_{31}[\mu^{LEF\_VL}(\gamma) * \mu^{PL\_H}(P)] \vee m_{32}[\mu^{LEF\_VL}(\gamma) * \mu^{PL\_Sg}(P)] \vee$$
$$\vee m_{33}[\mu^{LEF\_L}(\gamma) * \mu^{PL\_Sg}(P)] \vee m_{34}[\mu^{LEF\_L}(\gamma) * \mu^{PL\_M}(P)] \vee$$
$$\vee m_{35}[\mu^{LEF\_M}(\gamma) * \mu^{PL\_M}(P)] \vee m_{36}[\mu^{LEF\_M}(\gamma) * \mu^{PL\_L}(P)] \vee$$
$$\vee m_{37}[\mu^{LEF\_H}(\gamma) * \mu^{PL\_L}(P)] \vee m_{38}[\mu^{LEF\_H}(\gamma) * \mu^{PL\_VL}(P)] \vee$$
$$\vee m_{39}[\mu^{LEF\_VH}(\gamma) * \mu^{PL\_VL}(P)] \quad (3.5)$$

где $\mu^{M}(\Upsilon, \mathrm{P})$ – функция принадлежности выходной переменной Λ значению M из нечеткого терма (3.4);

$m_{3k}(k = 1,9)$ – весовой коэффициент для соответствующей k -й комбинации;

$\mu^{lefj}(\Upsilon)$ – функция принадлежности параметра Υ нечеткому терму lef_j из терм-множества LEF (3.2);

$\mu^{ldi}(P)$ – функция принадлежности параметра P к нечеткому терму ld_i из терм-множества LD (3.3).

Таким образом, вся база знаний формируется с использованием экспертных данных и выводится система нечетких логических уравнений.

Результатом представленной концепции и инструментария оценивания уровня частоты событий потерь и величины возможных потерь информационных активов является лингвистическое описание общего уровня информационных рисков в КИС.

Были построены колокол подобные функции принадлежности термов исходной переменной B к множественному числу (4) терма, параметры которых представлены в табл. 3.5:

$$\mu^T(x) = \frac{1}{1+\left|\frac{x-c}{a}\right|^{2b}} \qquad (3.6)$$

где T – произвольный нечеткий терм;

a – коэффициент концентрации;

b – коэффициент крутизны;

c – координата максимума функции, $\mu^T(c) = 1$.

Таблица 3.5. Параметры функций принадлежности термов к терм-множеству IR

Название терма	Функция принадлежности	Параметры		
		Коэффициент максимума c	Коэффициент концентрации a	Коэффициент крутизны b
L	$\mu^1(x)$	0	0,1	2
M	$\mu^2(x)$	0,33	0,1	2
H	$\mu^3(x)$	0,67	0,1	2
C	$\mu^4(x)$	1	0,1	2

Графическое представление функции принадлежности выходной переменной, базы логического вывода представлены на рис. 3.1 и 3.2 соответственно.

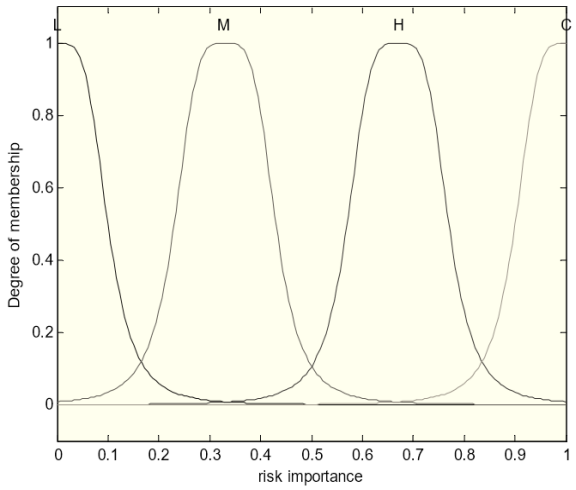

Рис. 3.1. Графики функций принадлежности показателя уровня информационных рисков в КИС

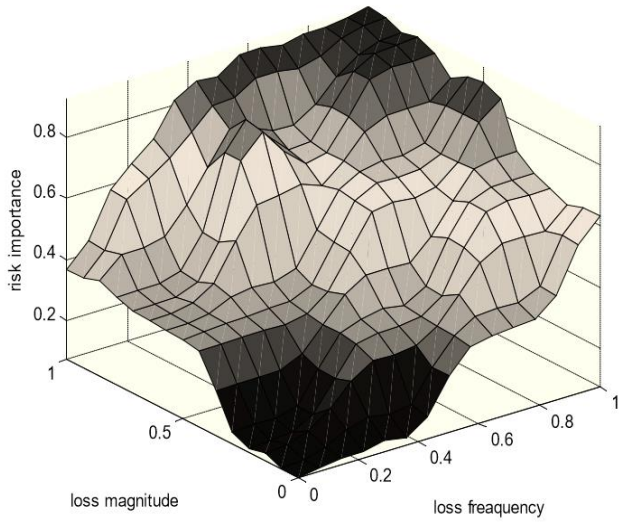

Рис. 3.2. Графическое представление системы нечеткого вывода показателя уровня информационных рисков

Результаты проведенных исследований относительно оценивания уровня информационных рисков в КИС представлены в табл. 3.6.

Таблица 3.6. Оценка уровня информационных рисков

Название предприятия	Величина возможных убытков	Уровень частоты возможных потерь	Уровень информационных рисков
Предприятие 1	PL_M 0,4012	LEF_L 0.3545	M 0,3751
Предприятие 2	PL_Sg 0,5971	LEF_M 0.5799	H 0,6348
Предприятие 3	PL_Sg 0,5991	LEF_M 0.4376	H 0,6252
Предприятие 4	PL_P 0,7749	LEF_L 0.1740	H 0,6109

Как видно из табл. 3.6, на Предприятии 2, Предприятии 3 и Предприятии 4 найденный уровень информационных рисков соответствует оценке "высокий", на Предприятии 1 - "средний".

По результатам оценки факторов информационных рисков было принято решение о методах снижения уровня информационных рисков на предприятиях. Например, на Предприятии 3 необходимо принять дополнительные меры по повышению уровня действенности средств защиты, поскольку высокий уровень уязвимости был вызван именно недостатками работы этих ресурсов и их несоответствия высокому уровню угроз информационной безопасности предприятия.

Можно прийти к выводу, что подобная модель оценки общего уровня риска гибкая и адаптивная и может быть настроена в соответствии с полученной базой знаний.

Выводы по третьей главе

Категория "информационный риск" должна рассматриваться с позиций руководителя предприятия, который желает управлять всеми рисками, связанными с использованием управленческой информации в бизнесе. Предлагается связать риски, связанные с информацией, не только с нарушениями информационной безопасности, но также и с потерей качества бизнес-процессов. Анализ информационных рисков является основой для построения подсистемы управления информационной безопасностью предприятия.

В ходе анализа и оценки уровня информационных рисков следует придерживаться следующих шагов:

- идентификация информационных ресурсов (активов) компании, которые могут быть объектом риска, возможных угроз актива и определения уровня угроз безопасности КИС предприятия;
- оценивания уровня действенности средств контроля безопасности корпоративной системы;

- оценивания уязвимости корпоративной системы, рассматривается как результат влияния факторов возможного уровня силы угрозы и уровня действенности средств контроля;

- оценивания частоты событий потерь от информационных рисков как результата влияния факторов частоты возникновения угрозы и уязвимости корпоративной системы;

- оценивания величины возможных убытков от информационных рисков в КИС;

- оценивания уровня информационных рисков в КИС как результирующей двух факторов: частоты событий потерь и величины возможных потерь от информационных рисков.

Построена модель оценки общего уровня информационных рисков в сегменте КИС с применением лингвистического подхода, обеспечивающего количественные описания отдельных элементов модели в условиях нечеткой информации о значении критериев оценки факторов (факторов) риска. Это дает возможность выделить значимые факторы риска, их последствия в условиях действия агента угрозы, и, тем самым, определить альтернативные пути для избегания негативного влияния риска:

- замена или модификация средств контроля безопасности;

- внедрение механизмов защиты в соответствии с возможным уровнем угроз определенных классов нарушителей информационной безопасности;

- реализация режима функциональной замкнутости, который исключал бы использование аппаратного и программного обеспечения, не имеет соответствующего паспорта безопасности и тому подобное.

Результатом представленной технологии и инструментария оценки уровня информационных рисков в сегменте КИС является лингвистическое описание и возможность анализа и оценки факторов информационных рисков, а именно, уровня частоты событий угроз и уязвимости КИС. Разработанный концептуальный подход позволяет нам создать модель не

только с возможностью адаптации ее к конкретной информационной системе, но и с учетом переоценки риска в дальнейшем. Подобная модель обладает свойствами гибкости и адаптивности, тонкой настройки в соответствии с полученной базы знаний.

Предложенная модель оценки уровня информационных рисков может быть положена в основу развития подсистемы управления информационными рисками как на стадии проектирования КИС предприятия, так и в ходе ее эксплуатации. Модель легко адаптируется для выполнения задач управления информационными рисками на уровне с другими задачами. При этом не требуется кардинально менять организационную структуру корпорации, нужно только реорганизовывать ее, максимально приспосабливая к решению задач управления защитой информации в КИС.

Несмотря на весомость осуществленных наработок, остается ряд нерешенных проблем, а именно:

- развитие математических моделей и соответствующего инструментария для снижения (факторов уязвимости) или повышение (факторов действенности средств защиты) влияния факторов на общий уровень информационных рисков;
- разработка положений по применению механизмов управления отдельными факторами информационных рисков.

ГЛАВА 4 МОДЕЛИРОВАНИЕ РАЦИОНАЛЬНОГО МОДЕЛЬНОГО СОСТАВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

4.1 Построение модели системы защиты информации

Под моделью защиты информации подразумевается описание (представленное в формализованном либо неформализованном виде) используемого в СЗИ комплекса аппаратных и программных средств и мер защиты организационного характера [21]. Модель защиты информации является фундаментом для разработки непосредственно СЗИ.

Корпоративная информационная система – это комплекс аппаратных средств (сервера и серверное оборудование, рабочие станции, каналы связи и др.), каналов связи и программного обеспечения данной системы. Обобщая наработки, сделанные в современных концепциях построения СЗИ [39], можно сделать вывод, что для создания эффективной системы защиты информации важно при разработке придерживаться ряда ключевых принципов, а именно:

- *комплексность*и *согласованность* – построение системы защиты информации предполагает применение достаточно широкий спектр инструментов и методов защиты, при этом важно поддерживать целостность системы и избегать "слабых мест" во взаимодействии отдельных компонентов системы;

- *дифференциация* – каждый уровень защиты должен разрабатываться с учетом уровня важности и критичности информации и вероятности потенциальных угроз (оценки потенциальных атак);

- *достаточность* механизмов защиты – подразумевает оценку соотношения затрат на создание и поддержание системы защиты информации и возможного ущерба.

Проанализировав возможные пути реализации угроз (осуществления несанкционированного доступа к информационной среде) и основываясь на вышеупомянутых принципах организации системы информационной

безопасности, предложена модель СЗИ, разработанная в виде тресторонней схемы:

I граница: *периметр объекта защиты*: набор функциональных подсистем, состав которых входит защита ИС от внешних угроз и разрушительных действий злоумышленников;

II граница: *периметр сегмента сети:* набор функциональных подсистем, обеспечивающих защиту от удаленных и межсегментных атак;

III граница: *внутренний периметр*: набор функциональных подсистем, задачей которых является защита информационной среды отдельных ПК и серверов.

Автор работы [33] отмечает, что в условиях развития средств информационных нападений и применения гибридных атак, для эффективной защиты информационной среды необходимо применение многоуровневой, эшелонированной системы защиты информации.

Схема предлагаемой трехсторонней защиты приведена на рис. 4.1.

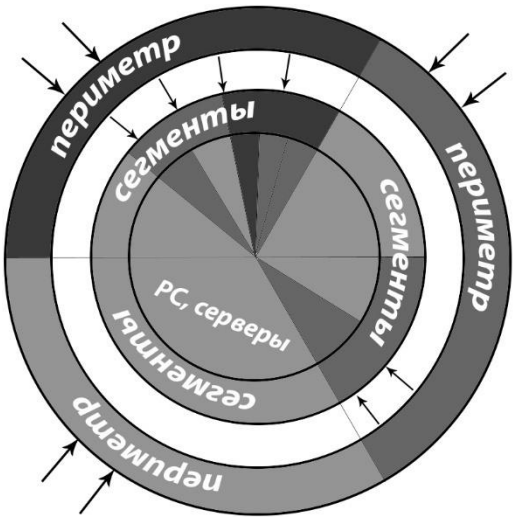

Рисунок 4.1 — Трехрубежная модель СЗИ (стрелки указывают на внешние и внутренние угрозы)

Таким образом, разработанная модель СЗИ будет включать три компонента:

- модель охраны периметра объекта защиты,

- модель безопасности сетевого сегмента,

- модель защиты внутреннего сегмента (ПК и рабочий сервер).

Для каждого из рассмотренных пределов, в зависимости от степени критичности обрабатываемой в нем информации и подлежащей защите, модель будет включать в себя N морфологических матриц (модель уровня N).

Задачей упорядочивания и системной организации информации является уменьшение неопределенности в процессе принятия решений о составе системы защиты информации, основываясь на информации о возможных потенциальных угрозах в данном контуре и данной информационной среде и соответствующих этим угрозам необходимых барьерах.

Таким образом, имея упорядоченную информацию о потенциальных угрозах и доступных средствах реализации защиты, основываясь на определенных процедурах, производится многокритериальное сравнение альтернативных реализаций средств защиты. Результатом такого сравнения является выявление среди имеющегося подмножества наилучшего (наиболее эффективного и соответствующего ограничениям по ресурсам) варианта реализации защиты информационного объекта.

4.2 Разработка моделей противодействия угрозам информационной безопасности в условиях неопределенности

Чтобы проанализировать процесс принятия решений по противодействию угрозам, мы рассмотрим несколько типичных типов информационных атак: межсегментная атака, внешняя атака через точку беспроводного доступа, внешняя атака через периметр через высокоскоростной канал доступа.

4.2.1 Принятие решений в случае потенциально возможной межсегментной атаки

Представьте себе модель противодействия в виде связного графа (рис. 4.2), где U_n – это варианты реагирования, а V_n – варианты исходов при реализации противодействия угрозам. Функция реализации, соответствующая данной матрице, представлена в табл. 4.1.

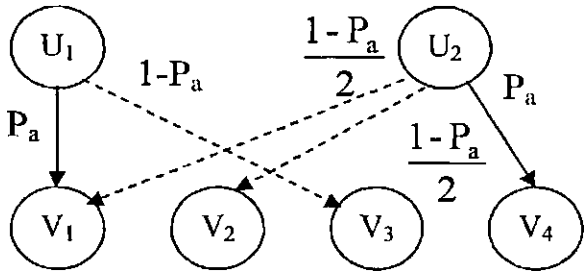

Рисунок 4.2 – Граф связи вариантов реагирования и исходов

Таблица 4.1 – Функция реализации

U	Z					
	$P(z_1)$	$P(z_2)$	$P(z_3)$	$P(z_4)$	$P(z_5)$	$P(z_6)$
U_1	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$
U_2	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$

Следующие варианты ответа показаны в таблице ниже:

U_1– завершает сеанс с атакующим узлом;

U_2 – отправка предупреждения пользователю или уменьшение приоритета пользователя.

Оценка возможных результатов проводится в соответствии с суммой возможных убытков в результате реализации функций защиты:

C (V_1) – нет повреждений;

C (V2) - незначительный ущерб (ущерб пользователю);

C (V_3) – средний урон (урон системе);

C (V_4) – максимальный урон, нанесенный системе в результате

осуществления атаки.

При выборе варианта реагирования U_1 с вероятностью $(1–P_a)$ будет получен средний ущерб, так как в качестве атаки приняты при стандартном режиме работы сети непреднамеренные вредные воздействия от пользователя либо ошибочное распознавание как атаки сигналов с сенсоров.

Реализация варианта реагирования (управляющего воздействия) U_2, может иметь три различных варианта исхода. Если события, распознанные как аномальные, действительно являются атакой, то с вероятностью P_a будет реализован максимальный ущерб при отсутствии блокировки атакующего воздействия. В случае, если распознанное аномальное событие имело причиной ошибочные действия пользователя, то ущерба не будет (он будет равен нулю). Если управляющее воздействие будет реализовано вследствие ошибочного распознавания сигналов как атаки и пользователю будет отправлено предупреждение и понижен его приоритет – будет нанесен незначительный ущерб пользователю. В последних двух вариантах вероятности исходов составят одну и ту же величину $(1-P_a)/2$.

После численных расчетов получаем:

- при P_a=0,238 минимальное значение целевой функции достигается при выборе альтернативы U_2: $J(U_1, z)$=0,381, $J(U_2, z)$=0,276;

- при P_a=0,57 минимальное значение целевой функции достигается при выборе альтернативы U_1: $J(U_1, z) = 0,215$, $J(U_2, z) = 0,5915$.

Для численных расчетов были приняты значения $C(V_1) =0$, $C(V_2) =0,1$, $C(V_3) =0,5$, $C(V_4) =1$.

4.2.2 Принятие решений по реагированию в случае потенциально возможного внешнего вторжения по радиоканалу (Wi-Fi, Wi-MAX соединение)

Для реализации внешнего вторжения в данном варианте атаки, злоумышленнику необходим доступ к беспроводному адаптеру и необходимо, чтобы он находился в радиусе действия беспроводной сети. В

отличии от атаки посредством проводной линии, имеем более высокую степень угрозы и возможность нанесения максимального ущерба.

Объектом, подверженным атаке, в данном случае, является точка доступа. Для обеспечения защиты используются системы WIDS (системы обнаружения беспроводных атак), основой работы которых является сигнатурный анализ и корреляция поведения. События безопасности (выработка управляющего воздействия на информационную систему) генерируются при обнаружении отклонения диагностируемых параметров точки доступа от заданных.

Формируется заранее определенный (эталонный) сетевой профиль, который включает поддерживаемые стандарты, применимые сетевые протоколы, используемую политику трафика и состояние физических и канальных уровней передачи данных, которые постоянно отслеживаются:

- допустимое количество подключений к точке доступа;
- качество сигнала;
- количество передаваемых и принимаемых широковещательных пакетов;
- частота и количество повторных передач пакетов;
- процентное соотношение цельных и фрагментированных фреймов;
- параметры передачи данных (скорость и ее изменения);
- возникновение и частота ошибок контрольной суммы при передаче пакетов;
- используемые для сообщений аутентификации MAC-адреса;
- применяемые при передаче данных технологии аутентификации и шифрования.

Для реализации защиты информации процедуры реагирования должны быть сформированы таким образом, чтобы был максимально снижен возможный ущерб как от реализации вторжения, так и от возможного сбоя взаимодействия через точку доступа.

Модель противодействия в графическом виде представлена на рис. 4.3, а соответствующие данной модели функции реализации – в таблице 4.2.

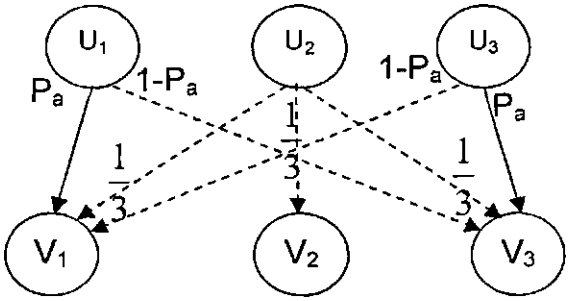

Рисунок 4.3 – Граф связи вариантов реагирования и исходов

Таблица 4.2 – Функция реализации

U	Z											
	$P(z_1)$	$P(z_2)$	$P(z_3)$	$P(z_4)$	$P(z_5)$	$P(z_6)$	$P(z_7)$	$P(z_8)$	$P(z_9)$	$P(z_{10})$	$P(z_{11})$	$P(z_{12})$
U_1	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$
U_2	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_3)$	$C(V_3)$	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_3)$	$C(V_3)$
U_3	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_3)$	$C(V_3)$	$C(V_3)$	$C(V_3)$	$C(V_3)$	$C(V_3)$

Имеем следующие варианты управляющих воздействий (реагирования системы):

U_1– блокирование точки доступа;

U_2 – осуществление DOS-атаки на станцию, реализующую атаку;

U_3 – отсутствие реагирования.

Распределим по величине возможного ущерба вероятные исходы управляющий воздействий:

C(V1) – нулевой ущерб;

$C(V_2)$ – средний ущерб;

$C(V_3)$ – максимальный ущерб.

Если система реализует реакцию (воздействие) U_1, то с вероятностью ущерб P_a ущерба системе не будет (канал полностью перекрыт и действия

злоумышленника пресечены). Вероятность P_a, в данном случае, равна вероятности атаки. Если за реализацию атаки были ошибочно распознаны сигналы сенсоров либо произошла ошибка в действиях пользователя, то ущерб при выборе управляющего воздействия U_1 будет максимальным (блокировка точки доступа произошла безосновательно, произошел сбой в нормальной работе системы). Вероятность $(1–P_a)$ такого исхода соответствует вероятности ошибочной интерпретации сигналов системой либо ошибки пользователя.

Если выбран вариант реагирования U_3, то в случае реализации атаки максимальный ущерб будет получен с вероятностью P_a (вероятность атаки) – атака злоумышленника не отслежена системой. Если данный вариант реагирования выбран в ситуации ошибочного распознавания сигналов сенсоров как атаки, то ущерб будет нулевым – система защиты не вмешивается в работу и продолжается работа в штатном режиме (вероятность составит $(1-P_a)$ для данного исхода).

Если системой выбран вариант реагирования U_2 (осуществление ответной DOS-атаки), то возможны три варианта исхода (нулевой – предотвращены действия злоумышленника, средний – заблокирован пользователь за ошибочные действия, или максимальный – нарушена работоспособность сети, ущерб), вероятности которых равны 1/3.

После выполнения численных расчетов мы находим, что минимальное значение целевой функции достигается путем выбора следующих альтернатив:

при P_a=0,3: альтернатива U_3: $J(U_1,z)$=0,699; $J(U_2,z)$=0,36; $J(U_3,z)$= 0,3;

при P_a=0,4: альтернатива U_2: $J(U_1,z)$ = 0,6; $J(U_2,z)$= 0,3663; $J(U_3,z)$ = 0,399;

при P_a=0,678: альтернатива U_1: $J(U_1, z)$ =0,322; $J(U_2, z)$ = 0,366; $J(U_3, z)$= 0,6774;

Расчеты проводились для числовых значений $C(V_1)$ =0; $C(V_2)$=0,1; $C(V_3)$=1.

4.2.3 Принятие решений по реагированию в случае потенциально возможного внешнего вторжения через периметр по линиям связи

Для этого варианта угроз модель противодействия проиллюстрирована на фиг. 4.4, функции реализации, соответствующие этой модели, приведены в приложении А.

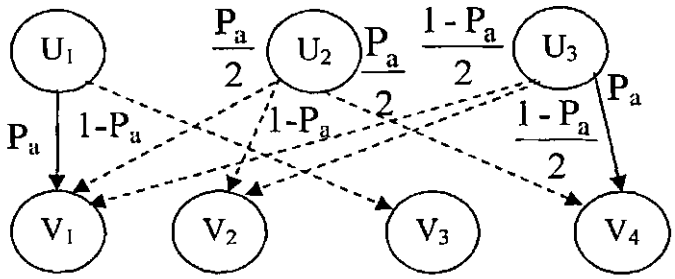

Рисунок 4.4 – Граф подключения вариантов ответа и результатов

Эта опция атаки генерирует следующие варианты ответа (управляющие действия):

U_1 – блокировка доступа пользователей к соответствующей услуге в сети;

U_2 – реконфигурация служб безопасности для блокировки взаимодействия с конкретным IP-адресом;

U_3– отправка оповещения (предупреждения) соответствующему пользователю по его IP-адресу, отправка информации администратору об увеличении активности этого пользователя.

Как и в предыдущих вариантах, ранжируем вероятные результаты по возможному ущербу:

C (V1) – нулевой ущерб;

C (V_2) – незначительный урон (ущерб, нанесенный только удаленному пользователю);

C(V_3) – средний урон (повреждение системы);

C(V_4) –максимальный урон (атака реализована и система повреждена).

Если система выбирает вариант реагирования U_1, то с вероятностью P_a, которая равна вероятности реализации атаки, ущерб информационной системе равен нулю (т.е., отсутствует), так как система защиты пресекла атаку.

Если же осуществлено данное управляющее воздействие (U_1), но произошло ложное срабатывание сенсоров либо была сделана ошибка пользователем, то ущерб будет средним (безосновательно заблокированы системой безопасности пакеты, приходящие по данному протоколу). Вероятность данного исхода составит $(1-P_a)$.

Реализация решения U_2 может привести либо к ущербу для удаленного пользователя (если аномальные события не были вызваны реализацией атаки) с вероятностью $(1-P_a)$, либо (если была реализована атака) возможны два равновероятных $(P_a/2)$ по принципу Бернулли исхода.

Когда контрольное действие U_3 и атака осуществлены, результатом будет максимальный урон (реализованная атака не будет подавлена системой защиты с вероятностью P_a, равной вероятности атаки. В случае ложного срабатывания датчиков или ошибка пользователя, с равной вероятностью $(1-P_a)/2$ конечному пользователю будет причинен незначительный ущерб, иначе не будет никакого ущерба как системе, так и пользователю.

По результатам численных расчетов, можно сказать, что минимальное значение целевой функции достигается при выборе:

- при P_a=0,05: альтернативы U_3: $J(U_1, z) = 0,4948$; $J(U_2, z) = 0,107$; $J(U_3, z) = 0,05948$;

- при P_a=0,238: альтернативы U_2: $J(U_1, z) = 0,380$; $J(U_2, z) = 0,195$; $J(U_3, z) = 0,276$;

- при P_a=0,742: альтернативы U_1: $J(U_1 z) = 0,129$; $J(U_2 z) = 0,3968$; $J(U_3 z) = 0,7549$.

Численные расчеты произведены для следующих численных значений:

$C(V_1) = 0$; $C(V_2) = 0,1$; $C(V_3) = 0,5$; $C(V_4) = 1$.

4.3 Разработка структуры системы интеллектуальной поддержки принятия решений по оперативному управлению защитой информации

Управление заключается в преобразовании информации о состоянии объекта управления в командную информацию [19]. Процесс управления включает в себя большое количество различных функций преобразования информации. Эти функции преобразования взаимосвязаны, реализация одной из функций обычно включает в себя реализацию других функций.

Оперативное управление является одной из ключевых функций в рамках обеспечения защиты информации, реализация которой может обеспечить эффективное функционирование СЗИ.

Оперативное управление обеспечивает стабильное функционирование системы за счёт гибкого реагирования на изменения среды функционирования информационной системы (воздействие внешних и внутренних угроз).

Синтез структуры СЗИ и параметров системы управления для обеспечения защиты определенных массивов информации является одной из ключевых задач теории управления. В зависимости от имеющейся в распоряжении информации об объекте управления, данных о среде, в которой функционирует система, а также о степени неопределенности данной информации, структурная схема системы оперативного управления может различаться. Существующая в системе неопределенность связана с неизвестными действиями потенциальных злоумышленников.

Оперативное управление в условиях информационной неопределенности (недостаточность данных о состоянии объекта или возможных угрозах, влекущая за собой высокую неопределенность при принятии управляющих решений) может быть эффективно организовано при реализации иерархического принципа в структуре управляющей системы.

Важную значимость в системах управления защитой информации приобретают процессы контроля и анализа, так как такая система не

ограничивается регулировочной функцией. Распределение функциональной нагрузки производится следующим образом: процесс регулирования возлагается на управляющие модули, а система поддержки принятия решений реализует такие функции как анализ, контроль, планирование и принятие решений (т.е. все те функции, которые не относятся непосредственно к процессу регулирования управления ЗИ).

Необходимость иерархической структуры построения управляющей оперативной системы обусловлена следующими факторами:

- параметры, которые контролируются управляющей системой могут иметь как количественный, так и качественный характер;

- связь между параметрами информационной системы, контролируемыми управляющей системой и вырабатываемыми управляющими воздействиями слабо формализована;

- имеющаяся информация (поступающая от сенсоров либо других систем) о состоянии контролируемого объекта в связи с изменениями среды в реальном времени может не в полной мере отражать состояние объекта управления.

Все это обуславливает необходимость создания многоуровневой системы управления для уменьшения степени неопределенности при принятии решений и повышения надежности системы.

Чтобы построить иерархическую структуру, выберите следующие элементы управления:

- средства управления (ОбУ) - средство и меры безопасности;

– модули управления (УМ), встроенные в защитное оборудование или сетевое оборудование;

– система поддержки принятия решений по оперативному управлению ЗИ (СППР ОУ),

Введем обозначения информационных потоков, циркулирующих в системе:

$U^{внш}$ – внешние угрозы,

$U'^{внш}$ – информация о состоянии окружающей среды доступна в СППР ОУ,

U – информация о команде на выходе СППР ОУ,

$U_{ум}$ – контрольное действие,

X – информация о состоянии ОУ — контролируемые параметры,

X' – информация о контролируемых параметрах доступна в СППР ОУ.

На рис. 4.4 показана иерархическая структура системы управления.

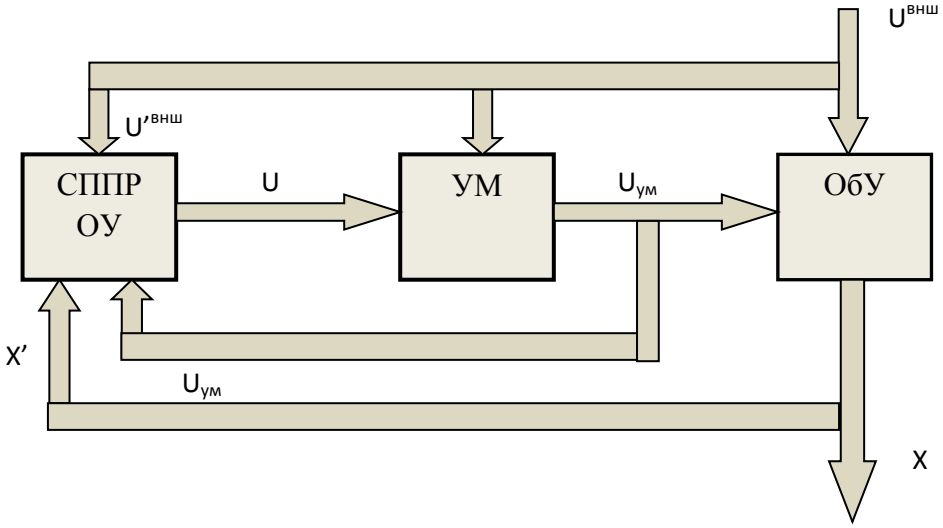

Рисунок 4.4 – Иерархическая структура управляющей системы

Снижение информационной неопределенности является ключевым фактором для повышения качества решений, принимаемых СППР ОУ. Принятие решений в СППР ОУ – это реализация многошагового процесса с помощью управляющих модулей, в процессе которого на основании имеющихся данных о результатах контроля решений выбирается вариант реакции на одно либо набор аномальных событий. Входные данные называются в данном случае переменными выбора (так как оказывают влияние на выбор управляющего решения), а их воздействие можно представить как усиление положительных и ослабление отрицательных реакций в управляющей системе.

В случае наличия задачи, где формализация задач и выработка решения на основе набора данных из набора имеющихся реакций невозможна, требуется использование интеллекта человека. Автоматизированные системы (в отличие от автоматических) рассчитаны на частичное выполнение задач такого класса человеком (примером такой задачи может служить экспертная оценка).

Кроме непосредственного управления, в СУЗИ обеспечивается накопление и анализ информации о процессах управления и результатах реализации различных решений. Таким образом, снижается неопределенность при принятии решений, повышается их эффективность, так как управляющая система накапливает данные, позволяющие точнее предсказать результат применения того или иного управляющего воздействия.

Разработка архитектурного решения СППР ОУ в соответствии с вышесказанным, предполагает использование интеллектуальных информационных технологий, а именно:

- реализация численной оценки вероятности того, что аномальное событие является атакой, выполняется с использованием механизма нечеткого вывода;

- информация и данные о системе, а также данные о событиях безопасности, накапливаемые системой в процессе работы, упорядочиваются в базе знаний управляющей системы;

- система реализует интеллектуальные алгоритмы выбора решений о реализуемом управляющем воздействии при возникновении аномальных событий в системе.

На рис. 4.5 представлено предлагаемое архитектурное построение СППР ОУ.

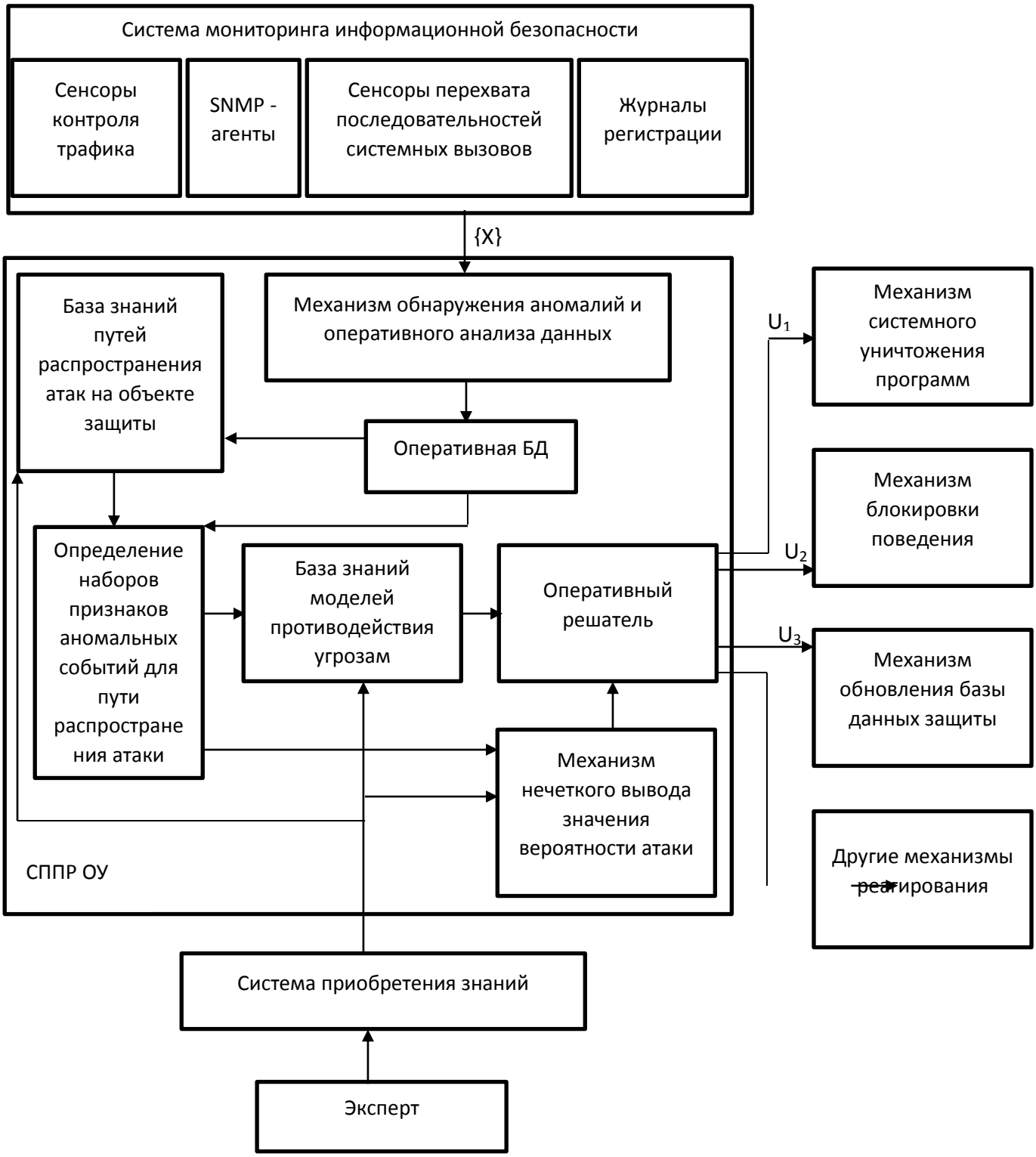
Система мониторинга информационной безопасности
Сенсоры контроля трафика
SNMP - агенты
Сенсоры перехвата последовательностей системных вызовов
Журналы регистрации
{X}
База знаний путей распространения атак на объекте защиты
Механизм обнаружения аномалий и оперативного анализа данных
Оперативная БД
Определение наборов признаков аномальных событий для пути распространения атаки
База знаний моделей противодействия угрозам
Оперативный решатель
Механизм нечеткого вывода значения вероятности атаки
СППР ОУ
U1
U2
U3
Механизм системного уничтожения программ
Механизм блокировки поведения
Механизм обновления базы данных защиты
Другие механизмы реагирования
Система приобретения знаний
Эксперт

Рисунок 4.5 – Структура системы интеллектуальной поддержки принятия решений в контуре оперативного управления ЗИ

Задачей СППР ОУ является выработка оптимального управляющего решения которое должно защитить информационную систему от воздействия внешних атак на объект защиты и, при этом, минимизировать последствия воздействия такого решения на нормальную работу самой информационной системы.

СППР ОУ работает в динамическом режиме, отслеживая и анализирую данные об объекте защиты, поступающие с датчиков, в режиме реального времени. Непрерывное наблюдение и анализ среды функционирования для выявления потенциально опасных событий реализует *система контроля информационной безопасности.*

Необходимость определения максимально возможного количества атак требует использования подсистем обнаружения аномалий, которые работают на разных уровнях КИС в системе управления. Подмножество контролируемых параметров может включать в себя параметры, которые описывают уровень сети, процессы и состояния пользовательских ресурсов, состояние системных ресурсов. Полученные данные, зарегистрированные в соответствующих журналах, подвергаются оперативному анализу.

Для получения данных применяются датчики, расположенные в различных сегментах сети (точки выхода в глобальную сеть, отдельные сегменты локальной сети информационной системы, коммутаторы, маршрутизаторы и др.). Каждый датчик собирает информацию о тех событиях безопасности, которые происходят в соответствующем узле, и передает их для протоколирования в соответствующих журналах. Также информация от датчиков может передаваться не напрямую, а через дополнительные программные компоненты.

Анализируя поступающие сведения от датчиков, *механизм обнаружения аномалий и оперативного анализа* данных определяет, являются ли происходящие события нормой или их можно классифицировать как аномальные, выявляя в последовательности событий отклонения от стандартных наборов действий.

Благодаря этому, система защиты информации может выявлять не только известные, ранее регистрироваться атаки, но те, которые системе не известны, как внешние, так и внутренние (например, нарушение пользователями допусков на доступ к информации).

Однако, следует отметить, что не каждый случай аномальных событий связан с попыткой реализации атаки. Такие события могут быть связаны, например, с ошибками пользователей, ложными срабатывания датчиков и т.д. В результате формирование управляющего воздействия, соответствующего атаке, может вывести систему из штатного режима работы при отсутствии угрозы безопасности (ложная тревога).

Для решения этой проблемы в предлагаемой СППР ОУ управляющие решения принимаются на основании расчета вероятности того, что рассматриваемое событие является атакой. Для проведения расчета этого **«коэффициента уверенности»** применяется механизм нечеткого логического вывода, что связано с невозможностью однозначного и полного описания параметров, позволяющих однозначно отнести аномальные события к классу атак, а также с тем, что не все показатели имеют количественное выражение.

Реализацию данного механизма в предложенной архитектуре СППР ОУ осуществляет модуль «***Механизм нечеткого вывода вероятности атаки».*** Реализованный с помощью такого подхода механизм принятия решений позволяет максимально эффективно использовать опыт и наработки экспертных знаний и преодолеть свойственные информационной среде проблемы неполноты и противоречивости информации о ее состоянии, тем самым сократив неопределенность при принятии решений.

В системе может быть использовано различное количество датчиков, сенсоров, подсистем обнаружения и для определения численного значения **«коэффициента уверенности»** необходимо обобщать данные, полученные от них. Для обобщения данных удобно использовать стандартизованный формат данных.

Анализатор должен передавать модуль вектора, имеющий вид

$$S = (I_0, I_p, T), \qquad (4.1)$$

где I_0 – системный идентификатор обнаружителя,

I_p – идентификатор пути атаки,

T – системное время.

Эффективность применяемого алгоритма при выборе управляющего решения имеет критическое значение для эффективности работы всей системы защиты информации. В предложенном варианте СППР ОУ вариант реагирования формируется в *оперативном решателе*, на основании рассчитанного «коэффициента уверенности», в котором значения вероятностей результатов рассчитываются как функция этого коэффициента.

Эффективным средством организации тематической информации является ее модельное представление. База данных моделей защиты от угроз в табличной форме хранит функции реализации для каждого типа пути распространения атаки, указанного экспертом.

Рассмотрим процессы накопления знаний автоматизированной системой СППРОУ. В данном процессе можно выделить несколько ключевых этапов.

На этапе концептуализации реализуются следующие процессы:

- выбор и формализация наборов переменных, которые описывают (характеризуют) события безопасности, происходящие в системе;

- экспертное задание функций принадлежности, определение характеристик событий безопасности, которые могут быть отнесены к классу атак;

- формирование экспертом правил, задающих реакцию системы в ответ на обнаружение потенциально опасных событий;

- формирование базы данных о возможных источниках и путях распространения атак;

- формирование структуры информационных источников о возможных угрозах и атаках;

- анализ вариантов реагирования, альтернатив действий системы (U_i) и сопоставление этих вариантов с вероятными исходами (V_j) и потенциальным ущербом от данных исходов (C_j).

Все знания задаются в базе знаний в единой формализованной форме представления.

Для реализации описанного выше метода принятия решения модель противодействия угрозам для каждой ситуации в базе знаний моделей может быть задана в табличной форме функцией реализации, причем каждый вариант ответа соответствует результату и его оценка зависит от состояния среды z_j.

Инженер по знаниям генерирует описание решения проблемы на формальном языке для операционного решателя. В рабочем решении вероятности $p(z_j)$, и функция J(U, z) рассчитываются для каждой альтернативы на основе функции реализации, определенной для ситуации из базы модели. Далее выбирается лучший вариант ответа U*, чтобы обеспечить минимальное повреждение системы.

Информация в базе знаний должна дополняться и актуализироваться по мере обновления и дополнения данных о текущем состоянии информационной системы и среды ее работы.

В модуле *«Определение наборов аномальных событий для пути распространения атаки»* генерируются блоки знаний, обобщается информация, поставляемая датчиками и сигнальными системами о реализуемых атаках и далее эта информация используется для актуализации базы знаний и дальнейшего применения при вычислении «коэффициента уверенности» и выбора функции реализации реакции системы из имеющейся в наличии базы знаний моделей противодействия угрозам. В ходе такой актуализации все сигналы, поступающие от анализаторов привязываются к единой временной оси и формируется путь распространения атаки. Таким

образом, каждая последовательность событий безопасности, которые могут быть квалифицированы как атака, имеет последовательность сообщений от сигнализаторов, упорядоченную по времени. Соответственно, каждый путь распространения атак обрабатывается индивидуально и выработка управляющего воздействия производится в зависимости от этого пути.

Точная и детальная настройка механизма нечеткой логики и формирование адекватной базы знаний является критично важным, так как с ростом вероятности обнаружения потенциальной атаки, растет и вероятность возникновения ложной тревоги, в случае, если механизм принятия решений при высокой чувствительности анализаторов не адекватно оценивает значимость событий безопасности.

Среди возможных вариантов реагирования (управляющих воздействий) системы безопасности могут быть запрограммированы как некритичные действия (такие как временное блокирование пользователя либо процесса, снижение его приоритета и др.), так и более серьезные воздействия (полное блокирование потенциально опасных процессов, портов, прерывание процессов, уничтожение программной системы).

Использование этой модели управления информационной безопасностью позволяет контролировать трафик и необходимые узлы, а также своевременно реагировать на изменения в операционной среде наиболее эффективным образом.

Выводы по четвертой главе

Математическая модель ИС, построенная на основе теоретического подхода к наборам, представляет собой информационную систему в виде набора элементов, распределенных по трем уровням конфиденциальности и взаимосвязанных определенными отношениями. Такой подход позволяет определить множество источников угроз для элементов каждого сегмента и пути возможных атак. Для каждого сегмента получены оценки числа путей распространения атак в количественном выражении. Чтобы принимать

обоснованные решения по управлению операциями, можно внедрить систему функциональных показателей, соответствующих реализации атаки на каждом пути.

Вводится понятие «коэффициента уверенности», который позволяет идентифицировать событие как атаку или вероятность атаки, на основе механизма нечеткого логического вывода. Используя опыт квалифицированных экспертов, обобщенный в виде базы правил и сформулированный на основе лингвистических переменных, соответствующих ненормальным событиям, мы имеем возможность количественно оценить вероятность атаки.

В предлагаемом методе принятия решений рациональным вариантом принятия заключается в том, что вероятность результата не устанавливается на основе статистических данных, а рассчитывается в соответствии с вероятностью атаки с использованием механизм нечеткого вывода, что повышает степень достоверности решения о наличии факта атаки, а также снижает риск принятия нерациональных решений.

Разработанная структура системы поддержки принятия решений для оперативного управления включает модули, основанные на интеллектуальных технологиях, эффективно решающие слабо формализованные задачи выбора рационального реагирования на события безопасности.

ЗАКЛЮЧЕНИЕ

В магистерской работе рассмотрены методологические основы управления информационной безопасностью в сегменте КИС с использованием принципов системного анализа и общих прав на создание систем управления, что является новым в построении архитектуры системы управления информационной безопасностью с использованием интеллектуальных технологий.

Модель противодействия угрозам, представленная в работе, базируется на оценке вероятности атаки, реализованной с использованием механизма нечеткой логики, который выбирает рациональное решение на основе оперативных данных о событиях безопасности из различных источников информации. Эта модель позволяет минимизировать ущерб от возможного осуществления атак на информационную систему и реагирования самой системы защиты информации.

На основе трехрубежной модели защиты информации проведены расчеты, позволяющие получить в количественном выражении оценку числа путей распространения атак к узлам в сегментах. Введен показатель «коэффициент уверенности», позволяющий отнести совокупность аномальных событий информационной системы к атаке с использованием механизма нечеткого логического вывода.

Иерархическая структура системы интеллектуальной поддержки принятия решений для оперативного управления информационной безопасностью, а также структура системы интеллектуальной поддержки принятия решений в оперативном управлении защитой информации. Предложенная структура решений, принимаемых системой, о выборе рационального варианта реагирования на события безопасности за счет применения интеллектуальных технологий для решения слабо формализованных задач классификации событий безопасности в системе и выбора путей реагирования на них.

Таким образом, поставленные перед магистерской работой задачи полностью выполнены.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 5.02.2010. №58 Москва «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»

2. ISO/IEC 27001 – «Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью».

3. ISO/IEC 27002 – «Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью»

4. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – М.: Издательство стандартов, 2002.

5. ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении»

6. Астахова Л.В., Цимбол В.И. Применение самообучающихся систем корреляции событий информационной безопасности на основе нечеткой логики при автоматизации систем менеджмента информационной безопасности // Вестник Южно-уральского государственного университета. Компьютерные технологии, управление, радиоэлектроника, 2016.

7. Баженов Р.И. Информационная безопасность и защита информации. Практикум / Биробмиджан, 2011. – 278 с.

8. Бикмаева Е.В., Баженов Р.И. Об оптимальном выборе системы защиты информации от несанкционированного доступа // Apriori/ Серия: Естественные и технические науки, 2014. – №6. – С. 5.

9. Бородакий Ю. В. Интеллектуальные системы обеспечения информационной безопасности: материалы конф. // Известия ТРТУ. Тематический выпуск. - Таганрог: ТРТУ, 2005. – № 4. – С. 65- 69.

10. Галицкий А. В. Защита информации в сети: анализ технологий и синтез решений / А. В. Галицкий, С. Д. Рябко, В. Ф. Шаньгин. – М.: ДМК Пресс, 2004. – 616 с.

11. Гаскаров Д. В. Интеллектуальные информационные системы: учебник для вузов. – М.: Высш. шк., 2003. – 431 с.

12. Груздева Л.М., Абрамов К.Г., Монахов Ю.М. Экспериментальное исследование корпоративной сети передачи данных с адаптивной системой защиты информации // Известия высших учебных заведений. Приборостроение, 2012.

13. Добрушский С. UEBA, или поведенческая аналитика. Базовая функция всех систем безопасности будущего // Информационная безопасность, 2017. – №4. Электронный доступ: http://www.itsec.ru/articles2/Inf_security/ueba--ili-povedencheskaya-analitika-bazovaya-funktsiya-vseh-sistem-bezopasnosti-buduschego/ (дата обращения 22.12.2017)

14. Дудоров Е.Н. Возможные варианты построения интеллектуальной системы обнаружения несанкционированной работы программного обеспечения. // Математические структуры и моделирование 2005, вып. 15, с. 116-124

15. Застрожнов И. И., Рогозин Е. А., Багаев М. А. Методологические основы безопасности использования информационных технологий в системах электронного документооборота: монография. – Воронеж: Научная книга, 2011. – 252 с.

16. Мельник Г. Модель оцінюваннярівняінформаційнихризиків в корпоративних системах // ВісникКиївськогонаціональногоуніверситетуім. Т.Г. Шевченко, 2015. –№ 6(171). – С. 54-60

17. Кирилов В.А., Касимова А.Р., Алёхин А.Д. Система сбора и корреляции событий (SIEM) как ядро системы информационной безопасности // Вестник Казанского технологического университета, 2016.

18. Липаев В. В. Функциональная безопасность программных средств / В. В. Липаев. – М.: СИНТЕГ, 2004. – 348 с.

19. Машкина К. В., Васильев В. И. Подход к разработке интеллектуальной системы защиты информации // Информационные технологии, 2007. –№ 6 . – С . 2-6.

20. Машкина И. В., Гузаиров М. Б.Интеллектуальная поддержка принятия решений по управлению защитой информации в критически важных сегментах информационных систем // Информационные технологии, 2009. – №7. – 32 с.

21. Машкина И. В., Рахимов, Е. А. Система поддержки принятия решений по управлению защитой информации // Безопасность информационных технологий, 2006. – №2. – С. 62-67.

22. Молдолвян Н. А., Молдовян А. А. Введение в криптосистемы с открытым ключом. – СПб.: БХВ–Петербург, 2005. – 288 с.

23. Мур М. Управление информационными рисками // Финансовый директор, 2003. – С.64–69.

24. Нестеренко В. А.Статистические методы обнаружения нарушений безопасности в сети //Информационные процессы, 2006. – т. 6. –Вып. 3. – С. 208-217.

25. Сапрыкина А. Обзор мирового и российского рынка SIEM-систем 2017. Электронный доступ: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem (дата обращения 22.12.2017)

26. Система защиты информации от несанкционированного доступа «DallasLock7.0». Описание применения Электронный доступ: http://www.confident.ru/isc/assets/files/secured_area/ dl70_doc.zip.

27. Система защиты информации от несанкционированного доступа «Блокхост-сеть». Руководство администратора. Электронный доступ: http://www.gaz-is.ru/products/windows/winbhnet.php? down=bhnet_adm.rar.

28. Система защиты информации от несанкционированного доступа «Страж NT». Описание применения. Электронный доступ: http:www.guardnt.ru/download/dor/App-Guide_NT_2_5.pdf

29. Система обнаружения вторжений «ФОРПОСТ 1.1». Электронный доступ: http://www.rnt.ru/to_content/action_desc/ id_46/lang_ru/

30. Система сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.OOOI.OIBHOO. Государственный Реестр сертифицированных средств защиты информации. Электронный доступ: http://www.fstec.ru/_doc/reestr_sszi/ _reestr_sszi.xls

31. Сканер защищённостиSecPointPenetrator. Электронный доступ: http://ftp.technoserv.ru/off-line/it/products/secur/secpoint/ secpoint.pdf

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

33. Основные научно-теоретические проблемы разработки систем защиты информации. / Актуальные проблемы подготовки инженерных кадров. Материалы региональной конференции. URL:https://pandia.org/text/78/534/90615-7.php(дата обращения: 12.11.2019)

34. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах. – М.: ДМК Пресс, 2002.

35. Средства адаптивного управления безопасностью. Электронный доступ: http://www.rnt.ru/price/

36. СТО БР ИББС – 1.0– 2006. – Электронный доступ: http://www.abiss.ru

37. Стенг Д. И. Секреты безопасности сетей. – К.: Диалектика, 1996. – 544 с.

38. Тюрнев Д. Грамотное обслуживание технических средств безопасности. Практические рекомендации // Системы безопасности, 2016. – №6.

39. Шабуров А.С., Борисов В.И. Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-системы // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления, 2016.

40. Шишкин В. М. К проблеме экспертизы безопасности сложных информационных систем: материалы конф. / VII Международ, научно-практич. конф. «Информационная безопасность». – Таганрог: ТРТУ, 2005. – С. 15-18

41. Шумский А. А. Системный анализ в защите информации: учеб. пособие / А. А. Шумский, А. А. Шелупанов. – М.: Гелиос АРВ, 2005. – 224 с.

42. Цыбулин А. М., Шипилева А. В. Математическая модель злоумышленника в корпоративной сети. Управление большими системами. Выпуск 19. – М.: ИГТУ РАН, 2007. – С. 127-133.

43. Черемных С. В. Моделирование и анализ систем: IDEF–технологии: практикум / С. В. Черемных, И.О. Семенов, В. С. Ручкин. – М.: Финансы и статистика. 2006. – 192 с.

44. Матвійчук А. В. Моделюванняекономічнихпроцесівіззастосуваннямметодівнечіткоїлогіки / А. В. Матвійчук. – К.: КНЕУ, 2007. – 264 с.

45. Ежегодный отчет Cisco по кибербезопасности за 2018 г.: топ-менеджеры в сфере безопасности делают ставку на автоматизацию, машинное самообучение и искусственный интеллект. [Электронный ресурс]: Официальный сайт компании Cisco: URL:https://www.cisco.com/c/ru_ru/about/press/press-releases/2018/03-12.html (дата обращения: 19.11.2019)

46. Miller, D.R. Security Information and Event Management (SIEM) implementation / D.R. Information Technology. Information Security. Information Assurancy. Электронныйдоступ: http://www.isaca.org.

47. Jones J. A. An Introduction to FAIR / J. A. Jones – Trustees of Norwich University, 2005. – 67 p.

48. Zadeh L. A. Fuzzy sets / L. A. Zadeh. – Information and Control, 1965. – №8.– P. 338–353.

49. Zadeh L. A. On optimal control and linear programming / L. A. Zadeh, B. H. Whalen. – IRE Trans. Automaticcontrol, Ac-7, 1962. – P. 45-46.

50. Zimmermann H.-J. Fuzzy Sets, Decision Making and Expert Systems / H.-J. Zimmermann. – Kluwer:Dordrecht, 1987. – 335 p.

ПРИЛОЖЕНИЕ А

Функция реализации

Таблица 4.3 – Функция реализации

U	Z																	
	$P(z_1)$	$P(z_{13})$	$P(z_{14})$	$P(z_{15})$	$P(z_{16})$	$P(z_{17})$	$P(z_{18})$	$P(z_8)$	$P(z_9)$	$P(z_{10})$	$P(z_{11})$	$P(z_{12})$	$P(z_{13})$	$P(z_{14})$	$P(z_{15})$	$P(z_{16})$	$P(z_{17})$	$P(z_{18})$
U_1	$C(V_1)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$	$C(V_1)$	$C(V_3)$
U_2	$C(V_1)$	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$	$C(V_1)$	$C(V_1)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$
U_3	$C(V_1)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_2)$	$C(V_2)$	$C(V_2)$	$C(V_2)$	$C(V_2)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$	$C(V_4)$