

Федеральное государственное казенное военное образовательное учреждение
высшего образования «Военная академия воздушно-космической обороны
имени Г.К. Жукова» (г. Тверь)



На правах рукописи

ЗМЕЕВ Анатолий Анатольевич

**МОДЕЛИ И МЕТОД РАЗГРАНИЧЕНИЯ ДОСТУПА В
ОБРАЗОВАТЕЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ НА
ОСНОВЕ ВИРТУАЛЬНЫХ МАШИН**

Специальность 2.3.6 — «Методы и системы защиты информации,
информационная безопасность»

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук, доцент
Лавлинский Валерий Викторович

Тверь — 2022

Содержание

ВВЕДЕНИЕ	4
1 Анализ систем разграничения доступа в информационных системах.....	21
1.1 Анализ уязвимостей образовательных информационных систем.....	24
1.2 Анализ существующих методов и моделей нарушителя для образовательных информационных систем	34
1.3 Анализ подходов для формирования профилей разграничения доступа в образовательных информационных системах	64
1.4 Выводы.....	73
2 Разработка формальной модели нарушителя для ранжирования слушателей на основе преобразования качественных показателей тестирования в количественные оценки их компетенций	76
2.1 Разработка нечёткой модели определения значимости команд при реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН80	
2.2 Формальная модель нарушителя в образовательных информационных системах с информацией специального назначения	92
2.3 Разработка нечёткой модели оценивания возможности по реализации угроз НСД в ОИСИСН к гипервизору через виртуальные машины на основе модифицированного подхода по формированию функций принадлежности, описывающих количественно уровни компетенций слушателей.....	96
2.4 Выводы.....	101
3 Разработка нейронечёткой модели оценивания динамики состояния ОИСИСН в условиях угроз безопасности информации к гипервизору через виртуальные машины и средства оценки её устойчивости к НСД.....	104
3.1 Математическая основа нейронечёткой модели оценивания динамики состояния ОИСИСН в условиях угроз НСД к гипервизору через виртуальные машины.....	104

3.2 Разработка средства оценки устойчивости состояний ОИСИСН в условиях угроз НСД на каждом этапе по методу бифуркаций и методу Ляпунова для автоматизации процесса создания профилей по разграничению профилей на основе технологии «тонкий клиент».....	114
3.3 Выводы.....	118
4 Алгоритм для реализации метода разграничения доступа на основе виртуальных машин при использовании образовательных информационных систем с информацией специального назначения и результаты экспериментальных исследований.....	119
4.1 Алгоритм для реализации метода разграничения доступа на основе виртуальных машин при использовании образовательных информационных системах с информацией специального назначения	119
4.2 Результаты экспериментальных исследований по оценке критерия устойчивости к НСД в ОИСИСН	125
4.3 Результаты экспериментальных исследований модели и средства оценки устойчивости для создания профилей разграничения доступа, построенной с применением технологии «тонкий клиент»	128
4.4 Выводы.....	132
ЗАКЛЮЧЕНИЕ	134
ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ ..	138
СПИСОК ЛИТЕРАТУРЫ	140
Приложение А. Публикации соискателя по теме диссертации	167
Приложение Б. Реализация алгоритма метода разграничения доступа....	177
Приложение В. Акты внедрения	186
Приложение Г. Свидетельства на программное обеспечение	191

ВВЕДЕНИЕ

Актуальность темы диссертации. В настоящее время в различных вузах страны широко применяются образовательные информационные системы (ОИС), предназначенные для обеспечения процесса обучения. Наличие большого контингента слушателей, как из России, так из многих других государств в силовых вузах страны требует своевременной настройки профилей системы разграничения доступа к информации. Так, например, в Федеральном государственном казённом образовательном учреждении высшего образования «Военной академии воздушно-космической обороны имени Г.К. Жукова» (г. Тверь) проходят обучение представители 39 стран ближнего и дальнего зарубежья. Исходя из того, что восприятие информации является субъективным фактором для каждого слушателя, значение этого фактора усиливается в зависимости от специфики самой информации для иностранных слушателей из разных стран. Ввиду этого, под информацией специального назначения (ИСН) понимается информация, определяемая спецификой преподаваемых дисциплин с учётом особенностей для слушателей различной государственной принадлежности. В связи с этим для образовательных информационных систем такого рода имеются свои специфические особенности: необходимость в смене ресурсов, предоставляемых обучаемым в кратчайшие сроки (как правило, определяется интервалами (переменами) между занятиями), и частая смена обучаемого контингента (например, 2–3 месяца, определяемая курсом дисциплин для повышения квалификации или переподготовки слушателей). Поэтому под ресурсами целесообразно понимать техническое и программное обеспечение образовательных информационных систем для проведения занятий по преподаваемым дисциплинам и сами слушатели различной государственной принадлежности, которые имеют возможность осуществления несанкционированного доступа (НСД) к информации другой государственной принадлежности. Исходя из этого, возрастает роль системы разграничения доступа (СРД). Ввиду этого существующие СРД в образовательных

информационных системах должны решать следующие противоречия: с одной стороны, предоставлять обучаемым ресурсы, а с другой стороны, своевременно разграничить доступ к информации.

Это обуславливает необходимость практически ежедневной перенастройки системы разграничения доступа (РД) в образовательных информационных системах к документам, данным, учебному материалу. Такое разграничение традиционными способами, основанными на ведении учетных записей и установлении полномочий средствами операционных систем (ОС), в рамках одной образовательной информационной системы на практике оказывается крайне сложным и долговременным.

Таким образом, имеет место противоречие между практической необходимостью своевременной перенастройки системы РД слушателей к обучающей информации с учётом быстро меняющегося контингента, имеющего разные уровни компетенции и различное программное и аппаратное обеспечение для обучения, и отсутствием формальных, в том числе дискретных и непрерывных динамических моделей в рамках виртуального «тонкого клиента» для обоснования правил разграничения доступа (ПРД). Такая реализация правил позволила бы повысить устойчивость информации к НСД в образовательных информационных системах и существенно ускорить настройку виртуальных машин в зависимости от возможностей или компетенций слушателей.

В связи с изложенным данная тема диссертационного исследования направлена на разработку моделей и метода разграничения доступа в образовательных информационных системах на основе виртуальных машин и является актуальной и востребованной практикой.

Степень разработанности темы. Интерес, связанный с анализом процессов разграничения доступа, широко изучается во всём мире (Zhi Wang, Huxian Jiang, Weidong Cui, Peng Ning). Созданы многочисленные формальные модели дискреционного, мандатного и ролевого разграничения доступа

(Харрисона-Руззо-Ульмана, Белла ЛаПадулла, Дороти Деннинг, П.Н. Девянина и др.). Вместе с тем в этих моделях отсутствует привязка правил разграничения доступа к возможностям потенциальных нарушителей.

Применительно к иным системам, не относящимся к рассматриваемым в данной работе образовательным информационным системам, проводились исследования, направленные на анализ и выявление актуальных угроз безопасности информации (Суховерхов А.С., Язов Ю.К., Рубцова И.О, Громов Ю.Ю.), в том числе с использованием теории риска (Остапенко А.Г., Карпеев Д.О., Плотников Д.Г. и др.), методов формализации НСД в ИС с использованием средств виртуализации (Сердечный А.Л.). Хотя авторы детально рассматривали различные подходы к оценке безопасности информации в ИС. Тем не менее ими не исследовались вопросы разграничения доступа пользователей к информации в образовательных информационных системах, предназначенных для процесса обучения слушателей, относящихся к различным силовым структурам (МО РФ, МЧС РФ, МВД РФ), где имеются частые изменения контингента и их компетенций по владению программным и техническим обеспечением, а также имеется ограничение на время, предоставляемое для осуществления настроек по технологии виртуальных машин.

Одним из способов решения такого рода задач является применение настроек тонкого клиента с использованием виртуальных машин. Таким исследованиям посвящены работы Радько Н.М., направленные на аналитическое моделирование доступа к операционным средам, адаптацию процессов моделирования НСД к гипервизору через виртуальные машины, работы Тулиганова Л.Р., Павлова И.А., Никольского А.В., посвященные разработке моделей угроз нарушения безопасности в информационных системах, базирующихся на технологии виртуализации, а также работы Евсеева В.Л., Данилкина В.А., Рогачева С.В., Трибунского А.И., в которых рассматривались вопросы защиты информации от НСД на базе программного

гипервизора. Тем не менее, подходы и даже изобретения, предложенные данными авторами, не могут быть использованы для образовательных информационных систем в связи со спецификой процесса обучения в силовых вузах страны. Это обусловлено тем, что в процессе обучения слушателям и пользователям образовательных информационных систем необходимо изучать те или иные программные (аппаратные) средства, которые при определенной подготовке (знаниях) дают им возможность реализовать НСД к гипервизору через виртуальные машины. Ввиду этого для осуществления конфигурирования ОИС на основе тонкого клиента **есть необходимость в оценке (ранжировании) уровня подготовки самих слушателей для осуществления НСД к гипервизору через виртуальные машины. Для этого необходима описательная и формальная модели нарушителя, определяющие степень его подготовленности к осуществлению НСД известными способами для реализации угроз безопасности информации путем эксплуатации уязвимостей, связанных с виртуальными машинами.**

Следует отметить, что описательные модели нарушителей ранее разрабатывались в ряде методических документов таких, как, например, восьмиуровневая модель нарушителя в ИС персональных данных, трехуровневая модель нарушителя для государственных ИС, не содержащих сведения, составляющие государственную тайну, в соответствии с нормативно-правовым актом, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. №17. Однако применение приведенных в этих моделях классификации и описания возможных нарушителей приводит к тому, что все слушатели будут составлять только один класс нарушителей без какого-либо различия, что не позволяет использовать указанные модели для рассматриваемых образовательных информационных систем.

Вместе с тем, владея навыками реализации уязвимостей для проникновения через виртуальные машины к гипервизору, нарушитель имеет возможность повысить привилегии или вызвать отказ в обслуживании,

выполнить произвольный код, записать данные на диск, предназначенный только для чтения, получить доступ к защищаемой информации о содержимом регистра и к памяти гипервизора, осуществлять атаки межсайтового выполнения сценариев и атаки на промежуточные прокси-серверы и т.д. Поэтому имеется необходимость в разработке **нечёткой модели для оценки возможностей реализации угроз за счет эксплуатации уязвимостей процессов разграничения доступа к информации в образовательных информационных системах, использующих технологии виртуализации и «тонкого клиента», и оценки устойчивости к НСД к гипервизору через виртуальные машины с учётом динамики смены контингента и компетенций субъектов по использованию программного и технического обеспечений. В настоящее время такие модели отсутствуют.**

Подобными исследованиями, реализующими оценки качественных параметров процесса РД на основе использования аппарата нейронных сетей с итерационной настройкой многослойной нейронной сети на основе метода наименьших квадратов, занимались Суханов Д.Я., Суханов А.Я. Синтезу нейронных сетей, в том числе в интересах РД к информации, посвящены работы Воеводы А.А., Романникова Д.О., а вопросам многокритериальной оценки альтернатив принятия решений о разграничении доступа в условиях недостаточности информации – работы Марданова М.Д., Рзаева Р.Р. и т.д. Однако указанными авторами даже не ставились задачи анализа пользователей (слушателей) и учета их возможностей по реализации угроз НСД через виртуальные машины, создаваемые на основе настроек тонкого клиента. Кроме того, **отсутствуют работы по оценке устойчивости к НСД в образовательных информационных системах.**

На основе анализа результатов научных работ по моделям процессов разграничения доступа к ИС можно сделать вывод о том, что существующие модели, алгоритмы и методы, полученные с их использованием результаты, не учитывают возможности нарушителя и не могут быть применены для РД в

рассматриваемых образовательных информационных системах в условиях часто меняющегося контингента слушателей и ограниченного времени на настройку правил разграничения доступа в них.

Цель исследования заключается в совершенствовании методов защиты от НСД к гипервизору при технологии виртуализации на базе тонкого клиента за счёт оценки устойчивости и сокращения времени настройки профиля по разграничению доступа в образовательных информационных системах в условиях быстро меняющегося контингента и компетенций субъектов доступа.

В интересах решения сформулированной научной задачи и достижения цели диссертационного исследования решались **следующие задачи диссертационного исследования:**

1. Разработка нечёткой модели определения значимости команд при реализации угроз несанкционированного доступа к гипервизору через виртуальную машину в образовательных информационных системах с использованием модифицированного подхода по формированию границ функций принадлежности для лингвистических значений входа «не важна» (НВ), «слабо важна» (СВ), «важна» (В), «очень важна» (ОВ) и лингвистических значений выхода «невероятный» (нВ), «средневероятный» (сВ) и «высоковероятный» (вВ) и основанную на них формальную модель нарушителя, позволяющую формировать качественные и количественные параметры, выявлять их взаимосвязь для обеспечения ранжирования слушателей по отдельным группам на основе оценённых компетенций для формирования профилей системы разграничения доступа.

2. Разработка нечёткой модели оценивания возможности по реализации угроз несанкционированного доступа к гипервизору через виртуальные машины в образовательных информационных системах, учитывающую результаты экспертной оценки неформализованных ответов слушателей по тесту знаний различных команд для определения критериев осведомлённости и их

ранжирования по трём группам в соответствии с показателем метода центра сумм.

3. Разработка нейронечёткой модели динамики состояния образовательных информационных систем в условиях угроз несанкционированного доступа, учитывающую релевантные параметры формальной модели нарушителя и их взаимодействие для каждого отдельного этапа, а также разработать средство оценки устойчивости к НСД к гипервизору через виртуальные машины, заблаговременно учитывающее возможности вновь поступающего контингента в зависимости от имеющегося при обучении программного и технического обеспечений с учётом профилей настроек разграничения доступа при технологии виртуализации для групп слушателей с целью автоматизации этого процесса.

4. Разработка алгоритма для реализации метода разграничения доступа с использованием виртуальных машин применительно к образовательным информационным системам с целью оценки устойчивости к несанкционированному доступу.

Объектом исследования являются системы разграничения доступа в образовательных информационных системах, использующих информацию специального назначения.

Предметом исследования являются модели, методы и средства для разграничения доступа с использованием виртуальных машин для слушателей (групп слушателей) с учетом частого изменения их контингента и компетенций, состава информации специального назначения и ограничений на время выполнения настроек.

Научная новизна диссертационной работы заключается в следующем. Все результаты, выносимые на защиту, являются новыми:

1. **Определён новый подход для формирования границ функций принадлежности** по обработке экспертных оценок, который позволяет снизить неопределённость исходных данных и определить значимость команд при

реализации угроз несанкционированного доступа к гипервизору через виртуальную машину в образовательных информационных системах на основе разработанной нечёткой модели.

Разработана формальная модель нарушителя, которая учитывает специфику технологии тонкого клиента на основе виртуальных машин и **позволяет** реализовывать качественные и количественные параметры с их взаимосвязями в виде оценённых **компетенций**.

2. Введён критерий **осведомлённости слушателей**, который учитывает результаты экспертной оценки неформализованных ответов, что позволяет осуществлять **ранжирование слушателей по трём группам** на основе разработанной нечёткой модели оценивания возможности для реализации угроз несанкционированного доступа в образовательных информационных системах к гипервизору через виртуальные машины со встроенными в неё правилами нечёткой логики на основе суммирования нечетких чисел с L - R правилом и использованием дефаззификации результирующего показателя методом центра сумм.

3. Определена **система уравнений**, которая **описывает динамику** состояния образовательной информационной системы в условиях угроз несанкционированного доступа к гипервизору через виртуальные машины **для каждого отдельного этапа и взаимодействие между этими этапами** на основе разработанной нейронечёткой модели, что **позволяет** учитывать такие релевантные параметры формальной модели нарушителя, как **количество этапов** для осуществления несанкционированного доступа к информации, **входные параметры и их количество для каждого этапа, значимость параметров на каждом этапе, возможность реализации параметров несанкционированного доступа и задержки выполнения этапа НСД слушателем** и их взаимосвязь.

Кроме того, определена возможность применения **метода бифуркаций и метода Ляпунова** с целью автоматизации процесса оценивания устойчивости к несанкционированному доступу к гипервизору через виртуальные машины.

4. Разработан алгоритм для реализации метода разграничения доступа с использованием виртуальных машин применительно к образовательным информационным системам обучения с информацией специального назначения, который **позволяет** оценивать возможность осуществления несанкционированного доступа на каждом из этапов с учётом определения устойчивости в автоматизированном режиме.

Теоретическая и практическая значимость работы. Разработанные метод, модели и алгоритм определяют новый подход для формирования границ функций принадлежности для лингвистических значений входа «НВ», «СВ», «В», «ОВ» о командах, функциях, утилитах, формируемых из тестовых опросов, введённый критерий осведомлённости слушателей, релевантные параметры формальной модели нарушителя, позволяющие строить нейронечёткие модели динамических систем для оценки устойчивости к НСД к гипервизору через виртуальные машины на основе метода бифуркации и метода Ляпунова.

Результаты, представленные в диссертации, являются научным инструментом для получения оценок устойчивости к НСД к гипервизору через виртуальные машины к ИСН в образовательных информационных системах, используются для построения профилей СРД в условиях частой смены слушателей, их подготовленности, ограничении времени при технологии виртуализации тонкий клиент с использованием программного обеспечения, разработанного в ходе диссертационных исследований (свидетельство о государственной регистрации программы для ЭВМ), что позволяет своевременно реализовывать автоматизированный процесс по созданию профилей разграничения доступа для отдельных групп слушателей.

Методология и методы исследования. Используемые в диссертации методы включают выполненные теоретические и экспериментальные

исследования, которые базируются на основных методах информационной безопасности, математической статистики, экспертных оценок, нечёткой логики и нейронных сетей, методов устойчивости, а также системного подхода и системного программирования.

Положения, выносимые на защиту, являются

1. Нечёткая модель определения значимости команд при реализации угроз несанкционированного доступа к гипервизору через виртуальные машины в образовательных информационных системах на основе модифицированного подхода по формированию границ функций принадлежности и основанную на них формальную модель нарушителя.

2. Нечёткая модель оценивания возможности для реализации угроз несанкционированного доступа в образовательных информационных системах к гипервизору через виртуальные машины для определения критериев осведомлённости и их ранжирования по трём группам в соответствии с показателем метода центра сумм.

3. Нейронечёткая модель оценивания динамики состояния образовательных информационных систем на основе оценки устойчивости к НСД к гипервизору через виртуальные машины с учётом профилей настроек разграничения доступа при технологии «тонкий клиент» для групп слушателей при автоматизации этого процесса.

4. Алгоритм для реализации метода разграничения доступа на основе виртуальных машин при использовании образовательных информационных систем для оценки методом устойчивости при несанкционированном доступе.

Степень достоверности результатов. Научные положения, полученные в диссертации, тесно связаны с проводимыми экспериментами. Теоретические и практические результаты в ходе исследований проверялись на адекватность разработанных моделей с использованием метода хи-квадрата, подтверждались математическими расчетами на основе современных методов научных исследований, многократной обработкой и проверкой собранных в ходе

исследований статистических данных. Полученные результаты подтверждают целесообразность введения критерия осведомлённости слушателей в модели и средстве оценки устойчивости, основываясь на отсутствии срывов занятий с использованием предложенного метода СРД и зафиксированных НСД к информации специального назначения в образовательных информационных системах.

Апробация результатов. Научные результаты, полученные в диссертации, внедрены в научно-исследовательскую работу, образовательный процесс и практику деятельности ФГКВОУ ВПО «Военный учебно-научный центр военно-воздушных сил «Военно-воздушная академия им. проф. Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж), ФГКОУ ВО «Воронежский институт МВД России» (г. Воронеж), ФГКВОУ ВО «Военная академия воздушно-космической обороны им. Г.К. Жукова» (г. Тверь), ОП «НПО РусБИТех-Тверь» (г. Тверь), 344 Центр боевого применения и переучивания лётного состава (авиационного персонала армейской авиации) (ВЧ45095), ФГБОУ ВО «ВГЛТУ им. Г.Ф. Морозова» (г. Воронеж).

Основные положения и результаты диссертации докладывались и обсуждались на следующих конференциях: XVIII Международной научно-технической конференции и Российской научной школы молодых ученых и специалистов «Системные проблемы надёжности, качества, компьютерного моделирования, кибернетических, информационных и телекоммуникационных технологий в инновационных проектах (Инноватика — 2013)» (Москва, 2013); Международной научно-практической конференции «Общественная безопасность, законность и правопорядок в III тысячелетии» (Воронеж, 2013); IV Международной научно-практической конференции «Образование, наука, транспорт в XXI веке: опыт, перспективы, инновации» (Самара, 2014); XI Международной научно-технической конференции «Современные инструментальные системы, информационные технологии и инновации» (Курск, 2014); V Международной научно-практической конференции

преподавателей, научных работников и специалистов «Социально-экономические проблемы инновационного развития» (Белгород, 2014); Международных научно-практических конференциях «Охрана, безопасность, связь — 2013, 2015» (Воронеж, 2013, 2015); Международной военно-научной конференции «Проблемы создания и перспективы развития единой (объединенной) системы противовоздушной и противоракетной обороны организации договора о коллективной безопасности» (Тверь, 2015); II Всероссийской научно-практической конференции с международным участием «Проблемы безопасности при ликвидации последствий чрезвычайных ситуаций» (Воронеж, 2013); IV Всероссийской научно-практической конференции с международным участием «Пожарная безопасность: проблемы и перспективы» (Воронеж, 2013); IX Всероссийской научно-практической конференции «Математические методы и информационно-технические средства» (Краснодар, 2013); Всероссийской конференции «Интеллектуальные информационные системы» (Воронеж, 2015); Всероссийской научно-практической конференции «Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений» (Воронеж, 2017); военно-научных конференциях «Проблемы применения войск (сил) воздушно-космической обороны на современном этапе развития Вооруженных Сил Российской Федерации» (Тверь, 2018).

Работа выполнена в соответствии с научным направлением ФГКВОУ ВПО «Военная академия воздушно-космической обороны им. Г.К. Жукова» (г. Тверь), связанным с разработкой моделей и средств формирования профилей разграничения доступа на основе технологии тонкого клиента в образовательных информационных системах с информацией специального назначения (далее ОИСИСН) в условиях частого изменения обучаемого контингента слушателей с различными уровнями подготовленности.

Публикации по теме диссертации. По результатам исследования опубликовано 58 работ, в том числе 3 монографии, 28 статей, 22 материала научных конференций. Основное содержание диссертации изложено в 27 публикациях, 3 из которых опубликованы в изданиях, соответствующих Перечню рецензируемых журналов ВАК РФ. Имеется 5 свидетельств о государственной регистрации программы для ЭВМ.

Личный вклад, А.А. Змеева в другие публикации сделанные с соавторами характеризуются следующим образом, ему принадлежат: в [124–146] — моделирование НСД; в [148–158] — оценка реализации угроз НСД; в [161–169] — оценка устойчивости к НСД; в [170–177] — модели для оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины и оценки состояния ОИСИСН в условиях угроз НСД, в [160] — средство оценки состояния ОИСИСН в условиях угроз НСД для создания профилей разграничения доступа для отдельных групп слушателей с учётом оценок вновь прибывающего контингента.

Структура и объем диссертации. Диссертация структурно содержит: оглавление, введение, четыре раздела, заключение, список использованной литературы (всего 176 наименований) и четыре приложения. Работа состоит из 195 страниц машинописного текста (основной текст — 166 страниц), 80 рисунков и 9 таблиц, 4 приложения (на 29 страницах).

Основное содержание работы.

Во введении сформулирована актуальность темы, определены цель и задачи исследования, обоснована научная новизна работы и положения, выносимые на защиту, определены теоретическая и практическая значимость работы; сформированы данные по публикациям и структуре работы.

В первой главе выполнен анализ образовательных информационных систем, к которым отнесены ИС, применяемые в казённых военных образовательных учреждениях, как объектов исследований, показаны особенности их построения и функционирования, временные характеристики

перенастройки ОИСИСН в ходе автоматизации обучения различных контингентов слушателей, состава защищаемой информации и применяемого системного и прикладного программного обеспечения (ПО). Также проведен **анализ существующих моделей нарушителя** с точки зрения возможного их применения в ОИСИСН, указаны реализуемые при этом принципы разграничения доступа (дискреционный, мандатный или ролевой) и условия их реализации, дана характеристика способов разграничения, который показал, что непосредственное применение существующих моделей нарушителей оказывается неприемлемым из-за отсутствия градации нарушителей и самой процедуры такой градации.

В данной главе также предложены основные пути решения недостатков, связанных с моделью нарушителя, оценки неформализованных результатов, получаемых от экспертов по командам, и результатов ответов слушателей на тест. Предложено оценивать модели динамических систем отдельных этапов НСД к информации специального назначения в образовательных информационных системах на основе критерия устойчивости. Также была разработана постановка научной задачи исследования, изложенная в данной главе, и намечены пути ее решения.

Вторая глава посвящена разработке нечёткой модели определения значимости команд при реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН. Определено место нечёткой модели значимости команд и формальной модели нарушителя в процессе исследования.

Представлена формальная модель нарушителя. Исходя из предложенных экспертами команд, функций, утилит для их выбора **впервые предложен новый подход для формирования границ функций принадлежности для лингвистических значений входа «НВ», «СВ», «В», «ОВ»**. Изложен процесс нормирования полученных числовых значений, что позволило определить для функций принадлежности граничные значения (как левую, так и правую), изменяемые в диапазоне $[0,1]$. Для каждого лингвистического значения входа

представлены полученные граничные значения «НВ»; «СВ»; «В»; «ОВ». Описан математический подход по снижению неопределённости при выборе команд для формальной модели нарушителя для НСД к гипервизору через виртуальные машины. Описан процесс для определения важности команд в модели на основе метода центра сумм. Описан процесс формирования качественных и количественных параметров с их взаимосвязями для дальнейшего обеспечения ранжирования слушателей по отдельным группам на основе оценённых компетенций для формирования профилей СРД с учётом специфики технологии тонкого клиента на основе виртуальных машин.

Также во второй главе предложена нечёткая модель оценки возможности для реализации угроз НСД в ОИСИСН к гипервизору через виртуальные машины и её место в диссертационных исследованиях. Так как ответы слушателей по тесту знаний различных команд носят неформализованный характер, то описана модель процесса формализации на основе сформированных функций принадлежности и полученных ответов слушателей по 10-балльной шкале, которые в дальнейшем обрабатываются экспертами на основе предложенных правил принятия решений. Также описаны L-R правила нечёткой логики с суммированием нечетких чисел и использованием дефазификации результирующего показателя методом центра, на основе которого определяется уровень осведомлённости слушателя и осуществляется ранжирование по трём группам слушателей. Кроме того, представлены результаты формирования групп слушателей на основе функционирования моделей с использованием критерия осведомлённости.

Третья глава посвящена нейронечёткой модели оценивания динамики состояния образовательных информационных систем с ИСН в условиях угроз НСД к гипервизору через виртуальные машины. Исходя из того, что формальная модель нарушителя содержит нечёткую неполную информацию, то для описания динамики состояния ОИСИСН в условиях угроз НСД к гипервизору через виртуальные машины был предложен математический

аппарат нейронных сетей, который способен смоделировать динамику как отдельного этапа НСД, так и доступ к гипервизору через виртуальную машину в целом. Представлена реализация системы уравнений в виде нечёткой модели в среде MATLAB. Исходя из того, что управление системой разграничения доступа (в условиях динамики состояния ОИСИСН к угрозам НСД к гипервизору через виртуальные машины) учитывает некоторую неопределённость качественных и количественных параметров, то её можно классифицировать как нечёткую систему управления с неизвестными моделями объектов. Ввиду этого для таких систем применены оценки по критерию устойчивости на основе **метода бифуркаций и метода Ляпунова**. Также приведены результаты оценки устойчивости состояний ОИСИСН в условиях угроз НСД на каждом этапе по методу бифуркаций и методу Ляпунова.

На основе полученных результатов для первых трех этапов (0, 1 и 2) доказано наличие бифуркаций, что определяет в этих точках возможность перехода из неустойчивого положения в два устойчивых (метод «вилка») более высокого порядка. После третьего этапа (3, 4, 5 и результирующего за все этапы б) такого не происходит. Следовательно, нечёткая система ведёт себя устойчиво. Кроме того, это подтверждается тем, что предложенную в нейронечёткой модели функцию

$$f = \frac{k \times t}{k \times t + e^{-t}}$$

можно использовать как функцию Ляпунова, так как она удовлетворяет её требованиям.

В четвёртой главе представлен алгоритм для реализации метода разграничения доступа на основе виртуальных машин при использовании образовательных информационных систем. Представлены и обработаны результаты, полученные при реализации алгоритма метода разграничения доступа на основе виртуальных машин при использовании образовательных информационных систем. Адекватность результатов подтверждаются свидетельством о государственной регистрации программы для ЭВМ «Программное средство разработки моделей и метода для анализа рисков

нарушения информационной безопасности в информационных системах специального назначения» с производительностью 0.01с для оценки конкретного набора слушателей с вероятностью 0.23×10^{-2} осуществления НСД за заданный интервал времени $T_{\text{зад}}$.

Кроме того, описан процесс реализации метода по формированию соответствующих профилей разграничения доступа по технологии тонкий клиент на основе виртуальных машин применительно к отдельной группе слушателей с соответствующими навыками работы с используемым ими программным и техническим обеспечением.

Приведены оценки своевременности формирования профилей для разграничения доступа с использованием предложенного метода за весь период проводимых исследований.

В заключении приведены результаты и выводы, полученные при выполнении диссертационного исследования.

1 Анализ систем разграничения доступа в информационных системах

Исходя из условий использования, передачи, обработки, хранения информации, в каждой информационной системе предъявляются свои специфические требования, связанные с разграничением доступа и методов оценки угроз информационной безопасности с точки зрения реализации уязвимостей, присущих тем или иным конфигурациям информационных систем.

Тем не менее, многие информационные системы имеют свою специфику в конфигурировании технических средств и специального программного обеспечения, разграничения доступа к информации и формировании отдельных профилей в разграничении доступа, а также в использовании специфического программного обеспечения и контингента пользователей.

К такому роду информационным системам относятся информационные системы с информацией специального назначения в таких силовых структурах, как Вооруженные силы РФ, МВД РФ, МЧС РФ. Однако эти информационные системы, как правило, обладают жёсткой структурой и ограничениями, связанными с соблюдением требований, обеспечивающих закрытие сведений, составляющих государственную тайну.

Тем не менее, в образовательных информационных системах с информацией специального назначения, к которым относятся информационные системы, применяемые в казённых военных образовательных учреждениях, имеется ряд специфических особенностей их построения и функционирования, связанных с процессом обучения. Также для них имеются дополнительные требования к временным параметрам перенастройки ОИСИСН в ходе автоматизации обучения различных контингентов слушателей, которые сменяются с определённой частотой. Кроме того, имеются отдельные специфические особенности к составу защищаемой информации, а также к необходимости в использовании обучаемыми того или иного системного и прикладного программного обеспечения (СПО и ППО). Это обусловлено тем,

что образовательные информационные системы с информацией специального назначения в военных вузах страны широко применяются для процесса обучения большого контингента слушателей как из России, так из многих других государств. Так, в Федеральном государственном казённом образовательном учреждении высшего образования «Военная академия воздушно-космической обороны имени Г.К. Жукова» (г. Тверь) проходят обучение представители 39 стран ближнего и дальнего зарубежья. При этом слушателям предоставляется информация, содержание которой существенно различается не только для российских и иностранных слушателей, но и для иностранных слушателей из разных стран. Это требует необходимости в разграничении доступа к специфической информации, присущей для обучения различного контингента слушателей.

Это влечёт за собой необходимость в частой перенастройке системы разграничения доступа (РД) в ОИСИСН к файлам в виде документов, данных, учебного материала. Такое разграничение традиционными способами, основанными на ведении учетных записей и установлении полномочий средствами операционных систем (ОС), в рамках одной информационной системы на практике оказывается крайне сложным и долговременным. Это обусловлено, во-первых, тем, что весьма велик контингент слушателей, а состав и содержание курсов обучения для разных групп имеет свои специфические различия. Во-вторых, слушатели из разных стран обучаются в одних и тех же оборудованных классах, в связи с чем требуется весьма объемная работа по изменению матрицы дискреционного разграничения доступа для всего множества субъектов и объектов. В-третьих, такие разграничения должны учитывать осведомленность слушателей, уровень и направленность их подготовки и компетенции, которые не позволили бы им реализовывать угрозы несанкционированного доступа (НСД) к защищаемой информации в ИС. В этом случае для таких ОИСИСН необходимо исследовать процессы формирования профилей по разграничению доступа в условиях временных ограничений,

обосновать наиболее эффективный для этого способ и повысить защищенность информации в ОИСИСН, существенно ускорить настройку профилей по разграничению доступа к информации в зависимости от возможностей слушателей.

В связи с этим необходимо осуществить *анализ уязвимостей ИСО с ИСН, применяемых в казённых военных образовательных учреждениях*, и определить состав угроз безопасности информации, которые могут быть реализованы внутренними нарушителями – пользователями ОИСИСН из состава различных контингентов слушателей.

Кроме того, целесообразно выполнить *анализ существующих моделей нарушителя* с точки зрения возможного их применения в ОИСИСН на основе различных принципов разграничения доступа (дискреционного, мандатного или ролевого) и условий их реализации.

Необходимо разработать *описательную модель нарушителя* для ОИСИСН, содержащую классификацию нарушителей из состава различных контингентов слушателей, характеристику компетенций и возможностей применения ими известных способов НСД к защищаемой информации в ОИСИСН.

В данных диссертационных исследованиях приняты следующие понятия и сокращения.

ИНФОРМАЦИЯ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ (ИСН) – это информация, определяемая спецификой преподаваемых дисциплин с учётом особенностей для слушателей различной государственной принадлежности.

РЕСУРСЫ – это техническое и программное обеспечения образовательных информационных систем с информацией специального назначения (ОИСИСН) для осуществления занятий по преподаваемым дисциплинам.

Исходя из того, что слушатели различной государственной принадлежности пользуются одним и тем же техническим и программным

обеспечением, имеется возможность осуществления несанкционированного доступа (НСД) к информации специального назначения другой государственной принадлежности.

ПРОТИВОРЕЧИЕ. Необходимость в предоставлении ресурсов обучаемым и необходимость в разграничении доступа к информации специального назначения. В этом случае наибольшую значимость для предоставления пользователям ресурсов при обучении с использованием информации специального назначения имеет СРД.

Виду этого к управлению СРД должны быть выдвинуты следующие требования:

- устойчивость (управление должно осуществляться в любых условиях воздействия злоумышленника);
- непрерывность (обеспечение постоянного функционирования взаимосвязи субъектов и объектов СРД в условиях выполнения НСД);
- оперативность (быстрое обеспечивающее упреждение злоумышленника в действиях, осуществление всех мероприятий по управлению СРД при подготовке и в ходе предоставления ресурсов при обучении с использованием информации специального назначения);
- скрытность (сохранение в тайне от злоумышленника всех мероприятий по управлению СРД).

1.1 Анализ уязвимостей образовательных информационных систем

В настоящее время Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспертному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») имеет возможность констатации факта около 300 угроз и 20000 уязвимостей для автоматизированных информационных систем и

информационных систем. На основе этого институт разрабатывает подходы, методы и руководящие документы по решению вопросов, связанных как с оценкой угроз, так и с оценкой опасностей реализации уязвимостей или оценкой степени защищенности.

Исходя из того, что в настоящее время на практике оценка опасностей уязвимостей сводится к общей системе оценке уязвимостей, применительно к информационным системам существует необходимость в её детализации и анализе. Исходя из того, что данная система состоит из трёх групп метрик или критериев: базовых, временных и контекстных [1], необходимо их применить к образовательным информационным системам с информацией специального назначения. В этом случае определяется, во-первых, опасность уязвимостей, взаимосвязанных с доступностью, целостностью и конфиденциальностью информации, то есть с её безопасностью. Во-вторых, определяется уязвимость с точки зрения изменений её характеристик во времени. В-третьих, определяют уязвимости, зависящие от среды функционирования программного обеспечения. Таким образом, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» предлагает осуществлять интегрированную оценку уязвимостей в виде вектора уязвимостей. В этом случае количественная оценка степени опасности уязвимости проводится по результатам анализа базового вектора уязвимости, относящегося к первой группе [1].

ФСТЭК России в этом случае предлагает представлять базовый вектор уязвимости в виде комбинированной информации о базовых метриках, которая является формализованной текстовой записью и численной оценкой X . Исходя из этой предпосылки, данный базовый вектор представляется в виде следующего кортежа:

$$BV = \{AV, AC, AU, C, I, A\},$$

где AV – способ получения доступа нарушителем; AC – сложность получения доступа нарушителем; AU – характеристики потребности нарушителя в аутентификации; C – влияние на конфиденциальность; I – влияние на

целостность; А – влияние на доступность; Х – числовое значение критерия. Как видно в кортеже имеются множества с различными уровнями детализации доступов: способ, свойство (сложность), параметры (характеристики) и процессы (влияние). Кроме того, каждый элемент кортежа имеет три составляющие. А именно: AVL – получение физического доступа к объекту; AVA – получение доступа к объекту из ЛВС; AVN – получение доступа к объекту из любой ВС, связанной с объектом атаки; АСН – для получения доступа требуется выполнение особых условий; АСМ – для получения доступа требуется выполнение специальных условий; ACL – для получения доступа выполнение специальных условий не требуется; АUN – аутентификация не требуется; AUS – требуется однократная аутентификация; АUM – требуется многократная аутентификация; CN – не оказывает влияния на конфиденциальность данных; СР – частичное нарушение конфиденциальности данных; СС – полное нарушение конфиденциальности данных; IN – не оказывает влияния на целостность данных; IP – частичное неправомерное уничтожение или модифицирование данных; IC – полное неправомерное уничтожение или модифицирование данных; AN – не оказывает влияния на доступность данных; AP – кратковременное неправомерное блокирование данных; AC – долговременное неправомерное блокирование данных; Х – числовое значение критерия изменяется от 0 до 10.

Следует отметить, что данные составляющие носят субъективный характер оценки доступа и характеризуются качественными показателями (частичное, кратковременное), которые сводятся к численным значениям базового вектора уязвимости. При этом ФСТЭК России предлагает четыре уровня опасностей: низкий (0-3.9), средний (4-6.9), высокий (7-9.9), критический (10).

В этом случае такой подход даёт следующие преимущества:

- нормализует значения уязвимостей;
- предоставляет открытую структуру;

- определяет приоритетность риска.

Однако метод CVSS (Common Vulnerability Scoring System) [1] (рис. 1.1) не позволяет осуществлять данную оценку в виде конкретной последовательности действий, связанных с руководящими документами, математическими расчётами, взаимосвязанными с конкретными угрозами или уязвимостями. Данный подход базируется на опыте каждого эксперта или его субъективных оценках, что затрудняет процесс автоматизации создания профилей для разграничения доступа в информационных системах обучения с информацией специального назначения.

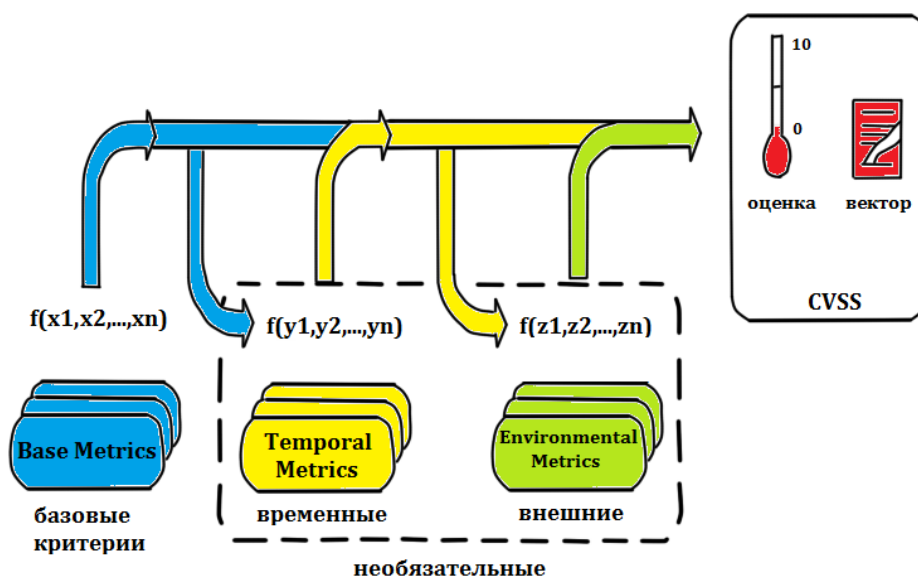


Рисунок 1.1 – Метод Common Vulnerability Scoring System (CVSS) [1]

Таким образом, в настоящее время ФСТЭК России разработана «Методика определения угроз безопасности информации в информационных системах» [2], согласно которой:

- 1) имеется **показатель возможностей нарушителя**, приведённый в таблице 1.1;
- 2) слушателей информационной системы обучения с информацией специального назначения, на основе классификации методики, можно отнести к внутренним пользователям;

3) оценка угрозы безопасности информации (УБИ) в ИС описывается следующим образом:

Таблица 1.1 – Таблица оценки показателей возможностей нарушителя [2]

Показатель возможностей нарушителя		Значения при идентификации уязвимости	Значения при используемости уязвимости
Затрачиваемое время	< 0,5 час	0	0
	< 1 день	2	3
	< 1 месяц	3	5
	> 1 месяц	5	8
Техническая компетентность нарушителя	Непрофессионал	0	0
	Специалист	2	3
	Профессионал	5	4
Знание проекта и информационной системы	Отсутствие знаний	0	0
	Ограниченные знания	2	2
	Знание чувствительной информации	5	4
Возможность доступа к информационной системе	< 0,5 час или не обнаруживаемый доступ	0	0
	< 1 день	2	4
	< 1 месяц	3	6
	> 1 месяц	4	9
	Невозможно		
Оснащённость нарушителя	Отсутствует	0	0
	Стандартное оборудование	1	2
	Специализированное оборудование	3	4
	Оборудование, сделанное на заказ	5	6

$УБИ_j = [\text{нарушитель (источник угрозы); уязвимости; способы реализации угрозы; объекты воздействия; последствия от реализации угрозы}]$.

4) введена актуальность угрозы безопасности информации, подлежащая нейтрализации:

$УБИ_j^A = [\text{вероятность (возможность) реализации угрозы (} P_j \text{); степень ущерба (} X_j \text{)}]$.

Потенциал нарушителей и их возможности приведены в таблице 1.2.

Исходя из того, что слушатели образовательных информационных систем с информацией специального назначения используют её за период обучения более одного месяца, и что эта система доступна им практически ежедневно с наличием стандартного и специализированного оборудования, то значения показателей возможностей нарушителя очень высоки и находятся в пределах 5-

8, 4-9 и 1-4 соответственно для затрачиваемого времени, возможности доступа к информационной системе и оснащённости нарушителя.

Таблица 1.2 – Потенциал нарушителей и их возможности [2]

№	Потенциал нарушителей	Виды нарушителей	Возможности по реализации угроз безопасности информации
1	Нарушители с базовым (низким) потенциалом	Внешние субъекты (физические лица), лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, пользователи информационной системы, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ	Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему
2	Нарушители с базовым повышенным (средним) потенциалом	Террористические, экстремистские группировки, преступные группы (криминальные структуры), конкурирующие организации, разработчики, производители, поставщики программных, технических и программно-технических средств, администраторы информационной системы и администраторы безопасности	Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомлённость о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путём проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы
3	Нарушители с высоким потенциалом	Специальные службы иностранных государств (блоков государств)	Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных

			<p>(ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищённых организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограмм), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок.</p> <p>Имеют хорошую осведомлённость о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе.</p> <p>Имеют возможность получить информацию об уязвимостях путём проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на неё. Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений</p>
--	--	--	--

Тем не менее, оценка технической компетентности и оценки знаний самой ОИСИСН является субъективной в данной методике и требует её модификации, которая позволит перейти от качественных (или субъективных оценок) к количественным оценкам, которые дадут возможность осуществить ранжирование нарушителей, а применительно к слушателям – распределить их по группам с соответствующим уровнем их осведомлённости.

Наиболее часто угрозы безопасности информации могут быть реализованы нарушителями за счет:

1) несанкционированного доступа и (или) воздействия на объекты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));

2) несанкционированного доступа и (или) воздействия на объекты общесистемного уровня (базовые системы ввода-вывода, **гипервизоры**, операционные системы);

3) несанкционированного доступа и (или) воздействия на объекты прикладного уровня (системы управления базами данных, браузеры, web-приложения, иные прикладные программы общего и специального назначения);

4) несанкционированного доступа и (или) воздействия на объекты сетевого уровня (сетевое оборудование, сетевые приложения, сервисы);

5) несанкционированного физического доступа и (или) воздействия на линии (каналы) связи, технические средства, машинные носители информации;

6) воздействия на пользователей, администраторов безопасности, администраторов информационной системы или обслуживающий персонал (социальная инженерия).

Как видно из возможностей реализаций НСД, одним из специфических объектов доступа на общесистемном уровне являются гипервизоры и операционные системы. Согласно методике [2] для оценки той или иной j-ой УБИ (Y_j) необходимо оценить два показателя: уровень защищенности информационной системы (Y_1) и потенциал нарушителя (Y_2), для заданных структурно-функциональных характеристик и способов разграничения доступа с используемыми политиками безопасности:

$$Y_j = [\text{уровень защищенности } (Y_1); \text{ потенциал нарушителя } (Y_2)].$$

Исходя из того, что методика ФСТЭК РФ базируется на методе CVSS, для которого необходимо оценить уязвимости на основе понятий информационной безопасности, а информация включает свойства доступности,

конфиденциальности, целостности и достоверности, то несанкционированный доступ можно рассматривать как нарушение двух свойств: доступности и конфиденциальности (рис. 1.2).

Угрозы										
Внешние					Внутренние					
Природные					Искусственные					
					Преднамеренные			Непреднамеренные		
Землетрясения	Наводнения	Пожары	Ураганы	Электромагнитные бури	Электромагнитное излучение	Вирусы или вложенные дефекты программ		Программные средства		Нарушение доступа пользователей
						Аппаратно-технические средства		Люди (субъекты)		
						Активные	Пассивные			
						Размолвавание людей	Подделка	Раскрытие информации	Дешифрация	Декодирование
										Перехват
										Потеря или утрата
										Неправомерные действия
										Ошибки в работе
						Разрушение	Искажение	Раскрытие		Нарушение доступности
						Несанкционированный доступ				
						Нарушение целостности	Утечка информации			
						Нарушение безопасности информации				
						Потери информации				

Рисунок 1.2 – Взаимосвязь различных видов угроз безопасности информации с видами нарушений

Как видно из рисунка 1.2, наибольшее значение среди всех видов угроз является НСД, при котором понимается доступ к информации или действия

с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному назначению и техническим характеристикам. Архитектуру взаимосвязи процессов при осуществлении НСД можно представить в виде рисунка 1.3. Таким образом, целесообразно проанализировать методы, процедуры, модели для оценки информационной безопасности информационных и автоматизированных систем, а также методы оценки угроз от НСД и их математические модели.

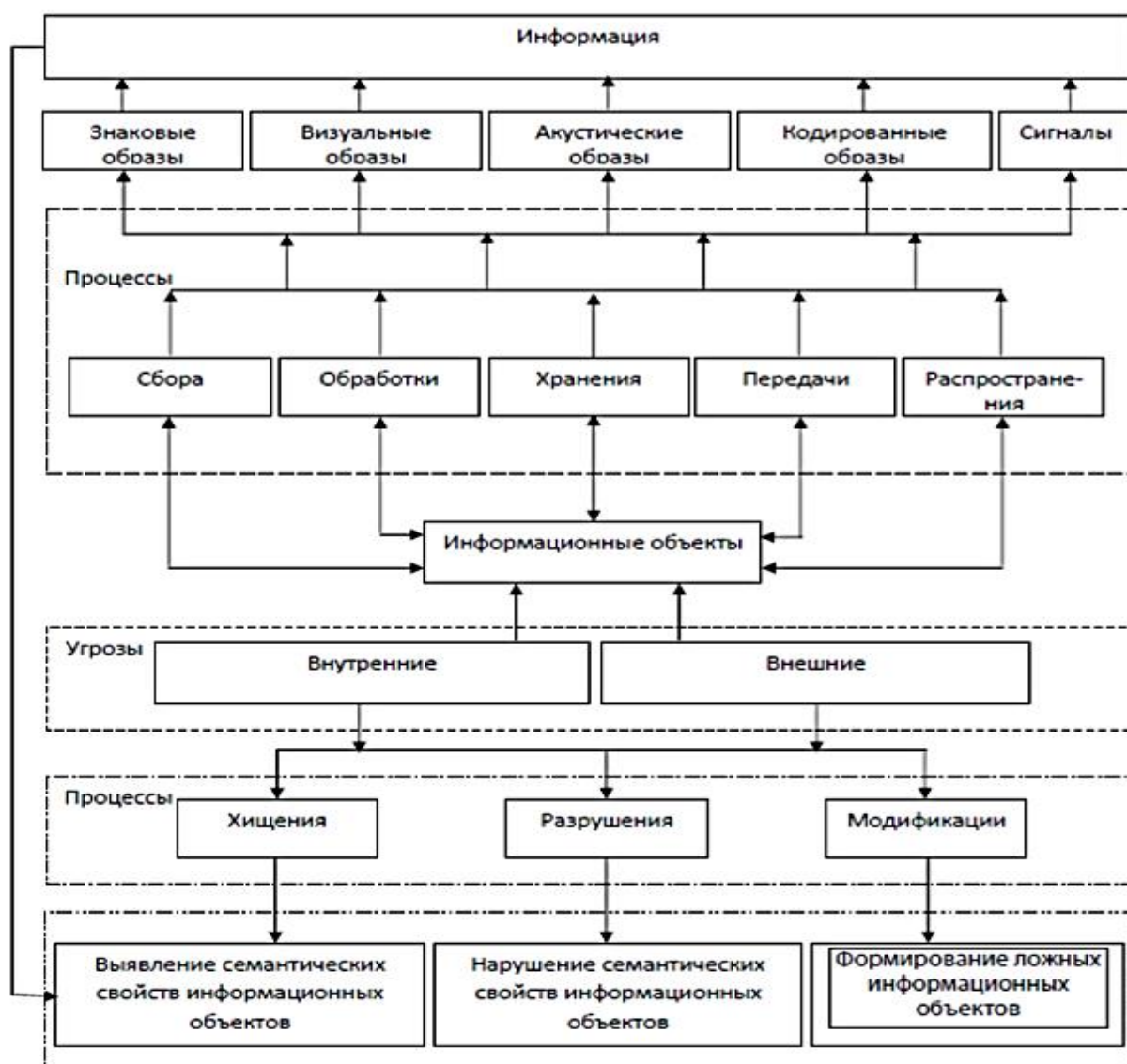


Рисунок 1.3 – Архитектура взаимосвязи процессов при осуществлении НСД

1.2 Анализ существующих методов и моделей нарушителя для образовательных информационных систем

В работе [3] авторы предлагают метод, связанный с обеспечением целостности информации на основе свойств избыточного модулярного кода. Целью их работы является возможность самовосстановления свойств хранимой информации после деструктивных воздействий. Тем не менее, исследования авторов не направлены на формирование модели нарушителя информации применительно к НДС к гипервизору через виртуальные машины.

Исследования, представленные автором в работе [4], направлены на построение дискретных процедур распознавания угроз информационной безопасности. Данные процедуры ориентированы на автоматизированные системы обработки данных критического применения. Работа описывает формирование дискретных процедур для распознавания угроз и метод моделирования различных политик безопасности. С помощью описанного метода имеется возможность разработать математические модели глобальной, локальной, дискреционной и блочной политик безопасности [4]. В работе автор предлагает модель уязвимостей для автоматизированных систем обработки данных критического применения, которая имеет следующий вид:

$$S_R = (EUM^*, SDN, RDN \cup ADN \cup MIF, IR),$$

где EUM^* – множество, в состав которого входит подмножество узлов, потенциально содержащих уязвимости; SDN – множество субъектов автоматизированной системы; RDN – множество рёбер графа состояний автоматизированной системы; ADN – множество рёбер графа состояний системы уязвимостей в соответствии с доступом; MIF – множество рёбер графа состояний системы уязвимостей в соответствии с информационным и потоками; IR – функции иерархии EUM^* . Автором введена оценка принадлежности объекта конкретному классу, а также информативная значимость признака. Это позволило автору повысить скорость работы алгоритма и установить баланс

между распознаванием угроз информационной безопасности, обеспечением целостности данных и эффективностью обработки информации.

Однако данный подход не применялся для угроз и уязвимостей, связанных с НСД к гипервизору ОИСИСН через виртуальные машины.

Подходам, описывающим эталонные модели защищённой АС, посвящена работа [5], которая рассматривает эти модели с использованием иерархических методов структуризации ресурсов с целью возможности унифицированного моделирования динамического и статического доступа к информации. Тем не менее результаты не позволяют раскрыть возможности по реализации пользователями образовательных информационных систем с информацией специального назначения уязвимостей, присущих НСД к гипервизору через виртуальные машины. Поэтому целесообразно рассмотреть вопросы, связанные со специфическими особенностями реализации НСД для выделенных в диссертационных исследованиях ограничениях.

Применительно к оценке таких параметров, как степень ситуационной неопределённости, скорость изменения типов доступа, возрастание вероятности атак на информационные ресурсы, а также возрастание стоимости причинённого ущерба посвящена работа [6] авторы выделили свойство оперативной адаптации как одно из наиболее релевантных свойств и расширили возможности использования экспертных подсистем, методов нечёткой логики, генетических алгоритмов и нейронных сетей, которые позволяют повысить эффективность функционирования СЗИ в целом. Тем не менее авторы проводили исследования применительно к автоматизированным системам управления специального назначения со структурой, представленной на рисунке 1.4, и не рассматривали возможность использования предлагаемого подхода применительно к адаптивному формированию профилей по разграничению доступа в ОИСИСН для защиты от НСД к гипервизору через виртуальные машины.

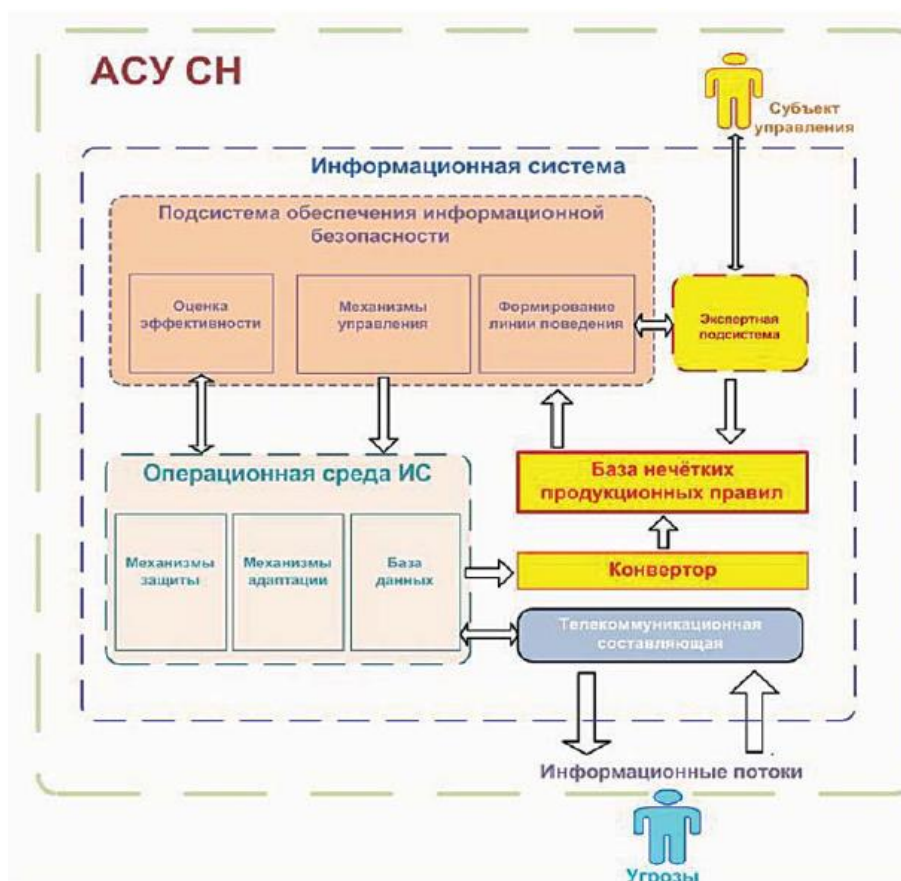


Рисунок 1.4 – Структура автоматизированной системы управления специального назначения [6]

Кроме того, авторы предложили нейро-нечёткую сетевую структуру на примере производственной сети Ванга-Менделя (рис. 1.5), что позволило им реализовать защиту от угроз безопасности информации в условиях неопределённости, а сам подход позволяет системе защиты самообучаться применительно к новым угрозам, что также следует учитывать при выборе методов решения задач, поставленных в данных диссертационных исследованиях.

Поэтому целесообразно такой метод использовать при разработке модели и средства оценки состояния ОИСИСН для выявления угроз НСД к информации через виртуальные машины к гипервизору.

Безопасность информационного сопряжения сетей общего пользования с категоризованными корпоративными сетями рассматривается в работе [7]. Автор в своей работе вводит *показатель средней информативности запроса*, который определяет оценку стойкости систем защиты информации

в зависимости от имеющихся уязвимостей за счёт реализации процессов несанкционированного доступа. Исследование работы по возможному несанкционированному доступу через терминальный сервер из сети общего пользования к категорированной сети объекта представлен на рисунке 1.6.

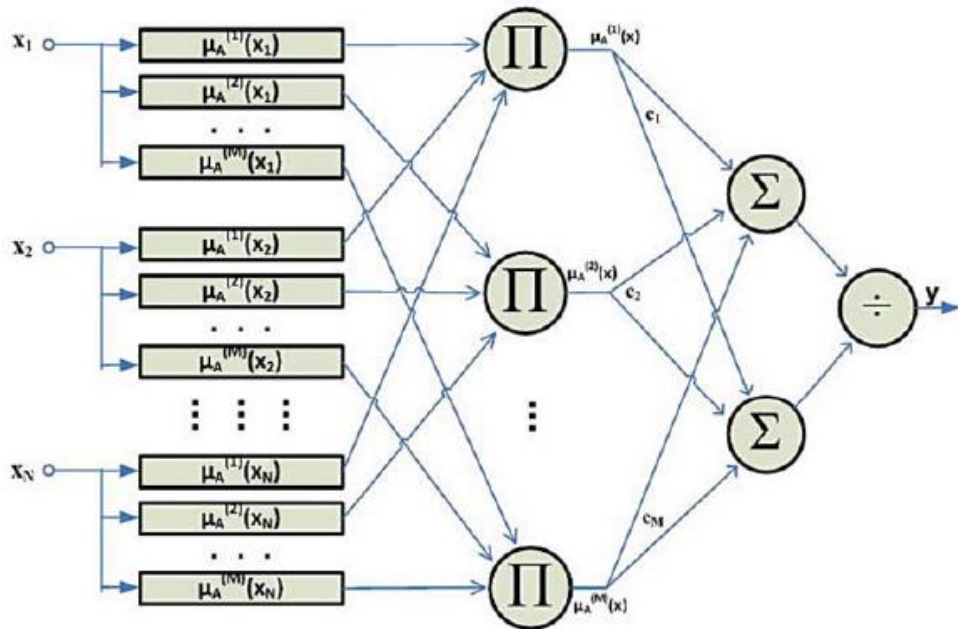


Рисунок 1.5 – Нейро-нечёткая сеть Ванга-Менделя [6]



Рисунок 1.6 – Доступ через терминальный сервер из сети общего пользования к категорированной сети объекта [7]

Автор также рассматривает процессы, происходящие в шлюзе взаимодействия сетей (рис. 1.7). Такой подход позволяет разработать и ввести критерий осведомлённости слушателя по знанию специальных средств для реализации уязвимостей, присущих при НСД к гипервизору через виртуальные машины.

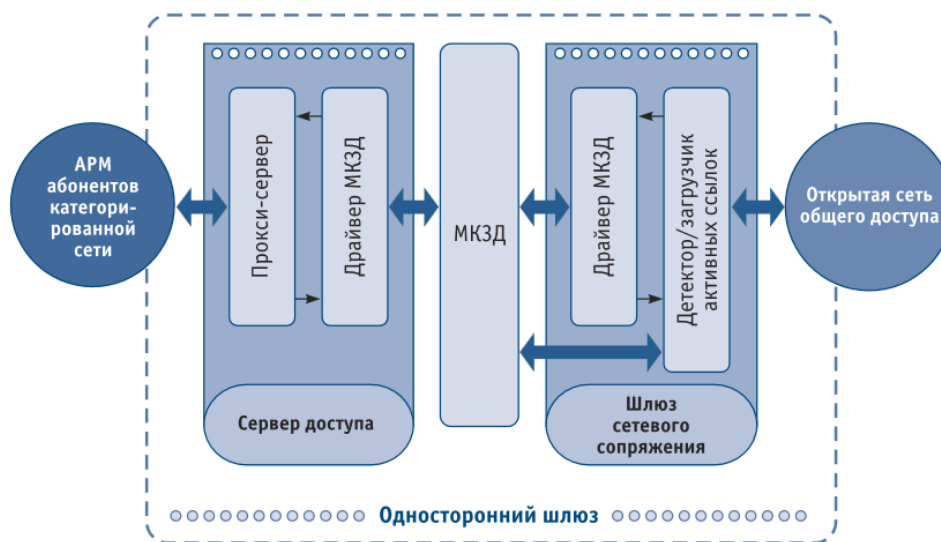


Рисунок 1.7 – Процессы, происходящие в шлюзе взаимодействия сетей [7]

Авторы в своей работе предлагают оценку информативности каждого запроса представлять на основе расчёта энтропии с использованием следующей формулы:

$$W = -p \log_2(p) - (1 - p) \log_2(1 - p).$$

В работе [8] авторы предложили метод и функциональную модель, которые позволяют определять численные значения по оценке риска нарушения информационной безопасности на основе использования качественных показателей на начальном этапе создания такой модели.

В связи с этим авторы в работе [8] предложили систему иерархических критериев качества применительно к средствам защиты и использовали математический аппарат нечёткой логики для оценивания риска нарушения безопасности (рис. 1.8).

Тем не менее, авторы не рассматривали возможность оценки таким методом риска нарушения безопасности применительно к ОИСИСН, учитывая

то, что такие системы имеют некоторые особенности: как в экспертных оценках, так и методиках расчёта. Это обусловлено тем, что, как отмечалось ранее, в таких системах имеется достаточно высокая динамика изменения как количественных, так и качественных параметров.

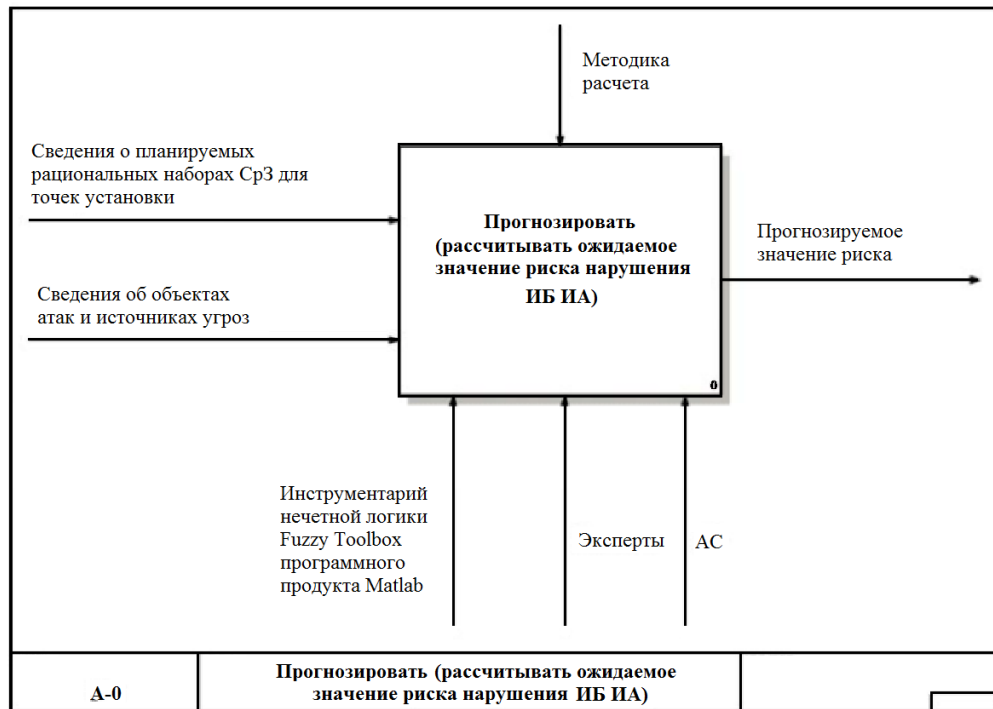


Рисунок 1.8 – Модель оценивания риска нарушения информационной безопасности на основе ER-диаграммы [8]

В работе [9] авторы уделяют внимание вопросам, носящим специфические аспекты применительно к информационным системам специального назначения, где ими предложена оценка защищённости речевой информации на основе метода главных компонент, а также приведены результаты исследований, выполненных по данному методу (рис. 1.9). Тем не менее данный подход не даёт полной оценки несанкционированного доступа к информационной системе специального назначения, однако может быть использован в совокупности с общей системой оценки риска угроз информационной безопасности.

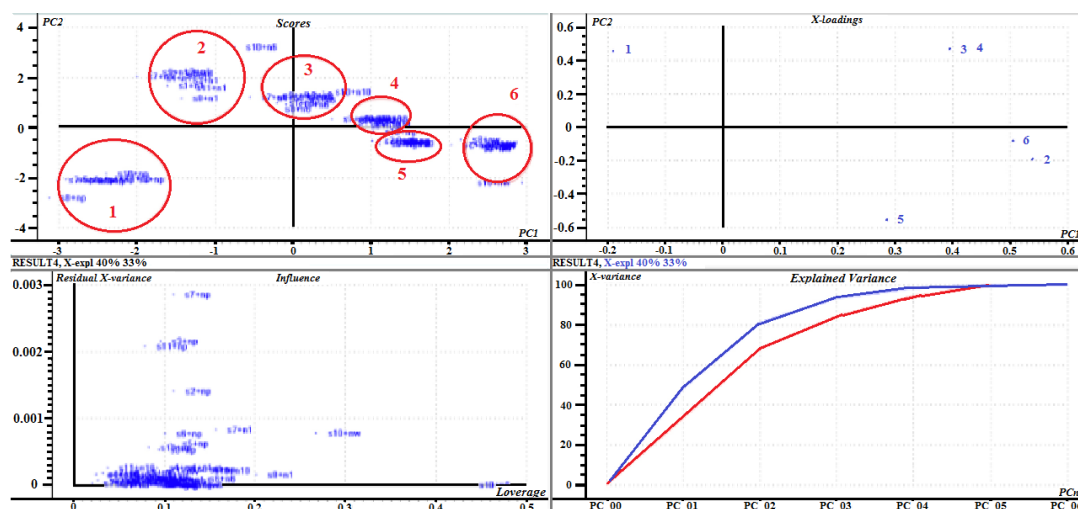


Рисунок 1.9 – Параметры акустического сигнала, обработанные методом главных компонент [9]

В работе [10] авторы предложили модель, направленную на процесс борьбы с противоправными действиями информационных системах специального назначения для органов внутренних дел (рис. 1.10- 1.12), которая может быть использована для описания взаимодействия процессов, происходящих в информационных системах в целом.

Исследованиям, связанным с информацией ограниченного распространения, посвящена работа [11]. Авторы предложили оценивать угрозы безопасности применительно к информации ограниченного распространения на основе вероятностной математической модели последствий несанкционированного доступа злоумышленника. Авторами был использован метод Марковского случайного процесса для описания динамических процессов, происходящих в автоматизированных информационных системах.

В своей работе авторы используют показательный закон для оценки вероятности воздействия угрозы за промежуток времени Δt , то есть оценивают скорость наступления угрозы в виде следующей зависимости:

$$P(t) = 1 - e^{-\lambda t},$$

где t — время воздействия угрозы; λ — интенсивность воздействия.

Тем не менее, для описания данного метода необходимо знать закон распределения времени между наступлением событий НСД или частоту

реализации уязвимостей в ОИСИСН, а это не всегда доступно для исследователя.



Рисунок 1.10 – Модель процесса борьбы с противоправными действиями в информационных системах специального назначения применительно к органам внутренних дел. Этап предупреждения [10]

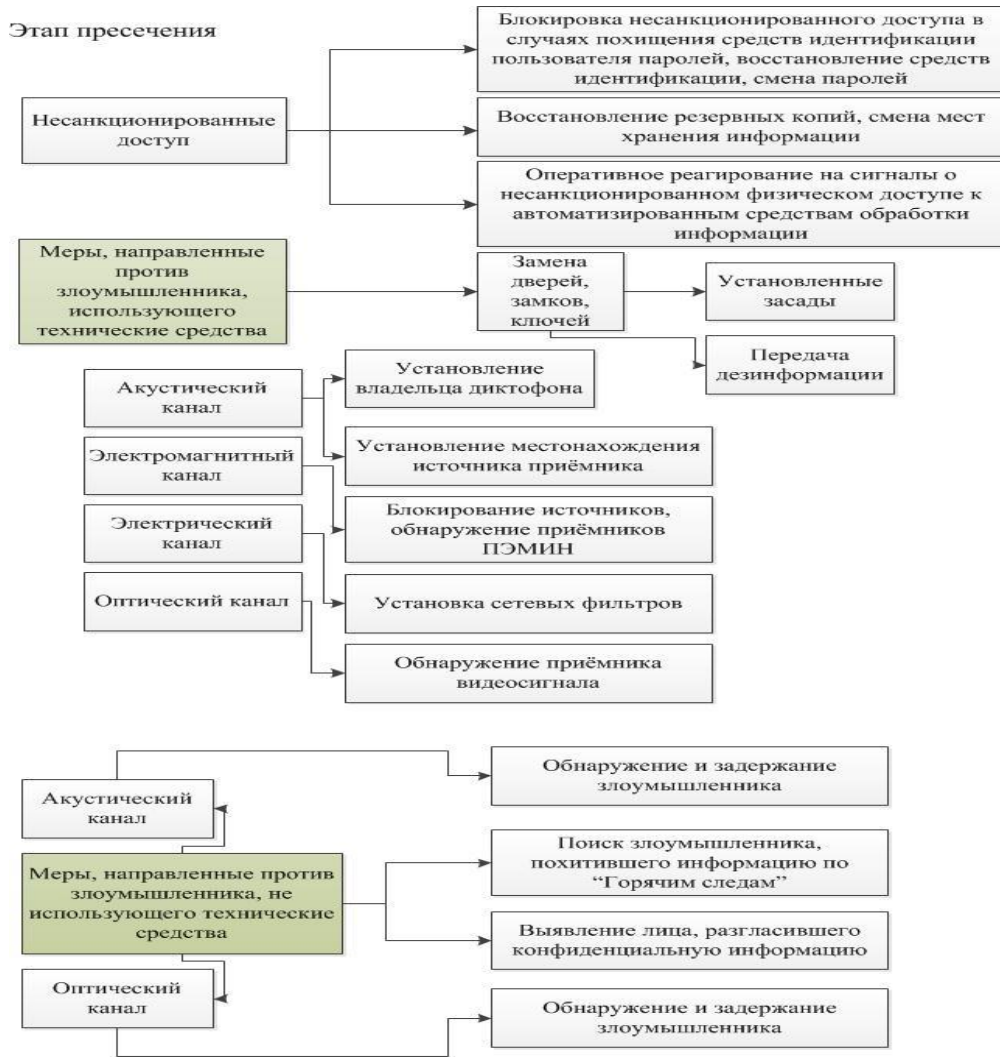


Рисунок 1.11 – Модель процесса борьбы с противоправными действиями в информационных системах специального назначения применительно к органам внутренних дел. Этап пресечения [10]

Этап раскрытия



Рисунок 1.12 – Модель процесса борьбы с противоправными действиями в информационных системах специального назначения применительно к органам внутренних дел. Этап раскрытия [10]

Кроме того, данный подход не способен использовать качественные показатели в условиях априорной неопределённости, что не даёт возможность его применения в диссертационном исследовании.

Использованию качественных и количественных подходов для методов оценки уровня защищённости информационных систем посвящены результаты анализа в работе [12]. Также авторы предложили структуру критериев оценки уровня защищённости информационных систем, связанных с базовой оценкой CVSS. Тем не менее ими оценивается показатель выполнения требований безопасности как соотношение количества реализуемых в информационной системе требований по безопасности к общему количеству задаваемых требований, причём без учёта реализации уязвимостей применительно НСД к гипервизору через виртуальные машины.

В работе [13] авторы уделили внимание исследованиям модели защиты персональных данных (ПДн) на примере информационной системы Пермского филиала ФГУП «Радиочастотный центр Приволжского Федерального округа» (рис.1.13).

Ими предложен порядок определения актуальных УБИ и разработки частной модели угроз безопасности информационной системы персональных данных. Такую систему можно отнести к образовательным информационным системам. Кроме того, авторы частично рассматривали модель на уровне выполняемой последовательности действий, направленных на реализацию угроз информационной безопасности, что следует учитывать в данном диссертационном исследовании. Тем не менее проведённый анализ выполнен на организационно-техническом уровне защиты и не охватывает возможность формирования профилей разграничения доступа к информации.

К исследованиям, связанным с системами специального назначения, относятся работы [14-49]. Так, в работе [14] авторы исследуют процессы для систем специального назначения применительно к органам МВД России. В данной работе сделан упор на осуществление контроля эффективности

функционирования объекта с целью своевременного реагирования на происходящие изменения. Этот подход аналогичен требуемому подходу для оценки контроля по осведомлённости и подготовленности слушателей, которые обучаются с использованием информационных систем специального назначения и сменяются в казённом военном образовательном учреждении с определённой периодичностью.

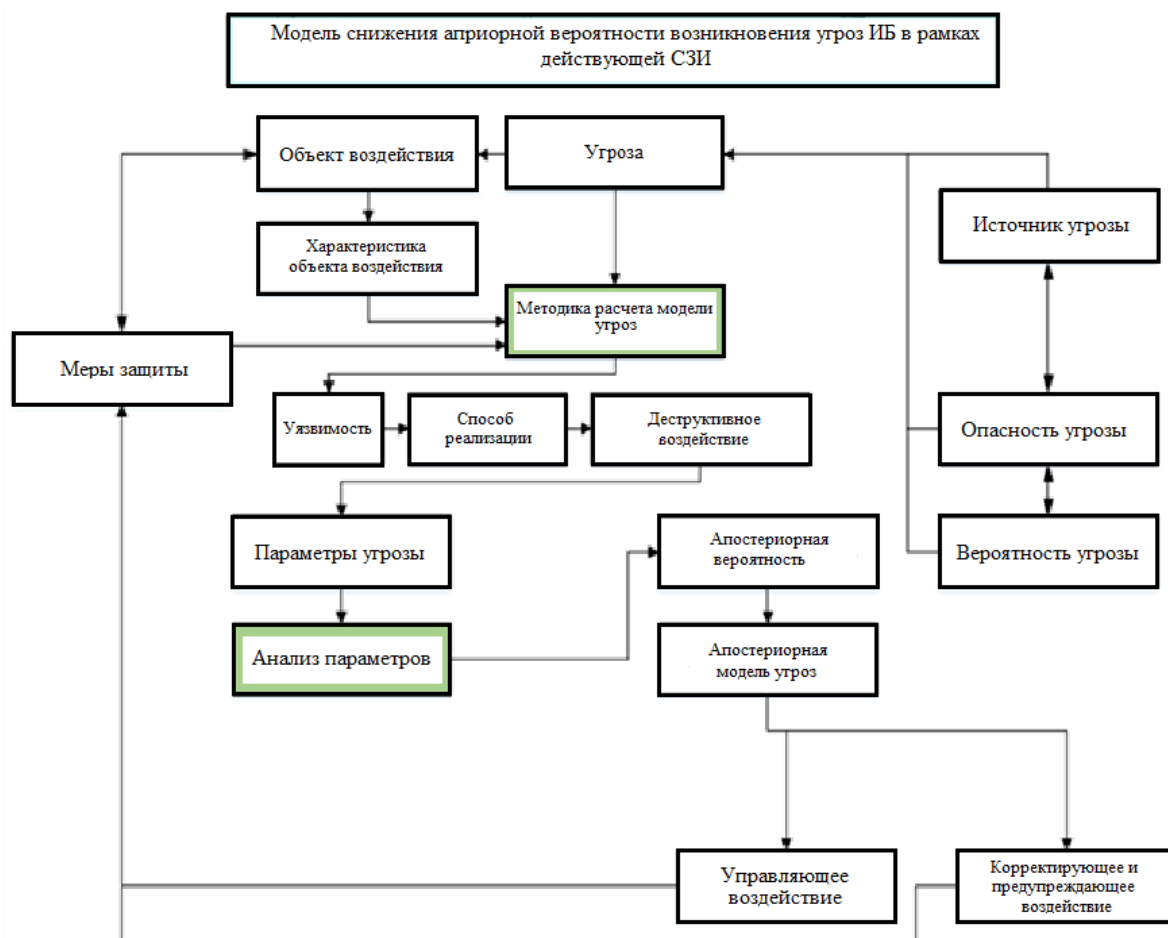


Рисунок 1.13 – Модель снижения априорной вероятности возникновения угроз ИБ в рамках действующей СЗИ для информационной системы [13]

В своей работе авторы дают характеристику возможностей администратора безопасности и определяют её как математическую зависимость убывающей функции объёма программных средств для защиты информации от НСД и соотношений между текущими и требуемыми величинами временных характеристик контроля. Как видно, авторами показан подход для решения задачи оптимизации при управлении организационно-

техническими средствами защиты информации. Тем не менее данный подход не использовался для оценки решения задачи по своевременному созданию профилей по разграничению доступа в ОИСИСН применительно к ограничениям, принятым в данном исследовании, относительно времени формирования профилей для групп слушателей с одинаковыми критериями информированности.

В работе [15] для системы специального назначения предлагается использовать методы теории возможностей. Авторы предлагают использование функций принадлежности с нечёткими границами для описания взаимосвязей между нарушителем и системой защиты информации. Исходя из полученных ими нечётких рамочных оценок, получены графики функций принадлежности для анализа информации средствами защиты и обнаружением нарушения на настоящий момент времени [15] и функций принадлежности для анализа информации средствами защиты и обнаружением нарушения на прогнозируемый момент времени [15], представленные на рисунках 1.14 и 1.15 соответственно.

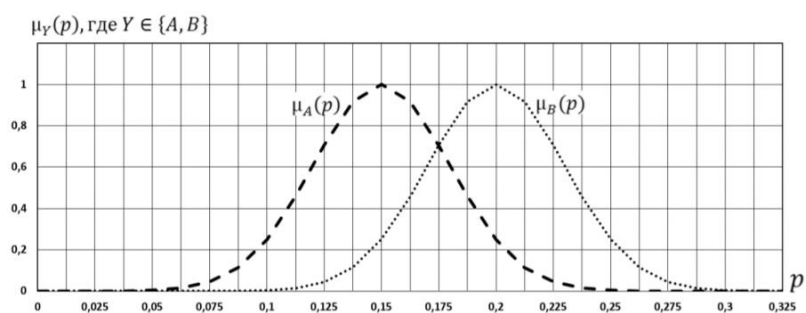


Рисунок 1.14 – Функции принадлежности для анализа информации средствами защиты и обнаружением нарушения на настоящий момент времени [15]

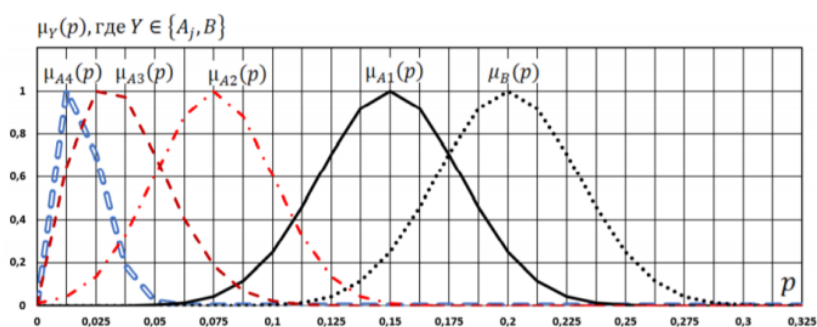


Рисунок 1.15 – Функции принадлежности для анализа информации средствами защиты и обнаружением нарушения на прогнозируемый момент времени [15]

Авторам метод теории возможностей позволил оценить эффективность вводимых ими скрытых меток в защищаемую информацию, что сократило средние значения интервалов возможных значений вероятностей их обнаружения. Тем не менее данным методом не была оценена вероятность осуществления НСД к гипервизору через виртуальные машины слушателями с различным уровнем подготовленности.

В работах [16-17] был выполнен анализ системы специального назначения, включая возможные угрозы НСД, хотя результаты решения задачи были сведены к организационным методам работы как с обслуживающим персоналом, так и с эксплуатирующим контингентом. Однако, к сожалению, это не всегда является эффективной мерой.

В работе [18] автор обоснованно выдвигает НСД в системах специального назначения на первое место по значимости и частоте реализации нарушителями. Автор выделила множество формальных условий в виде эффекта воздействия угроз нарушения конфиденциальности, угроз нарушения доступности, угроз нарушения целостности. Так автор, выделяет для нарушения конфиденциальности величину в виде композиции временных характеристик множества из восьмидесяти функций представления противоправных действий по несанкционированному копированию информации. Исходя из анализа, применительно к ОИСИСН, это нарушение выходит на первый план применительно к её слушателям, которое необходимо исследовать в данной диссертационной работе.

Автор в своей работе предложила математическую модель показателя эффективности защиты информации через функциональные механизмы защиты. Аналогично этой работе для диссертационных исследований предлагается описать показатели НСД к гипервизору через виртуальные машины, опираясь на их функциональные характеристики.

В работах [19-20] автор предлагает обнаруживать нарушителей на основе метода выявления аномального поведения субъектов без предварительной

оценки недостатков системы защиты информации. Для этого ей предлагаются правила анализа поведения субъекта и определяются пороговые значения контролируемых статистических параметров. Недостатком данного метода применительно к оценке слушателей ОИСИСН является необходимость отслеживания их поведения уже в ходе обучения и пользования этой системой. В отличие от этого метода в данном диссертационном исследовании предлагается выполнить заблаговременное тестирование слушателей для оценки их осведомлённости о возможности (подготовленности) ими осуществлять НСД к защищаемой информации (на примере НСД к гипервизору через виртуальные машины) и определить критерий осведомлённости для ранжирования слушателей и распределения их в соответствующие группы.

В работе [21] авторами решается задача распределения временного резерва применительно к системам специального назначения. Тем не менее данная задача распределения времени не направлена на решение своевременной настройки профилей по разграничению доступа, применительно к технологии тонкий клиент, для отдельных групп слушателей с требуемым набором программного и технического обеспечения.

В работе [22] введён показатель своевременности обработки информации как вероятность того, что время реализации процедур обработки информации не превысит требуемую величину. Аналогично данному показателю в диссертационном исследовании предлагается использовать показатель своевременной настройки профилей по разграничению доступа как вероятность того, что время автоматизированной настройки не превысит заданную величину.

В работах [23–24] авторы предлагают Марковскую модель средств защиты автоматизированных систем специального назначения, в которой они используют равновероятный закон распределения информации. Тем не менее такой закон не имеет место при реализации НСД, так как он носит, как правило, нормальный или экспоненциальный законы распределения. Это необходимо

учитывать при описании функции процесса реализации НСД конкретным субъектом (слушателем, злоумышленником), учитывающей как временной параметр t , так и оценку возможностей k -той реализации угроз НСД отдельной группой слушателей.

В работе [25] был выполнен анализ деструктивных программных воздействий, включая НСД. Однако НСД к гипервизору через виртуальные машины автором не рассматривался.

Описанию имитационной модели процессов функционирования системы специального назначения в условиях воздействия угроз НСД посвящена работа [26]. Авторы предполагают стационарность моделируемых процессов, однако динамика замены слушателей ОИСИСН применительно к диссертационным исследованиям носит периодический характер, а процессы НСД в ней стохастичны и зависят от уровня подготовленности слушателей. Хотя, с точки зрения описания задач обработки информации, авторы предлагают подход для возможного представления отдельных фаз обслуживания в виде отдельных состояний (рис. 1.16), что может быть использовано для описания этапов осуществления НСД к гипервизору через виртуальные машины при создании формальной модели нарушителя.

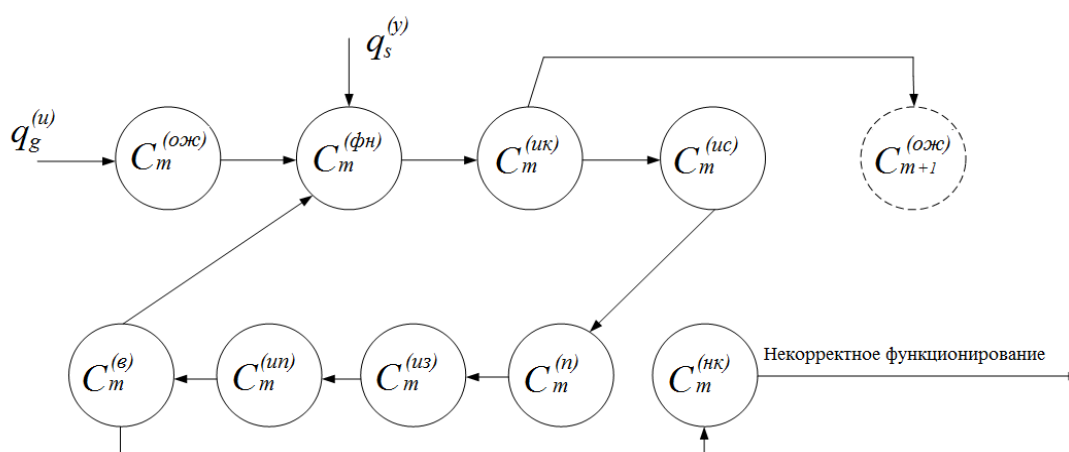


Рисунок 1.16 – Описание состояний фаз обслуживания СЗИ в ИС СН [26]

Также подходу создания имитационной модели для описания условий действия злоумышленника посвящена работа [27], где определяются параметры

модели и их взаимодействие. Тем не менее данные параметры не детализированы применительно к описанию последовательности выполнения команд, необходимых для осуществления НСД к гипервизору через виртуальные машины в исследуемых ОИСИСН.

В работе [28] авторами предложена логико-вероятностная модель, позволяющая получить значения показателя эффективности СЗИ применительно к автоматизированной системе управления специального назначения (рис. 1.17).

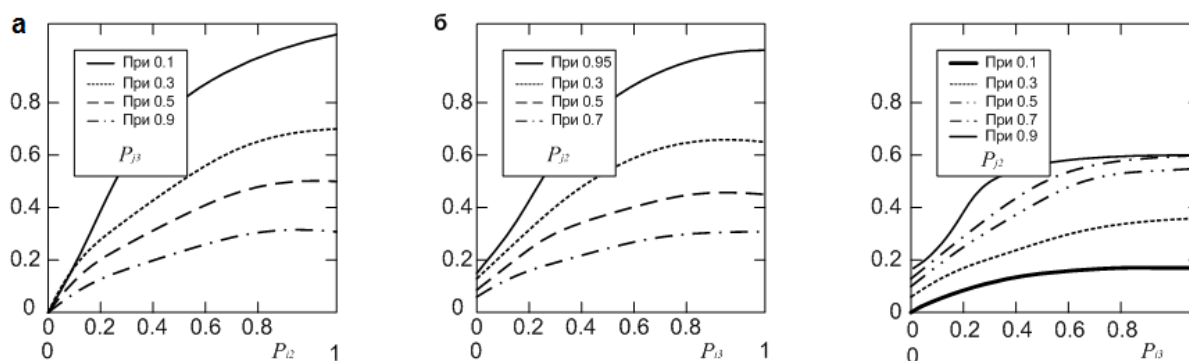


Рисунок 1.17 – Значения показателя эффективности СЗИ применительно к автоматизированной системе управления специального назначения [28]

Полученные зависимости показателя эффективности СЗИ позволяют уточнять весовые коэффициенты защищённости различных уровней применительно к модели *и средству оценки состояния ОИСИСН в условиях угроз НСД к гипервизору через виртуальные машины* для отдельных групп слушателей за требуемые временные промежутки.

В работе [29] авторами были исследованы функциональные возможности многопользовательской операционной системы специального назначения с возможностями разграничения доступа и расширенным комплексом средств защиты от НСД.

Авторами были проанализированы децентрализованные механизмы защиты, которые для каждого объекта его владельца имеют возможность

задания правил назначения прав доступа к этому объекту индивидуально и основываются на дискреционной модели разграничения доступа.

Кроме того, были проанализированы централизованные механизмы защиты от НСД на основе администрирования правил назначения доступа к объектам, специально выделенным лицом, которые относятся к мандатной модели разграничения доступа. Авторы также проанализировали интегрированную в ОС подсистему безопасности PARSEC. Следует отметить, что рассмотренный в работе [29] механизм разграничения доступа встроен в саму операционную систему с подключаемыми модулями аутентификации. Для предлагаемого авторами разграничения доступа в операционной системе доступ пользователю разрешается, если он возможен и для дискреционных, и для мандатных правил разграничения доступа одновременно, и запрещён в противном случае.

Однако особенностью НСД к гипервизору через виртуальные машины является его способность миновать СЗИ операционной системы и осуществить доступ к конфиденциальной информации напрямую. Тем не менее при реализации *средства оценки состояния ОИСИСН в условиях угроз НСД*, которые позволяют создавать профили разграничения доступа для отдельных групп слушателей за требуемые временные промежутки, необходимо учитывать возможность использования технологии тонкий клиент.

Применительно к деструктивным воздействиям были выполнены исследования в работе [30], где авторы на основе вычислительного эксперимента определяют ВВХ СЗИ от НСД. Однако расчёты, связанные с НСД к гипервизору через виртуальные машины, ими не рассматривался, ввиду чего отсутствуют их вероятностно-временные характеристики, которые необходимо будет получить в данных диссертационных исследования на основе *нечёткой модели и средства оценки состояния ОИСИСН в условиях угроз НСД*, которые позволяют создавать профили разграничения доступа для отдельных групп слушателей за требуемые временные промежутки.

В работе [31] авторами был выполнен анализ уязвимостей и угроз, предложена модель нарушителя и модель угроз, также предложен один из способов борьбы с НСД на основе использования комплекса защиты информации по технологии «тонкий клиент» и средств виртуализации, однако реализация профилей по разграничению доступа ими не описывалась, поэтому требует детализации и более детального исследования в этой области.

Работа [32] посвящена проблемам обучения иностранных военных специалистов на примере информационной системы обучения с информацией специального назначения Военной академии связи имени С.М. Будённого. Тем не менее работа акцентирует внимание только на решении проблем, связанных с обучением и не рассматривает вопросов по разграничению доступа к информации для иностранных слушателей.

В работе [33] выполнен анализ способов реализации угроз в инфокоммуникационных системах специального назначения, а также описаны особенности моделей нарушителя применительно к рассматриваемой авторами структуре системы, где предлагается описывать ограничения и предположения о характере возможных действий нарушителей. Тем не менее, описание действий нарушителя применительно к диссертационным исследованиям на примере НСД к гипервизору через виртуальные машины авторами не проводились. Поэтому есть необходимость в разработке такого рода модели нарушителя для образовательных информационных систем с информацией специального назначения.

Применительно к определению вероятностно-временных характеристик технической компьютерной разведки были выполнены исследования и представлены результаты в работе [34]. Результатом такой оценки авторы определили, что при вероятности обнаружения с величиной 0,9 и задании параметра функции распределения вероятности равного 0,9, время, необходимое на проведение технической компьютерной разведки составляет 100 минут. Этот параметр может быть использован как критерий ограничений

на время формирования профилей по разграничению доступа на основе технологии «тонкий клиент».

Работа [35] посвящена методам исследования для описания пользователей, выполняющим свою функциональную задачу и оценки механизма контроля доступа на основе профилей пользователей в целях проверки корректности настроек политики безопасности. Авторы предлагают разбивать последовательность событий доступа на фрагменты деятельности пользователя и формировать информационный профиль пользователя с целью дальнейшего ранжирования их в однородные группы на основе матрицы вероятностей переходов, что позволяет оценивать типовые схемы использования ими информационных ресурсов. Однако в данной работе решается обратная задача, то есть определяется мера качества, которая показывает соответствие группы и предоставляемой ей информации.

В данном диссертационном исследовании необходимо определить группу для слушателей на основе наличия у них определённых знаний, что влечёт за собой необходимость в разработке тестовых наборов для оценки осведомленности слушателя по качественным показателям с переводом результатов тестирования в количественные оценки осведомленности на основе правил нечёткой логики, а также разработки нечёткой модели для оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН с описанием сути модификации подхода по формированию функций принадлежности, описывающих количественно уровни компетенций.

Исследованию средств доверенной загрузки посвящена работа [36] применительно к различным семействам операционных систем (Windows, Unix, Linux). Определены показатели качества средств доверенной загрузки, однако метод их использования авторами не описывался.

В работах [37-38] имеются результаты анализа имеющихся особенностей используемого программного кода, которые представлены в таблице 1.3, при использовании кибератак.

Таблица 1.3 – Особенности используемого программного кода [37]

Наименование закладки	Возможности	Объекты размещения (атаки)	Особенности
FEEDTROUGH	Установка двух программных закладок BANANAGLEE и ZESTYLEAK	Juniper: ns5xt, ns25, ns50, ns200, ns500 и ISG 1000	Сохраняется при обновлении ОС
GOURMETTROUGH	Скрывает закладку BANANAGLEE и позволяет её сохранить после загрузки или обновления ОС	Некоторые модели Juniper	Имеется возможность пользовательской настройки
SOUFFLETROUGH	Закладка для BIOS	Juniper SSG 500 и SSG 300 серии	Возможно удалённое обновление и установка
SCHOOLMONTANA	Модификация BIOS	Juniper J-серии	Сохраняет закладки при обновлении и замене ОС, в том числе и при физической замене флеш карты роутера
SIERRAMONTANA	Обеспечивает присутствие сетевых закладок	Juniper M-серии	Аналогичны SCHOOLMONTANA
STUCCOMONTANA	Обеспечивает присутствие сетевых закладок	Juniper T-серии	Аналогичны SCHOOLMONTANA

Результаты данной работы показывают неизменность некоторых программных закладок при модификации операционных систем, что определяет и подтверждает необходимость в исследовании процессов НСД на уровне команд.

В работе [39] одной из задач, решаемых авторами, является определение критериев многокритериальной оптимизации на основе метода последовательных уступок, который включает оценку циклического обслуживания в виде аппроксимаций с использованием закона псевдосохранения, предложенного Эвериттом. Тем не менее, применительно к модели и средству выявления угроз НСД к информации в виртуальной среде ОИСИСН, построенной с применением технологии «тонкий клиент», с автоматизацией процесса создания профилей настроек разграничения доступа для слушателей необходима детализация весовых коэффициентов.

Аналогично работе [40], где автор выполнил корреляционную оценку угроз безопасности и способов их нейтрализации, в данных диссертационных исследованиях необходимо оценить взаимосвязь между оценкой осведомленности слушателя и оценкой возможностей реализации им угроз НСД к гипервизору через виртуальные машины в ОИСИСН. Однако на настоящее время имеются только качественные оценки, которые необходимо преобразовать в количественные оценки.

Исходя из классификации угроз безопасности информации и их видов, выполненных в работе [41], применительно к исследуемой ОИСИСН её можно отнести к тому, что источником угрозы является человеческий фактор, аппаратные или программные средства; источник угрозы является внутренним; источник угрозы направлен на нарушение конфиденциальности информации и является преднамеренным; длительность воздействия источника угрозы периодический.

Особенности архитектур описаны в работе [42] на основе протоколов. Однако использование протоколов в данной диссертационной работе не исследуется.

В работе [43] описаны модель атак, модель нарушителя, модель потоков воздействий, модель оценки уровня защищённости программного обеспечения, применительно к сложным организационно-техническим системам, что требует уточнения особенностей для модели нарушителя применительно к ОИСИСН.

Математическая модель нарушителя также представлена в работе [44], где оцениваются вероятности ошибок последовательности действий нарушителем, их возможных ошибочных действий, а также трудоёмкость поиска нарушителем необходимой информации. Аналогично последнему критерию оценки может быть использован критерий осведомлённости нарушителя, который позволит оценить возможные действия нарушителя до начала их выполнения.

Работы [45-48] отражают исследования по описанию процессов, связанных с защитой информации в сетях различного типа, что накладывает свою специфику за счёт использования протоколов различного уровня (от

физического до прикладного) в них. Такие сети могут быть использованы для образовательных информационных систем с информацией специального назначения только в рамках территориальной принадлежности к определённому казённому образовательному учреждению. В данной диссертационной работе такие исследования не проводились.

Работа [49] описывает модель нарушителя для применительно к реализации уязвимости класса инъекции SQL-кода. Модель описана на основе дискреционной политики безопасности. В данной модели, аналогично разрабатываемой в диссертационной работе модели нарушителя, принят тот факт, что нарушителем может быть каждый пользователь ОИСИСН, введены утверждения и сформированы условия, при которых определяется истина для определения конкретных предикат.

В работе [50] автор описывает модель нарушителя исходя из уровней мотивации и доступных им ресурсов, тем не менее параметры или критерии для оценки возможностей каждого нарушителя им не рассматривались.

На основе результатов работы [66] можно определять внешний вид зависимостей вероятностей выявления нарушений с различными ограничениями (рис. 1.18, а-в).

Пример модели непосредственного доступа к операционной системе в работе [67] был выполнен на основе аппарата сетей Петри-Маркова, где авторы математически описали все имеющиеся этапы доступа подбора паролей (рис. 1.19) и получили зависимости изменения вероятности доступа от затрачиваемого нарушителем времени (рис. 1.20).

Применительно к исследованию операционных систем, использующих методы виртуальной защиты (виртуальные машины), в работе [68] было определено, что наличие в них уязвимостей позволяет нарушителям осуществлять НСД к гостевым операционным системам и виртуальным машинам, если имеется возможность обработки информации с различным уровнем доступа на одном физическом носителе. Однако, применительно к работе [68], авторами сведения об уязвимостях были взяты из Международной

базы NVD и предложена модель в виде таблицы. Исходя из таблицы, предложенной авторами, можно выбрать уязвимости, относящиеся к уязвимостям, применительно к образовательным информационным системам в таблице 1.4.

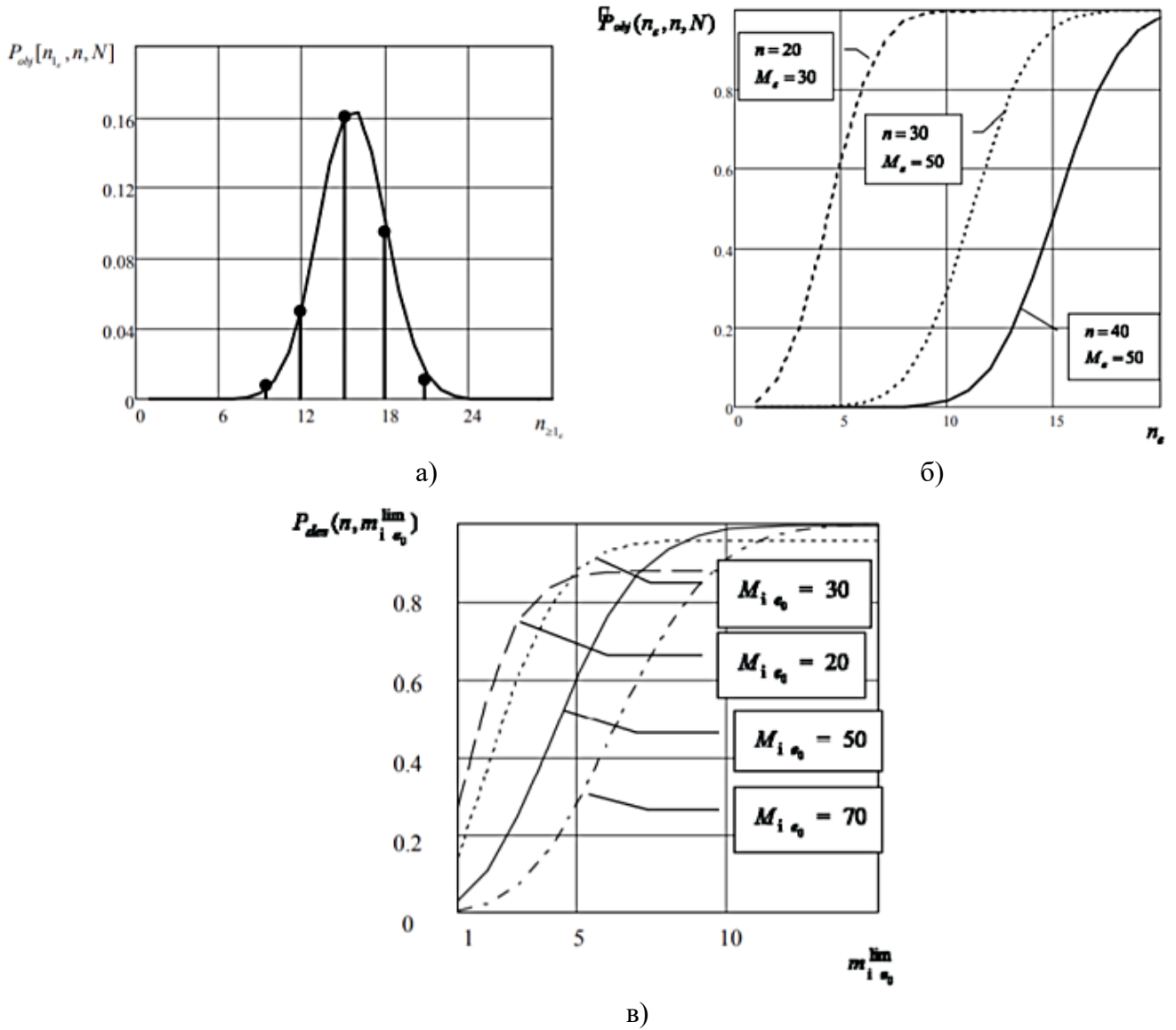


Рисунок 1.18 – Вид зависимостей вероятностей выявления нарушений [66]

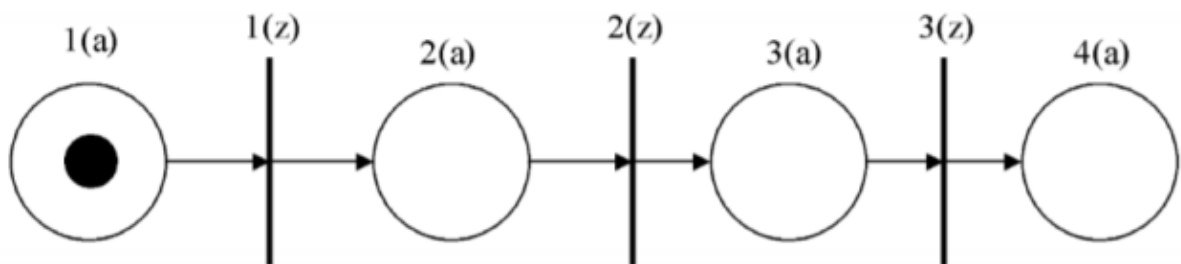


Рисунок 1.19 – Модель этапов доступа к операционной системе на основе сети Петри-Маркова [67]

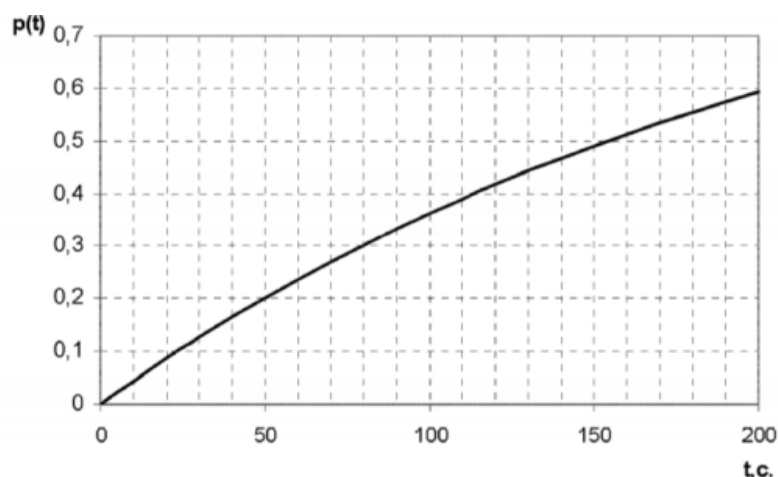


Рисунок 1.20 – Зависимость вероятности доступа от времени на основе модели этапов доступа к операционной системе с использованием сети Петри-Маркова [67]

Таблица 1.4 – Экспертные оценки статического анализа на отсутствие не декларированных возможностей [83]

Задача	Платформа (язык программирования)		
	<i>JVM (Java)</i>	<i>NET (C#)</i>	<i>x86(C/C++)</i>
Возможность декомпиляции	+	+	+
Качество декомпиляции	5	5	2
Поиск уязвимости в декомпилированном тексте	5	5	2
Компиляция исполняемых файлов из полученных исходных текстов	5	4	3
Список функциональных объектов	5	5	3
Список информационных объектов	5	5	-
Матрица связей по информации	4	5	-
Матрица связей по управлению	5	5	3
Трассы вызовов	4	4	-

Таблица 1.4 сформирована на основе выполненной выборки результатов работы [68] для основных элементов, присущих образовательной информационной системе с информацией специального назначения и функционирующей в Федеральном государственном казённом образовательном учреждении высшего образования «Военной академии воздушно-космической обороны имени Г.К. Жукова» (г. Тверь).

Так, например, в ходе исследований был проанализирован гипервизор VMWare. Результаты анализа авторов в работе [68] показали наличие уязвимости CVE-2014-1208. Исходя из этого можно сделать вывод о том, что имеется возможность удаленному пользователю вызвать отказ в обслуживании,

перехватывать и вносить изменения в трафик. Кроме того, наличие уязвимости CVE-2014-1207 дает возможность удаленному пользователю также считывать или изменять произвольные файлы за счет использования виртуальной машины опытным локальным пользователем или администратором.

Тем не менее данная модель требует постоянного совершенствования с точки зрения обеспечения её полным набором возможных угроз. Данная диссертация направлена именно на исследование вопросов, связанных с НСД к гипервизору через виртуальные машины ОИСИСН, их этапов и используемых команд, что расширяет возможности в предложенной модели для оценки виртуального сегмента.

Опираясь на результаты исследования авторов работы [68], необходимо учитывать, во-первых, то, что модель угроз должна включать в себя перечень потенциально возможных угроз (исходя из принятой ПБИ), которые могут воздействовать на информацию в процессе ее обработки, а, во-вторых, учитывать тот момент, что необходимо исследовать преднамеренные угрозы, которые представляют собой целенаправленные действия нарушителя (слушателя) по поиску и использованию уязвимостей. Другими словами, есть необходимость в разработке такой формальной модели нарушителя, которая позволила бы выявлять угрозы НСД к гипервизору и оценивать возможность реализации уязвимостей конкретным нарушителем, обладающим определённой осведомлённостью.

Аналогично работе [68] при моделировании преднамеренных угроз необходимо стремиться к полноте описания всех возможных путей их проникновения, а не к описанию бесконечного множества возможных механизмов их реализации. Применительно к данным диссертационным исследованиям в виртуальных средах необходимо исследовать специфические пути вторжения через виртуальные машины к гипервизору ОИСИСН, использующих виртуальные инфраструктуры системы защиты информации для

выбранных политик безопасности разграничения доступа (дискреционной, мандатной).

На основе представленной в работе [68] структурной вербальной модели угроз были выбраны источники угроз, присущие ОИСИСН в виде выборки угроз.

Данная структура вербальной модели угроз, которая включает в себя сведения об объектах атак (источниках информации), источниках угроз, о структуре угрозы, путях их распространения в виртуальных средах и т.п., была принята в диссертационных исследованиях за основу.

Таким образом, информационная безопасность образовательных информационных систем с информацией специального назначения во многом определяется самой технологией виртуализации. Применительно к ОИСИСН, функционирующей в Федеральном государственном казённом образовательном учреждении высшего образования «Военная академия воздушно-космической обороны имени Г.К. Жукова» (г. Тверь) целесообразно исследовать возможность использования технологии виртуализации на основе использования технологии разграничения доступа «тонкий клиент».

В работе [69] рассматривается новая концепция ПГБ, построенных на технологии АВ.

В этом случае АПВР (гипервизор) представляет собой комплекс программного обеспечения, осуществляющий начальную низкоуровневую инициализацию аппаратных средств с целью создания независимого контекста исполнения, дублирующего в определенной мере аппаратную среду реальной машины [69].

Для реализации НСД к гипервизору через виртуальные машины необходимо иметь знания, подходы или осведомлённость о наборе регистров в виде РОН, S-регистров, C-регистров режимами процессора, MSR-регистров. Кроме того, нарушителю необходимо быть осведомлённым о наборе команд, которые управляют виртуальной машиной. Исходя из того, что ядро

гипервизора отвечает за последовательность осуществления команд (операций) входа в гостевую систему, выхода из неё по некоторой причине и обработки события, послужившего причиной выхода на уровень гипервизора из гостевой системы, НСД к гипервизору даёт нарушителю возможность нарушения конфиденциальности и целостности информации.

Поэтому суть оценки возможностей нарушителей по реализации угроз НСД к гипервизору должна сводиться к разработке таких моделей, которые позволят, исходя из осведомленности нарушителя, определять вероятности обнаружения и устранения активности, происходящей внутри гостевой системы, на уровне обработчиков событий (выходов) или создаваемых профилей разграничения доступа на основе технологии «тонкий клиент». Так как операции входов и выходов выполняются аппаратным обеспечением (на основе выполнения соответствующих инструкций в коде гостевой системы с использованием команд прерывания гостевой операционной системы передавая управление гипервизору). Это повышает безопасность с точки зрения нарушения целостности гостевого программного обеспечения, однако не исключает это нарушение полностью.

Хотя в этом случае события безопасности обрабатываются общим для всех процессов программным комплексом – гипервизором уровня приложений, сам механизм НСД к гипервизору через виртуальные машины осуществляется, минуя механизмы защиты и саму систему защиты. Кроме того, часто гипервизор выполняет часть работы за код гостевой системы, что также повышает возможности нарушителя при условии его НСД к гипервизору через виртуальные машины.

Модель защиты от НСД на базе ПГБ для исполнения программного обеспечения, не модифицируемого штатными средствами, основывается на идеях модификации бинарного кода гостевого программного обеспечения, проверки соответствия данного кода ряду ограничений в момент его загрузки гипервизором для исполнения и контроля исполнения кода за счет обработки вызовов, размещенных в бинарном коде в момент его модификации. Таким

образом, планируется добиться большей управляемости машинного кода. Тем не менее, такой подход невозможно реализовывать в операционных системах, применяемых в образовательных информационных системах с информацией специального назначения.

При разработке формальной модели нарушителя следует особое внимание уделять классу инструкций, который требует контроля со стороны гипервизора, а также запросам разрешения к гипервизору на исполнение этих инструкций. Следует уделять внимание исследованиям следующих инструкций:

- операциям перехода и управления ходом исполнения программы;
- операциям работы со стеком;
- операциям обращения к памяти на запись и чтение.

В зависимости от дисциплины управления безопасностью данный набор команд (инструкций) может значительно расширяться.

Алгоритм работы гипервизора заключается в обработке запросов от исполняемого программного обеспечения, проверки этого запроса, распознавании семантики инструкции. Если инструкция прошла проверку, то гипервизор возвращает управление коду программы, который продолжает выполнение, в противном случае отменяет выполнение кода программы.

Исходя из выводов работы [69] использование комплекса программного обеспечения, осуществляющего начальную низкоуровневую инициализацию аппаратных средств, может быть применено для организации безопасных встраиваемых операционных сред, в случае отсутствия любых аппаратных средств защиты памяти на целевой платформе для целевых встраиваемых систем военного назначения. Таким образом, целесообразно разработать аналогичное программное средство для осуществления разграничения доступа на основе технологии «тонкий клиент», которое позволит адаптировать существующие операционные системы для работы в защищенных средах на основе разграничения доступа по технологии «тонкий клиент».

К недостаткам данного подхода можно отнести увеличение объема бинарного кода после модификации в среднем на 30-40 %, а также саму

необходимость, пусть и однократной, его модификации, которая требует временных затрат.

В работе [70] авторы рассматривают подход, обеспечивающий разграничение доступа в распределённой вычислительной среде. Авторы предложили декомпозицию индикаторной функции контроля применительно к виртуальным соединениям. Обобщённая архитектура распределённой вычислительной среды с внедрёнными средствами разграничения доступа авторами представлена на рисунке 1.21.

Опираясь на то, что архитектура образовательных информационных систем с информацией специального назначения имеет особенности, аналогичные распределённой вычислительной среде [70]:

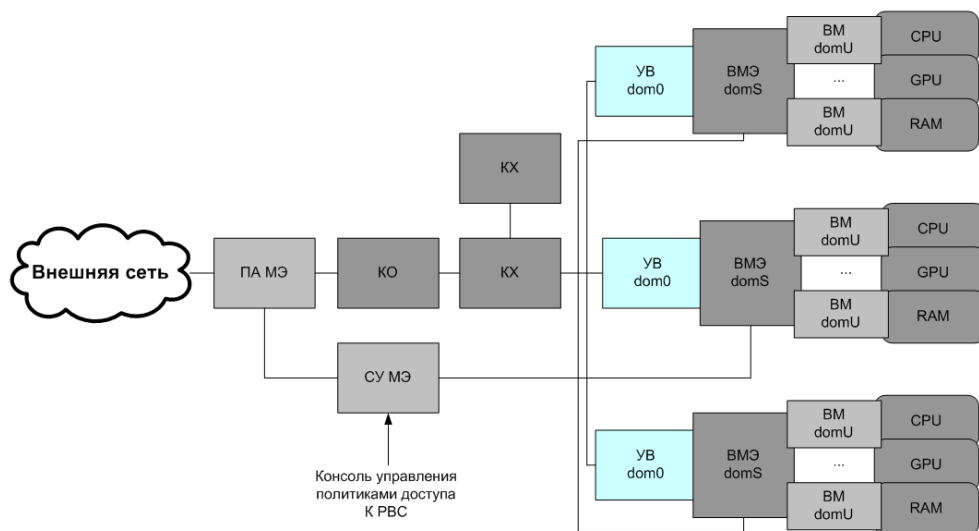


Рисунок 1.21 – Архитектура распределённой вычислительной среды с виртуальными машинами [70]

- 1) имеет множество виртуальных машин (ВМ);
- 2) имеет широкий круг пользователей с различным кругом решаемых задач;
- 3) виртуальные машины разных групп пользователей могут функционировать в рамках одного гипервизора;
- 4) используется широкий спектр общего и системного программного обеспечения;

5) различные аппаратные конфигурации с виртуальными многоядерными процессорами (CPU, GPU), оперативной памятью (RAM), виртуальными межсетевыми экранами (ВМЭ), управлением виртуальным доменом (УВ dom0), системой управления межсетевыми экранами (СУ МЭ), контроллером кластера (КК), контроллером облака (КО), контроллером хранилища (КХ), программно-аппаратным межсетевым экраном (ПА МЭ).

В работе [71] рассматривается совмещение нескольких политик управления доступом, однако разграничение доступа на основе виртуализации авторы не исследовали, что определяет необходимость в выполнении практических экспериментов для возможности использования технологии «тонкий клиент» при защите от НСД к гипервизору через виртуальные машины.

В работе [72] была предложена модель, базируемая на основе стандарта CVSS, определяющая влияние на доступность, конфиденциальность, целостность в виде нечёткого значения параметра отсутствует, частичное, полное. Ввиду этого можно определить, что максимальное количество состояний для одного сетевого объекта определяется как 3^3 , а граф атак можно представить этими состояниями соединёнными рёбрами, описывающими реализации уязвимостей (рис. 1.22).

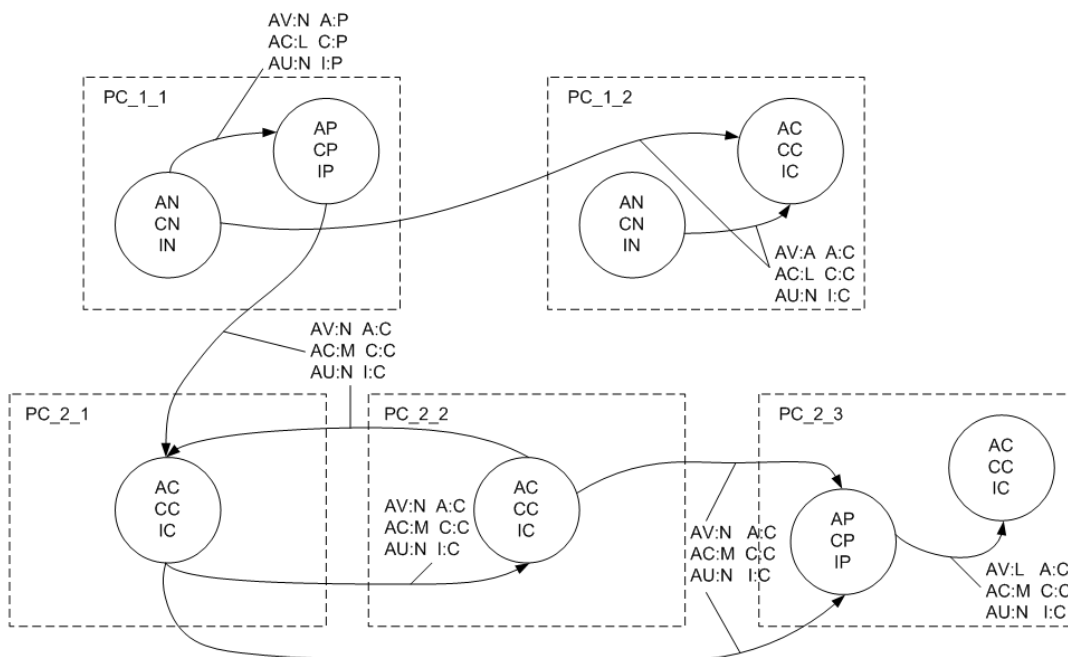


Рисунок 1.22 – Граф атак [72]

В работе [76] автором предложены модели для оценки полноты тестирования программного обеспечения, что даёт возможность использовать данный подход для выявления тестовых ошибок и методов проведения независимых экспертиз.

В работе [77] авторы предлагают описывать процессы выявления уязвимостей программного обеспечения на основе описания каждого этапа и шагов на каждом этапе. Поэтому целесообразно для разработки модели нарушителя детализацию осуществлять аналогично предложенному в работе процессу выявления уязвимостей.

1.3 Анализ подходов для формирования профилей разграничения доступа в образовательных информационных системах

Для определения и анализа подходов для формирования профилей разграничения доступа в образовательных информационных системах с информацией специального назначения необходимо понять функцию назначения гипервизора с технологией виртуализации.

Так, в работах [78-79] выделяются следующие основные функции гипервизора:

- мониторинг виртуальных машин;
- повышение сервисных возможностей компьютеров;
- снижение эксплуатационных расходов компьютеров;
- проверка достоверности использования команд гостевых программ.

Кроме того, исследуется возможность реализации угрозы «тонкого гипервизора» Blue Pill, при которой при запуске операционной системы осуществляется её захват. В это же время аппаратные прерывания, запросы данных и даже системное время будут перехватываться гипервизором, который будет формировать фальшивые ответы.

Ввиду этого должна быть обеспечена доверенная загрузка как к физическому оборудованию, так и к среде виртуализации (защитная мера ЗСВ.5):

- в информационных системах должна обеспечиваться доверенная загрузка серверов виртуализации, виртуальных машин (контейнеров) и серверов управления виртуализацией в соответствии с мерой защиты «Обеспечение доверенной загрузки средств вычислительной техники»;

- доверенная загрузка должна обеспечивать блокирование попыток несанкционированной загрузки гипервизора, хостовой и гостевых операционных систем;

- доверенная загрузка гипервизоров обеспечивается с использованием средств доверенной загрузки, функционирующих на серверах виртуализации;

- доверенная загрузка виртуальных машин (контейнеров) обеспечивается с использованием многокомпонентных средств доверенной загрузки, отдельные компоненты которых функционируют в гипервизорах.

Исходя из работ [78, 79] для BIOS используют гипервизор первого типа в виде СПО, устанавливаемого на сервере виртуализации (рис. 1.23). Для защиты этого типа гипервизора необходимо установить модуль доверенной загрузки базовой системы ввода-вывода, направленного на контроль целостности виртуального оборудования, гостевых операционных систем и файлов в них.



Рисунок 1.23 – Схема доверенной загрузки уровня BIOS виртуальной инфраструктуры с гипервизором первого типа [78]

Второй тип гипервизора необходимо устанавливать на виртуальную машину (рис. 1.24).



Рисунок 1.24 – Схема доверенной загрузки уровня BIOS виртуальной инфраструктуры с гипервизором второго типа [78]

Кроме того, имеются патенты на изобретения, полезные модели и регистрации программ, позволяющие совершенствовать эффективность функционирования гипервизоров, их мониторинг и контроль.

В работе [82] представлен рисунок, схематично отражающий архитектуру функционирования гипервизора первого типа (рис. 1.25).

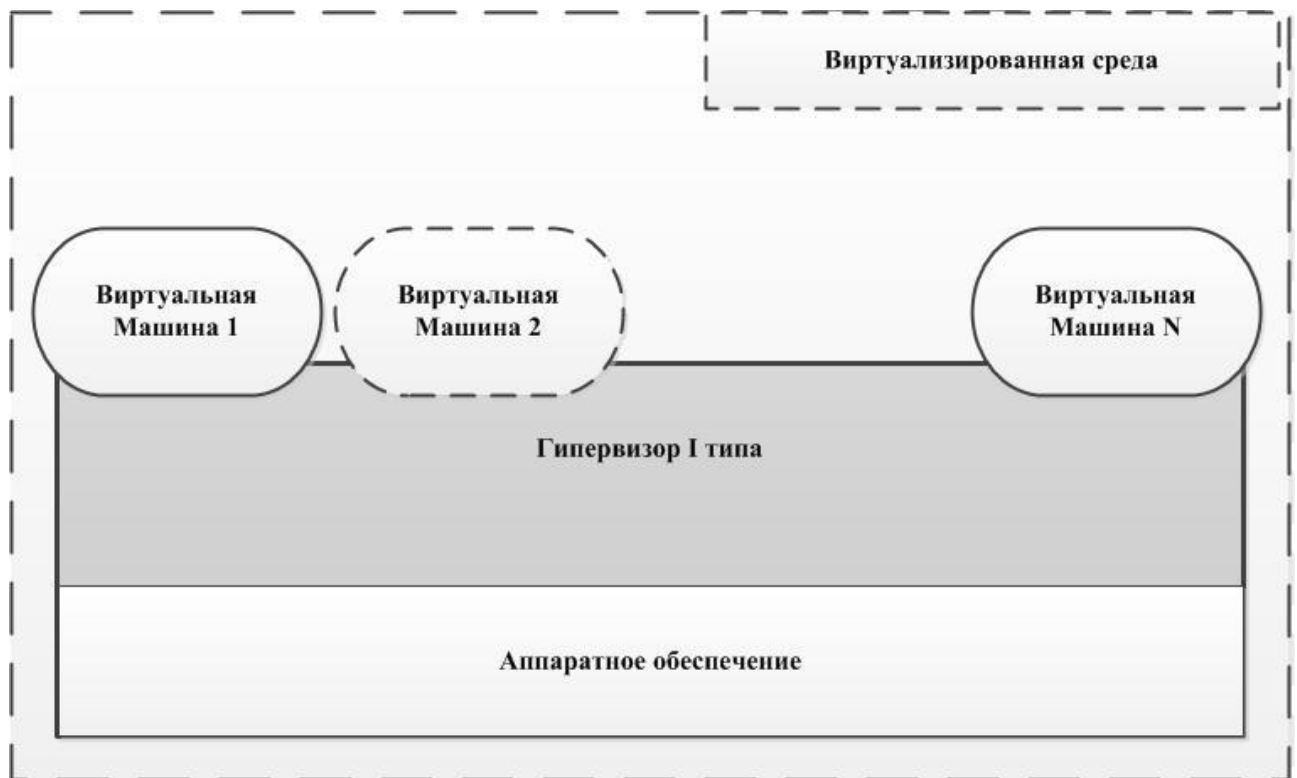


Рисунок 1.25 – Архитектура функционирования гипервизора первого типа [82]

Тем не менее в данных работах не рассматривается возможность реализации уязвимостей на уровне команд гипервизора и их доступности, что определяется уровнем осведомлённости слушателей.

Применительно к оценке возможности выявления уязвимостей программного кода при отсутствии исходных текстов программ посвящена работа [83], где выделен ряд современных систем программирования, которые на настоящий момент времени позволяют провести высококачественную декомпиляцию с соблюдением требований безопасности информации. К таким системам программирования относится байт-код ВМ JAVA (Java Virtual Machine, JVM) в виде следующих языков программирования: Java, NetRexx, Ruby (JRuby), JavaScript (Rhino), Python(Jython), Groovy, PHP (Quercus), Clojure, Scala и др.

Также для платформы .NET, где применяется CLR (Common Language Runtime), возможно исполнение кода, написанного на языках программирования: ASP.NET, C# , Visual Basic .NET, C++/CLI , F# , J# , JScript .NET, Windows PowerShell, ActionScript Virtual Machine и Microsoft P-CODE Virtual Machine). Для этих языков исходные коды компилируются в промежуточное бинарное представление, которое уже на этапе выполнения будет преобразовано в инструкции процессора.

На основе результатов исследования, проводимых в работе [83] на основе экспериментов, была доказана возможность по выявлению уязвимостей кода, а также проведению основных проверок (и формирования отчетов) в рамках статического анализа на отсутствие не декларированных возможностей, которые ими приведены в виде таблицы 1.4 экспертных оценок по 5-балльной шкале.

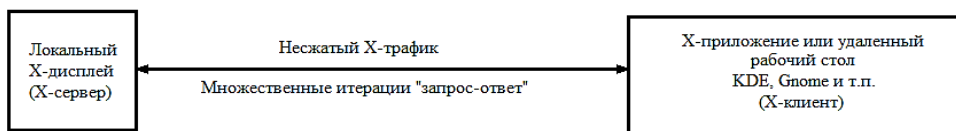
Таким образом, при выполнении поиска и осуществлении экспериментов по выявлению уязвимостей в кодах, реализующих НСД к гипервизору через виртуальные машины информационной системы обучения с информацией специального назначения, целесообразно использовать язык C#.

Применительно к блочной, локальной, глобальной и дискреционной политикам безопасности были изложены результаты исследований в работе [84] в виде их формального задания на основе правил согласования признаков допустимости авторизации, что является основой для разграничения доступа пользователей.

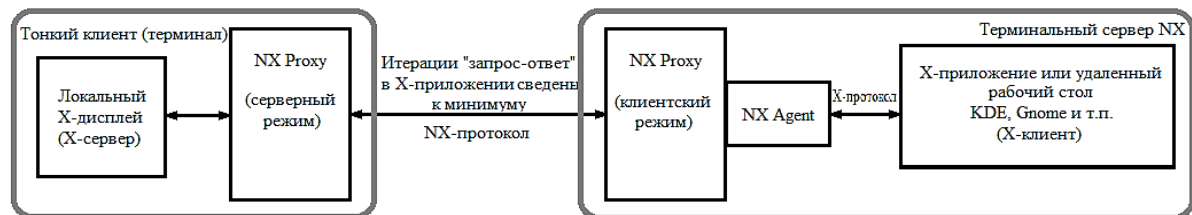
Базируясь на результатах работы [85], можно сделать вывод, что при использовании «тонкого клиента», сервер имеет свои отличительные особенности, которые влияют на работу операционных систем и определяют их конфигурацию. Поэтому при исследовании НСД к гипервизору через виртуальные машины целесообразно определять последовательность действий нарушителя на уровне использования системных команд, что позволит создать более точную модель нарушителя.

В работах [86-87] рассматриваются различные варианты настроек тонкого клиента (рис. 1.26). В работе [88] представлен алгоритм настройки тонкого клиента применительно к беспроводным сетям.

1. Традиционная работа по X-протоколу



2. Использование технологии NX



3. Одновременная работа с разными агентами NX

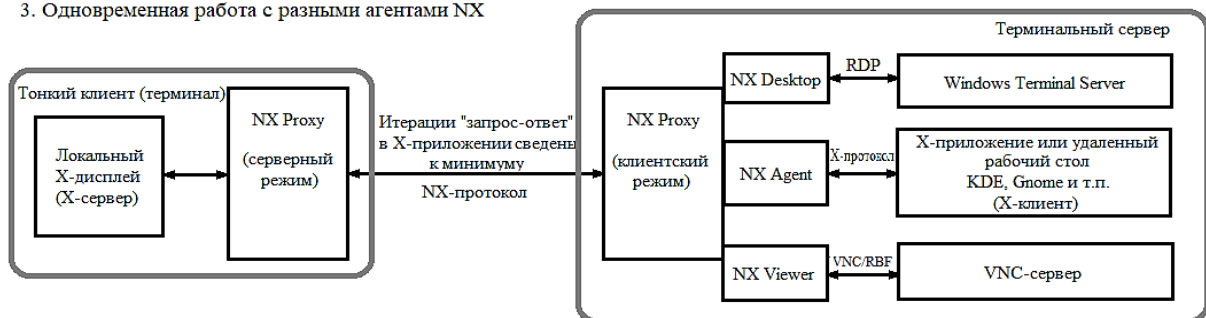


Рисунок 1.26 – Один из вариантов настроек «тонкого клиента» [86]

Исследования ролевого распределения доступа проводились в работе [89], где представлена классификация информации и распределение прав доступа на примере АИС ФССП, основываясь на разделении информации по уровням секретности и категориям. Такой подход проще, чем заполнять неструктурированную матрицу доступа. Тем не менее, применительно к ИС СН, рассматривалась необходимость использования только конфиденциальной информации.

Решение, представленное в «тонком клиенте» для АИС ФССП, обеспечивает комплексную защиту конфиденциальных данных и базируется на трёх уровнях защиты, находящихся в различных функциональных частях трёхзвенного приложения.

Первый уровень защиты обеспечивает разграничение доступа на уровне меню и его элементов, которые обеспечивают переход к витринам данных, и элементов этих витрин (таблиц, графиков, панелей). В этом случае необходимо формировать специальные системные таблицы в базе данных для каждого пользователя (слушателя), а также таблицы с описанием роли для каждого слушателя, что очень затруднительно в ограниченное время настроек. Кроме того, на основе отношений «многие ко многим» должна быть сформирована вспомогательная таблица пользователей и их ролей. В этом случае система настройки доступа пользователей является гибкой и позволяет производить разграничение прав доступа к той или иной части основного меню.

При использовании такого подхода на уровне тонкого клиента обеспечивается разграничение доступа со стороны авторизованных пользователей к ресурсам системы. Разработанное решение позволяет администратору гибко настроить и управлять доступом пользователей на каждом уровне.

Решая актуальную задачу в системах федерального уровня в разграничении доступа к ресурсам, предложенное решение базируется на комплексном подходе к задаче безопасности на трёх уровнях: на уровне

визуального отображения меню, элементов витрин данных, ограждая пользователей от конфиденциальной для них информации; на уровне документов, назначая документам и пользователя метки безопасности и группы доступа; и на уровне безопасности базы данных, где ограничивается доступ непосредственно к объектам базы данных. Таким образом, формирование защищённой системы с гибкими настройками безопасности и с авторизацией через базу данных занимает очень много времени, что не удовлетворяет требованиям, предъявляемым к образовательным информационным системам.

Многие исследования направлены на разработку программ, реализующих отдельные функции хранения данных в системе. Применительно к функционированию программы как тонкого клиента при доступе к системной реализации посредством программной прослойки, выполненной в виде REST API, была посвящена работа [90] в виде свидетельства на регистрацию программы, разработанной на языках программирования JavaScript и Python. Ещё одно свидетельство на регистрацию программы [91] авторы разработали для управления интегрированными между собой серверными модулями на основе предварительной настройки виртуальных машин. Основной составляющей программы является возможность управления сервером для загрузки тонких клиентов, что позволяет ей автоматизировать первичную настройку виртуальной машины, резервное копирование конфигурации виртуальной машины с использованием языков программирования Python и Bash Shell Script.

В работе [92] представлено свидетельство на регистрацию программы, предназначенное для осуществления функциональных возможностей фронтэнд системы в виде тонкого клиента и работы с любым браузером. Кроме того, программа позволяет осуществлять такие процессы, как логирование всех процессов системы и разграничение прав пользователей системы с использованием языков программирования: Bash, SQL, Java, HTML, JavaScript, Python.

В работе [93] представлено свидетельство на регистрацию программы, предназначенной для настройки разрешений в тонком клиенте (на узле Project Web App) с использованием языков программирования: C#, Asp.Net.

Согласно работе [94], **тонкий (браузерный) клиент** позволяет использовать SciVi без установки на компьютер пользователя какого-либо специализированного программного обеспечения, что даёт выигрыш во времени при разграничении доступа для групп слушателей ОИСИСН, что требует более детального внимания при решении задачи разработки средства оценки состояния ОИСИСН в условиях угроз НСД создаёт профили разграничения доступа для отдельных групп слушателей с учётом оценок вновь прибывающего контингента, его компетенций, с ограничениями на состав и содержание предоставляемой им учебной информации в виде программных и технических обеспечений, и своевременностью осуществления профилей настроек за требуемые временные промежутки.

Также при решении этой задачи необходимо учитывать результаты работы [95], в которой предложено в содержимое энергонезависимой флэш-памяти использовать дополнительный блок с клиентской частью программного обеспечения «тонкого клиента».

Схематично взаимосвязь СРД при предоставлении пользователям (субъектам) необходимых ресурсов (объектов) при обучении с использованием информации специального назначения представлена на рисунке 1.27.

Уровень и направленность подготовки слушателей и их компетенции, которые позволили бы реализовать угрозы несанкционированного доступа (НСД) к защищаемой информации в ОИС, в настоящее время могут быть представлены следующим образом на рис. 1.28.

Это негативное обстоятельство может быть преодолено путем использования технологии виртуализации, когда для каждой группы слушателей создается своя виртуальная машина, управляемая общим

гипервизором. Такой подход может быть представлен схематично на рисунке 1.29.

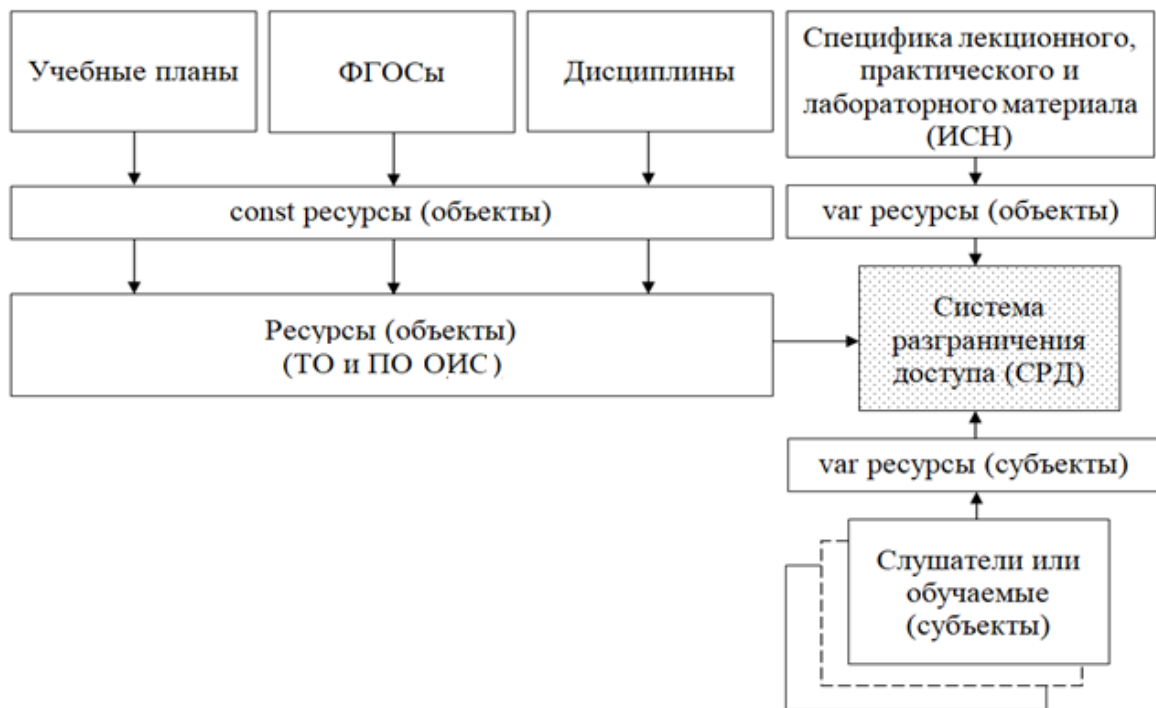


Рисунок 1.27 – Взаимосвязь СРД и ресурсов ОИСИСН



Рисунок 1.28 – СРД для ОИСИСН в настоящее время

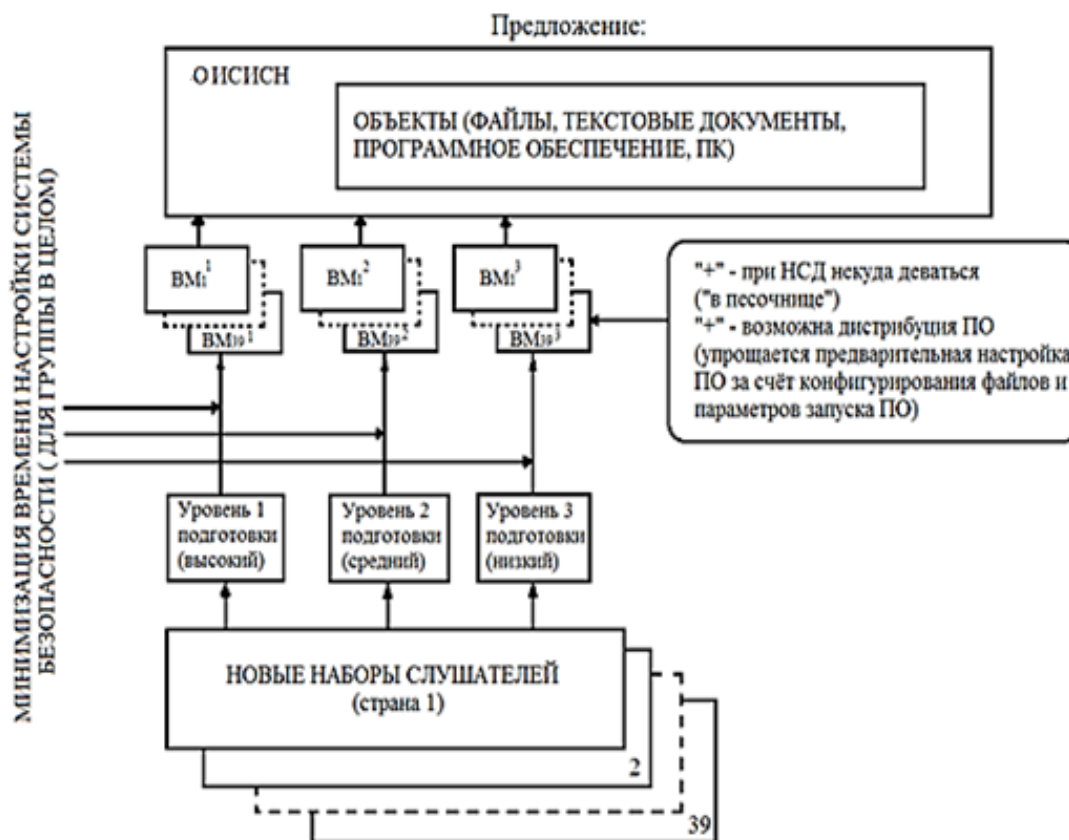


Рисунок 1.29 – Предлагаемая СРД для ОИСИСН

В данном диссертационном исследовании предполагается именно такая система разграничения для информационной системы обучения с информацией специального назначения.

1.4 Выводы

Таким образом, в первой главе был выполнен анализ ОИСИСН, к которым отнесены ИС, применяемые в образовательных учреждениях, принадлежащих к силовым структурам, как объектов исследований, показаны особенности их построения и функционирования, временные характеристики перенастройки образовательных информационных систем с информацией специального назначения в ходе автоматизации обучения различных контингентов слушателей, состава защищаемой информации и применяемого системного и прикладного программного обеспечения. Кроме того, дана характеристика имеющихся в программном обеспечении уязвимостей, применяемых для

эксплуатации эксплойтов, и на этой основе определен состав УБИ, которые могут быть реализованы внутренними нарушителями – пользователями ОИСИСН из состава различных контингентов слушателей. В результате анализа было определено, что для осуществления настроек профилей тонкого клиента по технологии виртуальных машин необходимо учитывать осведомлённость слушателя, так как возникает противоречие между необходимостью предоставления доступа к электронным базам данных с материалом для обучения слушателей разных контингентов, а также к программному и аппаратному (техническому) обеспечению процесса обучения и ограничениями на доступ, обусловленными технологией «тонкий клиент».

Далее проведен анализ существующих моделей нарушителя с точки зрения возможного их применения в ОИСИСН, указаны реализуемые при этом принципы разграничения доступа (дискреционный, мандатный или ролевой) и условия их реализации, дана характеристика способов разграничения, основанных, в том числе, на ведении учётных записей и установлении полномочий средствами операционных систем в ОИСИСН, а также на применении специальных средств и систем разграничения доступа. В результате анализа было показано, что непосредственное применение существующей моделей нарушителей в образовательных информационных системах с информацией специального назначения оказывается неприемлемым, так как в них отсутствует как градация нарушителей, относящихся к категории пользователей, так и сама процедура такой градации. С учетом результатов анализа существующих моделей была разработана описательная модель нарушителя для ОИСИСН, содержащая классификацию нарушителей из состава различных контингентов слушателей, характеристику компетенций и возможностей применения ими известных способов НСД к защищаемой информации в ОИС.

Далее был проведен анализ проработанности темы исследований, в ходе которого было установлено, что, во-первых, исследования, направленные на

разработку как описательных, так и формальных моделей внутренних нарушителей из состава пользователей информационных систем, практически отсутствуют. Как правило, описание внутреннего нарушителя включалось в состав более общей описательной модели угроз безопасности информации без должной детализации его компетенций и возможностей. Следствием этого стало отсутствие моделей количественной оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН, позволяющих учитывать различные уровни компетенций субъектов доступа, а также отсутствие формальной модели и средства выявления угроз НСД к информации в виртуальной среде ОИСИСН, построенной с применением технологии «тонкий клиент», с автоматизацией процесса создания профилей настроек разграничения доступа для слушателей.

Таким образом, **научная задача диссертационного исследования** состоит в решении **противоречий между необходимостью минимизации времени при перенастройке системы разграничения доступа в ОИСИСН из-за частого изменения контингента и компетенций субъектов доступа (слушателей) и отсутствия** моделей и метода, обеспечивающих формирование профилей по разграничению доступа к информации специального назначения, применительно к использованию тонкого клиента на основе виртуальных машин с учётом оценки устойчивости к несанкционированному доступу.

2 Разработка формальной модели нарушителя для ранжирования слушателей на основе преобразования качественных показателей тестирования в количественные оценки их компетенций

Необходимость формальной модели нарушителя для ранжирования слушателей на основе преобразования качественных показателей тестирования в количественные оценки их компетенций обусловлена, во-первых, практической необходимостью автоматизации процесса для быстрой перенастройки СРД для ОИСИСН в ходе смены контингента обучаемых слушателей–пользователей, во-вторых, необходимостью применения формальных процедур оценки нарушителя по его компетенциям и возможностям реализации НСД в условиях ограниченного времени такой оценки и большого количества слушателей.

Опираясь на опыт Федерального государственного казённого образовательного учреждения высшего образования «Военной академии воздушно-космической обороны имени Г.К. Жукова» (г. Тверь) и исходя из того, что восприятие информации является субъективным фактором для каждого слушателя, значение этого фактора усиливается в зависимости от специфики самой информации для иностранных слушателей из разных стран. В этом случае устойчивое функционирование системы разграничения доступа для рассматриваемого процесса определяется правильностью формируемого профиля СРД. Однако имеется следующее противоречие: с одной стороны, необходимо обучаемым предоставлять ресурсы, а с другой стороны, необходимо разграничивать доступ к информации специального назначения.

Это обусловлено, во-первых, тем, что весьма велик контингент слушателей, а состав и содержание курсов обучения для разных групп имеет свои специфические различия, во-вторых, слушатели из разных стран обучаются в одних и тех же оборудованных классах, в связи с чем требуется весьма объемная работа по изменению матрицы дискреционного разграничения

доступа для всего множества субъектов и объектов. В-третьих, такие разграничения должны учитывать осведомленность слушателей, уровень и направленность их подготовки и компетенции, которые позволили бы реализовать угрозы несанкционированного доступа к защищаемой информации в ОИС.

В этих условиях наиболее приемлемым могло бы быть применение технологии «тонкий клиент», однако традиционные способы разграничения доступа, реализуемые при применении такой технологии, основаны на загрузке в терминальное устройство каждого слушателя весьма ограниченной по возможностям версии ОС. Это обстоятельство преодолевается путем использования технологии виртуализации, когда для каждой группы слушателей создается своя виртуальная машина, управляемая общим гипервизором.

Однако далее возникает задача нужной настройки каждой виртуальной машины с учетом анализа уязвимостей процессов разграничения доступа и возможности потенциальных нарушителей по осуществлению НСД к гипервизору через виртуальную машину (ГВМ). Сегодня исследования, направленные на обоснование указанных настроек в зависимости от потребностей в разграничении доступа к защищаемой информации, компетенций и осведомленности слушателей, содержания учебного и иного материала, предоставляемого им в ходе обучения, не проводились.

Как правило, сами ограничения для технологии «тонкого клиента» вводятся администратором экспертно на основе опыта преподавателей и во многих случаях без должного анализа задач обучения, используемого программного и технического обеспечения и тем более возможностей потенциальных нарушителей. Кроме того, традиционные способы разграничения доступа по технологии «тонкий клиент» обуславливают весьма значительные временные затраты на перенастройку оборудования при смене слушателей. Это обстоятельство преодолевается путем использования

технологии виртуализации, когда для каждого слушателя или группы слушателей создается своя виртуальная машина, управляемая общим гипервизором. Однако возникает задача нужной настройки каждой виртуальной машины с учетом анализа уязвимостей процессов разграничения доступа и возможности потенциальных нарушителей по осуществлению НСД к гипервизору через виртуальные машины. Сегодня исследование, направленные на обоснование указанных настроек в зависимости от потребностей в разграничении доступа к защищаемой информации, компетенций и осведомленности слушателей, содержания учебного и иного материала, предоставляемого им в ходе обучения, не проводились.

Вышеизложенное обуславливает важность и значимость задачи построения моделей и метода, обеспечивающих формирование профилей по разграничению доступа к информации специального назначения, для минимизации времени при перенастройке СРД в ОИС, функционирующих на основе тонкого клиента с использованием виртуальных машин в условиях частого изменения контингента и компетенций субъектов доступа (слушателей) на основе оценки устойчивости к НСД.

Однако решение поставленных в диссертационных исследованиях задач должно основываться в первую очередь на формальной модели нарушителя.

Согласно работе [2], формальная модель нарушителя должна включать в себя:

- описание типов, видов, потенциала и мотивации нарушителей, от которых необходимо обеспечить защиту информации в ОИС,
- описание способов реализации УБИ.

Также должны включаться предположения, касающиеся нарушителей (в частности, предположение об отсутствии у нарушителя возможности доступа к оборудованию, сделанному на заказ и применяемому при реализации угрозы, предположение о наличии (отсутствии) сговора между внешними и внутренними нарушителями или иные предположения). Также необходимо

включать любые ограничения, касающиеся определения нарушителей (в частности, исключение администраторов информационной системы или администраторов безопасности из числа потенциальных нарушителей или иные предположения).

Раздел «Актуальные УБИ» содержит описание актуальных угроз безопасности, включающий:

- наименование УБИ;
- возможности нарушителя по реализации угрозы;
- используемые уязвимости ИС;
- описание способов реализации УБИ;
- объекты воздействия;
- возможные результат и последствия от реализации УБИ.

Кроме того, согласно работе [2], проведение экспертной оценки при определении УБИ в ИС проводят по следующим параметрам:

- цели реализации УБИ (мотивация нарушителей);
- типы и виды нарушителей;
- уязвимости, которые могут быть использованы для реализации УБИ;
- способы реализации УБИ;
- степень воздействия УБИ на каждое из свойств БИ;
- последствия от реализации УБИ;
- вероятность реализации УБИ;
- уровень защищенности ИС;
- потенциал нарушителя, требуемый для реализации УБИ (в случае отсутствия потенциала в банке данных УБИ).

Тем не менее, осуществление НСД к гипервизору через виртуальные машины требует особых знаний у нарушителя, причём не только знаний, но и умений воспользоваться ими на уровне специфических команд. Каким образом с определённой достоверностью можно оценить осведомлённость слушателей, не прибегая к их практическим навыкам реализаций, существующих

уязвимостей ОИСИСН? Для этого предлагается вновь поступившим слушателям проходить тестирование, способное оценить их уровень подготовки, что позволит осуществлять распределение их по соответствующим группам. Ввиду этого необходимо разработать специальную систему тестов для получения данных о знаниях слушателей на основе неполноты априорной информации о них.

2.1 Разработка нечёткой модели определения значимости команд при реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН

Анализ работы [83] показал, что целесообразно выделить ряд современных систем программирования, которые на настоящий момент времени позволяют провести высококачественную декомпиляцию с соблюдением требований безопасности информации. В этой же работе авторами была представлена схема общеязыковой исполняющей среды и её связи с деассемблированием (рис. 2.1).

Также, исходя из результатов анализа, представленного в подразделе 1.3, выбор команд должен осуществляться на базе следующих языков программирования: Java, NetRexx, Ruby (JRuby), JavaScript (Rhino), Python(Jython), Groovy, PHP (Quercus), Clojure, Scala, ASP.NET, C# , Visual Basic .NET, C++/CLI , F# , J# , JScript .NET, Windows PowerShell, ActionScript Virtual Machine и Microsoft P-CODE Virtual Machine.

Например, к ключевым и зарезервированным словам языка Java можно отнести слова, представленные в таблице 2.1. Пример команды Java можно привести в следующем виде: *java-verbose Application*.

Эта команда составляет список всех классов, загруженных в память в данном сеансе работы.

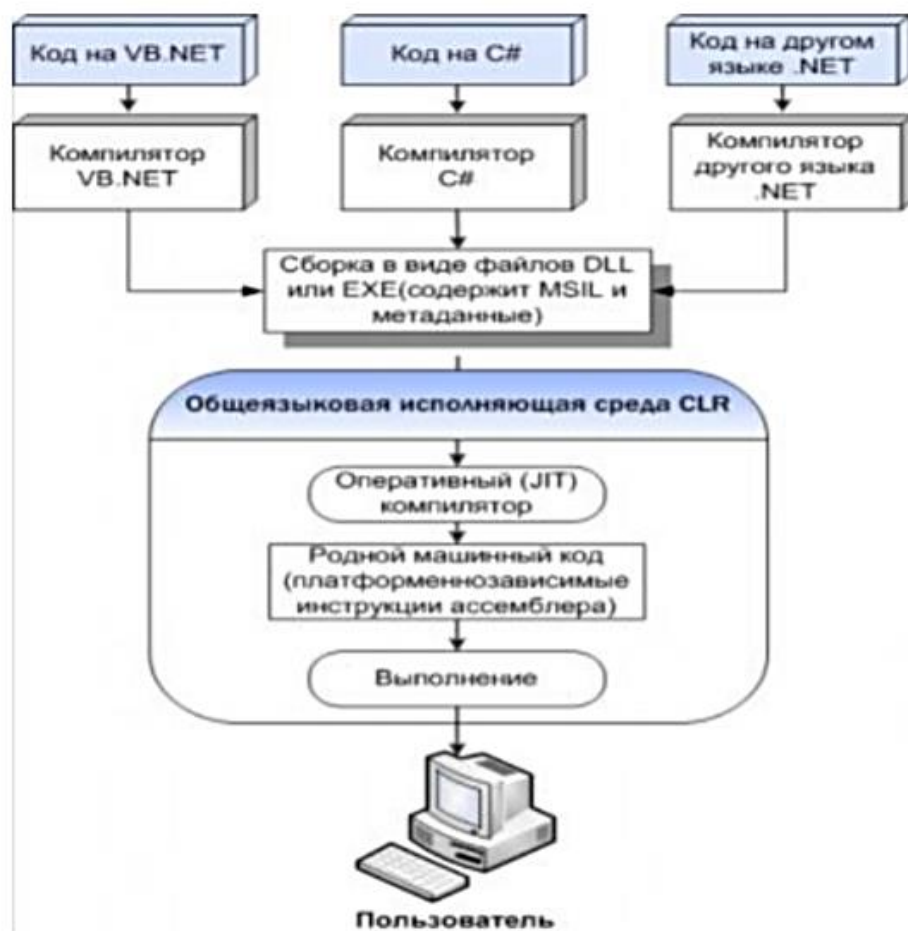


Рисунок 2.1 – Схема общезыковой исполняющей среды и её связи с деассемблированием [83]

Таблица 2.1 – Ключевые и зарезервированные слова языка Java

abstract	continue	for	new	switch
assert	default	goto*	package	synchronized
boolean	do	if	private	this
break	double	implements	protected	throw
byte	else	import	public	throws
case	enum	instanceof	return	transient
catch	extends	int	short	try
char	final	interface	static	void
class	finally	long	strictfp	volatile
const	float	native	super	while

Также к ключевым и зарезервированным словам языка Python можно отнести `and`, `del`, `from`, `not`, `while`, `as`, `elif`, `global`, `or`, `with`, `assert`, `else`, `if`, `pass`, `yield`, `break`, `except`, `import`, `print`, `class`, `exec`, `in`, `raise`, `continue`, `finally`, `is`, `return`, `def`, `for`, `lambda`, `try`.

Как видно из анализа, некоторые ключевые и зарезервированные слова этих языков совпадают. Поэтому при указании нескольких языков принадлежности (например, для `if`) определяет более высокую осведомлённость слушателя в языках.

Аналогично обстоит дело и с остальными указанными языками программирования, которые пересекаются друг с другом по назначению и роли использования их в коде, а также имеют свои специфические особенности. Ввиду этого в тестовый набор должны быть включены все команды и ключевые слова из языков программирования, указанных в таблице 1.4: Java, C#, C/C++. Именно из набора этих языков возможно качественное деассемблирование и поиск уязвимостей при НСД к гипервизору через виртуальные машины. Так, в таблице 2.2 представлены ключевые слова языка программирования C#, а в таблице 2.3 представлены ключевые слова языка программирования C++.

Таким образом, предлагаются наборы тестов, которые, помимо множества ключевых слов из различных языков программирования (таблицы 2.1-2.3), должны содержать команды, функции, процедуры, утилиты или их параметры, включающие информацию о программном обеспечении, знание которой нарушителем определяет его осведомлённость о возможности реализации угрозы НСД к гипервизору через виртуальные машины.

Ввиду этого выбор команд был выполнен экспертами по НСД к гипервизору через виртуальную машину. Результаты экспертов по каждой команде в ходе диссертационных исследований предложено осуществлять методом оценки входных лингвистических переменных с различными значениями их важности. Таким образом, место нечёткой модели определения значимости команд, основанного на предложенном в ходе диссертационного

Таблица 2.2 – Ключевые слова языка программирования C#

Floor	Округление до меньшего целого	double	Floor (double x)
IEEERemainder	Остаток от деления	double	IEEERemain (double x, double y)
Log	Натуральный логарифм	double	$\log_e x$ записывается как Log(x)
Log10	Десятичный логарифм	double	$\log_{10} x$ записывается как Log10(x)
Max	Максимум из двух чисел	перегружен	Max(x, y)
Min	Минимум из двух чисел	перегружен	Min(x, y)
PI	Значение числа π	double	3,14159265358979
Pow	Возведение в степень	double	x^y записывается как Pow(x, y)
Round	Округление	перегружен	Round(3.1) даст результате 3 Round(3.8) даст в результате 4
Sign	Знак числа	int	аргументы перегружены
Sin	Синус	double	Sin(double x)
Sinh	Гиперболический синус	double	Sinh(double x)
Sqrt	Квадратный корень	double	\sqrt{x} записывается как Sqrt(x)
Tan	Тангенс	double	Tan(double x)
Tanh	Гиперболический тангенс	double	Tanh(double x)

Таблица 2.3 – Ключевые слова языка программирования C++

asm	auto	bool	break
case	catch	char	class
const	const_cast	continue	default
delete	do	double	dynamic_cast
else	enum	explicit	export
extern	false	float	for
friend	goto	if	inline
int	long	mutable	namespace
new	operator	private	protected
public	register	reinterpret_cast	return
short	signed	sizeof	static
static_cast	struct	switch	template
this	throw	true	try
typedef	typeid	typename	union

исследования методе, и формальной модели нарушителя, исходя из определения команд и последовательности их выполнения для осуществления НСД в ОИСИСН, может быть представлено следующим образом (рис. 2.2).

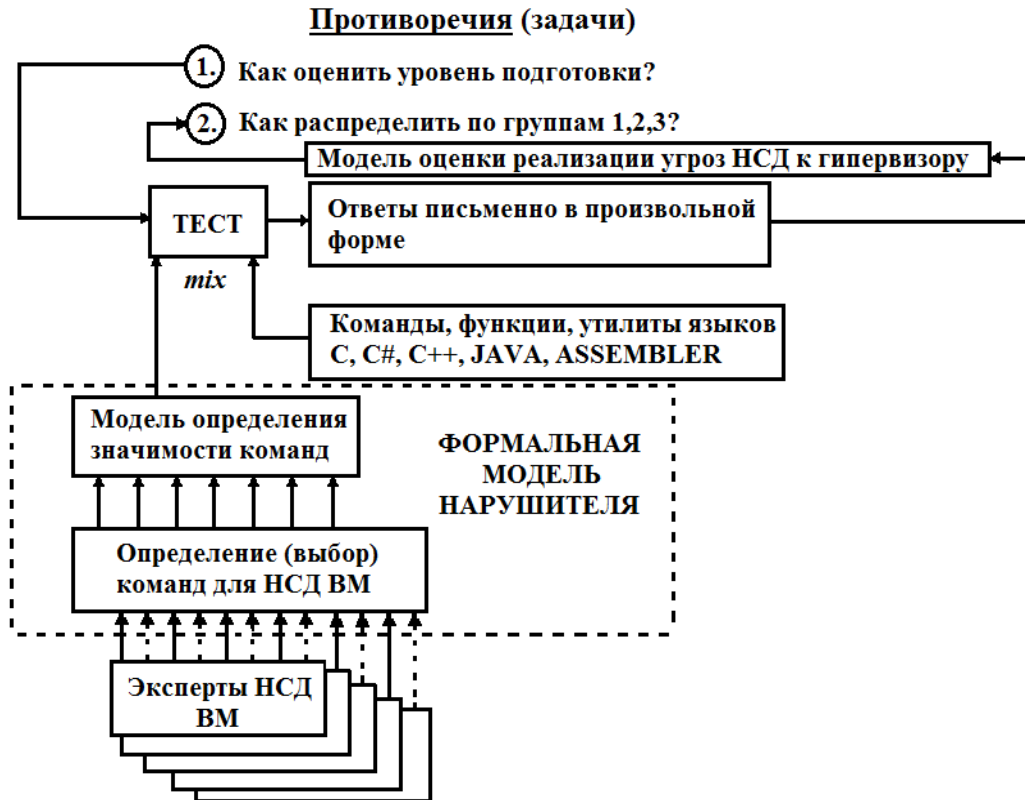


Рисунок 2.2 – Место нечёткой модели определения значимости команд и формальной модели нарушителя в процессе исследования

Исходя из того, что любая команда определяется множеством, характеризующимся набором любого языка программирования с возможным использованием системных и API-функций, позволяющих в различной мере осуществлять тот или иной доступ к гипервизору, минуя защиту операционной системы, а также сама последовательность осуществления НСД к гипервизору через виртуальные машины (как самих команд, так и этапов, на которых они используются) чётко не определена, это вносит дополнительную неопределенность в оценку их важности.

Ввиду этого в диссертационных исследованиях вводятся понятия нечёткой лингвистической переменной входа **УРОВЕНЬ ВАЖНОСТИ (ВАЖНОСТЬ, ЗНАЧИМОСТЬ)** и её лингвистические значения (например, команда «НВ», «СВ», «В» или «ОВ») при осуществлении НСД к гипервизору

через виртуальные машины. Эти лингвистические значения входа до начала тестирования слушателей были определены субъективно каждым экспертом в отдельности. Из-за субъективности оценки нечётких лингвистических значений входа (команда «НВ», «СВ», «В» или «ОВ») было предложено использовать метод нечёткой логики, позволяющий найти функциональные зависимости между качественными и количественными соотношениями применительно к показателям важности команд и их частоты использования.

Для построения функций принадлежности были определены числа, оценивающие степень принадлежности к нечёткому терм-множеству «НВ», «СВ», «В» или «ОВ» по каждой команде, а также были обработаны результаты от двадцати экспертов. Эти субъективные данные явились основой для определения функций принадлежности с левой и правой границами терм-множества переменной входа `input1` в отдельности для каждого лингвистического значения «НВ», «СВ», «В» или «ОВ», а также для функций принадлежности с левой и правой границами терм-множества переменной входа `input2` в отдельности для каждого лингвистического значения «редко», «средне» и «часто» на основе правил принятия решений с использованием метода Mamdani.

Так, исходя из того, что имеется важность A (`input1`) по реализации команд, для которых их количество соответствует набору из N команд, используемых в тесте, вид и значение функции принадлежности применительно к «НВ» предлагается рассчитывать следующим образом. Во-первых, был выполнен экспертный опрос относительно каждой отдельной команды из множества N , обеспечивающий важность A на отдельном этапе её выполнения.

Например, если сделать выборку команд, определяемую количеством $N=11$, и привлечь к процедуре их оценки экспертов в количестве 20 (двадцати) человек, то, исходя из рассмотренных исходных данных характеристики функции принадлежности лингвистических значений «НВ», можно определить следующие её левые и правые граничные значения, а также предложить

использовать трапецевидную функцию принадлежности. Использование специфической формы трапецевидной функции принадлежности позволит уменьшить размытость границ, что повысит детерминированность итоговых значений выходной функции принадлежности.

Исходя из предложенных экспертами команд, функций, утилит для их выбора *впервые предложен новый подход для формирования границ функций принадлежности* лингвистических значений входа «**НВ**», «**СВ**», «**В**», «**ОВ**». В ходе эксперимента выбран набор из 11 команд, предложенный 20 экспертами. Каждый эксперт определил каждую команду к категории «**НВ**». Таким образом, запись вычислений для показателя качества «**НВ**» должна быть определена на основе следующих исходных данных. Так как имеется набор команд с 0 по 10, каждый эксперт должен определить условия, к которым та или иная команда относится к выбранной категории «**НВ**». Так были получены следующие результаты:

0-ую команду отметили все 20 экспертов;

1-ую команду отметили 16 экспертов;

со 2-ой по 10-ую команды не отметил ни один эксперт.

Для этого с использованием метода нечёткой логики, было получено следующее уравнение:

$$x_1 = \frac{0|20 + 1|16 + 2|0 + 3|0 + 4|0 + 5|0 + 6|0 + 7|0 + 8|0 + 9|0 + 10|0}{20 + 16} =$$

$$= \frac{0 \cdot 20 + 1 \cdot 16 + 2 \cdot 0 + 3 \cdot 0 + 4 \cdot 0 + 5 \cdot 0 + 6 \cdot 0 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 0 + 10 \cdot 0}{36} = \frac{16}{36} = 0,444.$$

Также при определении функции принадлежности «**СВ**» и её граничных значений были получены следующие результаты:

0-ую команду не отметил ни один эксперт;

1-ую команду отметили все 20 экспертов;

2-ую команду отметили 8 экспертов;

3-ую команду отметил 1 эксперт;

с 4-ой по 10-ую команды не отметил ни один эксперт.

Для этого, согласно теории нечёткой логики, было получено следующее уравнение:

$$x_2 = \frac{0|0+1|20+2|8+3|1+4|0+5|0+6|0+7|0+8|0++9|0+10|0}{20+8+1} = \frac{39}{29} = 1,345.$$

Также при определении функции принадлежности «**B**» и её граничных значений были получены следующие результаты:

0-1, а также с 7-ой по 10-ую команды не отметил ни один эксперт;

2-ую команду отметили 6 экспертов;

3-ую команду отметили 8 экспертов;

4-ую и 5-ую команды отметили все 20 экспертов;

6-ую команду отметили 5 экспертов.

Для этого, согласно теории нечёткой логики, было получено следующее уравнение:

$$x_3 = \frac{0|0+1|0+2|6+3|8+4|20+5|20+6|5+7|0+8|0+9|0+10|0}{6+8+20+20+5} = \frac{246}{59} = 4,169.$$

Также при определении функции принадлежности «**OB**» и её граничных значений были получены следующие результаты:

с 0-ой по 2-ую команды не отметил ни один эксперт;

3-ую команду отметили 3 эксперта;

4-ую команду отметили 6 экспертов;

5-ую команду отметили 9 экспертов;

с 6-ой по 10-ую команды отметили все 20 экспертов.

Для этого, согласно теории нечёткой логики, было получено следующее уравнение:

$$x_4 = \frac{0|0+1|0+2|0+3|3+4|6+5|9+6|20+7|20+8|20+9|20+10|20}{3+6+9+20+20+20+20+20} = \frac{878}{118} = 7,441.$$

Количественное значение важности команды целесообразно определить в виде обобщённого показателя следующим образом:

$$\begin{aligned} x &= 0.444|20+1.345|20+4.169|20+7.441|20 = \\ &= \frac{8.88+26.9+83.38+148.82}{20+20+20+20} = \frac{267,98}{80} = 3,349. \end{aligned}$$

В данном подходе предлагается нормировать значения, что даёт возможность использовать значения каждой функции принадлежности в диапазоне от 0 до 1, а также определять в этом диапазоне значения функций принадлежности для оценки границ (левой и правой). Ввиду этого для лингвистического терм-множества переменной входа получены следующие граничные значения: «НВ» [0, 0.06]; «СВ» [0.06,0.18]; «В» [0.18, 0.56]; «ОВ» [0.56, 1]. Следовательно, для определения значимости команд в нечёткой модели NSD_SV.fis среды MATLAB сформированы функции принадлежности вида $mf1 \rightarrow \text{trampf} \rightarrow [0 \ 0 \ 0.06 \ 0.06]$; $mf2 \rightarrow \text{trampf} \rightarrow [0.06 \ 0.06 \ 0.18 \ 0.18]$; $mf3 \rightarrow \text{trampf} \rightarrow [0.18 \ 0.18 \ 0.56 \ 0.56]$; $mf4 \rightarrow \text{trampf} \rightarrow [0.56 \ 0.56 \ 1 \ 1]$, что позволяет снизить неопределённость при выборе команд для формальной модели нарушителя для НСД в ИСО с ИСН к гипервизору через VM.

Рассчитанные функции принадлежности входной переменной input1 представлены на рис. 2.3.

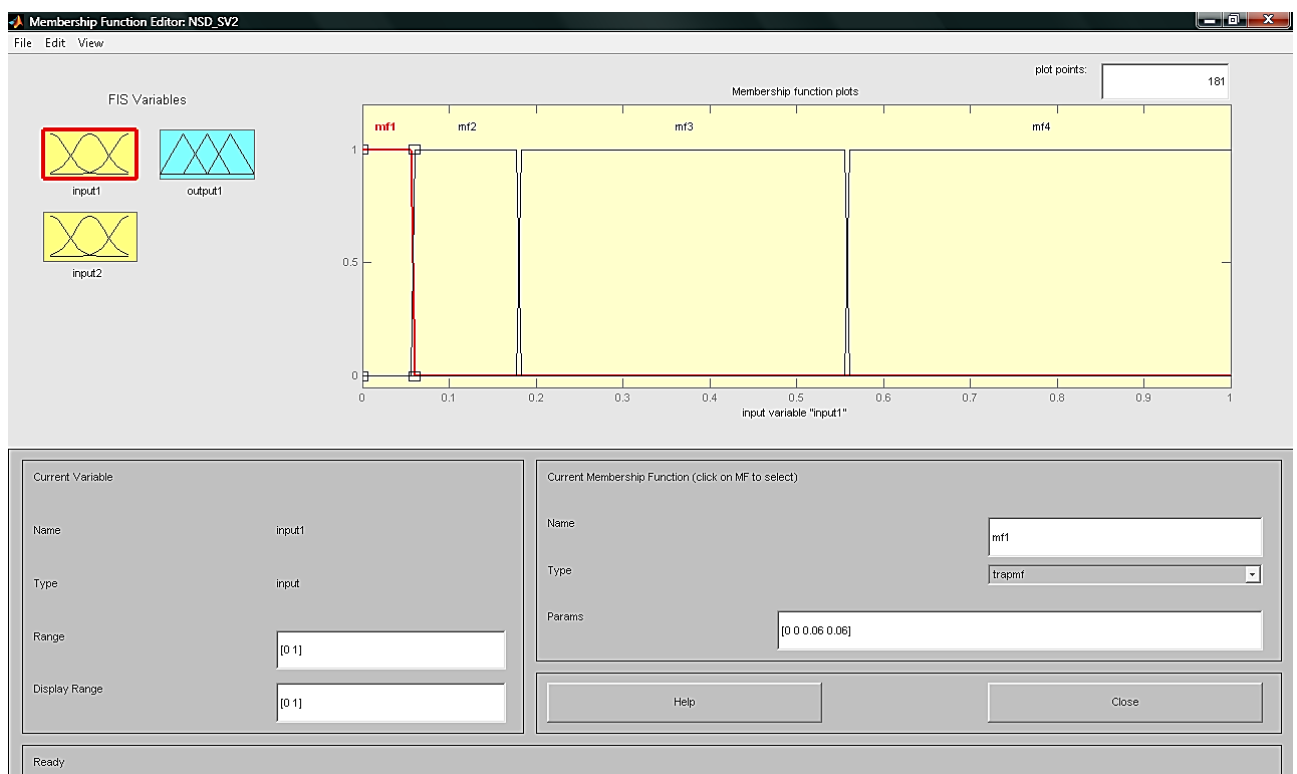


Рисунок 2.3 – Функции принадлежности в MATLAB «не важна» (mf1), «слабо важна» (mf2), «важна» (mf3) или «очень важна» (mf4)

Выбор трапецеидальных форм функций принадлежности снижает нечёткость для пограничных значений в полученных результатах.

Результаты функционирования нечёткой модели оценивания возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН, исходя из взаимосвязи лингвистических значений входа «НВ», «СВ», «В» или «ОВ», частоты В (input2) лингвистических значений входа по реализации команд «редко», «средне» и «часто» используемой команды и лингвистических значений выхода output1 «нВ», «сВ» и «вВ» НСД к гипервизору через виртуальные машины, представлены на рис. 2.4 - 2.6.

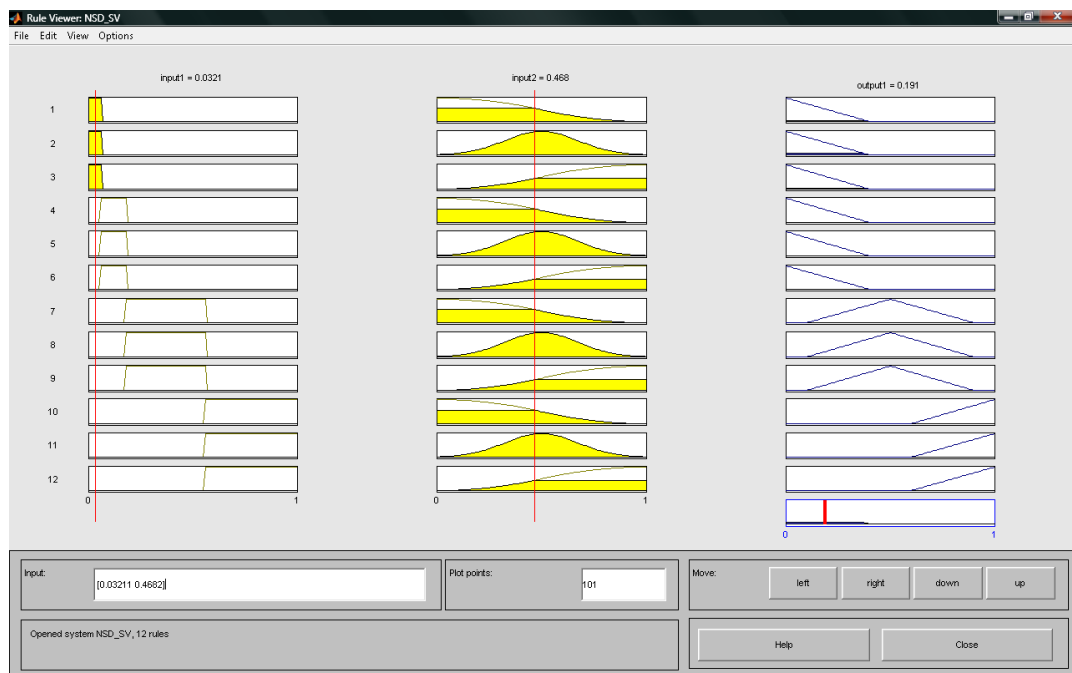


Рисунок 2.4 – Результаты моделирования функции принадлежности «невероятный»

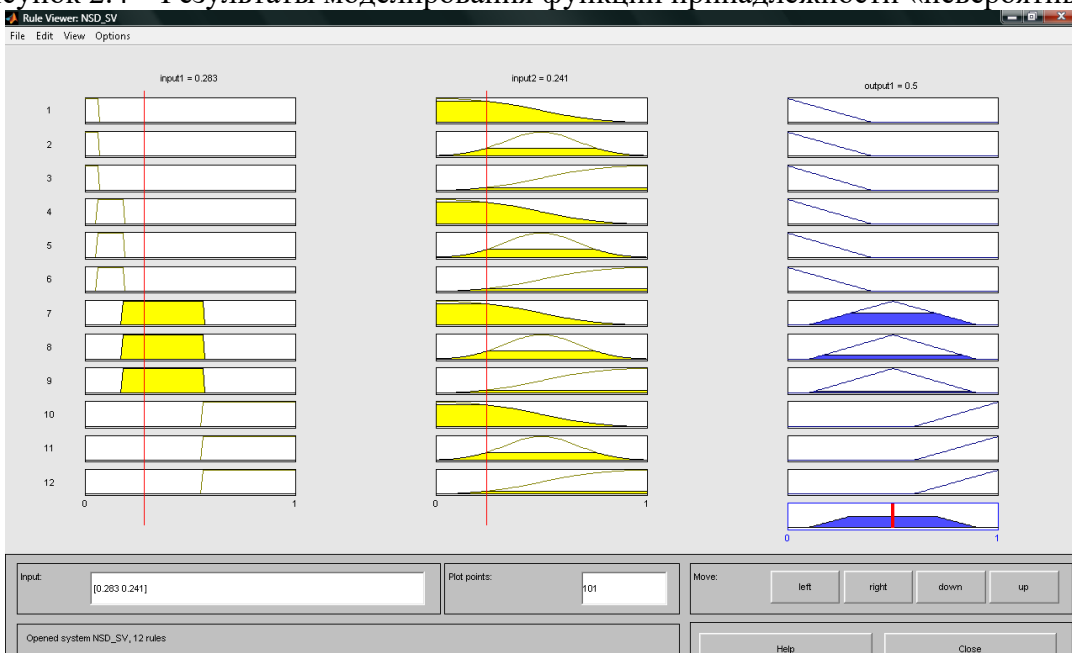


Рисунок 2.5 – Результаты моделирования функции принадлежности «средневероятный»

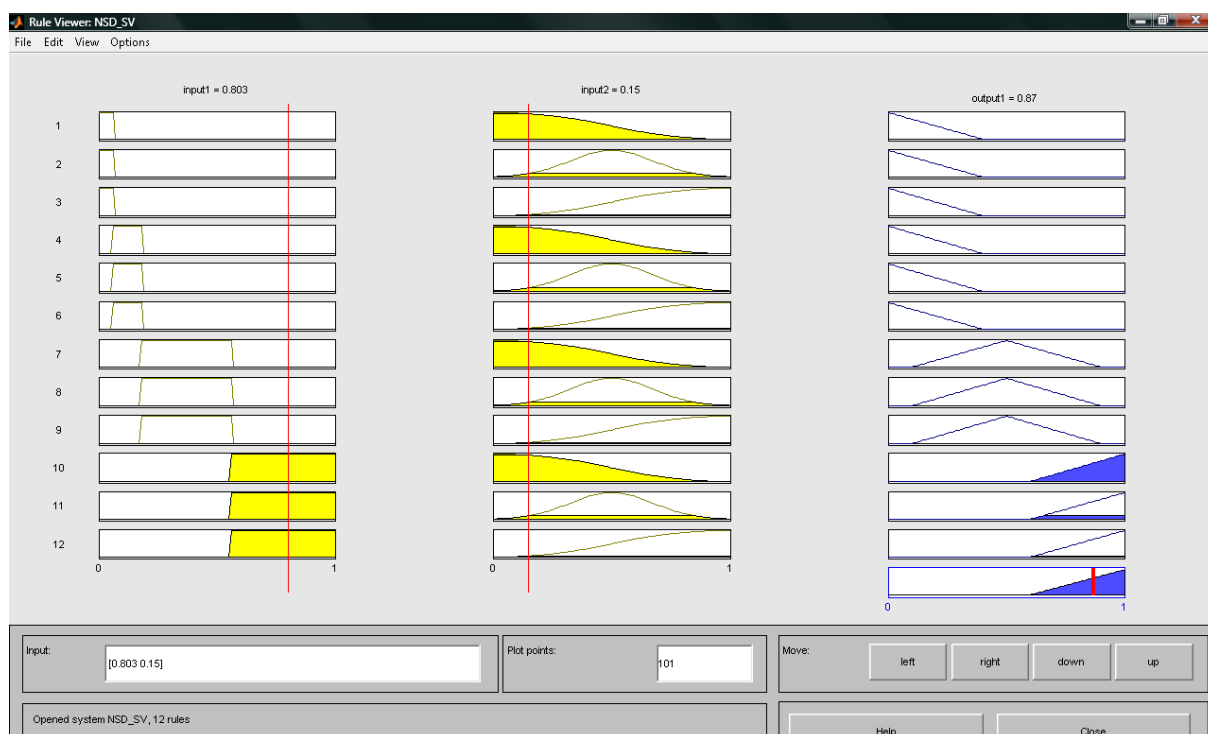


Рисунок 2.6 – Результаты моделирования функции принадлежности «высоковероятный»

Таким образом, в среде MATLAB разработана нечёткая модель (*NSD_SV.fis*) определения значимости команд НСД к гипервизору через виртуальные машины в ОИСИСН на основе модифицированного подхода по формированию функций принадлежности, описывающих количественно уровни компетенций слушателей. Нечёткая модель позволяет оценить значимость команд для НСД к гипервизору через виртуальные машины на основе оценки лингвистических значений выхода «нВ», «сВ» и «вВ» с использованием правил принятия решений.

Правила принятия решений, осуществляющих дефаззификацию для получения результирующего вывода в виде нахождения чёткого значения множества output1 «невероятный», «средневероятный» и «высоковероятный» НСД к гипервизору через ВМ на основе использования метода центра сумм, представлены на рис. 2.7.

Результирующий вывод в виде нахождения значения множества output1 «невероятный» определяется как значение *оценки важности команды для НСД к гипервизору через виртуальные машины в ОИСИСН*, равное 0.191.

Результирующий вывод в виде нахождения значения множества output1 «средневероятный» определяется как значение *оценки важности команды для НСД к гипервизору через виртуальные машины в ОИСИСН*, равное 0.5.

Результирующий вывод в виде нахождения значения множества output1 «высоковероятный» определяется как значение *оценки важности команды для НСД к гипервизору через виртуальные машины в ОИСИСН*, равное 0.863.

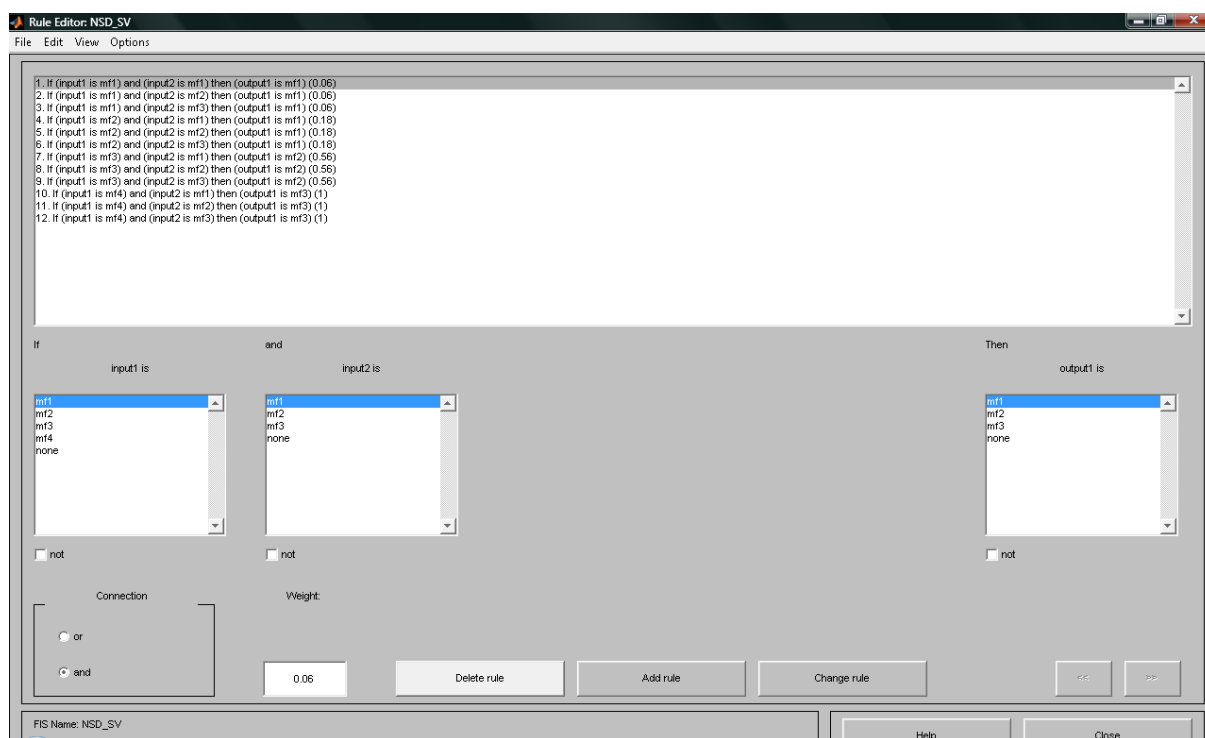


Рисунок 2.7 – Правила принятия решения при моделировании функции принадлежности «невероятный», «средневероятный» и «высоковероятный»

Следует отметить тот факт, что полученные на основе нечёткой модели оценивания важности команды для НСД к гипервизору через виртуальные машины в ОИСИСН результаты не противоречат реальным условиям оценки взаимосвязи между значимостью команд для реализации НСД к гипервизору через виртуальные машины.

То есть, можно сделать вывод, что использование методов нечеткой логики для оценки взаимосвязи между значимостью команд и их частотой использования для реализации НСД к гипервизору через виртуальные машины на основе экспертного опроса допустимо для апробированных в ходе

диссертационных исследований в виде зависимостей функций принадлежности для лингвистических значений входа с использованием новых информационных технологий в среде MATLAB.

Исходя из полученных результатов исследований в среде SIMULINK пакета MATLAB разработана нечёткая модель NSD_SV.fis.

Выбор функции принадлежности в трапециевидной форме позволяет снизить неопределённость от лингвистических терм-множеств переменной входа к лингвистическому терм-множеству переменной выхода.

В предложенной нечёткой модели определения важности команд использован метод центра сумм. На основе обработки экспертных оценок, и основанная на ней формальная модель нарушителя, в отличие от существующих, учитывает специфику технологии «тонкого клиента» на основе виртуальных машин и позволяет формировать качественные и количественные параметры с их взаимосвязями для дальнейшего обеспечения ранжирования слушателей по отдельным группам на основе оценённых компетенций для формирования профилей СРД.

2.2 Формальная модель нарушителя в образовательных информационных системах с информацией специального назначения

Исходя из результатов исследований в работах [49–84] для осуществления НСД одной из последних стадий на этапе сбора информации является поиск нарушителями уязвимостей. На этом этапе могут быть использованы как автоматизированные, так и ручные средства по определению слабого звена ОИСИСН, которое может быть использовано для осуществления конкретного вида НСД.

Кроме того, для корректной привязки уровней компетенций нарушителей к угрозам безопасности информации был проведен анализ таких угроз с учетом

известных, содержащихся в электронных базах уязвимостей CVE и ФСТЭК России уязвимостей гипервизора и виртуальных машин [2, 114–126].

Применительно к определению уязвимости для реализации угрозы НСД к гипервизору через виртуальные машины нарушителю необходимо знать, не только какое программное обеспечение установлено на узле, но и какая его версия. При этом главной задачей НСД является подбор информации об уязвимостях и наличии специальных программ, которые используют уже существующую уязвимость («эксплойт»). В качестве таких автоматизированных средств могут быть использованы программные средства типа «Shadow Security Scanner», «nmap», «Retina» и т.д.

Тем не менее использование общего и специального программного обеспечения в исследуемой ОИСИСН определяется учебным процессом. Поэтому формирование модели злоумышленника (нарушителя) должно учитывать все имеющиеся пути обхода системы защиты информации и операционной системы на уровне использования команд на системном уровне.

Это будет определяться уровнем подготовки (осведомлённости) слушателей, временем, проводимым в рамках обучения на ОИСИСН и знанием алгоритма реализации уязвимостей применительно к операционным системам и системам защиты информации, осуществляющих технологию «тонкий клиент».

Разработка «эксплойтов» [79, 105] предполагает наличие уязвимостей в программах системного уровня. В этом случае слушатель-нарушитель должен либо обнаружить новую уязвимость, либо воспользоваться уже известной. Методы поиска новых уязвимостей включают отыскание некорректного кода в исходном тексте программных систем, отправку неожиданных данных приложению и изучение программы на предмет наличия логических ошибок. В процессе поиска уязвимости анализируются следующие аспекты:

доступность исходного текста программы;

сколько людей уже знакомы с исходным текстом и кто эти люди;

имеет ли смысл тратить силы на автоматизированное генерирование случайных исходных данных для программы;

сколько времени потребуется для организации тестовой среды.

Разработка «эксплойтов» [62, 72, 79, 105] ориентирована на наиболее распространённые классы ошибок, например, переполнение стека, затирание кучи, атаки на форматную строку, переполнение целых чисел и возникающие гонки. Тем не менее осуществление НСД к гипервизору через виртуальные машины, требует знаний более высокого уровня, то есть знаний специфических функций или команд на системном уровне. К сожалению, контроль того или иного НСД возможен уже после непосредственного проникновения в ОИС, включая ОИСИСН. Таким образом, первоначально должна быть создана база для дальнейших атак (получены права пользователя root), и только после этого реализуется проникновение на другие узлы. Этот подход используется для скрывания или затруднения обнаружения фактов НСД.

Исходя из существующих исследований и фактов поиска уязвимостей на основе общего и специального программного обеспечений, имеющих возможность для деассемблирования, предложена следующая структура формальной модели нарушителя (рис. 2.8).

Структура формальной модели нарушителя позволяет учитывать специфику технологии тонкого клиента на основе виртуальных машин и формировать качественные и количественные параметры с их взаимосвязями, что разрешает в некоторых случаях снижать параметры неопределённости до нуля для дальнейшего обеспечения ранжирования слушателей по отдельным группам на основе оценённых компетенций для формирования профилей СРД.

Поэтому в дальнейшем предлагается формировать тесты по следующим принципам. Во-первых, тесты должны включать наборы команд из разных языков программирования с возможными на них ответами: не знаю, знаю (без указания языка программирования), знаю (с указанием языка программирования). Такой набор ответов о знаниях команд в виде

качественных показателей позволит оценивать осведомлённость слушателей о знаниях ими тех или иных языков программирования.

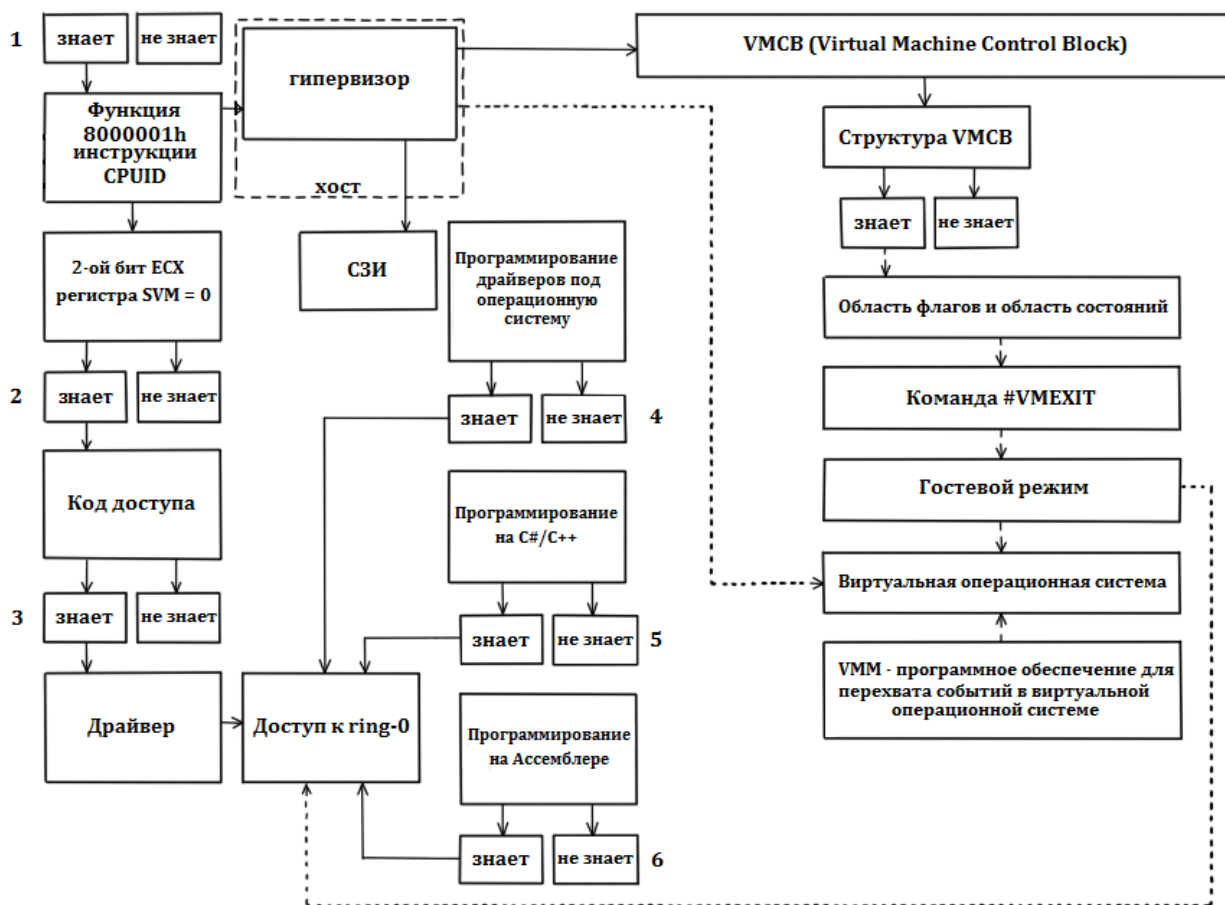


Рисунок 2.8 – Структура формальной модели нарушителя

Во-вторых, тесты должны включать отдельные структуры команд для описания их назначения. В этом случае ответы могут содержать следующее: не знаю, знаю (описание общего назначения команды), знаю (описание назначения: как самой команды, так и её аргументов). В-третьих, тесты должны включать коды из различных программ с имеющимися в них ошибочными командами. В этом случае ответы могут содержать следующее: не знаю; знаю, в какой команде ошибка; знаю, как исправить код программы на правильный. Такой набор ответов о знаниях команд в виде качественных показателей позволит оценивать осведомлённость слушателей об уровнях знаний конкретных языков программирования.

2.3 Разработка нечёткой модели оценивания возможности по реализации угроз НСД в ОИСИСН к гипервизору через виртуальные машины на основе модифицированного подхода по формированию функций принадлежности, описывающих количественно уровни компетенций слушателей

Исходя из результатов проведённых диссертационных исследований, предложена нечёткая модель оценивания возможности по реализации угроз НСД в ОИСИСН к гипервизору через виртуальные машины, место которой в исследованиях представлено на рис.2.9.

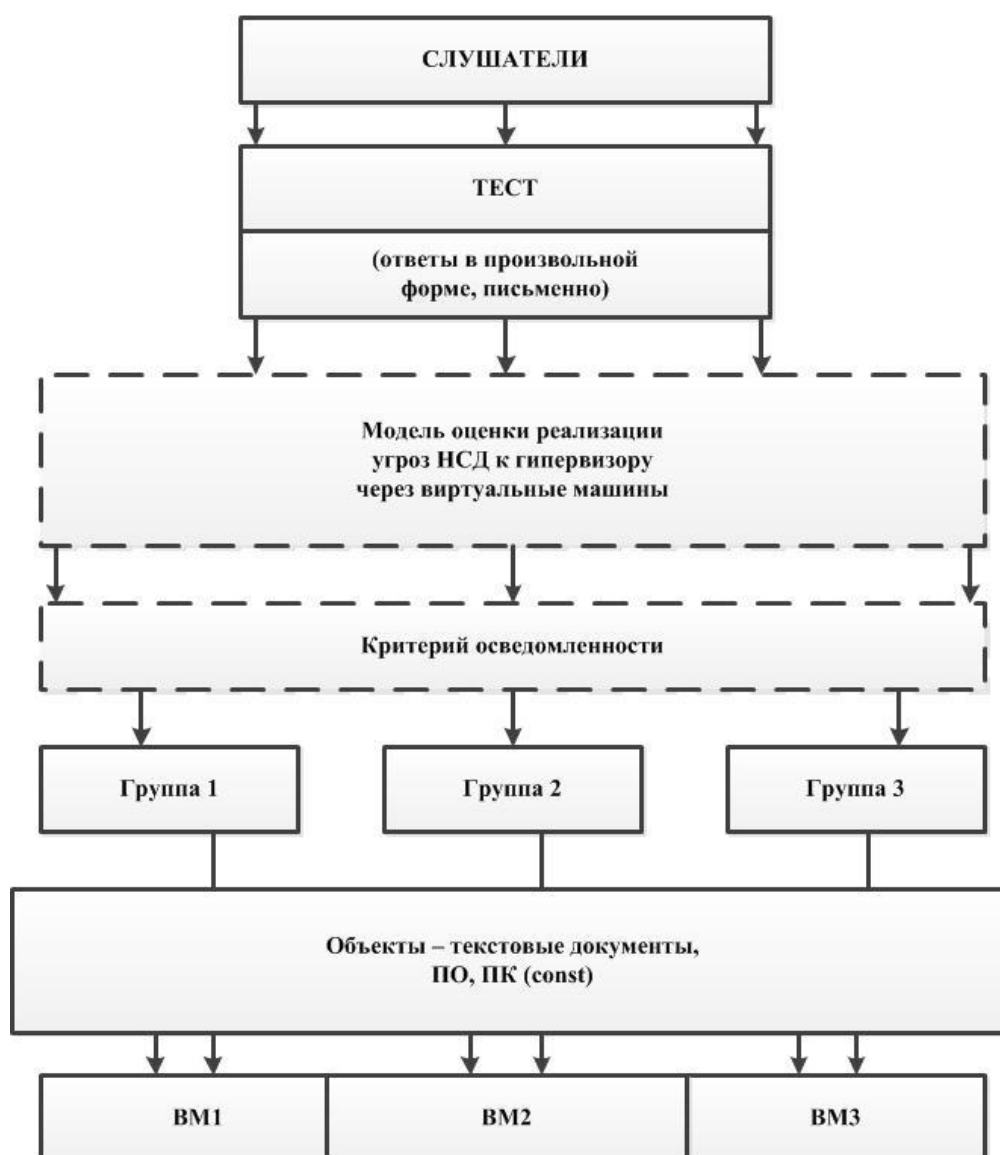
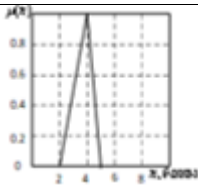
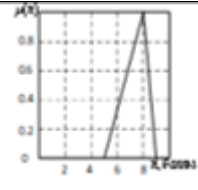


Рисунок 2.9 – Место нечёткой модели NSD_SV_0.fis оценки возможности для реализации угроз НСД в ОИСИСН к гипервизору через виртуальные машины

Так как ответы слушателей по тесту знаний различных команд носят неформализованный характер, эксперты определяют каждый ответ слушателя по 10-балльной шкале, которые в дальнейшем обрабатываются на основе сформированных функций принадлежности, представленных в таблице 2.4.

Таблица 2.4 – Фрагмент результатов обработки ответов слушателей на вопросы теста

№	Вопрос	Характеристика ответа	Оценка ответа (по десятибалльной шкале)	Вид функции принадлежности, указывающей на разброс уверенности в ответе
1	Назначение регистра ЕСХ и его бит	Дан полный ответ	10	-
		ответ дан частично или без необходимой детализации	4	
		Ответа нет (ответ не знаю)	0	-
2	Назначение функций Windows API	Дан полный ответ	10	-
		ответ дан частично или без необходимой детализации	4	
		Ответа нет	0	-

Исходя из результатов исследования, разработана нечёткая модель NSD_SV_0.fis с использованием Fuzzy Logic среды MATLAB, где учтены все правила и параметры как самих слушателей (знание команд), так и параметры формальной модели нарушителя (рис. 2.8), позволяющая ранжировать слушателей в соответствии с критерием осведомлённости, границы которых представлены в табл. 2.5. Пример ранжирования в сильную (первую) и среднюю (вторую) группы представлены на рис. 2.10 и 2.11 соответственно.

Поэтому результат оценок осведомлённости слушателя должен быть в количественном виде для возможности распределения их в отдельные группы, однако ответы на вопросы тестов подразумевают качественную оценку.

Таблица 2.5 – Правило ранжирования слушателей и определение групп

Диапазон значений критерия осведомленности	Ранг слушателя при возможности реализации угроз								
	Низкая (Н)			Средняя (С)			Высокая (В)		
	с частотой смены контингента								
	В	С	Н	В	С	Н	В	С	Н
Менее 0.3	3	3	3	3	3	2	3	2	2
(0.3 – 0.69]	3	3	2	2	2	2	2	1	1
(0.7 – 1]	3	2	2	1	1	1	1	1	1

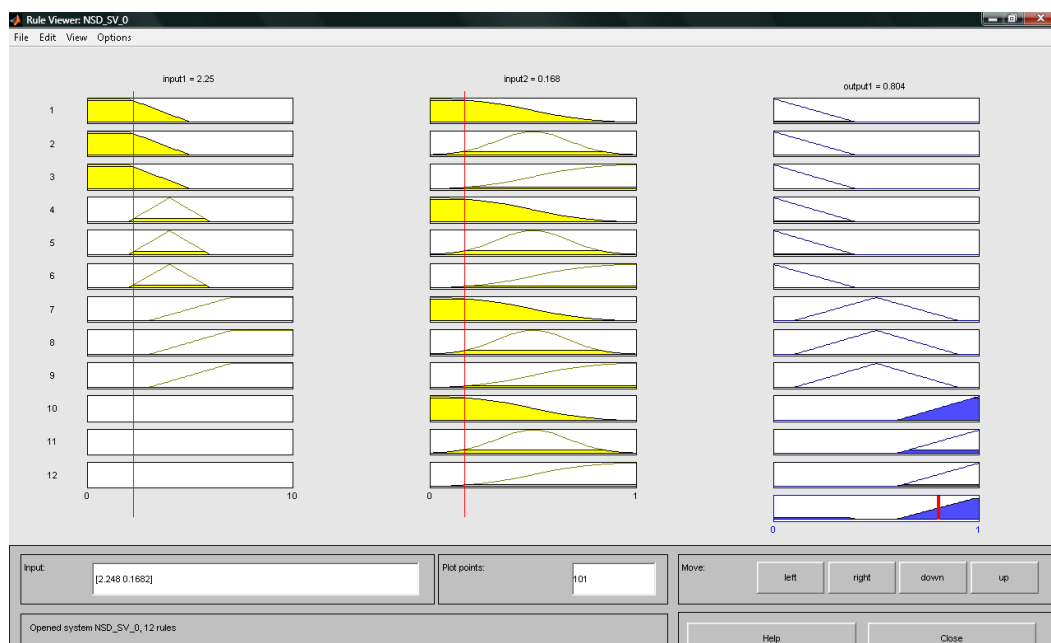


Рисунок 2.10 – Результаты ранжирования в сильную (первую) группу (критерий осведомлённости 0,804 (выше 0,7))

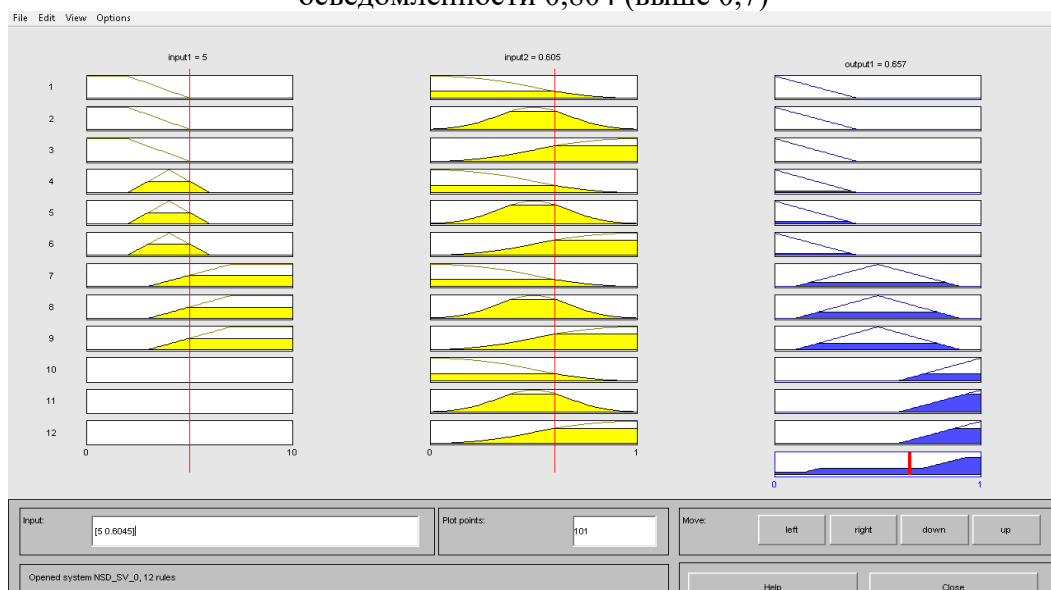


Рисунок 2.11 – Результаты ранжирования в среднюю (вторую) группу (критерий осведомлённости 0,657 (в пределах 0,3- 0,69))

Исходя из того, что тестовые наборы для оценки осведомленности слушателя по качественным показателям должны быть преобразованы в количественные оценки осведомленности, предлагается использовать правила нечёткой логики на основе метода Fuzzy Logic. Если предположить, что отсутствие некоторых знаний приводит или к невозможности, или к снижению возможностей реализации угроз за счет случайного подбора нарушителем необходимых для этого функций, процедур, параметров, настроек и т.п., то предлагается использовать процедуры обработки нечеткой оценки ответов респондентов по балльной шкале для определения соответствующих функций принадлежности для каждого ответа и на этой основе осуществлять процедуру расчета нечёткого значения показателя осведомленности с последующей его дефаззификацией. Фрагмент результатов тестирования слушателей с примерами нечётких оценок ответов приведен в таблице 2.4.

Расчет нечеткого значения результирующего показателя (I_k) осведомленности k -го слушателя осуществляется путем свёртки оценок ответов по каждому вопросу по формуле:

$$I_k = \frac{1}{10 \cdot U} \sum_{u=1}^U \frac{1}{J_k^{(u)}} \sum_{j=1}^{J_k^{(u)}} \sum_{f=1}^{F_j^{(u)}} \alpha_f^{(k)} \cdot n_f^{(k)},$$

где U – общее количество актуальных угроз в ИСО с ИСН; $J_k^{(u)}$ – количество вопросов, заданных k -му слушателю, связанных с u -й угрозой; $F_j^{(u)}$ – количество команд (функций, процедур и т.п.), содержащихся в j -м вопросе, связанным с u -й угрозой; $\alpha_f^{(k)}$ – весовой коэффициент важности f -й команды (функции, процедуры и т.п.) для реализации угрозы; $n_j^{(k)}$ – нечеткая оценка количества баллов, выставленных за ответ, связанный с f -й командой (функцией, процедурой и т.п.) с треугольной функцией принадлежности.

На этом этапе с помощью экспертов выполнялась фаззификация, то есть выявление (определение) элементов входа в виде функций принадлежности

входных параметров. В таблице 2.4 показаны сформированные экспертами функции принадлежности входных параметров, к которым относятся команды (функции, процедуры и т.п.) для реализации угрозы.

Операции вывода на данном этапе включают базу правил логического вывода, механизм (метод) вывода и функцию принадлежности выходного параметра.

Тем не менее, правила логического вывода определяют причинно-следственные отношения между нечёткими значениями её входных величин (низкая, средняя и высокая частота смены слушателя и высокий, средний и низкий ранг слушателя при возможности реализации угроз) с выходной нормированной величиной диапазона значения критерия осведомлённости (низкий, средний, высокий), что даёт возможность реализации алгоритма ранжирования слушателей по их количественному критерию осведомленности и возможности реализации угроз НСД к гипервизору через виртуальные машины. В отличие от известных приемов и алгоритмов ранжирования в предложенный алгоритм введены процедуры учета, во-первых, динамики (частоты) смены контингента слушателей (длительность периода обучения), во-вторых, возможности реализации каждой из актуальных угроз. Ранжирование проводилось по правилу, представленному в таблице 2.5.

Для ранжирования введено 3 уровня (ранга) слушателей. Возможность реализации угрозы в данной главе оценивается лишь по качественному показателю со значениями «низкая», «средняя» и «высокая» на основе результатов анализа уязвимостей в программном обеспечении ОИСИСН, состава актуальных угроз, настроек операционной среды и возможности использования команд, функций и процедур, необходимых для реализации угроз.

Суммирование нечетких чисел проводилась с использованием, так называемого $L-R$ их представления, когда суммируются соответствующие крайние и срединные точки нечетких чисел. Дефазификация результирующего показателя проводилась известным методом центра сумм.

Однако следует заметить, что треугольная функция принадлежности вносит размытость крайних значений, поэтому для снижения неопределённости граничных значений функций принадлежности входных параметров предлагается модифицировать подход по формированию функций принадлежности, количественно описывающих уровни компетенций слушателей.

2.4 Выводы

Таким образом, разработанная формальная модель нарушителя включает в себя:

1) тестовые наборы для оценки осведомленности слушателя по качественным показателям с переводом результатов тестирования в количественные оценки осведомленности на основе правил нечёткой логики. Существенным отличием данной методики от известных методик тестирования является, во-первых, то, что в ней впервые применен *предложенный критерий осведомленности слушателя* с позиции определения его возможностей по реализации угроз безопасности информации в ОИС.

При этом показатель рассчитывался на основе обработки системы специально подготовленных тестов, часть из которых содержала упоминания команд, функций, процедур, утилит или их параметров и иную информацию о ПО, знание которых дает нарушителю возможность реализации каждой из актуальных угроз НСД к гипервизору через виртуальные машины. Полагалось, что отсутствие некоторых знаний приводит или к невозможности, или к снижению возможностей реализации угроз за счет случайного подбора нарушителем необходимых для этого функций, процедур, параметров, настроек и т.п. Также введены процедуры обработки нечеткой оценки ответов респондентов по балльной шкале с определением соответствующих функций принадлежности для каждого ответа и на этой основе – процедура расчета

нечёткого значения показателя осведомленности с последующей его дефазификацией.

Для корректной привязки уровней компетенций нарушителей к угрозам безопасности информации был проведен анализ таких угроз с учетом известных, содержащихся в электронных базах уязвимостей CVE и ФСТЭК России уязвимостей гипервизора и виртуальных машин.

По результатам такого анализа была сформирована описательная модель угроз безопасности информации в ОИСИСН, содержащая применительно к наиболее компетентному внутреннему нарушителю (слушателю) описание используемых уязвимостей, способов реализации угроз (эксплуатации уязвимостей), оценки времени, необходимого для реализации каждой угрозы, а также содержания несанкционированного действия с защищаемой информацией (копирования, модификации, перемещения или уничтожения) с оценками возможного выбора каждого из таких действий. Далее применительно к каждому уровню осведомленности слушателей составлялся кортеж угроз, которые могут быть реализованы нарушителями в ОИСИСН;

2) правила ранжирования слушателей по количественному критерию их осведомленности и возможностям реализации угроз НСД к защищаемой информации. В отличие от известных приемов и алгоритмов ранжирования в предложенный алгоритм введены процедуры учета, во-первых, динамики смены контингента слушателей (длительность периода обучения), во-вторых, возможности реализации каждой из актуальных угроз.

Для ранжирования введены 3 уровня (ранга) слушателей. Возможность реализации угрозы в данной главе оценивается лишь по качественному показателю со значениями «низкая», «средняя» и «высокая» на основе результатов анализа уязвимостей в ПО ОИСИСН, состава актуальных угроз, настроек операционной среды и возможности использования команд, функций и процедур, необходимых для реализации угроз.

Приведена структура формальной модели нарушителя.

Также представлены результаты по разработке нечёткой модели оценивания возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН. В данной модели был модифицирован подход по формированию функций принадлежности, описывающих количественно уровни компетенций и используемые в дальнейшем для оценки возможностей реализации угроз на основе аппарата нейронных сетей.

Опираясь на имеющиеся команды в тестовых наборах для оценки осведомленности слушателей необходимо сформировать численные значения левых и правых границ функций принадлежности на основе экспертных данных.

С этой целью была выполнена оценка значимости команд, описываемых в тестах, для реализации НСД к гипервизору через виртуальные машины. Для решения такой задачи в диссертационных исследованиях использован метод нечеткой логики Mamdani, что обеспечивает устранение такого недостатка, как возможность снижения неполноты знаний для оценки важности команд (функций, инструкций, процедур, утилит или их параметров, а также иной информации о программном или техническом обеспечении, знание которых дает нарушителю возможность реализации каждой из актуальных угроз НСД к гипервизору на основе формальной модели нарушителя) и качественных ответов экспертов в необходимости знаний о данных командах при осуществлении НСД к гипервизору через виртуальную машину. Это позволяет осуществлять учёт исходных данных, которые определяют неоднозначность в оценке качественных показателей и перевод их в количественные показатели.

3 Разработка нейронечёткой модели оценивания динамики состояния ОИСИСН в условиях угроз безопасности информации к гипервизору через виртуальные машины и средства оценки её устойчивости к НСД

Опираясь на полученные ранее результаты, имеется возможность разработать динамическую непрерывную нейронечёткую модель динамики состояния ОИСИСН в условиях угроз НСД к гипервизору через виртуальные машины и средство оценки её устойчивости к НСД, которые позволят создать профили разграничения доступа для отдельных групп слушателей за требуемые временные промежутки.

3.1 Математическая основа нейронечёткой модели оценивания динамики состояния ОИСИСН в условиях угроз НСД к гипервизору через виртуальные машины

Результаты исследований, описанных в предыдущих главах, показали выявленные недостатки, присущие работе экспертов при настройке профилей и определении возможностей реализации угроз НСД. Поэтому предлагается формировать функцию принадлежности исходя из предоставленного множества, состоящего из команд, доступных злоумышленнику, и количества этапов, которые необходимы для реализации каждой выбранной команды.

Применительно к модели нарушителя, представленной ранее на рис. 2.8, имеются нечёткие исходные данные, которые дают возможность воспринимать разрабатываемые модели как системы нечёткой логики или системы с нечёткими параметрами управления. Ввиду этого предлагается описывать нейронечёткую модель динамики состояния ОИСИСН в условиях угроз НСД к гипервизору через виртуальные машины именно как динамику систем с нечёткими параметрами управления.

Поэтому целесообразно представить данную систему в виде кортежа параметров (3.1):

$$S^R = \langle K, I, W, p, b \rangle, \quad (3.1)$$

где S^R – множество реализации угроз НСД к гипервизору через ВМ или физическую сеть, K – количество этапов для осуществления НСД к информации, I – количество и определение входных параметров каждого этапа, W – значимость параметров для каждого этапа, p – реализация параметров НСД слушателем и b – задержка выполнения этапа НСД.

Аналогично сформированному кортежу в данных диссертационных исследованиях определена новая функциональная зависимость оценки состояния ОИСИСН в условиях угроз НСД, которая описана с помощью математического аппарата нейронных сетей в виде информационного ограничения качественных параметров $a_k = f(I_k, W_k, p_k, b_k)$.

Предложенная в данной главе нейронечёткая модель оценки состояния ОИСИСН в условиях угроз НСД к гипервизору через виртуальные машины основывается на системе уравнений (3.2), состоящих из уравнений для описания в отдельности процесса для каждого этапа НСД.

$$\begin{aligned} a^1(2) &= f_1(r_{1h}) \cdot (I_{1,1}W_{1,1}p_1(2) + b_1) \\ a^2(2) &= f_2(r_{2h}) \cdot (I_{2,1}W_{2,1}[p_1(2) \vee p_1(1)] + I_{2,2}W_{2,2}p_2(1)) \\ a^3(2) &= f_3(r_{3h}) \cdot (I_{3,1}W_{3,1}[p_2(2) \vee p_2(1)] + I_{3,2}W_{3,2}p_3(1)) \\ a^4(2) &= f_4(r_{4h}) \cdot (I_{4,1}W_{4,1}[p_3(2) \vee p_3(1)] + I_{4,2}W_{4,2}p_4(1)) \\ a^5(2) &= f_5(r_{5h}) \cdot (I_{5,1}W_{5,1}[p_4(2) \vee p_4(1)] + I_{5,2}W_{5,2}p_5(1)) \\ a^6(2) &= f_6(r_{6h}) \cdot (I_{6,1}W_{6,1}[p_5(2) \vee p_5(1)] + I_{6,2}W_{6,2}p_6(1)) \\ a^7(2) &= f_7(r_{7h}) \cdot (L_{7,1}W_{7,1}a^1(2) + L_{7,2}W_{7,2}a^2(2) + L_{7,3}W_{7,3}a^3(2) + \\ &+ L_{7,4}W_{7,4}a^4(2) + L_{7,5}W_{7,5}a^5(2) + L_{7,6}W_{7,6}a^6(2) + L_{7,7}W_{7,7}a^7(1) + b_7) \end{aligned} \quad (3.2)$$

Согласно рис. 2.8, на котором показаны цифры 1-6, обозначающие этапы выполнения нарушителям НСД к гипервизору через виртуальные машины. Так, в первой формуле системы уравнений (3.2) определяется возможность преодоления первого этапа НСД на основе двух входных величин: показателя

(критерия) осведомлённости его об инструкции CPUID и времени нахождения в системе. Таким образом, $a^1(2)$ характеризует возможность преодоления первого этапа НСД на основе двух входных величин. Данная величина зависит от функции принадлежности, описываемой данного слушателя $f(r_{1h})$, $I_{1,1}$ – количество и определение входных параметров 1 этапа, $W_{1,1}$ – значимость параметров для 1 этапа, $p_1(2)$ – возможность реализации двух параметров на 1 этапе НСД слушателем и b_1 – задержка выполнения 1 этапа НСД. Со второй формулы по шестую они формируются аналогичным образом с тем лишь отличием, что учитывается связь с предыдущими этапами и возможностями их реализации.

Для решения системы уравнений (3.2) был предложен математический аппарат нейронных сетей с вновь предложенной функцией для описания процесса реализации НСД конкретным субъектом (слушателем, злоумышленником), учитывающего как временной параметр t , так и оценку возможностей k -ой реализации угроз НСД отдельной группой слушателей:

$$f = \frac{k \times t}{k \times t + e^{-t}}. \quad (3.3)$$

Нечёткая модель оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН (modelUgrSZI.mdl) разработана в среде моделирования MATLAB, которая реализует математические выражения, представленные в (3.2). Общий её вид представлен на рис. 3.1.

Седьмая формула объединяет все возможные реализации на каждом этапе в отдельности, включая задержку выполнения этапа за счёт смещения времени её выполнения. Общая внутренняя взаимосвязь в нейронечёткой модели представлена на рис. 3.2.

Исходя из этого в нейронечёткой модели оценивания возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН

(modelUgrSZI.mdl) с помощью аппарата нейронной сети предложено иметь шесть уровней в модели и один скрытый уровень.

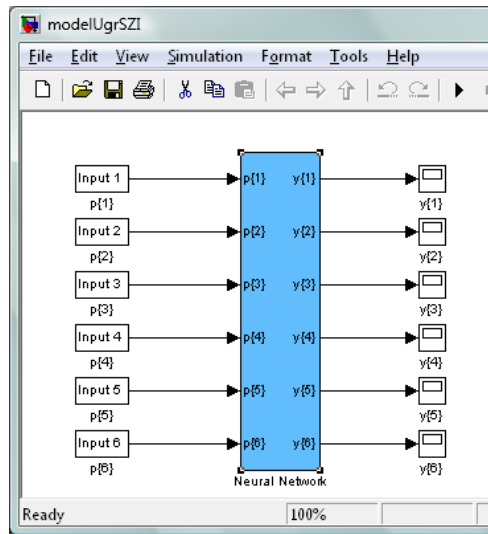


Рисунок 3.1 – Общий вид нейронечёткой модели оценивания возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИЧ (modelUgrSZI.mdl)

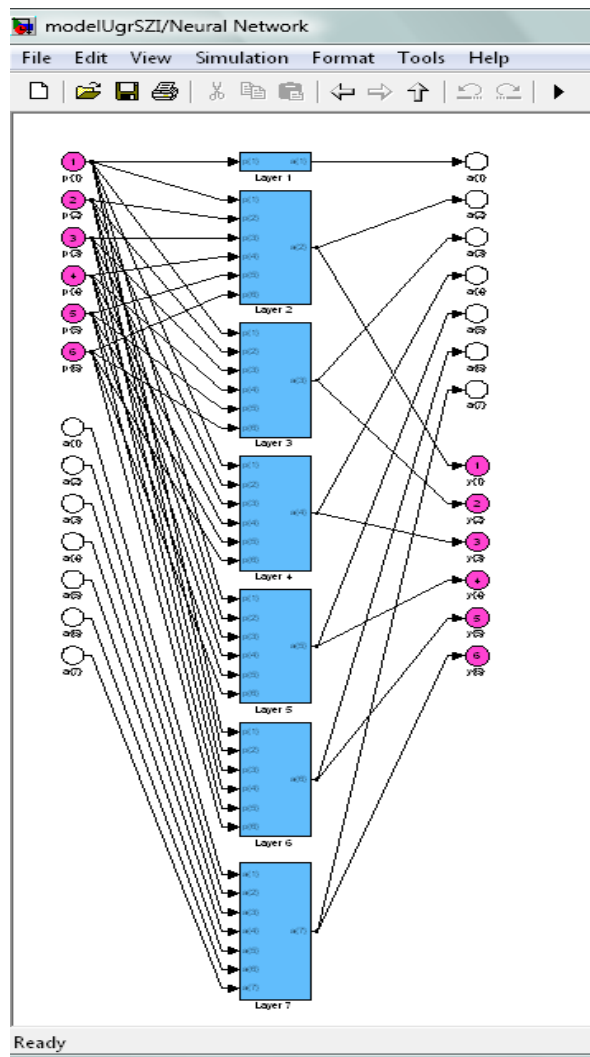


Рисунок 3.2 – Общая внутренняя взаимосвязь в нейронечёткой модели modelUgrSZI.mdl

Каждый этап в модели представляет собой структуру, представленную на рис. 3.3. Временные задержки в модели осуществляют компоненты TDL, представленные на рис. 3.4. Описание распределения весовых коэффициентов для 1 этапа представлено на рис. 3.5.

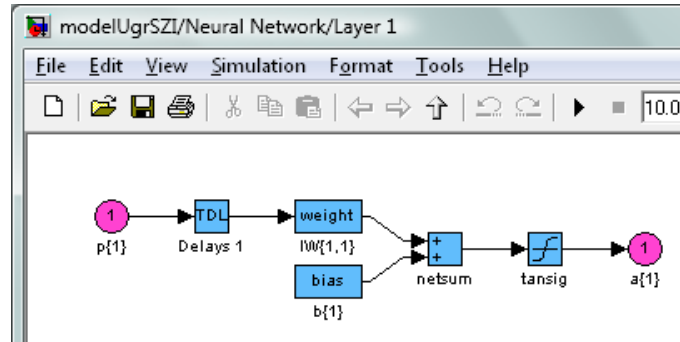


Рисунок 3.3 – Описание 1 этапа НСД в нейронечёткой модели modelUgrSZI.mdl

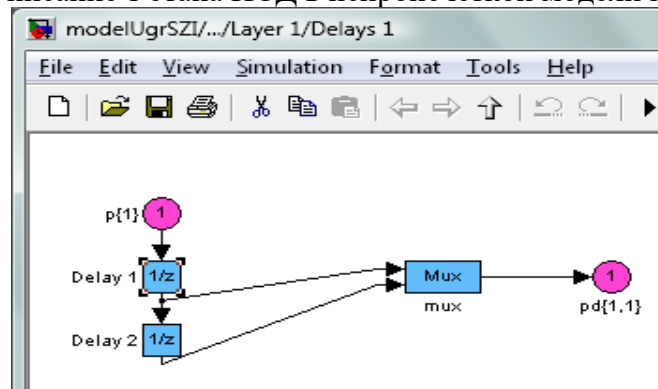


Рисунок 3.4 – Описание задержки выполнения 1 этапа НСД в нейронечёткой модели modelUgrSZI.mdl

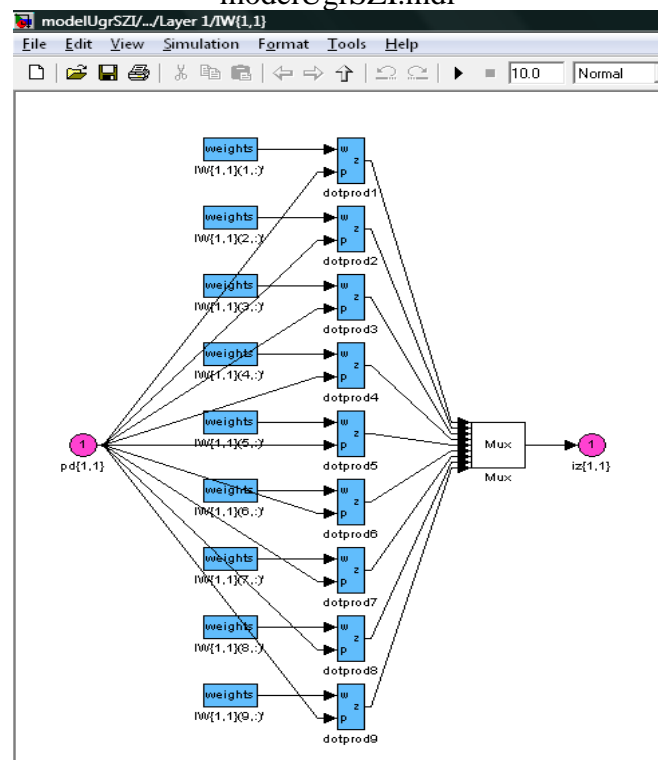


Рисунок 3.5 – Описание распределения весовых коэффициентов для 1 этапа

Применительно ко второму уровню, соответствующему рис. 2.8, предложена структура (рис. 3.6), реализующая решение второй формулы системы уравнений (3.2) и описывающая второй этап НСД в нейронечёткой модели modelUgrSZI.mdl.

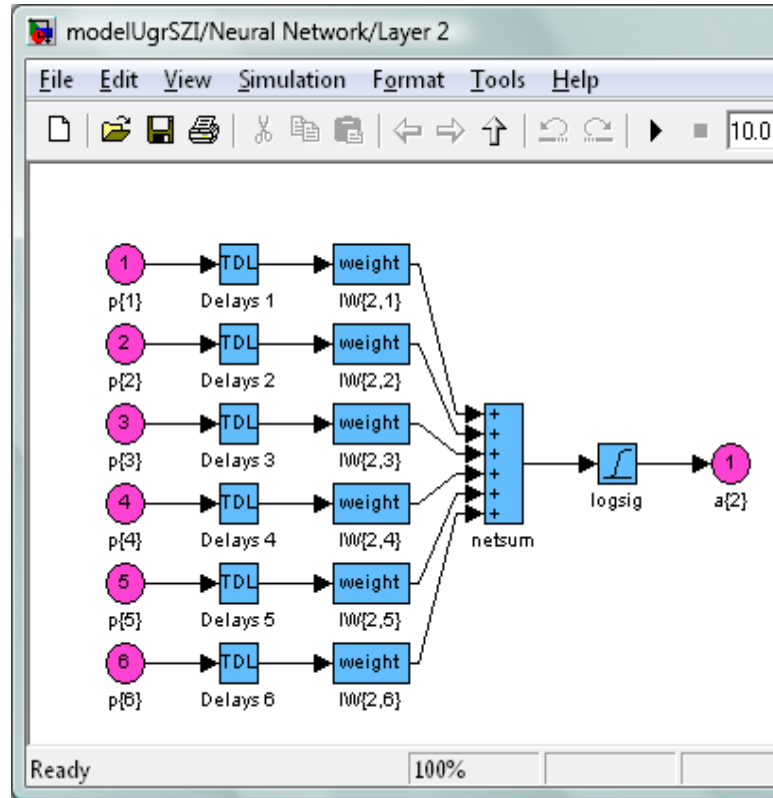


Рисунок 3.6 – Описание 2 этапа НСД в нейронечёткой модели modelUgrSZI.mdl

Описание задержки выполнения 2 этапа НСД в нейронечёткой модели modelUgrSZI.mdl представлено на рис. 3.7, описание распределения весовых коэффициентов второго этапа с первым представлено на рис. 3.8, описание распределения весовых коэффициентов второго этапа с третьим представлено на рис. 3.9.

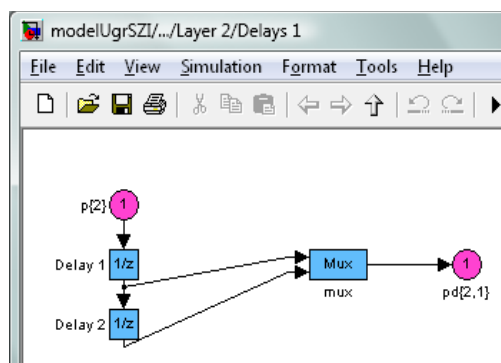


Рисунок 3.7 – Описание задержки выполнения 2 этапа НСД в нейронечёткой модели modelUgrSZI.mdl

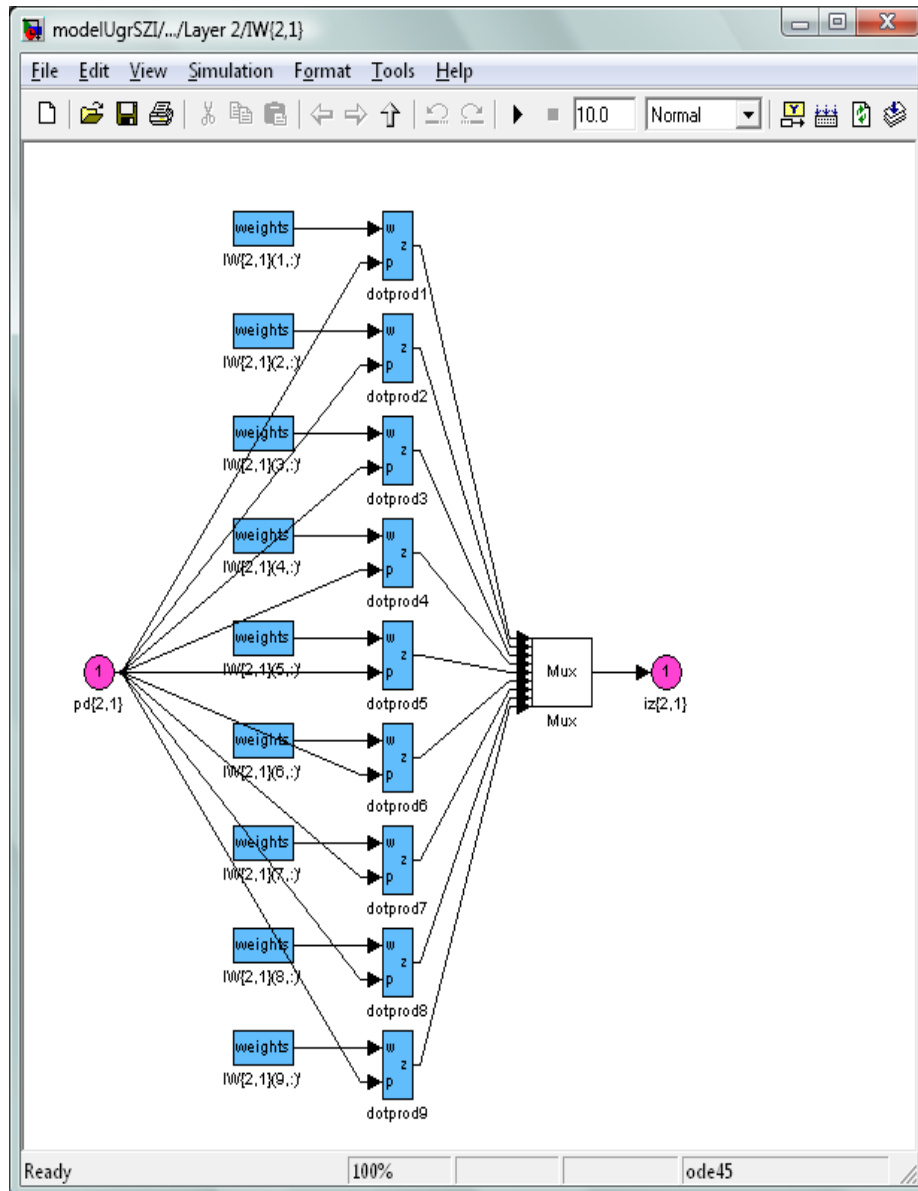


Рисунок 3.8 – Описание распределения весовых коэффициентов второго этапа с первым

Далее моделирование формул с третьей по шестую системы уравнений (3.2) выполняется аналогичным образом, за исключением последней седьмой, так как данный уровень является скрытым.

На рис. 3.10 представлено описание заключительного этапа НСД в нейронечёткой модели modelUgrSZI.mdl, описывающего взаимодействие всех этапов НСД на основе правил нечёткой логики и где имеется отличие в формировании задержки выполнения этого этапа (рис. 3.11).

Описание весовых коэффициентов для заключительного этапа в нейронечёткой модели modelUgrSZI.mdl представлено на рис. 3.12.

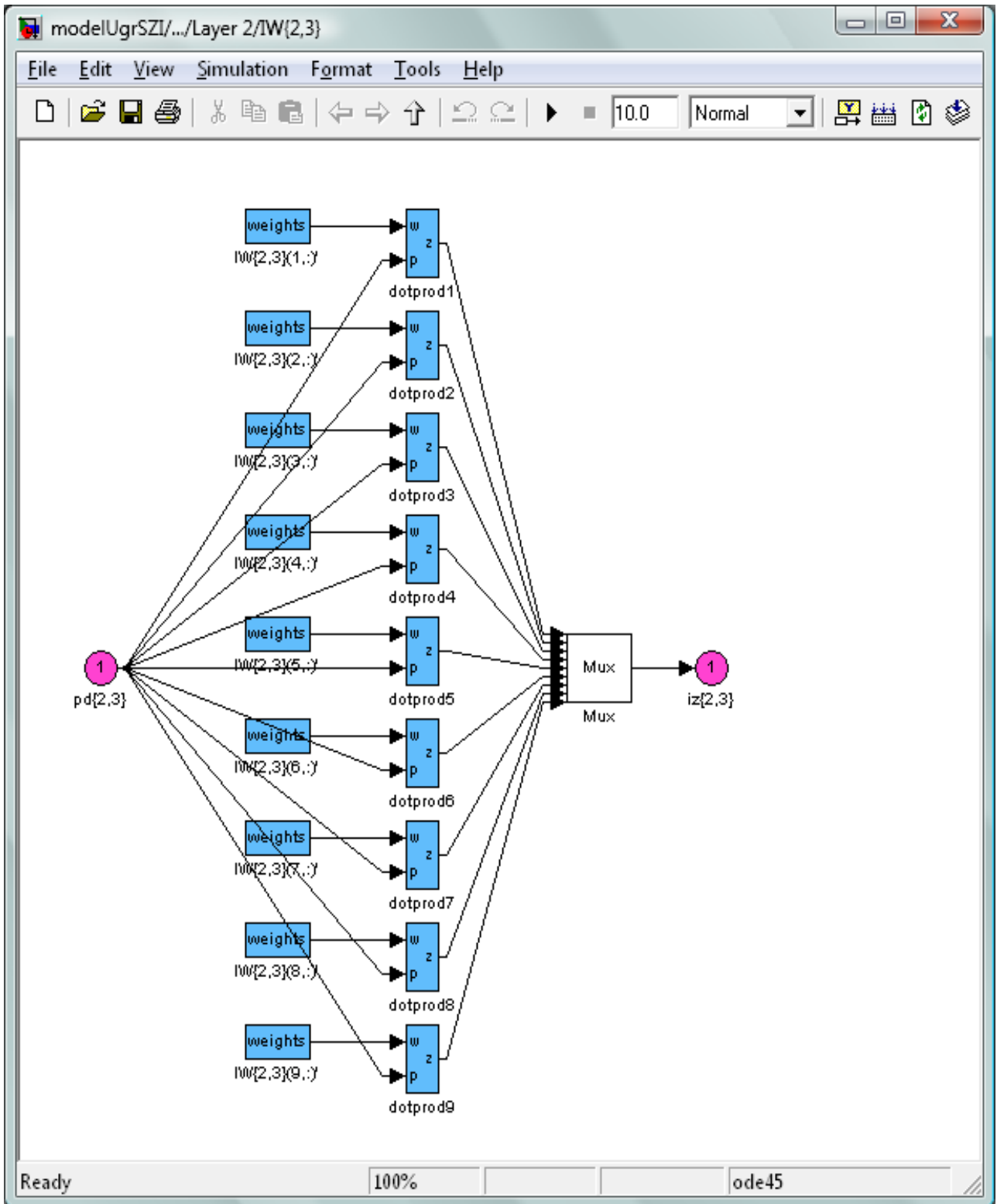


Рисунок 3.9 – Описание распределения весовых коэффициентов второго этапа с третьим

Рисунок 3.13 предоставляет возможность оценки задержки (смещения) из-за внешних факторов воздействия на нарушителя.

Детализация компонентов modelUgrSZI.mdl представлена на рис. 3.14.

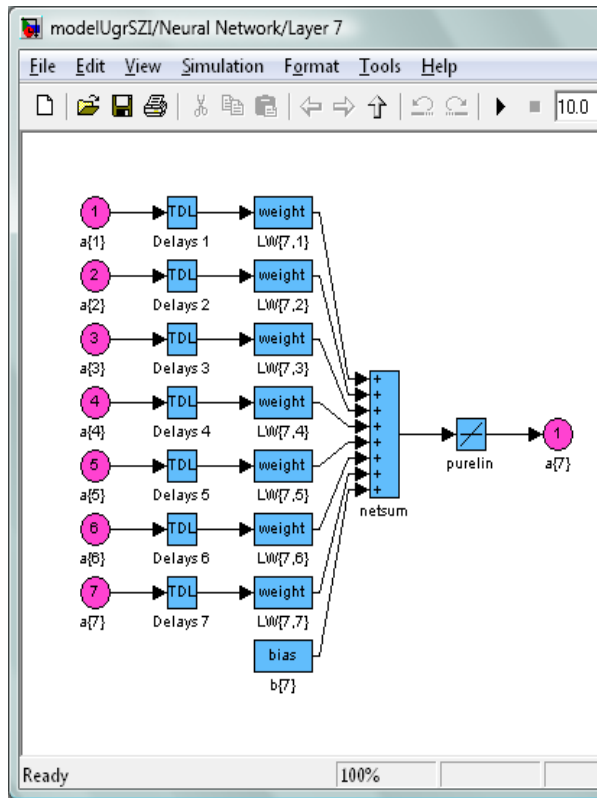


Рисунок 3.10 – Описание заключительного этапа НСД в нейронечёткой модели modelUgrSZI.mdl

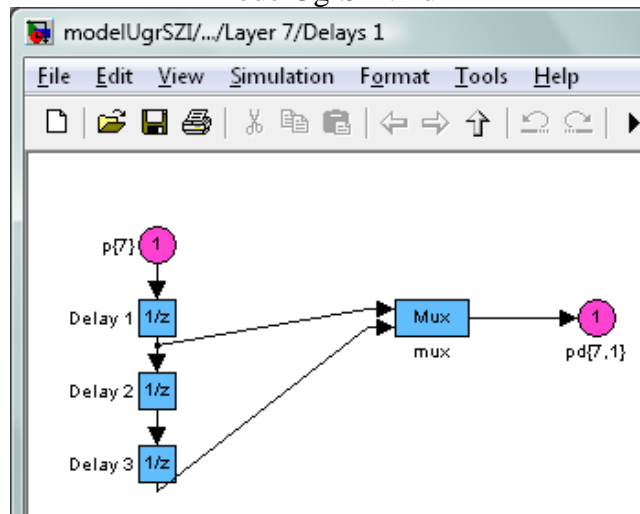


Рисунок 3.11 – Описание задержки выполнения заключительного этапа

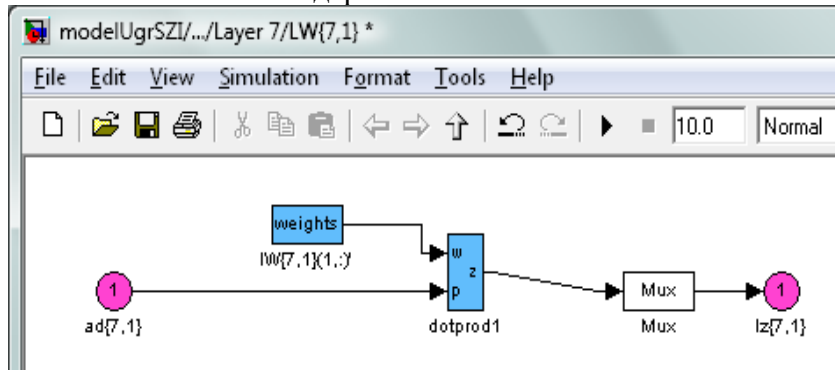


Рисунок 3.12 – Описание весовых коэффициентов для заключительного этапа

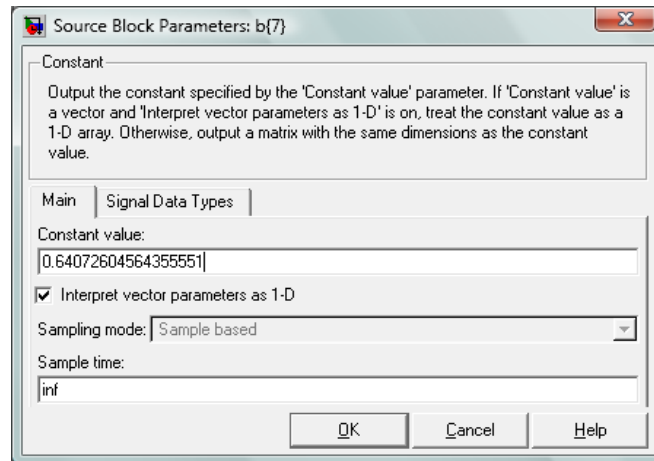


Рисунок 3.13 – Описание весовых коэффициентов для заключительного этапа

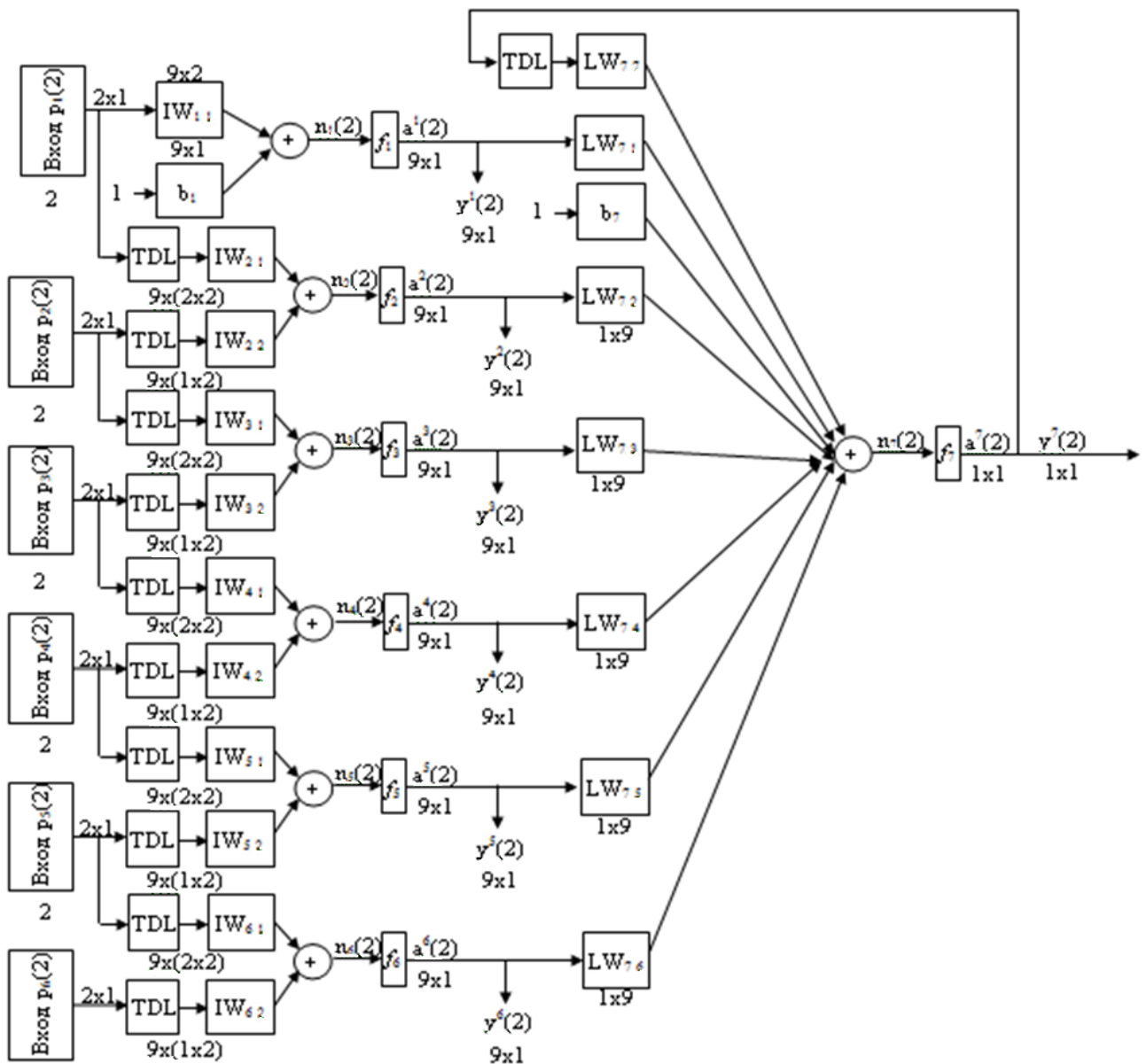


Рисунок 3.14 – Детализация компонентов нейронечёткой модели (modelUgrSZI.mdl) оценивания возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН

В данных исследованиях также было предложено учитывать такой параметр, как частота смены пользователей из-за наличия специфики при процессе обучения слушателей (обучаемых) конкретным программным и аппаратным средствам.

Однако такие нормативные документы, как ГОСТ Р ИСО/МЭК 15408, 27001, не позволяют определять объекты, которые необходимо в минимальные сроки поддерживать для осуществления требуемой информационной безопасности.

Правила интерпретации нейронечёткой модели оценивания состояния образовательной информационной системы в условиях угроз несанкционированного доступа к гипервизору через виртуальные машины и описание системы уравнений на основе аппарата нейронных сетей представлено в приложении диссертации.

3.2 Разработка средства оценки устойчивости состояний ОИСИСН в условиях угроз НСД на каждом этапе по методу бифуркаций и методу Ляпунова для автоматизации процесса создания профилей по разграничению профилей на основе технологии «тонкий клиент»

Аналогично результатам работ [85–95] имеется возможность использования программного кода для формирования настроек профилей разграничения доступа на основе тонкого клиента. Кроме того, применяя в соответствии с работой [86] Thinstation, имеется возможность автоматически настраивать тот или иной профиль, записанный для определённой заранее группы слушателей. Профили расположения необходимых файлов для процесса обучения определяются на основе результатов моделирования modelUgrSZI.mdl (рис. 3.15).

Алгоритм функционирования средства оценки состояния информационной системы обучения с информацией специального назначения в

условиях угроз НСД с целью автоматизации процесса создания профилей по разграничению профилей на основе технологии «тонкий клиент» можно представить следующим образом (рис. 3.16).

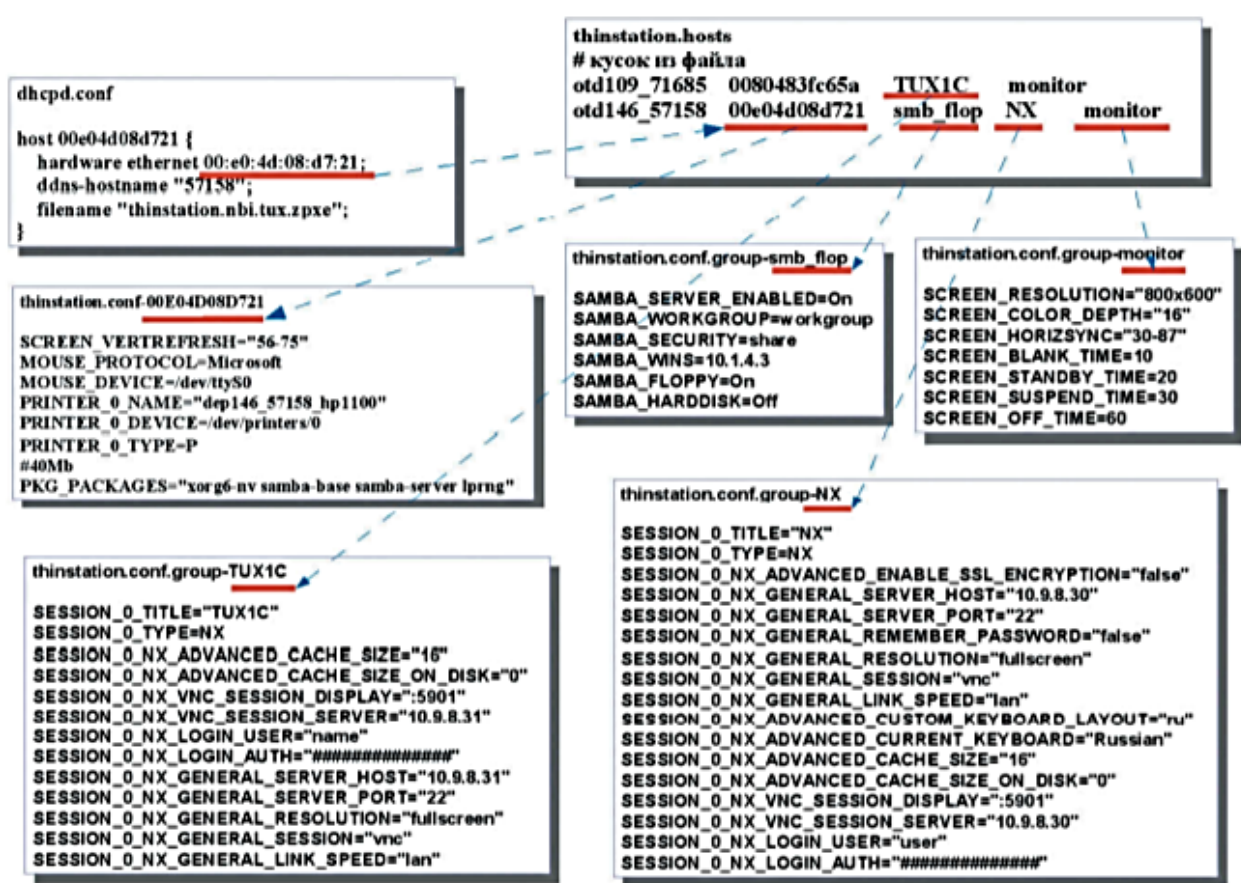


Рисунок 3.15 – Автоматическая реализация профилей тонкий клиент Thinstation [86]

Исходя из того, что управление системой разграничения доступа (в условиях динамики состояния ОИСИСН к угрозам НСД к гипервизору через виртуальные машины) учитывает некоторую неопределённость качественных и количественных параметров, её можно квалифицировать как нечёткую систему управления с неизвестными моделями объектов.

Ввиду этого для таких систем могут иметь место оценки по критерию устойчивости. Поэтому выбран подход на основе *метода бифуркаций и метода Ляпунова*.

Кроме того, предложенную в нейронечёткой модели функцию

$$f = \frac{k \times t}{k \times t + e^{-t}}$$

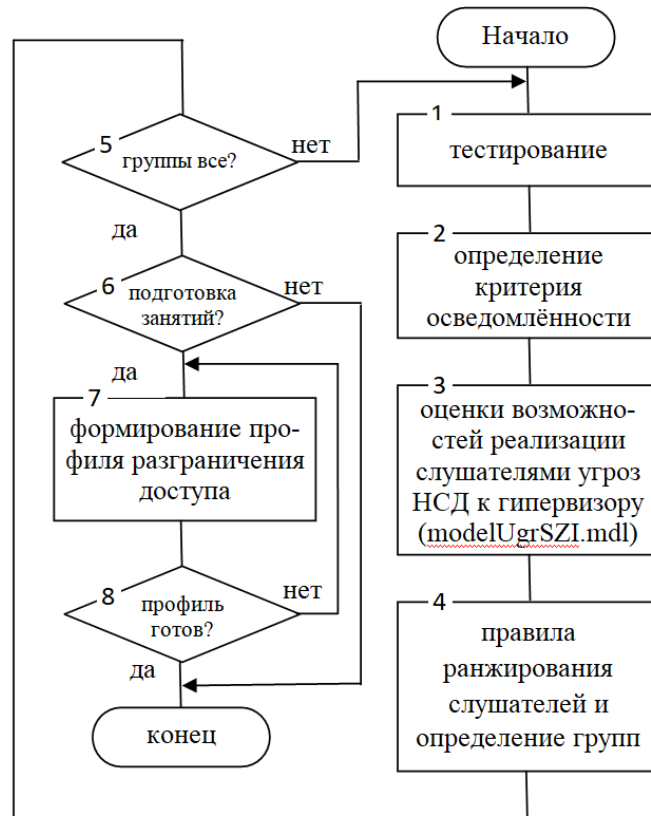


Рисунок 3.16 –Алгоритм функционирования средства оценки динамики состояния информационной системы обучения с информацией специального назначения в условиях угроз НСД с целью автоматизации процесса создания профилей по разграничению профилей на основе технологии «тонкий клиент»

можно использовать как функцию Ляпунова, так как она удовлетворяет её требованиям [175, 176]: непрерывна, монотонна и дифференцируема. Кроме того, если система нелинейных дифференциальных уравнений удовлетворяет условиям симметрии, неотрицательности и монотонности, то функция Ляпунова этой системы удовлетворяет условию dE/dt меньше или равно нулю. То есть, если функция Ляпунова E обладает этим глобальным свойством, то, согласно первой теореме Ляпунова, эта система является глобально устойчивой, что подтверждается рис. 3.17 и 3.18.

Таким образом, для рассчитываемой группы из 9 человек (с определёнными в ходе исследования параметрами осведомлённости слушателей) имеется один корень, равный **0**, а все остальные – **отрицательны**, следовательно, система состояний **устойчива** к НСД к гипервизору через виртуальные машины в ОИСИСН на основе метода Ляпунова. Кроме того, из

рис. 3.17 видно, что для слушателей 2-9 имеется устойчивое положение между первым и вторым этапом, а для слушателя 1 это положение смещается между вторым и третьим этапами НСД.

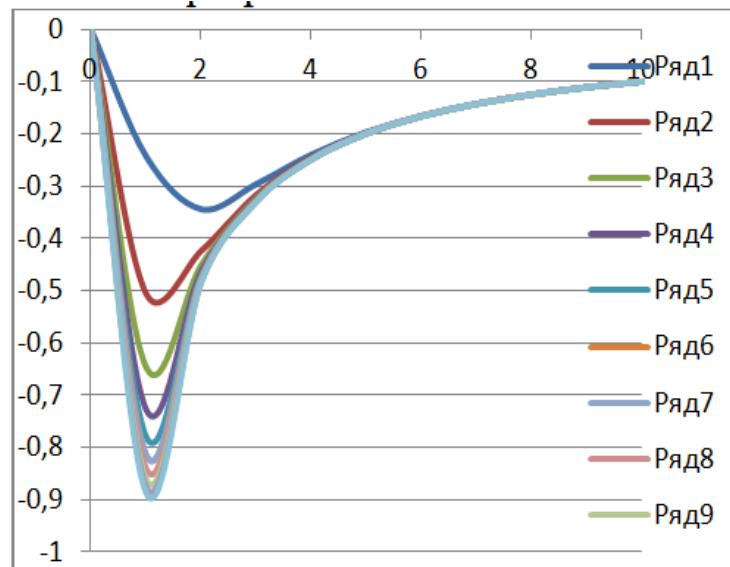


Рисунок 3.17 – Рассчитанные значения корней характеристического уравнения дифференциальной системы уравнений с использованием метода Ляпунова

На рис. 3.18 ряд определяет отдельного слушателя в группе, а по оси абсцисс отмечены этапы НСД к гипервизору через виртуальные машины в ОИСИСН. Данные результаты демонстрируют сходимость значений функции Ляпунова для двух параметров к точке состояния (0,0).

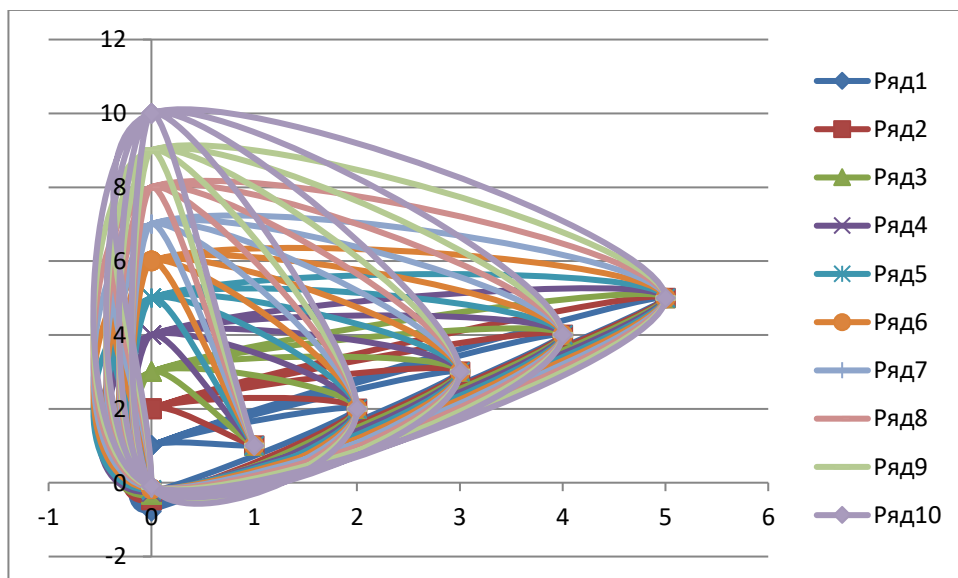


Рисунок 3.18 – Сходимость значений функции Ляпунова для двух параметров

3.3 Выводы

Таким образом, разработанная **нечёткая модель оценки возможности для реализации угроз несанкционированного доступа в образовательных информационных системах с информацией специального назначения к гипервизору через виртуальные машины** *отличается тем*, что учитывает результаты экспертной оценки неформализованных ответов слушателей по тесту знаний различных команд и даёт оценку критерия *осведомлённости слушателей*, а также осуществляет *их ранжирование по трём группам* в соответствии со встроенными в неё правилами нечёткой логики на основе суммирования нечетких чисел с L - R правилом и использованием дефаззификации результирующего показателя методом центра сумм.

Кроме того, разработанная **нечёткая модель оценивания динамики состояния образовательных информационных систем с информацией специального назначения в условиях угроз несанкционированного доступа к гипервизору через виртуальные машины** *отличается* тем, что, на основе математического аппарата нейронных сетей в виде *системы уравнений, описывает динамику каждого отдельного этапа и их взаимодействие, которая* учитывает такие релевантные параметры формальной модели нарушителя, как *количество этапов* для осуществления несанкционированного доступа к информации, *входные параметры и их количество для каждого этапа, значимость параметров на каждом этапе, возможность реализации параметров несанкционированного доступа и задержки выполнения этапа НСД слушателем* и их взаимосвязь. Кроме того, разработанное **средство оценки устойчивости к несанкционированному доступу к гипервизору через виртуальные машины** отличается тем, что имеет возможность применять *метод бифуркаций и метод Ляпунова* с целью автоматизации процесса оценки.

Нечёткая модель оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН разработана в среде MATLAB.

4 Алгоритм для реализации метода разграничения доступа на основе виртуальных машин при использовании образовательных информационных систем с информацией специального назначения и результаты экспериментальных исследований

4.1 Алгоритм для реализации метода разграничения доступа на основе виртуальных машин при использовании образовательных информационных системах с информацией специального назначения

Согласно оценке критерия осведомлённости слушателей по осуществлению НСД к гипервизору через виртуальные машины, выбираемого на основе правил в таблице 2.5, формируются условия оценки критерия осведомлённости на основе экспертных оценок слушателей.

Согласно нечёткой модели NSD_SV_0.fis оценивания критерия осведомлённости определяется в соответствии с правилами. На рис. 4.1 показаны входные функции принадлежности. Конечная оценка различных вариантов решения показана на рис. 4.2, 4.3, 4.4, 4.5, 4.6 для принадлежности (ранжирования) слушателей в сильную группу, а рис. 4.7, 4.8, 4.9, 4.10 для принадлежности (ранжирования) слушателей в среднюю группу.

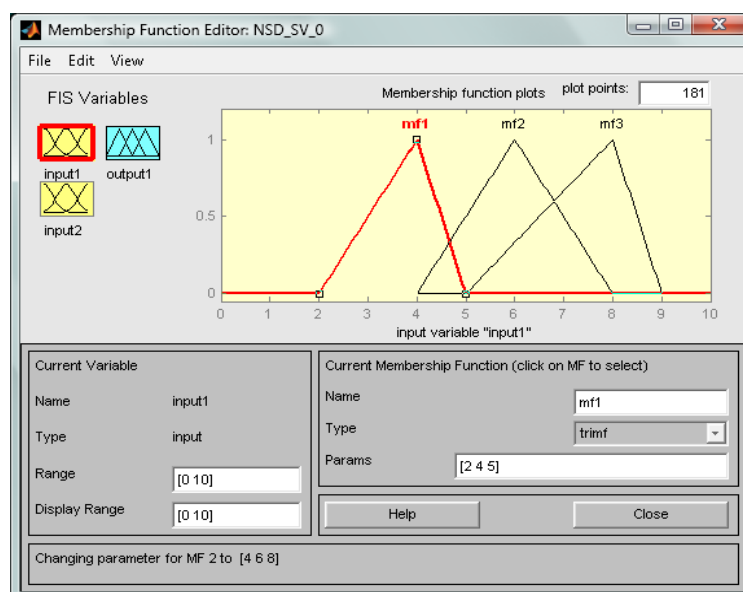


Рисунок 4.1 – Функции принадлежности входов, соответствующие фрагменту таблицы 2.5 (mf1 с параметрами 2,4,5; mf3 с параметрами 5, 8, 9)

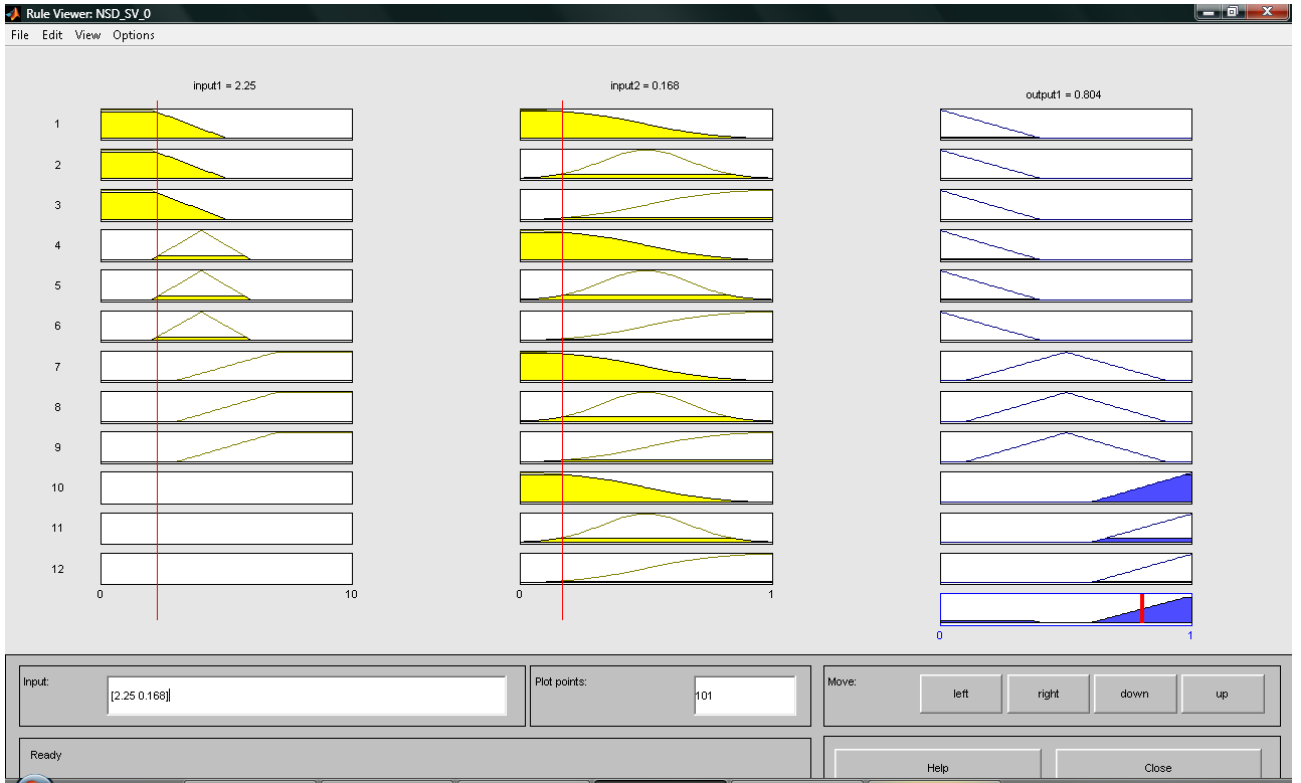


Рисунок 4.2 – Результаты ранжирования в сильную группу (критерий осведомлённости выше 0,7)

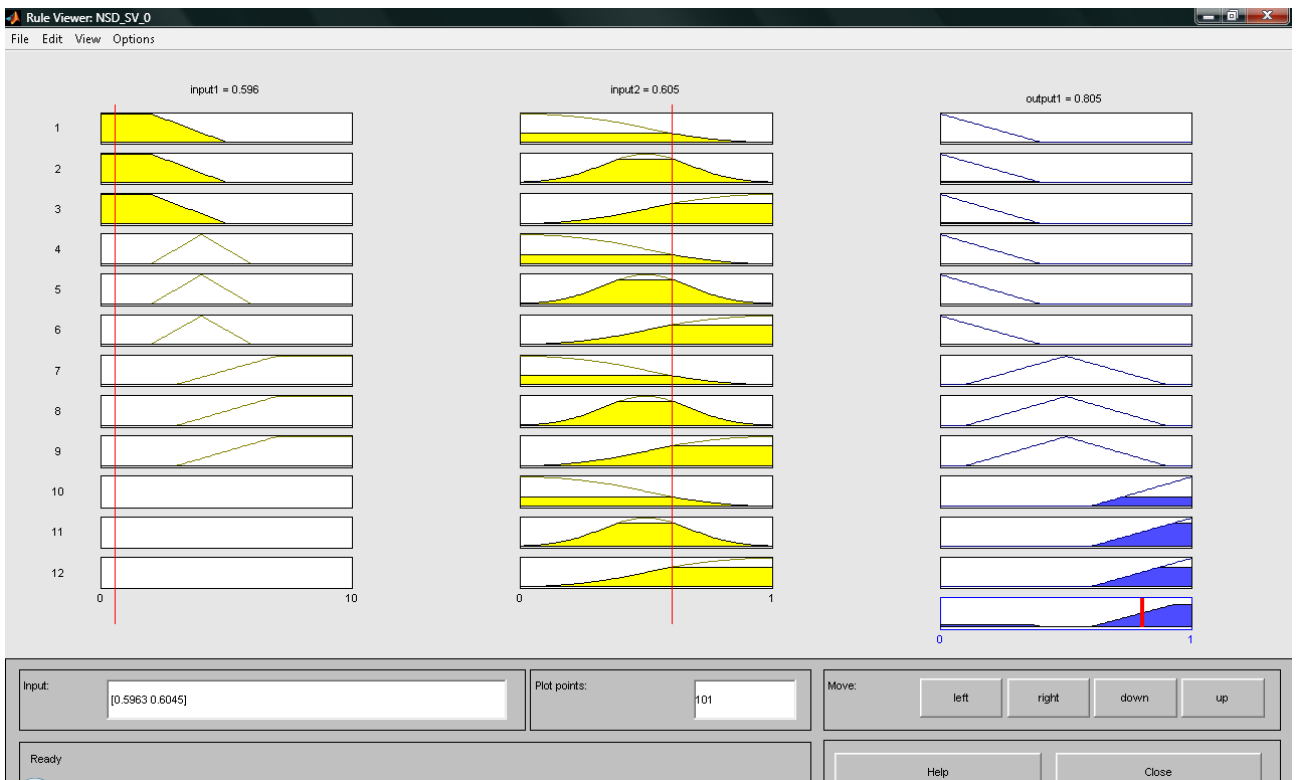


Рисунок 4.3 – Результаты ранжирования в сильную группу (критерий осведомлённости выше 0,7)

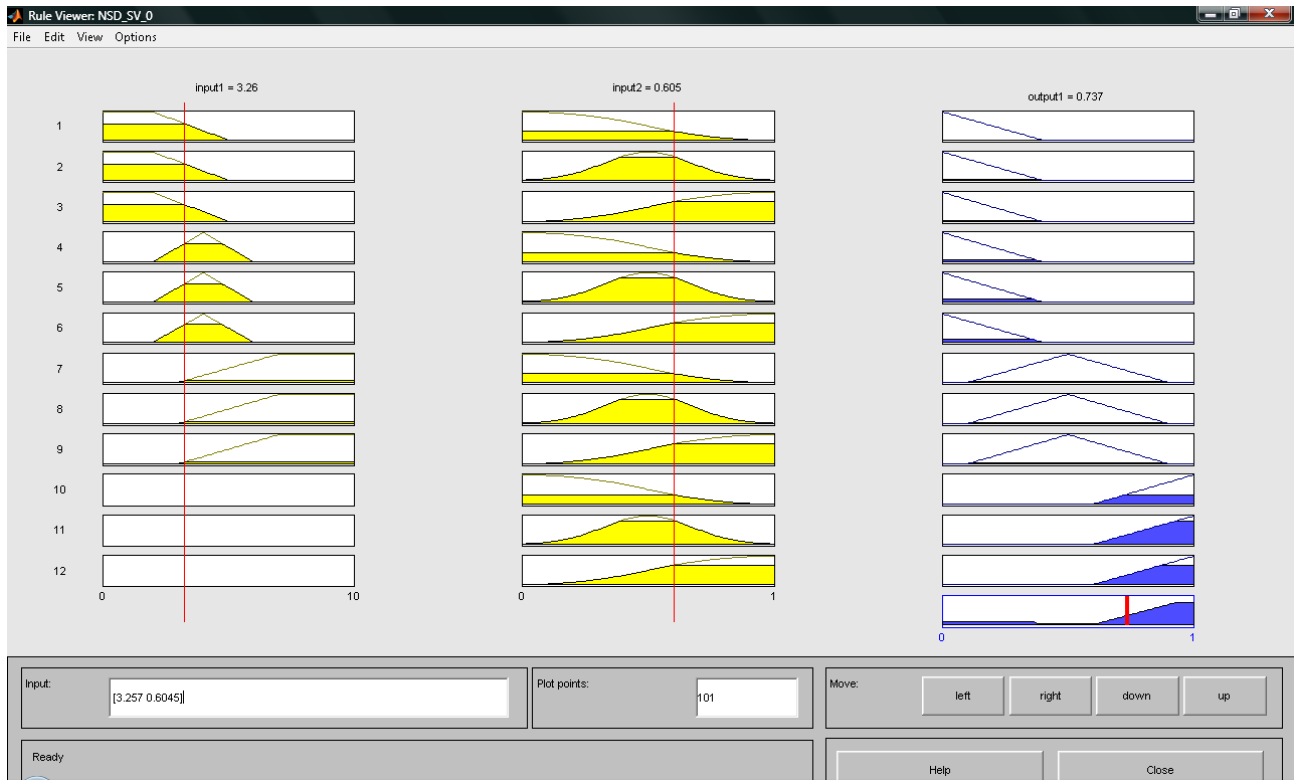


Рисунок 4.4 – Результаты ранжирования в сильную группу (критерий осведомлённости выше 0,7)

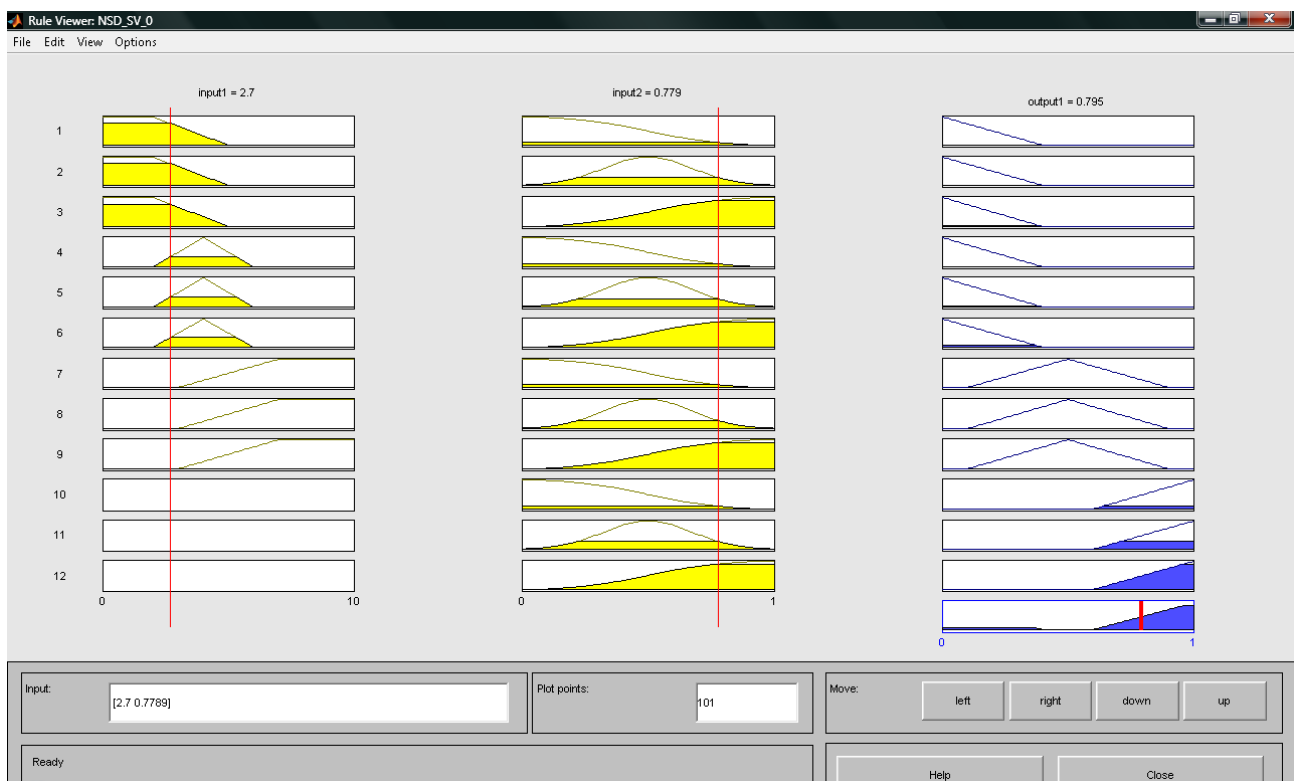


Рисунок 4.5 – Результаты ранжирования в сильную группу (критерий осведомлённости выше 0,7)

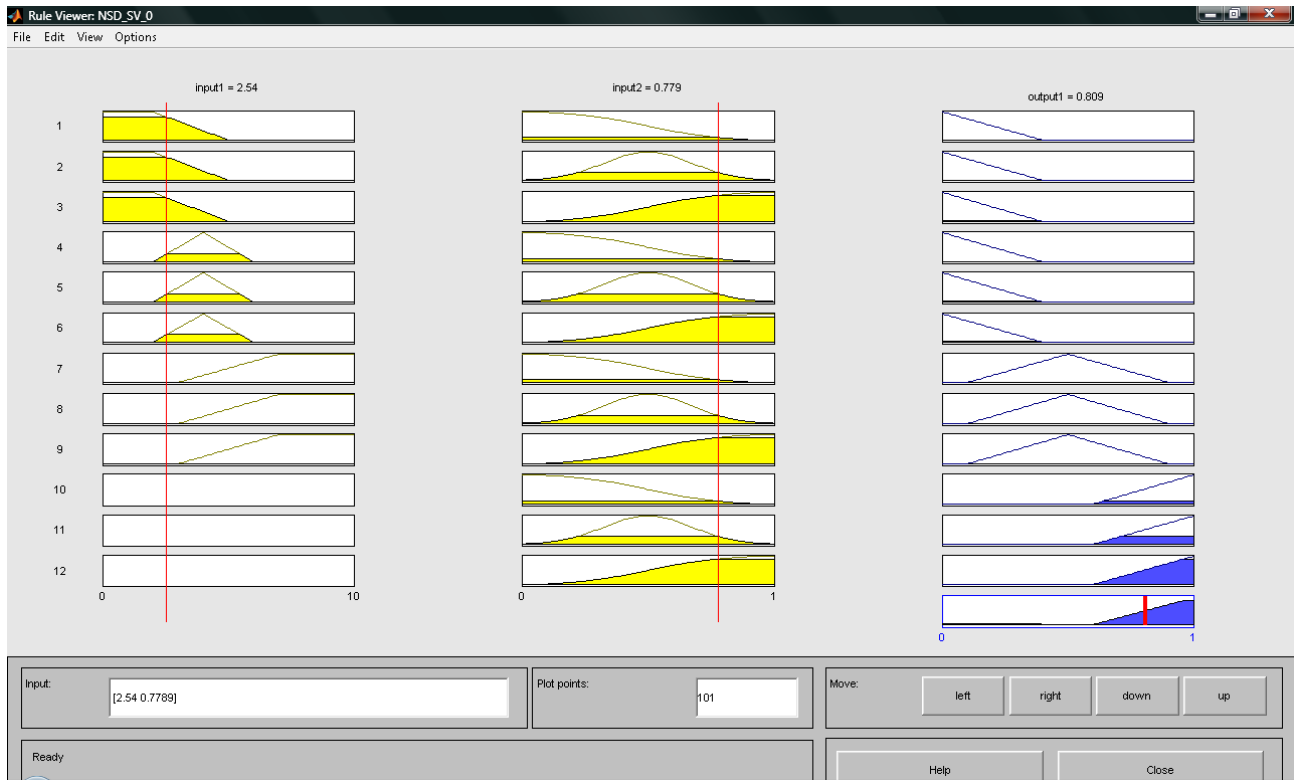


Рисунок 4.6 – Результаты ранжирования в сильную группу (критерий осведомлённости выше 0,7)

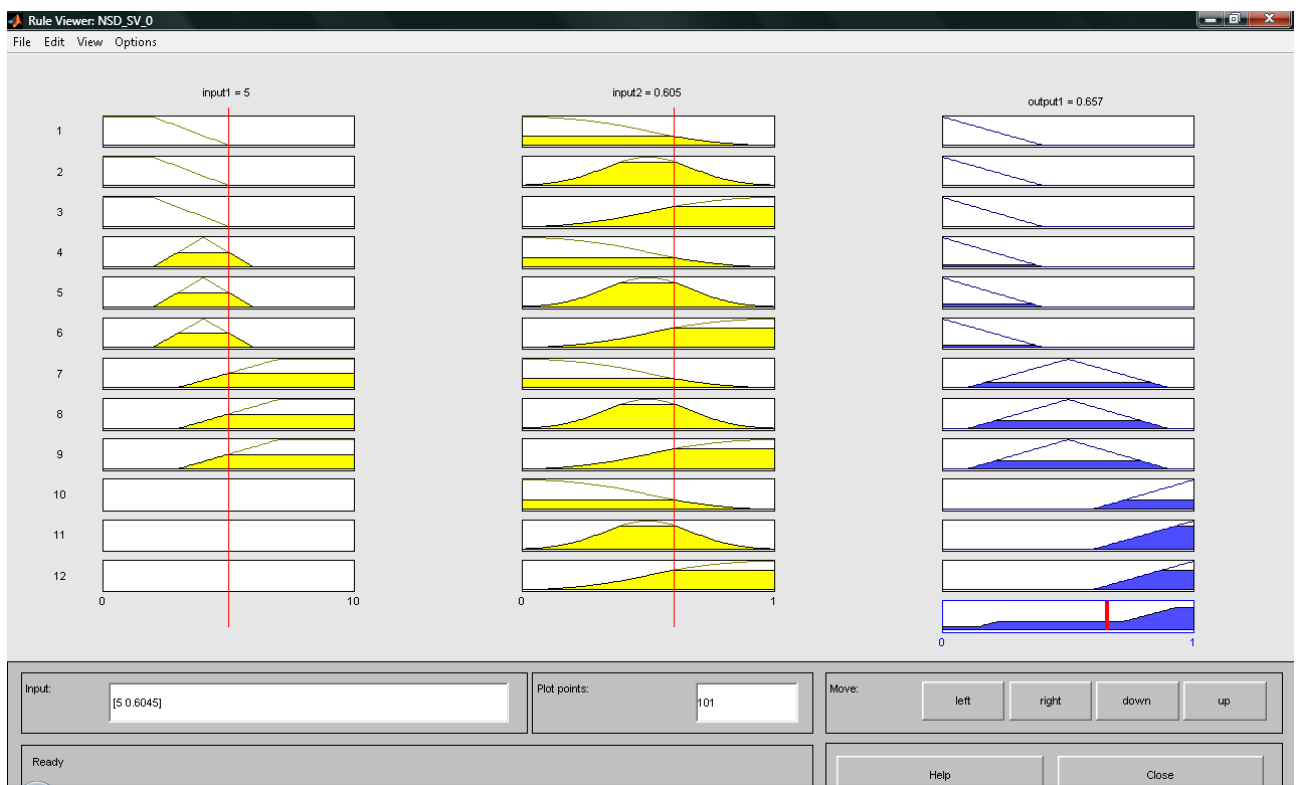


Рисунок 4.7 – Результаты ранжирования в среднюю группу (критерий осведомлённости в пределах 0,3- 0,69)

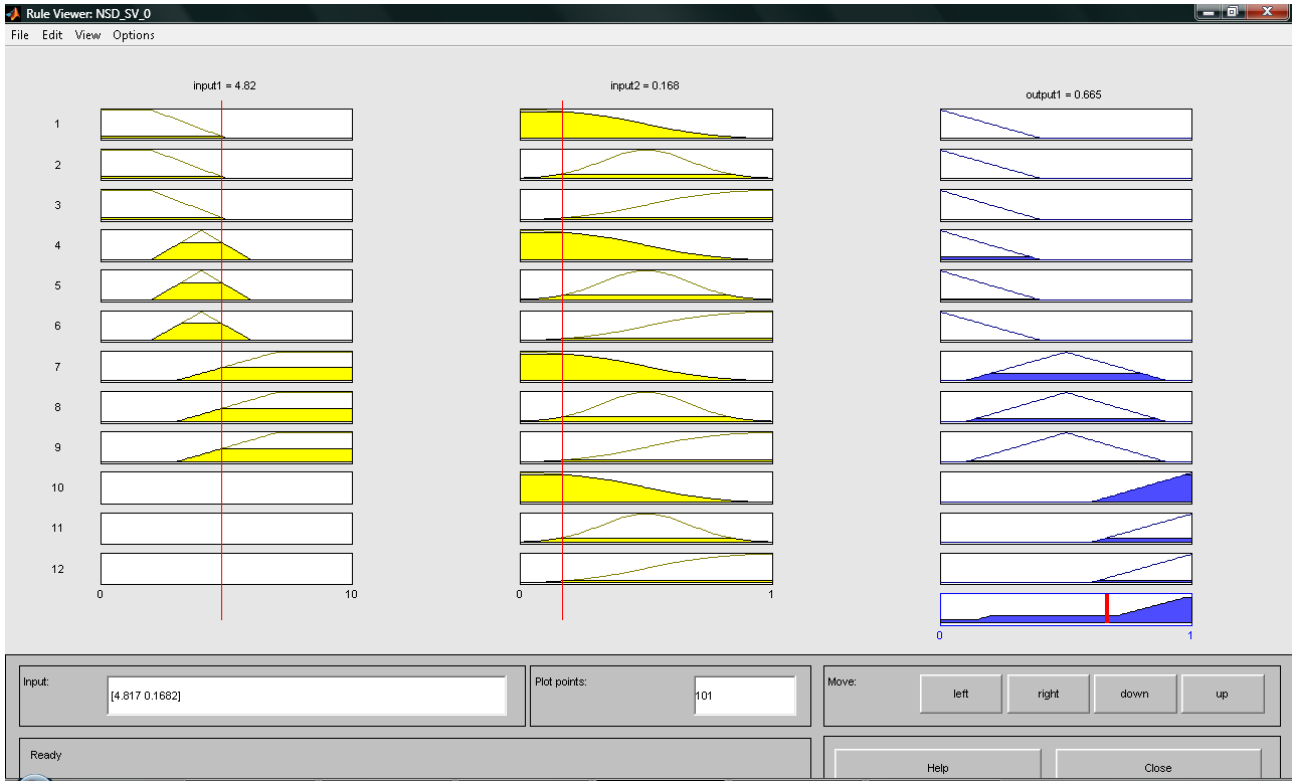


Рисунок 4.8 – Результаты ранжирования в среднюю группу (критерий осведомлённости в пределах 0,3- 0,69)

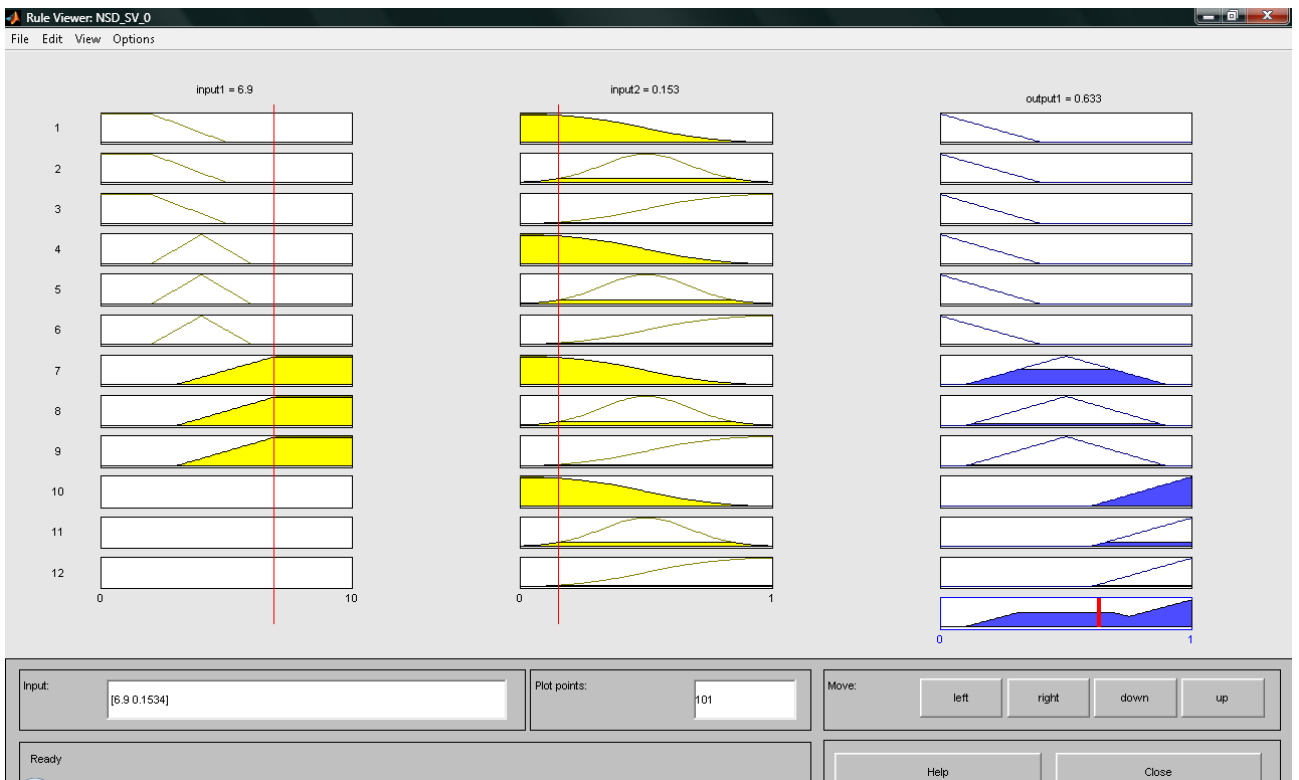


Рисунок 4.9 – Результаты ранжирования в среднюю группу (критерий осведомлённости в пределах 0,3- 0,69)

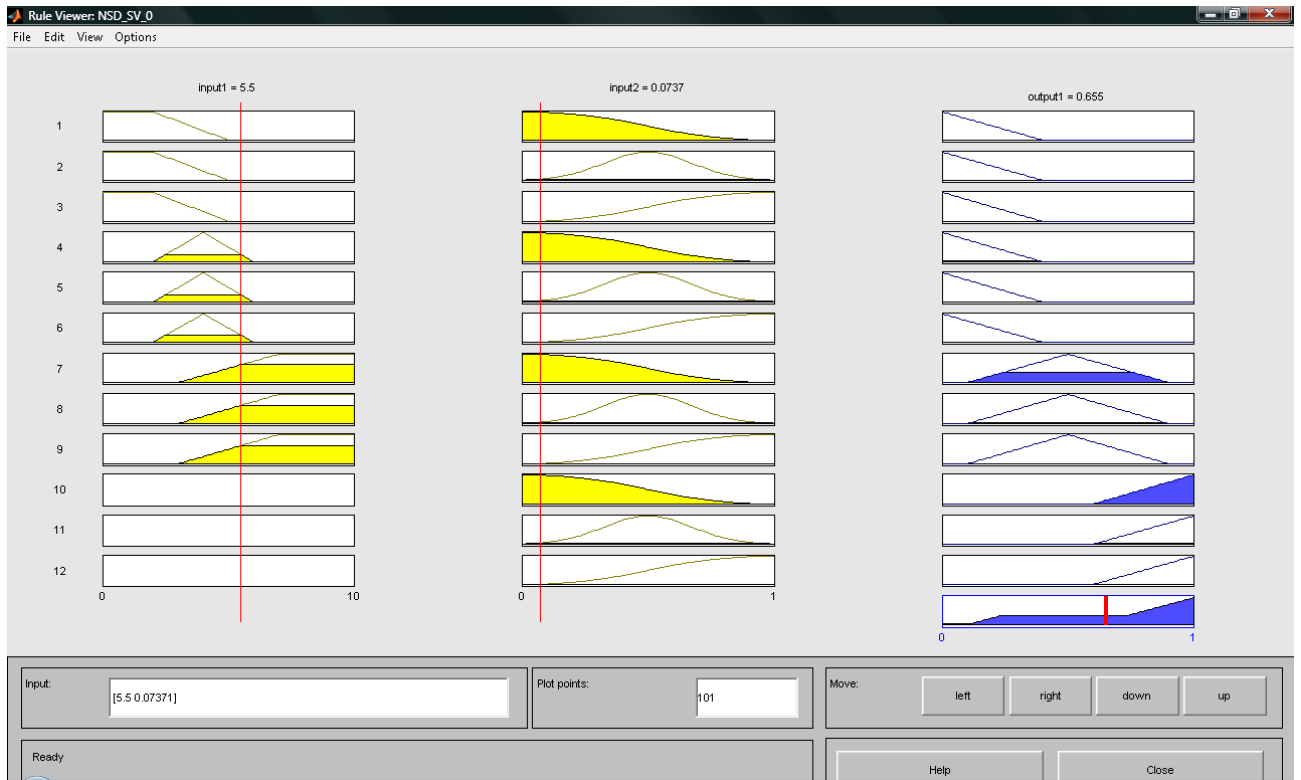


Рисунок 4.10 – Результаты ранжирования в среднюю группу (критерий осведомлённости в пределах 0,3- 0,69)

Таким образом, на основе реализации нечёткой модели NSD_SV_0.fis и её оценки обработка результатов тестов показала довольно высокий потенциал прибывших на обучение слушателей.

Сам алгоритм *метода разграничения доступа* на основе виртуальных машин при использовании образовательных информационных систем с информацией специального назначения представлен на рис. 4.11.

Своевременность формирования профилей разграничения доступа с использованием предложенного метода возросло на 19,65% без снижения устойчивости к НСД к гипервизору через виртуальные машины. Несвоевременность настройки параметров СРД с предложенным методом разграничения доступа на основе виртуальных машин за весь период проводимых исследований не выявлено.

4.2 Результаты экспериментальных исследований по оценке критерия устойчивости к НСД в ОИСИСН

Применительно к нечёткой модели (NSD_SV.fis) оценивания возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН оказались более низкими, что определяет сложность при выполнении практических навыков в условиях противодействия СЗИ от НСД и разграничения доступа к информации. К тому же имеется ограничение действий по времени.

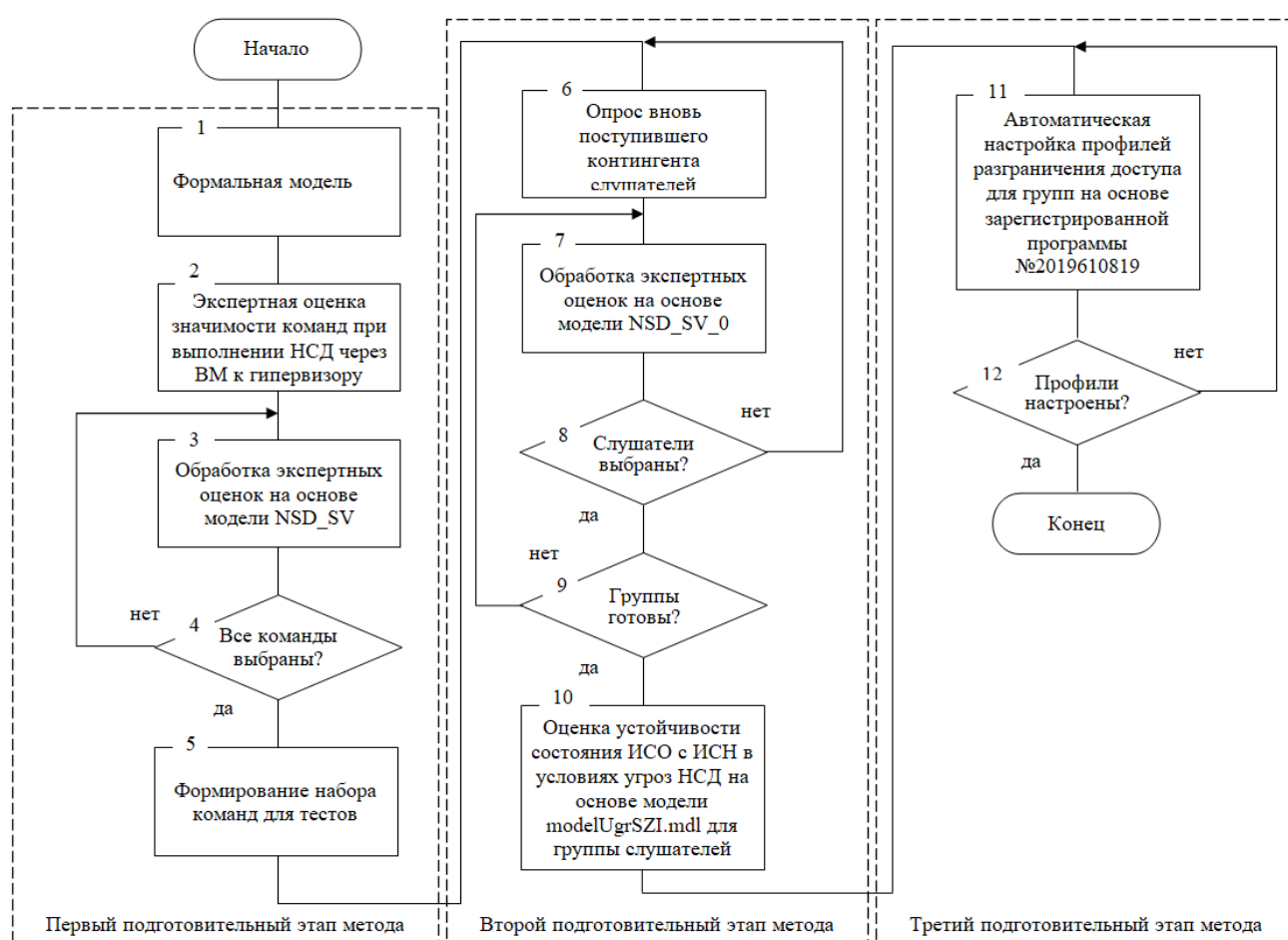


Рисунок 4.11 – Алгоритм *метода разграничения доступа* на основе виртуальных машин при использовании образовательных информационных систем с информацией специального назначения

Это определяется следующими результатами функционирования нечёткой модели (NSD_SV.fis) оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины в ОИСИСН.

Для значений со средним уровнем знаний оценка возможностей реализации угроз НСД к гипервизору через виртуальные машины снижается значительно (рис. 4.12, 4.13, 4.14).

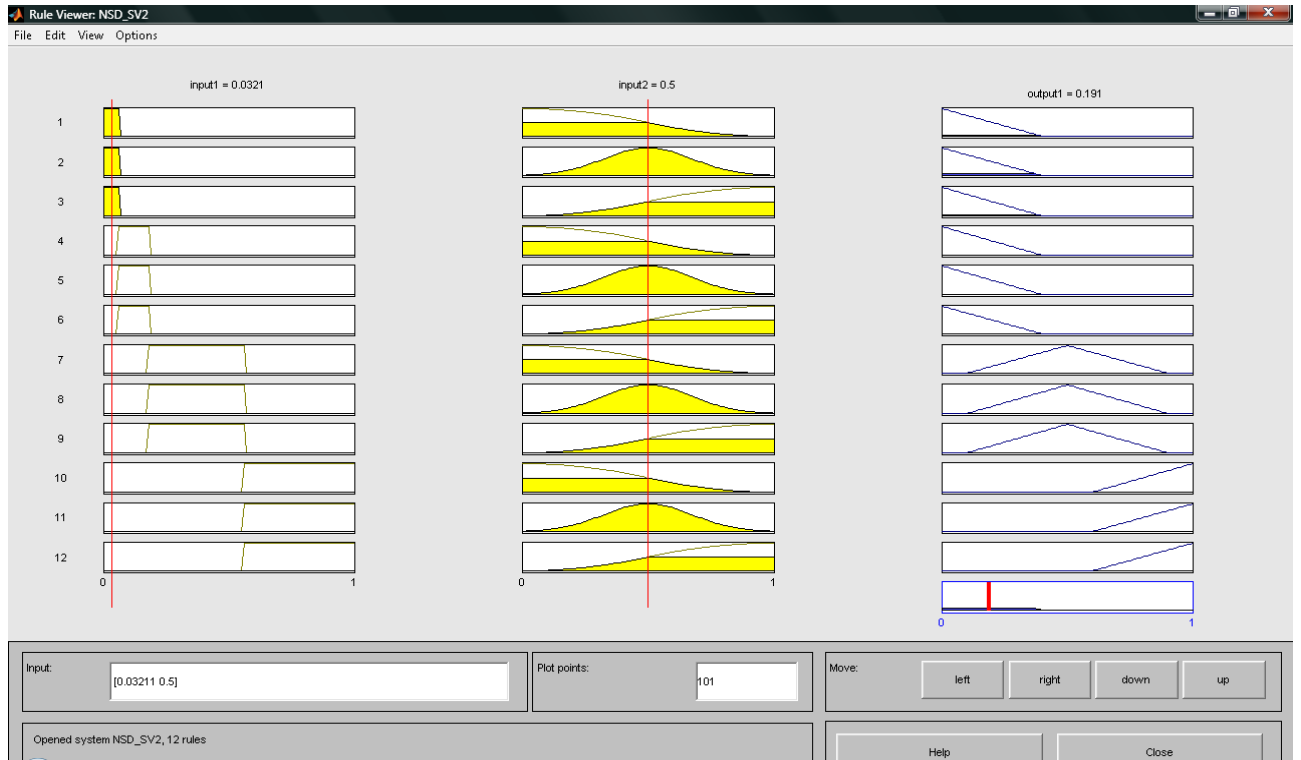


Рисунок 4.12 – Результаты оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины со средним уровнем знаний

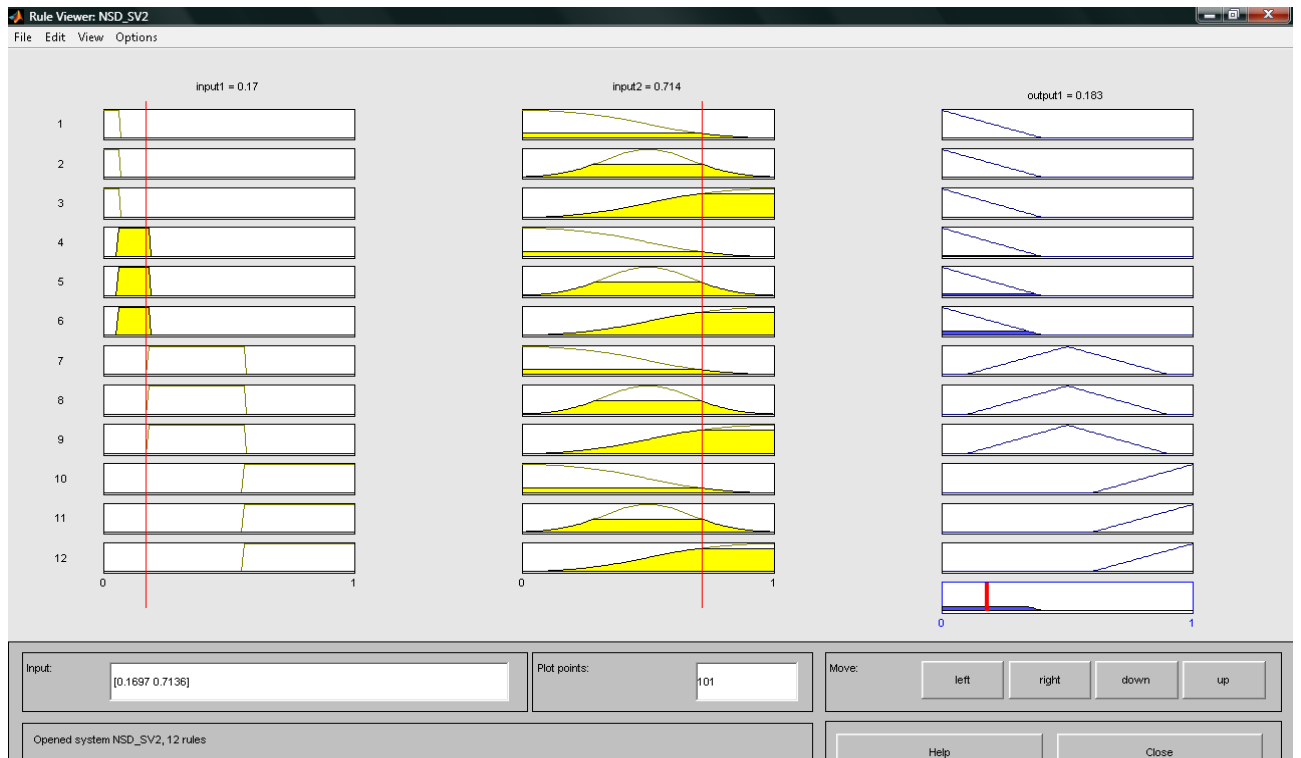


Рисунок 4.13 – Результаты оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины со средним уровнем знаний

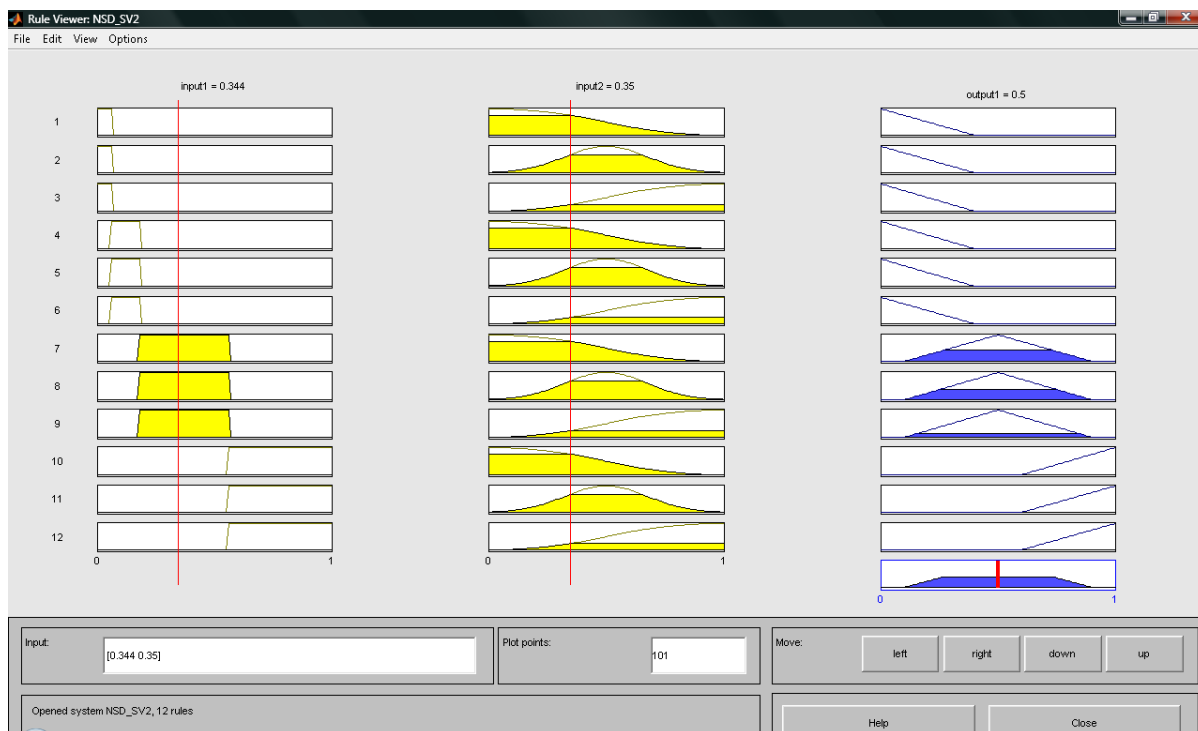


Рисунок 4.14 – Результаты оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины со средним уровнем знаний

Для слушателя с высокими навыками работы на системном уровне оценка возможностей реализации угроз НСД к гипервизору через виртуальные машины снижается незначительно (рис. 4.15). Это доказывает адекватность построенных моделей на основе правил нечёткой логики.

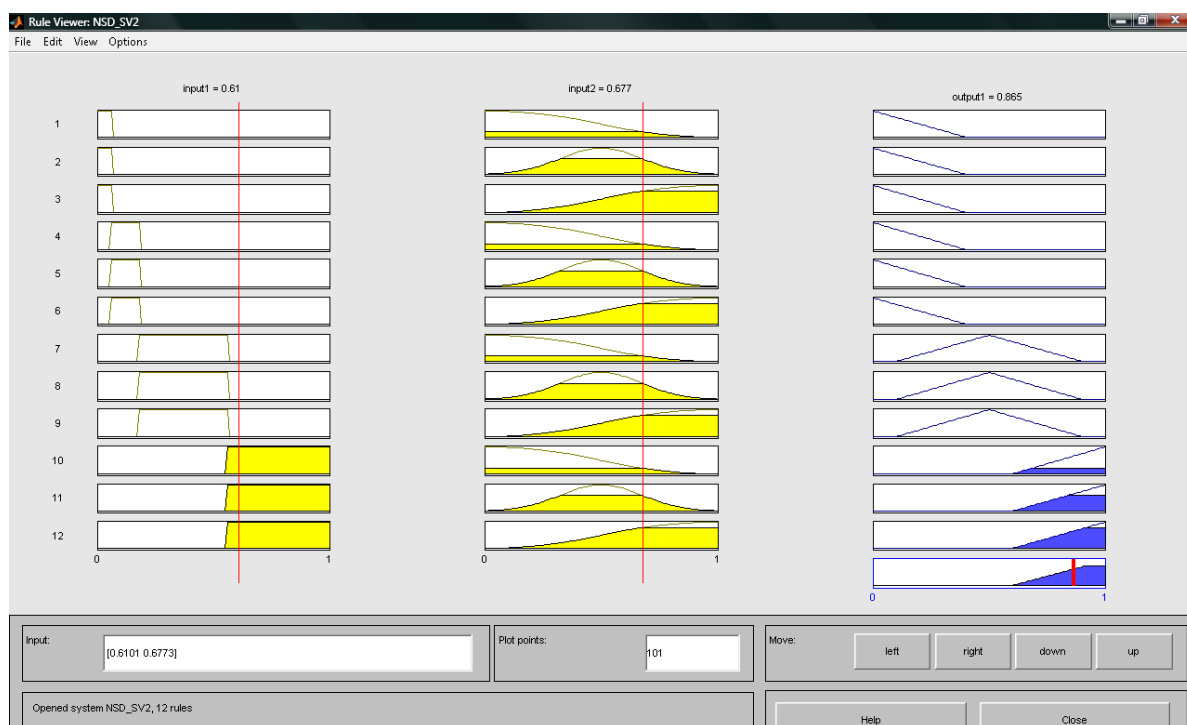


Рисунок 4.15 – Результаты оценки возможностей реализации угроз НСД к гипервизору через виртуальные машины с высокими навыками работы на системном уровне

Таким образом, получаемые результаты нейронечёткой модели оценивания возможностей реализации угроз НСД к гипервизору через виртуальные машины адекватны реальным процессам, происходящих в образовательных информационных системах с информацией специального назначения.

4.3 Результаты экспериментальных исследований нейронечёткой модели и средства оценки устойчивости для создания профилей разграничения доступа, построенной с применением технологии «тонкий клиент»

Получаемые результаты на основе разработанной нейронечёткой модели modelUgrSZI.mdl выявления угроз НСД к информации в виртуальной среде ОИСИСН, построенной с применением технологии «тонкий клиент», позволяют учитывать этапы НСД, критерий осведомлённости, взаимодействие временных процессов как нарушителя, так и СЗИ на основе технологии «тонкий клиент».

Исходя из того, что управление системой разграничения доступа (в условиях динамики состояния ОИСИСН к угрозам НСД к гипервизору через виртуальные машины) учитывает некоторую неопределённость качественных и количественных параметров, её можно квалифицировать как нечёткую систему управления с неизвестными моделями объектов. Ввиду этого для таких систем используется оценка по критерию устойчивости на основе метода бифуркаций и метода Ляпунова. Результаты оценки устойчивости состояний ОИСИСН в условиях угроз НСД на каждом этапе по методу бифуркаций (y_1 - y_5) представлены на рис. 4.16-4.20. На них показано, что на первых трех этапах (0, 1 и 2) имеются бифуркации, и это определяет в этих точках возможность перехода из неустойчивого положения в два устойчивых (метод «вилка») более высокого порядка. После третьего этапа (3, 4, 5 и результирующего за все этапы 6) такого не происходит, что характеризует устойчивость к НСД.

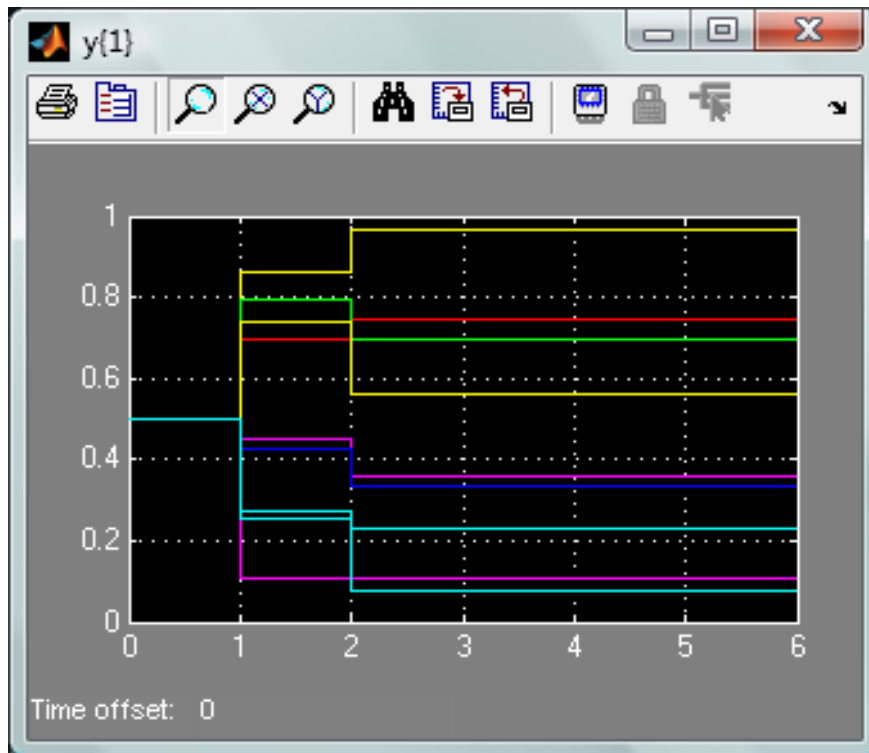


Рисунок 4.16 – Результаты осуществления оценки устойчивости состояния ОИСИСН в условиях угроз НСД для создания профилей разграничения доступа для отдельной группы слушателей на 2 этапе

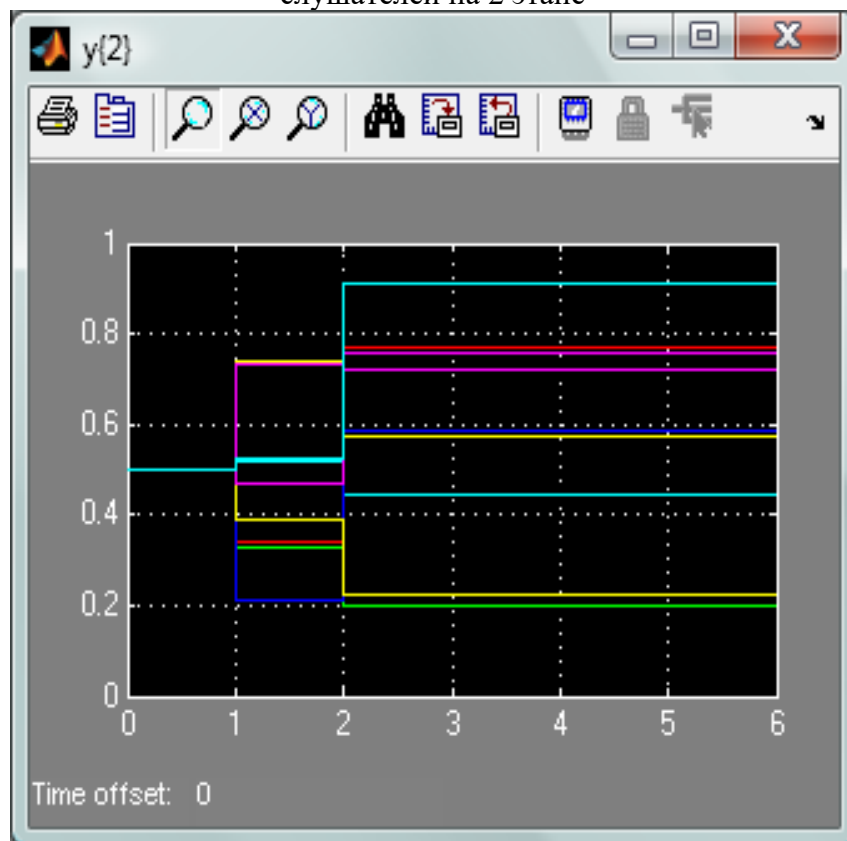


Рисунок 4.17 – Результаты осуществления оценки устойчивости состояния ОИСИСН в условиях угроз НСД для создания профилей разграничения доступа для отдельной группы слушателей на 3 этапе

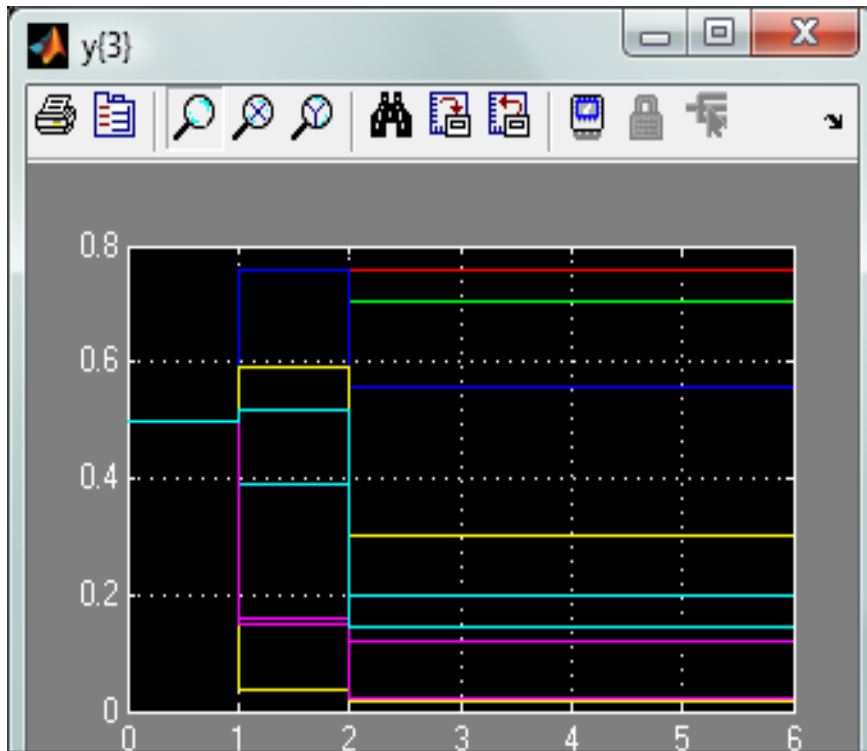


Рисунок 4.18 – Результаты осуществления оценки устойчивости состояния ОИСИСН в условиях угроз НСД для создания профилей разграничения доступа для отдельной группы слушателей на 4 этапе

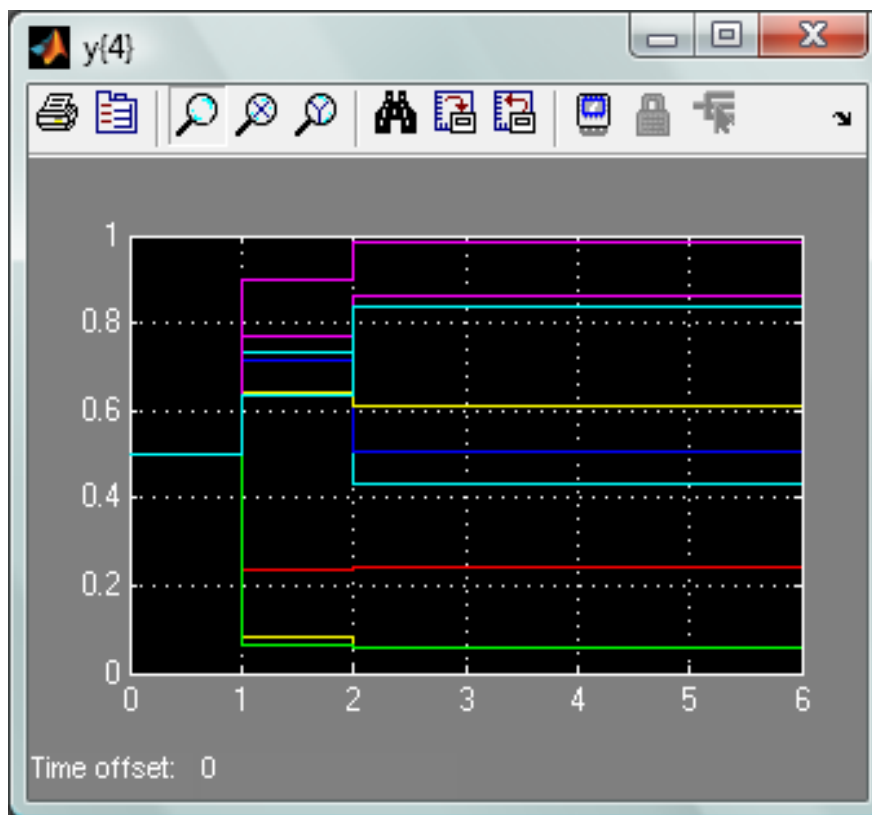


Рисунок 4.19 – Результаты осуществления оценки устойчивости состояния ОИСИСН в условиях угроз НСД для создания профилей разграничения доступа для отдельной группы слушателей на 5 этапе

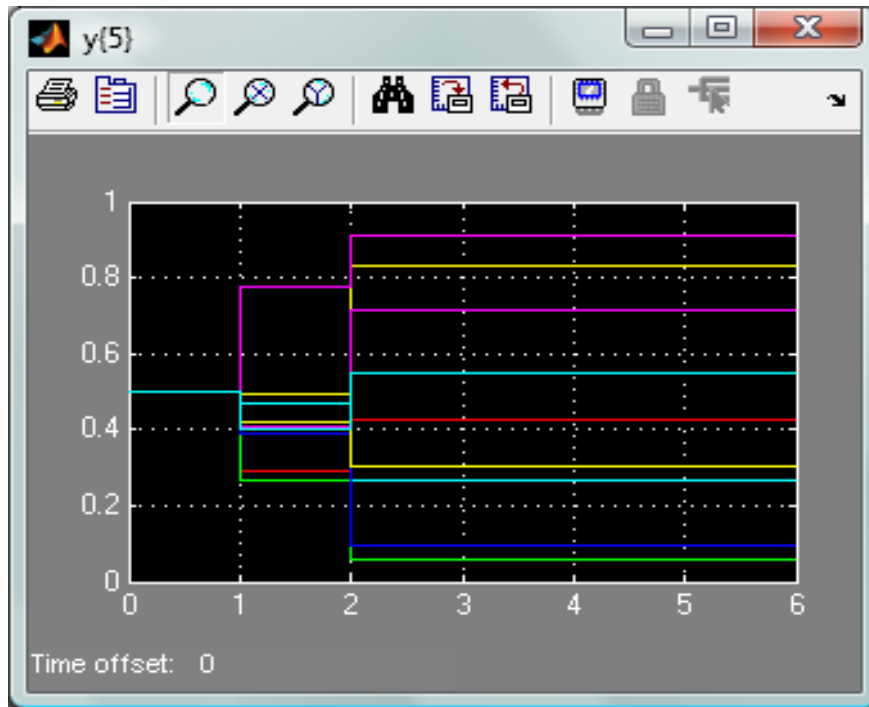


Рисунок 4.20 – Результаты осуществления оценки устойчивости состояния ОИСИСН в условиях угроз НСД для создания профилей разграничения доступа для отдельной группы слушателей на 6 этапе

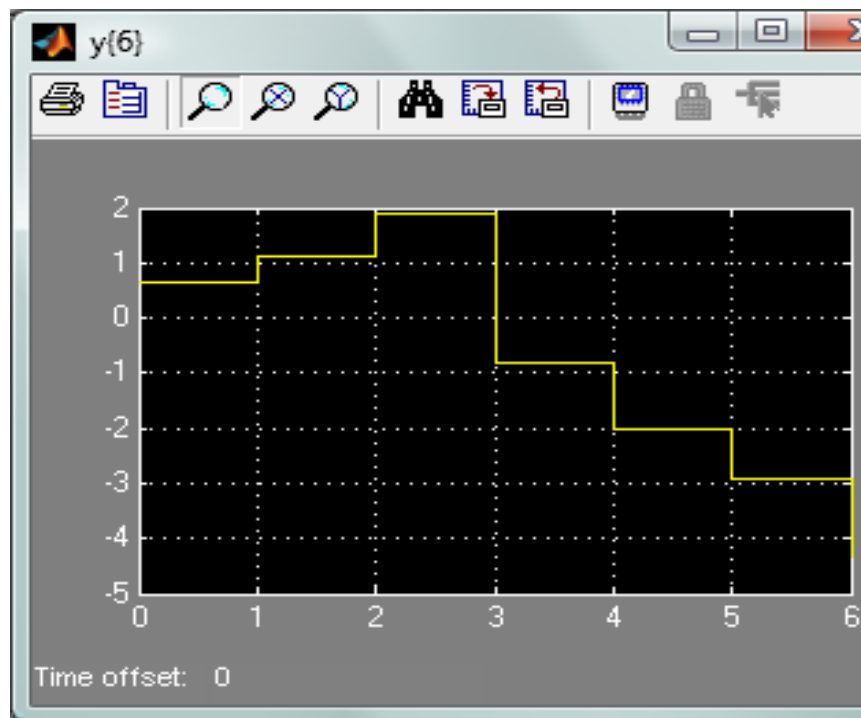


Рисунок 4.21 – Результаты осуществления оценки устойчивости ОИСИСН в условиях угроз НСД для создания профилей разграничения доступа для отдельных групп

Результирующая оценка (рис. 4.21) показывает, что после 3 этапа никому не удалось преодолеть разграничение доступа на основе технологии «тонкий

клиент», во-первых, по критерию метода «вилка» нет перехода в неустойчивое состояние и поэтому в целом после третьего этапа НСД СРД становится устойчивой, во-вторых, по критерию Ляпунова для каждого из первых трёх этапов имеются положительные оценки, что подразумевает наличие неустойчивости к НСД для осуществления начальных этапов, однако для последующих этапов и для НСД к гипервизору через виртуальные машины в целом не реализуется. Таким образом, СРД для выбранных условий является устойчивой.

В случае удовлетворения таких результатов формируется соответствующий профиль разграничения доступа по технологии «тонкий клиент» на основе виртуальных машин применительно к отдельной группе слушателей с соответствующими навыками работы с используемым ими программным и техническим обеспечением.

4.4 Выводы

Полученные результаты экспериментальных исследований подтверждают адекватность разработанных моделей и средств оценки возможностей реализации угроз НСД. Так, функционирование модели позволяет выявлять возможные нарушения либо на конечном, либо на промежуточном этапе НСД, что определяется набором исходных параметров, который приводит к вероятности нарушения. Реализованный алгоритм *метода разграничения доступа* с использованием виртуальных машин применительно к ОИСИСН *отличается* тем, что основан на использовании совокупности предложенных моделей и метода диссертационных исследований, а также на основе зарегистрированной программы для ЭВМ, что позволяет оценивать возможность осуществления несанкционированного доступа на каждом из этапов с учётом определения устойчивости.

Предложенное «Программное средство разработки моделей и метода для анализа рисков нарушения информационной безопасности в информационных

системах специального назначения» имеет производительность 0.01с для оценки конкретного набора слушателей с вероятностью $0.23 \cdot 10^{-2}$ осуществления НСД за заданный интервал времени $T_{\text{зад}}$ (рис. 4.22).

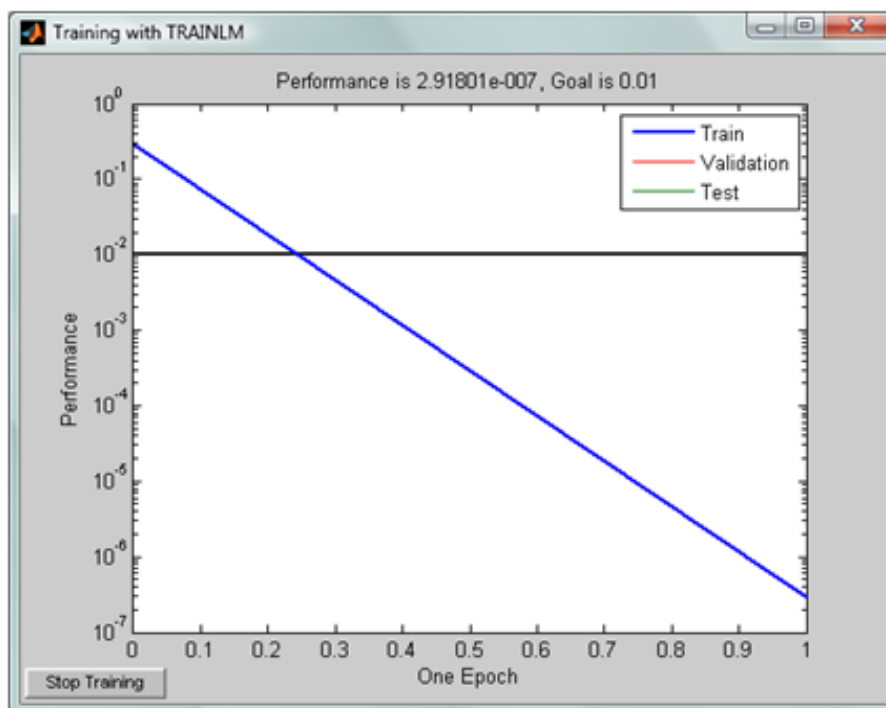


Рисунок 4.22 – Время оценки устойчивости состояния ОИСИСН в условиях угроз НСД к гипервизору через виртуальные машины

ЗАКЛЮЧЕНИЕ

В диссертационной работе решена научная задача создания моделей нечёткой логики и нейронных сетей, учитывающих нечёткие релевантные параметры при технологии виртуализации на базе «тонкого клиента» для оценки устойчивости к несанкционированному доступу к гипервизору через виртуальные машины. Была обеспечена своевременность настройки профиля разграничения доступа к информации специального назначения в образовательных информационных системах в условиях быстро меняющегося контингента и компетенций субъектов доступа. Решенная задача имеет существенное значение для развития подходов по формированию моделей и методов выявления угроз нарушения информационной безопасности объектов различного вида и класса; технологии определения осведомлённости пользователей и субъектов информационных процессов, совершенствовании системы разграничения доступа; а также модификации моделей, методов и средств оценки состояния информационных систем с информацией специального назначения от НСД.

Кроме того, в работе получены следующие **научные результаты**, составляющие **итоги исследования**:

1. Разработана **нечёткая модель определения значимости команд при реализации угроз НСД к гипервизору через виртуальные машины в образовательных информационных системах, опирающаяся на новый подход для формирования границ функций принадлежности для лингвистических значений входа «не важна», «слабо важна», «важна», «очень важна»** на основе обработки экспертных оценок, что дало возможность сформировать **формальную модель нарушителя**, учитывающую специфику технологии «тонкого клиента» на основе виртуальных машин и позволяющую формировать качественные и количественные параметры с их взаимосвязями, что разрешает в некоторых случаях снижать параметры неопределённости до

нуля для дальнейшего обеспечения ранжирования слушателей по отдельным группам на основе оценённых **компетенций** для формирования профилей СРД.

2. Разработана **нечёткая модель оценивания возможности для реализации угроз НСД в ОИСИСН к гипервизору через виртуальные машины**, опирающаяся на результаты экспертной оценки неформализованных ответов слушателей по тесту знаний различных команд для определения **осведомлённости слушателей** на основе критериев, базируемых на правилах нечёткой логики в соответствии с методом суммирования нечетких чисел с L – R правилом и использованием дефаззификации результирующего показателя методом центра сумм, дающая возможность **ранжирования на три группы**.

3. Разработана **нейронечёткая модель оценивания динамики состояния ОИСИСН в условиях угроз НСД к гипервизору через виртуальные машины**, опирающаяся на такие релевантные параметры формальной модели нарушителя, как **количество этапов** для осуществления НСД к информации, **входные параметры и их количество для каждого этапа, значимость параметров на каждом этапе, возможность реализации параметров НСД и задержка выполнения этапа НСД слушателем** и их взаимосвязь на основе математического аппарата нейронных сетей в виде **системы уравнений, описывающих динамику каждого отдельного этапа и их взаимодействие**. В модели используется **оценка устойчивости к НСД к гипервизору через виртуальные машины** на основе методов **бифуркаций и Ляпунова**, а также реализация **средства** автоматизации этого процесса с использованием зарегистрированной программы для ЭВМ, что влечёт за собой сокращение времени определения состояния системы разграничения доступа до 10^{-2} с.

4. Разработан **алгоритм для реализации метода разграничения доступа** с использованием виртуальных машин применительно к образовательным информационным системам с информацией специального назначения, отличающийся от имеющихся тем, что позволяет оценивать возможность осуществления НСД на каждом из этапов с учётом определения устойчивости,

за счёт чего своевременность формирования профилей разграничения доступа возросло на 19,65% без снижения устойчивости к НСД к гипервизору через виртуальные машины, а также несвоевременность настройки параметров СРД с предложенным методом разграничения доступа на основе виртуальных машин за весь период проводимых исследований не выявлена.

Сформулированы **рекомендации** по применению разработанного алгоритма по **методу разграничения доступа** на основе виртуальных машин при использовании ОИСИСН и в дальнейших научных исследованиях. Результаты диссертационных исследований, дают возможность для формирования нового подхода раграничения доступа к информации специального назначения, используемой в процессе обучения и требующей дополнительного ограничения на время переконфигурирования этой системы. Предложенные модели формируют дополнительные средства по осуществлению разграничения доступа в условиях априорной неопределённости об осведомлённости слушателей.

В качестве **перспектив дальнейшей разработки** тематики можно выделить исследования, связанные с расширением возможности использования введённого показателя оценки устойчивости не только для НСД к гипервизору через виртуальные машины, но и для более широкого спектра угроз, влияющих на оценку защищённости информации как в информационных системах, так и в образовательных информационных системах. Целесообразно расширять спектр применения разработанных в ходе диссертационных исследований моделей, а также введённых критериев оценки устойчивости к внешним и внутренним угрозам информационной безопасности в целом, что также влияет на повышение эффективности функционирования системы разграничения доступа, особенно для защиты информации специального назначения.

Результаты являются развитием научных работ [121–174]. Они позволят снизить время на настройку систем разграничения доступа от НСД к гипервизору через виртуальные машины, оценить устойчивость к

несанкционированным действиям в условиях неопределённости исходных данных о контингенте информационных систем обучения. Практическая значимость результатов диссертационного исследования состоит в том, что они могут быть успешно реализованы в рамках компонента анализа защищенности от НСД к информационным системам, использующим технологии виртуальных машин на базе тонкого клиента. Апробация полученных результатов проводилась на 13 научно-технических конференциях. Основные результаты, полученные автором, опубликованы в 54 научных работах.

Полученные результаты работы соответствуют специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

ОИС – образовательная информационная система;

ИСН – информация специального назначения;

ОИСИСН – образовательная информационная система с информацией специального назначения;

НСД – несанкционированный доступ;

ОС – операционная система;

РД – разграничение доступа;

СЗИ – система защиты информации;

СРД – система разграничения доступа;

НСД к ГВМ – несанкционированный доступ к гипервизору через виртуальную машину;

BIOS – базовая система ввода-вывода;

СПО – системное программное обеспечение;

С-регистр – регистр управления;

S-регистр – сегментный регистр;

РОН – регистры общего назначения;

АПВР – аппаратно-программное виртуализационное решение;

АВ – аппаратная виртуализация;

ПГБ – программный гипервизор безопасности;

ПБ – политика безопасности;

ВВХ – вероятностно-временные характеристики;

АС – автоматизированная система;

УБИ – угрозы безопасности информации;

БИ – безопасность информации;

ВМ – виртуальная машина;

нВ – невероятный;

сВ – средневероятный;

вВ – высоковероятный;

НВ – не важна;

СВ – слабо важна;

В – важна;

ОВ – очень важна.

СПИСОК ЛИТЕРАТУРЫ

1. **Мелл, П.** Полное руководство по общей системе оценки уязвимостей: версия 2.0 [Электронный ресурс]/ П. Мелл, С. Романоски. – Режим доступа: <https://www.first.org/cvss/v2/guide> (по состоянию на 23.04.2020).
2. Методика определения угроз безопасности информации в информационных системах. Методический документ ФСТЭК России: проект. – М.:Стандартинформ, 2015. – 43 с.
3. **Абасов, Н.Д.** Метод преобразования и хранения данных, на основе модулярной арифметики, обеспечивающий целостность информации свойствами самовосстановления и контроля / Н.Д. Абасов, А.М. Абасова, О.А. Финько // Информационное противодействие угрозам терроризма. – М., 2013. – № 20. – С. 88-92.
4. **Лахно, В.А.** О построении дискретных процедур распознавания угроз информационной безопасности автоматизированных систем обработки данных критического применения / В.А. Лахно // Вестник БГУ. Серия 1, Физика. Математика. Информатика. – Брянск, 2014. – № 2. – С. 113-118.
5. **Дубровин, А.С.** Общенаучные итоги создания эталонной модели защищенной автоматизированной системы / А.С. Дубровин, А.В. Скрыпников, Т.В. Лютова, Е.В. Глазкова, Е.В. Чернышова // Фундаментальные исследования. – М., 2015. – № 2-15. – С. 3247-3251.
6. **Клянчин, В.К.** О применении нечётких продукционных моделей в подсистемах обеспечения информационной безопасности автоматизированных систем управления специального назначения / В.К. Клянчин, Т.К. Сашников // Научные технологии в космических исследованиях Земли. – М., 2016. – Т. 8. – № S2. – С. 27-32.
7. **Тарасюк, М.В.** Шлюзы информационного взаимодействия категоризированных сетей с сетями общего пользования / М.В. Тарасюк // Защита информации. Инсайд. М., 2009. – № 3 (27). – С. 22-27.

8. **Машкина, И.В.** Разработка метода и функциональной модели численной оценки риска нарушения информационной безопасности и уровня защищенности информации на основе вероятностно-статического подхода / И.В. Машкина, С.Н. Алекса // Известия ЮФУ. Технические науки. – Ростов-на-Дону, 2008. – № 8 (85). – С. 47-54.

9. **Волколуп, М.В.** Оценка защищенности речевой информации на основе анализа многомерных данных / М.В. Волколуп, Д.С. Салита // Труды молодых ученых Алтайского государственного университета. – Барнаул, 2016. – № 13. – С. 268-272.

10. **Козьминых, С.И.** Моделирование систем и процессов обеспечения информационной безопасности в органах внутренних дел / С.И. Козьминых, П.С. Козьминых // Вестник Московского университета МВД России. – М., 2016. – № 2. – С. 161-168.

11. **Росенко, А.П.** Математическая модель определения вероятности последствий от реализации злоумышленником угроз безопасности информации ограниченного распространения / А.П. Росенко, И.В. Бордак // Известия ЮФУ. Технические науки. Ростов-на-Дону, 2015. – № 7 (168). – С. 6-19.

12. **Курочкин, С.И.** Методы оценки уровня защищенности информационных систем / С.И. Курочкин, И.В. Заводцев // Перспективы развития информационных технологий.– М, 2016. – № 29. – С. 197-204.

13. **Екимов, О.Б.** О реализации требований по защите персональных данных в информационной системе Пермского филиала ФГУП «Радиочастотный центр Приволжского федерального округа» / О.Б. Екимов, А.С. Шабуров, И.П. Исаков, П.В. Мазунин, А.Н. Шляков // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления.– Пермь, 2013. – № 8. – С. 144-154.

14. **Белокуров, С.В.** Моделирование способов технического управления защитой информации от несанкционированного доступа в информационно-

телекоммуникационных системах специального назначения / С.В. Белокуров, И.И. Сапрыкин, О.А. Кондратов, А.П. Сидельников // Сборник: Актуальные проблемы деятельности подразделений УИС: сборник материалов Всероссийской научно-практической конференции. Федеральная служба исполнения наказаний, ФКОУ ВПО "Воронежский институт ФСИН России". – Воронеж, 2016. – С. 203-206.

15. **Калиниченко, С.В.** Подход к защите цифровой информации в автоматизированных системах специального назначения на основе применения скрытых метящих средств / С.В. Калиниченко, П.В. Корчагин, В.К. Платонов // Известия ТулГУ. Технические науки. – Тула, 2018. – Вып. 4. – С. 141-149.

16. **Усачев, И.В.** К вопросу о проблеме обеспечения защиты информации в автоматизированных системах специального назначения / И.В. Усачев, А.В. Кий, О.П. Зибров, А.С. Башкирцев, А.Ю. Щербаков // Сборник: Региональная информатика и информационная безопасность. М., 2017. – С. 177-179.

17. **Кондрашов, Ю.В.** Проблема организационно-технического сопряжения систем защиты информации различных автоматизированных систем управления специального назначения / Ю.В. Кондрашов, Е.А. Максименко // Сборник: Региональная информатика и информационная безопасность. М., 2017. – С. 113-114.

18. **Рубцова, И.О.** Функциональный характер показателя эффективности защиты информации от несанкционированного доступа в системах электронного документооборота специального назначения / И.О. Рубцова // Вестник Воронежского института МВД России. Воронеж, 2018. – № 3. – С. 56-63.

19. **Обухова, Л.А.** Направления совершенствования организации защиты информации в системах специального назначения / Л.А. Обухова // Охрана, безопасность, связь. М., 2017. – № 1-2. – С. 210-215.

20. **Обухова, Л.А.** Направления совершенствования программных систем защиты информации в системах специального назначения / Л.А. Обухова // Сборник: Информационные технологии в деятельности правоохранительных органов: проблемы использования и пути повышения эффективности. Сборник научных статей. Редколлегия: Л.Д. Матросова [и др.]. – Орел, 2016. – С. 28-33.

21. **Скрыль, С.В.** Задача распределения временного резерва в интересах оптимизации механизмов защиты информации в инфокоммуникационных системах специального назначения / С.В. Скрыль, С.А. Никулин, Р.А. Хворов, П.Е. Краснов // Информация и безопасность. М., 2013. – Т. 16. – № 1. – С. 69-74.

22. **Никулин, С.А.** Оптимизация механизмов защиты информации в инфокоммуникационных системах специального назначения: утверждения и доказательства / С.А. Никулин, Т.В. Мещерякова, Р.А. Хворов, П.Е. Краснов // Информация и безопасность. – М., 2013. – Т. 16. – № 1. – С. 75-80.

23. **Тептин, Г.М.** Марковские модели средств защиты автоматизированных систем специального назначения / Г.М. Тептин, К.В. Иванов // Ученые записки Казанского государственного университета. Серия: Физико-математические науки. – Казань, 2008. – Т. 150. – № 4. – С. 41-53.

24. **Иванов, К.В.** Марковские модели средств защиты автоматизированных систем специального назначения / К.В. Иванов // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – СПб., 2007. – № 39. – С. 10-19.

25. **Янушкевич, В.Ч.** Защита инфокоммуникационных систем специального назначения от деструктивных программных воздействий / Янушкевич В.Ч. // Инновационные технологии: теория, инструменты, практика. – М., 2014. – № 1. – С. 453-459.

26. **Кочедыков, С.С.** Алгоритм имитационной модели противодействия несанкционированному доступу к автоматизированной информационной системе специального назначения средствами защиты информации / С.С.

Кочедыков, А.В. Душкин, В.И. Новосельцев, Р.Р. Назмиев // Сборник: Математические методы и информационные технологии управления в науке, образовании и правоохранительной сфере. Сборник материалов Всероссийской научно-технической конференции. Московский государственный технический университет имени Н.Э. Баумана, Академия ФСИН России, Рязанский государственный университет имени С.А. Есенина. – М., 2017. – С. 98-103.

27. **Лазарев, А.А.** Модель имитации информационных систем для защиты вычислительных сетей специального назначения в условиях действия злоумышленника / А.А. Лазарев, А.В. Калач, А.А. Зенин // Вестник Воронежского института ФСИН России. – Воронеж, 2018. – № 4. – С. 74-81.

28. **Барсуков, О.М.** Модель процессов защиты автоматизированной системы управления специального назначения от внешних воздействий / О.М. Барсуков, С.А. Будников, В.В. Донской // Информация и безопасность. – М., 2010. – Т. 13. – № 3. – С. 431-434.

29. **Гринь, Д.В.** Защита информации от несанкционированного доступа в автоматизированных системах под управлением операционной системы специального назначения ASTRA LINUX SE / Д.В. Гринь, О.Б. Ильина, О.П. Купчиненко, А.В. Скоропад // Сборник: Региональная информатика и информационная безопасность. – М., 2017. – С. 76-78.

30. **Скрыпников, А.В.** Экспериментальный метод определения вероятностно-временных характеристик систем защиты информации от несанкционированного доступа в автоматизированных информационных системах / А.В. Скрыпников, А.Д. Попов, Е.А. Рогозин, В.А. Хвостов // Вестник Воронежского государственного университета инженерных технологий. – Воронеж, 2017. – Т. 79. – № 4 (74). – С. 90-96.

31. **Бородакий, Ю.В.** О подходах к реализации централизованной системы управления информационной безопасностью АСУ военного и специального назначения / Ю.В. Бородакий, А.Ю. Добродеев, П.А. Нащекин, И.В. Бутусов // Вопросы кибербезопасности. – М., 2014. – № 2 (3). – С. 2-9.

32. **Волостных, В.А.** Проблемы подготовки иностранных военных специалистов к изучению дисциплин, связанных с защитой информации / Волостных В.А., Митрофанов М.В. // Сборник: Русский язык в полиэтническом образовательном пространстве военного вуза Материалы межвузовской научно-практической конференции. Под редакцией Н.В. Давыдовой, Н.Ю. Васильевой. – М., 2017. – С. 473-479.

33. **Буренин, А.Н.** Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей / А.Н. Буренин, К.Е. Легков // Научные технологии в космических исследованиях Земли. – М., 2015. – Т. 7. – № 3. – С. 46-61.

34. **Лаута, О.С.** Подход к оценке защищенности информационно-телекоммуникационной сети специального назначения от технической компьютерной разведки / О.С. Лаута, И.А. Клишов, В.В. Ястребов, Е.В. Русаков // Сборник: Региональная информатика и информационная безопасность – М., 2017. – С. 121-122.

35. **Грязев, А.Н.** Формирование эталонных профилей пользователей для разграничения доступа пользователей в автоматизированных системах специального назначения / А.Н. Грязев, А.В. Кий, И.Б. Саенко, С.А. Ясинский // Труды ЦНИИС. Санкт-Петербургский филиал. – СПб, 2017. – Т. 1. – № 4. – С. 12-23.

36. **Паращук, И.Б.** Вариант формулировки показателей качества современных средств доверенной загрузки и их роль при решении проблем безопасности алгоритмов управления инфотелекоммуникационными системами специального назначения / И.Б. Паращук, А.С. Башкирцев, Л.А. Саяркин // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – М., 2016. – № 5-6 (95-96). – С. 47-51.

37. **Харченко, Е.Б.** Вопросы кибербезопасности инфокоммуникационных систем специального назначения / Е.Б. Харченко, А.М. Сазыкин, Ю.Н.

Лысенков // Известия Российской академии ракетных и артиллерийских наук. – СПб, 2017. – № 2 (97). – С. 38-47.

38. **Петренко, А.А.** Способ повышения устойчивости LTE-сети в условиях деструктивных кибератак / А.А. Петренко, С.А. Петренко // Вопросы кибербезопасности. – М., 2015. – № 2 (10). – С. 36-42.

39. **Легков, К.Е.** Управление инфокоммуникационными услугами в мультисервисных сетях специального назначения / К.Е. Легков, А.И. Мясникова // Научные технологии в космических исследованиях Земли. – М., 2012. – Т. 4. – № 3. – С. 20-22.

40. **Матвиенко, Ю.А.** Методика формирования комплекса мероприятий по защите АСУ СН в условиях информационного противоборства / Ю.А. Матвиенко // Информационные войны. – М., 2007. – № 4 (4). – С. 25-32.

41. **Агеев, С.А.** Управление безопасностью защищенных мультисервисных сетей специального назначения / С.А. Агеев, И.Б. Саенко // Труды СПИИРАН. – М., 2010. – № 2 (13). – С. 182-198.

42. **Буренин, А.Н.** Особенности архитектур, функционирования, мониторинга и управления полевыми компонентами современных инфокоммуникационных сетей специального назначения / А.Н. Буренин, К.Е. Легков // Научные технологии в космических исследованиях Земли. – М., 2013. – Т. 5. – № 3. – С. 12-17.

43. **Буренин, А.Н.** Основные проблемы безопасности подсистем обеспечения единым временем элементов систем управления сложными организационно-техническими объектами / А.Н. Буренин, К.Е. Легков // Т-Сотт: Телекоммуникации и транспорт. – М., 2019. – Т. 13. – № 1. – С. 45-53.

44. **Синюк, А.Д.** Математическая модель нарушителя открытого ключевого согласования сети с минимальным числом корреспондентов / А.Д. Синюк, О.А. Остроумов // Научные технологии в космических исследованиях Земли. – М., 2013. – Т. 5. – № 1. – С. 20-24.

45. **Макаренко, С.И.** Описательная модель сети связи специального назначения / С.И. Макаренко // Системы управления, связи и безопасности. – М., 2017. – № 2. – С. 113-164.

46. **Буренин, А.Н.** Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: управление безопасностью сетей / А.Н. Буренин, К.Е. Легков // Научные исследования в космических исследованиях Земли. – М., 2015. – Т. 7. – № 4. – С. 42-51.

47. **Буренин, А.Н.** Некоторые модели управления безопасностью инфокоммуникационных сетей специального назначения / А.Н. Буренин, К.Е. Легков // Научные исследования в космических исследованиях Земли. – М., 2013. – Т. 5. – № 4. – С. 46-50.

48. **Легков, К.Е.** Модели управления процессами обмена в службе передачи и доставки файлов инфокоммуникационных сетей специального назначения / К.Е. Легков // Научные исследования в космических исследованиях Земли. – М., 2014. – Т. 6. – № 4. – С. 38-43.

49. **Назаров, И.О.** Обеспечение безопасности управлением доступом и информационными потоками в WEB-системе на основе СУБД / И.О. Назаров // Вестник КГТУ им. А.Н. Туполева. – Казань, 2008 - №2 – С.56-59.

50. **Куприянов, А.А.** Модели угроз и защиты от НСД к информации взаимодействия КСА объектов автоматизированных систем / А.А. Куприянов, В.Л. Михеев // Проблемы создания интегрированной АСУ. – Автоматизация процессов управления. – М., 2008. – № 1. – С. 52-60.

51. **Залогин, Р.А.** Методическое обеспечение и математическая модель комплексной оценки угроз НСД к информации при проектировании автоматизированных систем критического применения / Вестник ВГТУ. – Воронеж, 2020. – №1 – С.32-35.

52. **Бокова, О.И.** Разработка имитационной модели системы защиты информации от несанкционированного доступа с использованием программной среды CPN TOOLS / О.И. Бокова, Д.И. Коробкин, С.А. Кухарев, А.Д. Попов //

Безопасность информационных технологий. – М., 2019. – Том 26 – № 3 – 80-89.

53. **Касаткина, Т.И.** Математическое моделирование процесса оценки безопасности обработки информации в автоматизированной системе управления / Т.И. Касаткина и др. // Промышленные АСУ и контроллеры. – М., 2017. – № 11. – С. 15-28.

54. **Досмухамедов Б.Р.** Анализ угроз информации систем электронного документооборота / Б.Р. Досмухамедов // Компьютерное обеспечение и вычислительная техника. – М., 2009. – №3. – С.140-143.

55. **Патент № 2394271 Российская Федерация, МПК G06F 21/00 (2006.01).** Способ прогнозирования и оценки безопасности достижимых состояний защищённых информационных систем: опубликовано 2008/ Зегжда Д.П., Зегжда П.Д., Калинин М.О. – 16с.

56. **Патент № 105486 U1 Российская Федерация, МПК G06F 21/00 (2006.01).** Система формирования правил политик безопасности, реализующих модели безопасности на основе состояний информационных систем: опубликовано 2011 / Зегжда Д.П., Калинин М.О. – 28с.

57. **Патент № 2530279 Российская Федерация, МПК G06F 21/00 (2006.01).** Способ автоматического адаптивного управления сетевыми потоками в программно-конфигурируемых сетях: опубликовано 2013/ Зегжда Д.П., Зегжда П.Д., Калинин М.О., Павленко Е.Ю. – 9с.

58. **Патент № 2379752 C1 Российская Федерация, МПК G06F 21/00 (2006.01).** Способ сопоставления состояний безопасности операционных систем семейства Windows: опубликовано 2010 / Зегжда Д.П., Калинин М.О. – 11с.

59. **Патент № 2379754 C1 Российская Федерация, МПК G06F 21/00 (2006.01).** Способ автоматической оценки защищённости информационных систем и система для его осуществления: опубликовано / Зегжда Д.П., Зегжда П.Д., Калинин М.О. – 17с.

60. **Патент № 101300 U1 Российская Федерация, МПК G06F 21/00 (2006.01).** Система определения показателей эффективности управления безопасностью для оптимизации настройки безопасности операционных систем : опубликовано 2011 / Зегжда Д.П., Калинин М.О., Москвин Д.А. – 25с.

61. **Зегжда, Д.П.** Имитационное моделирование высокопроизводительной виртуализированной сетевой системы защиты информации / Д.П. Зегжда, М.О. Калинин // Инновации, качество и сервис в технике и технологиях. – М., 2015. – С.148-150.

62. **Патент № 2619716 С1 Российская Федерация, МПК G06F 21/00 (2006.01).** Способ управления рабочим множеством виртуальных вычислителей в виртуальной сетевой системе защиты информации : опубликовано 2017 / Зегжда Д.П., Зегжда П.Д., Калинин М.О., Сухопаров Е.А., Минин А.А. – 10с.

63. **Демидов, Р.А.** Унифицированная модель многоуровневых угроз нарушения информационной безопасности в сетях с динамической топологией / Р.А. Демидов, П.Д. Зегжда // Интеллектуальные технологии на транспорте. – М., 2019. – С.10-14.

64. **Язов, Ю.К.** Метод формализации процесса несанкционированного доступа в информационных системах, построенных с использованием средств виртуализации, основанный на математическом аппарате сетей Петри / Ю.К. Язов, А.Л. Сердечный, А.В. Бабурин // Информация и безопасность. – М., 2013. – Т. 16. – № 4. – С. 518-521.

65. **Назаров, И.Г.** Особенности организации обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных / И.Г. Назаров, Ю.К. Язов, Е.С. Остроухова // Информация и безопасность. – М., 2009 – №1 – С. 71-76.

66. **Язов, Ю.К.** К вопросу об оценке эффективности выборочного контроля защищенности информации в информационных системах от несанкционированного доступа / Ю.К. Язов, О.А. Машин, Б.Ф. Платонов // Вопросы кибербезопасности – М., 2015 – №3(11). – С.15-22.

67. **Радько, Н.М.** Аналитическое моделирование непосредственного доступа в операционную среду компьютера посредством подбора паролей / Н.М. Радько, Ю.К. Язов // Информация и безопасность. – М., 2008. – №1. – С.54-61.

68. **Тулиганова, Л.Р.** Разработка моделей объекта защиты и угроз нарушения безопасности в информационной системе, базирующейся на технологии виртуализации / Л.Р. Тулиганова, И.А. Павлова, И.В. Машкина // Известия ЮФУ. Технические науки. – Ростов-на-Дону, 2008. – №1. – С.54-61.

69. **Евсеев, В.Л.** Гипервизоры безопасности, использующие технологию аппаратной виртуализации / В.Л. Евсеев, В.А. Данилкин, С.В. Рогачев, А.И. Трибунский // Безопасность информационных технологий. – М., 2013. – Т. 20. – № 3. – С. 54-57.

70. **Заборовский, В.С.** Архитектура системы разграничения доступа к ресурсам гетерогенной вычислительной среды / В.С. Заборовский, А.А. Лукашин, С.В. Купреенко, В.А. Мулюха // Уфа : УГАТУ, 2011. – Т. 15. – № 5(45). – С. 170–174.

71. **Кругликов, С.В.** Политика управления доступом в системе защиты информации высокопроизводительной системы обработки геолого-геофизических данных / Кругликов С.В., Дмитриев В.А., Степанян А.Б., Максимович Е.П. // Вопросы кибербезопасности – №3(27) – М., 2018. – С.22-28.

72. **Абрамов, Е.С.** Применение графов атак для моделирования вредоносных сетевых воздействий / Е.С. Абрамов, А.В. Андреев, Д.В. Мордвин // Известия ЮФУ. Технические науки Информационная безопасность. – С. 165-174.

73. **Патент № 53522 U1 Российская Федерация, МПК G06F 21/00 (2006.01).** Устройство разграничения доступа между двумя сетями передачи данных в протоколе IP-межсетевой экран без операционной системы (Варианты): опубликовано 2006 / Дмитриев Г.Г., Пашковский И.А., Кочергин М.Ю. – 23с.

74. **Барабанов, А.В.** 28 магических мер разработки безопасного программного обеспечения / А.В. Барабанов, А.С. Марков, В.Л. Цирлов // Вопросы кибербезопасности. Специальный выпуск. – М., 2015 – №5(13) – С. 2-10.

75. **Авезова, Я.Э.** Вопросы обеспечения доверенной загрузки в физических и виртуальных средах / Я.Э. Авезова, А.А. Фадин // Вопросы кибербезопасности. – М., 2016. – №1(14). – С.24-30.

76. **Веряев, А.С.** Формализация требований безопасности информации к средствам анализа защищённости / А.С. Веряев, А.А. Фадин // Вопросы кибербезопасности. – М., 2015. – №4(12). – С.23-27.

77. **Патент № 101555 U1 Российская Федерация, МПК G06F 21/00 (2006.01).** Устройство для доверительной загрузки : опубликовано 2011 / Вареница В.В., Вылегжанин В.В. , Марков А.С., Никулин М.Ю. , Фадин А.А., Цирлов В.Л. – 11с.

78. **Патент № 168346 U1 Российская Федерация, МПК G06F 21/00 (2006.01).** Устройство выявления уязвимостей : опубликовано 2017 / Марков А.С., Цирлов В.Л., Фадин А.А., Варин Д.Ф. – 6с.

79. **Патент № 2581552 C2 Российская Федерация, МПК G06F 21/00 (2006.01).** Способ доверенной загрузки в виртуальных средах : опубликовано 2016 / Веряев А.С., Вылегжанин В.В. , Марков А.С., Рязанцев А.А. , Фадин А.А., Цирлов В.Л. – 9с.

80. **Барабанов, А.В.** Оценка возможности выявления уязвимостей программного кода при отсутствии исходных текстов программ / А.В. Барабанов, А.С. Марков, А.А. Фадин // Информационное противодействие угрозам терроризма. Научно-практический журнал. – М., 2009. – №13. – С. 106-110.

81. **Дубровин, А.С.** Математическая модель политики безопасности эталонной автоматизированной системы на основе ЭМЗАС-сети / А.С.

Дубровин, В.И. Сумин, М.В. Коротков, А.Ю. Немченко // Вестник ВГУ. Серия: Физика. Математика. – Воронеж, 2005. – №2 – С.147-155.

82. **Печерицин, А.А.** Настройка ХКВ на тонких клиентах SUN RAY / А.А. Печерицин // Математические структуры и моделирование. – М., 2009. – Вып. 20. – С.113-120.

83. **Бушков, Е.** Подробное руководство по настройке тонких клиентов на основе дистрибутива Thinstation и протокола NX. Часть 1. / Е. Бушков // Системный администратор. Администрирование. – М., 2006. – №12. – С.16-23.

84. **Бушков, Е.** Подробное руководство по настройке тонких клиентов на основе дистрибутива Thinstation и протокола NX. Часть 2. / Е. Бушков // Системный администратор. Администрирование. – М., 2007. – №1. – С.32-35.

85. **Патент № 2357282 С2 Российская Федерация, МПК G06F 21/00 (2006.01).** Конфигурирование параметров сетевой настройки устройств тонких клиентов, используя переносные носители данных : опубликовано 2009 /Ник Бенджамин, Абрахам Дален, Манчестер Скотт, Фримэн Тревор В. – 38с.

86. **Горчаков, Д.А.** Разграничение прав доступа к тонкому клиенту в автоматизированной информационной системе Федеральной службы судебных приставов Российской Федерации (АИС ФССП) / Д.А. Гончаров // Муромский институт Владимирского гос. ун-та, г. Муром. – Муром, 2016. – С. 43-51.

87. **Свидетельство на государственную регистрацию программы для ЭВМ №2019616541 от 24.05.2019 г. Бюл. №6.** Пользовательский интерфейс управления системой хранения данных. / Е.Е. Ивашко, А.И. Шабает, А.А. Кекконен, В.А. Пономарёв, А.Е. Шварц, Д.П. Косицин // ФС по интеллектуальной собственности. – М., 2019. – 1с.

88. **Свидетельство на государственную регистрацию программы для ЭВМ №2015619531 от 18.06.2015 г.** Система виртуальных серверов Школьный Сервер на базе свободного программного и свободного аппаратного

обеспечения / П.А. Фролов // ФС по интеллектуальной собственности. – 2015. – 1с.

89. **Свидетельство на государственную регистрацию программы для ЭВМ № 2017661400 от 12.10.2017 г.** «Программа для ЭВМ «Атлас. Смарт Кластеризейшен (Atlas. Smart Clusterization)» / Н.С. Малыгина // ФС по интеллектуальной собственности. – 2017. – 1с.

90. **Свидетельство на государственную регистрацию программы для ЭВМ № 2016616121 от 06.06.2016 г.** МАСТЕРПЛАН / Ю.В. Семесько, А.В. Николаева // ФС по интеллектуальной собственности. – 2016. – 1с.

91. **Рябинин, К.В.** Новые возможности адаптации систем научной визуализации к сторонним решателям / К.В. Рябинин, С.И. Чуприна, А.Ю. Бортников // 26-я Международная конференция. Н.-Новгород, 2016. – С. 126-130.

92. **Патент № 181870 U1 Российская Федерация, МПК G06F 21/00 (2006.01).** Устройство контроля целостности компонентов программной среды средств вычислительной техники : опубликовано 2017 / Дударев Д.А., Панасенко С.П., Полтавцев А.В., Романец Ю.В., Салманова Ш.А., Сырчин В.К. – 13с.

93. **Суханов, Д.Я.** Метод итерационной настройки многослойной нейронной сети на основе метода наименьших квадратов / Д.Я. Суханов, А.Я. Суханов // Доклады ТУСУР. – Томск, 2004. – №2. – С.111-115.

94. **Воевода, А.А.** Синтез нейронной сети для реализации рекуррентного метода наименьших квадратов / А.А. Воевода, Д.О. Романников // Научный вестник НГТУ. – Новосибирск, 2018. – Т. 72. – № 3. – С. 33–42.

95. **Марданов, М. Дж.** Методы многокритериальной оценки альтернатив в логическом базисе нейронных сетей / М.Дж. Марданов, Р.Р. Рзаев // Автоматизация и измерения в машинном приборостроении. – М., 2018. – С.75-85.

96. **Чиркин, И.Е.** Применение нейронных сетей с использованием методов глубокого обучения для анализа информационных рисков промышленных объектов / Чиркин И.Е., Тушев А.Н. // Сборник: Измерение, контроль, информатизация. Материалы XIX международной научно-технической конференции. Под редакцией Л.И. Сучковой. – М., 2018. – С. 179-182.

97. **Афонин, С.С.** Разработка математической модели оценки техногенных рисков системы "человек - электроустановка - среда" на основе методов глубокого обучения / С.С. Афонин, А.Н. Тушев // Сборник: Измерение, контроль, информатизация. Материалы XX Международной научно-технической конференции. Под ред. Л. И. Сучковой. – М., 2019. – С. 108-111.

98. **Ларина, А.Ю.** Разработка алгоритма работы интеллектуальной системы ранжирования списка дел / А.Ю. Ларина, А.Н. Тушев // Ползуновский альманах. – М., 2019. – № 4. – С. 81-85.

99. **Чиркин, И.Е.** Разработка математической модели оценки и управления рисками системы информационной безопасности на основе нейронных сетей глубокого обучения / И.Е. Чиркин, А.Н. Тушев // Сборник: Программно-техническое обеспечение автоматизированных систем. Материалы Всероссийской молодежной научно-практической конференции. Под ред. Л.И. Сучковой. – М., 2018. – С. 272-275.

100. **Тушев, А.Н.** Применение нейронных нечетких сетей, учитывающих причинно-следственные связи, для оценки техногенных рисков электроустановок / А.Н. Тушев, Л.Ю. Качесова, И.В. Юрченкова // Сборник: Программно-техническое обеспечение автоматизированных систем. Материалы Всероссийской молодежной научно-практической конференции. Под ред. Л.И. Сучковой. – М., 2018. – С. 59-63.

101. **Тушев, А.Н.** Оценка техногенных рисков системы "человек - электроустановка-среда" на основе нейронных нечетких сетей / А.Н. Тушев, Л.Ю. Качесова, И.В. Юрченкова // Сборник: Измерение, контроль,

информатизация. Материалы XIX международной научно-технической конференции. Под редакцией Л.И. Сучковой. – М., 2018. – С. 23-27.

102. **Андреев, В. В.** Метод остаточного обучения глубоких нейронных сетей / В. В. Андреев // Программные средства и информационные технологии. Решетневские чтения. – М., 2018 – С.237-238.

103. **Казаков, М. А.** К вопросу об оптимизации конструктивного метода обучения нейронных сетей / М. А. Казаков // Вестник КРАУНЦ. Физ.-мат. науки. 2018. № 3(23). С. 184-189.

104. **Яшин, Д.В.** Использование нейронной сети для выбора методов прогнозирования временного ряда в гибридной комбинированной модели / Д.В. Яшин // Сборник: Шестнадцатая Национальная конференция по искусственному интеллекту с международным участием КИИ-2018. Труды конференции: в 2-х томах. – М., 2018. – С. 213-221.

105. **Яшин, Д.В.** Использование методов машинного обучения для настройки параметров комбинированной модели прогнозирования временного ряда / Д.В. Яшин // Сборник: Нечеткие системы и мягкие вычисления. Промышленные применения. материалы Первой всероссийской научно-практической конференции. – М., 2017. – С. 389-393.

106. **Жангиров, Т.Р.** Анализ алогичного поведения нейронных сетей в задачах классификации при экологическом мониторинге водоемов / Т.Р. Жангиров, А.С. Перков, А.А. Лисс, А.В. Экало, С.А. Иванова, Н.Ю. Григорьева // Международная конференция по мягким вычислениям и измерениям. – М., 2019. – Т. 1. – С. 317-320.

107. **Перков, А.С.** Применение нейронной сети прямого распространения для решения регрессионных задач в экологическом мониторинге / А.С. Перков, Т.Р. Жангиров, С.А. Иванова // Наука настоящего и будущего. – М., 2019. – Т. 1. – С. 95-98.

108. **Григорьева, Н.Ю.** Применение нейронных сетей для автоматизации экологического мониторинга цианобактериальных "цветений"

водоемов / Н.Ю. Григорьева, Л.В. Чистякова, А.А. Лисс, Д.М. Клионский, А.С. Перков, Т.Р. Жангиров // Международная конференция по мягким вычислениям и измерениям. – М., 2018. – Т. 2. – С. 210-213.

109. **Жангиров, Т.Р.** Применение дискриминантного анализа в задаче классификации цианобактерий / Т.Р. Жангиров, А.С. Перков // Наука настоящего и будущего. – М., 2018. – Т. 1. – С. 186-190.

110. **Перков, А.С.** Исследование градиентных методов обучения многослойных нейронных сетей в задачах классификации / А.С. Перков, Т.Р. Жангиров // Наука настоящего и будущего. – СПб., 2018. – Т. 1. – С. 200-203.

111. Гостехкомиссия РФ. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. — М.: Воениздат, 1992.

112. Гостехкомиссия РФ. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. — М.: Воениздат, 1992.

113. Гостехкомиссия РФ. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. — М.: Воениздат, 1992.

114. Гостехкомиссия РФ. Руководящий документ. Концепция защиты средств вычислительной техники от несанкционированного доступа к информации. — М.: Воениздат, 1992.

115. Гостехкомиссия РФ. Руководящий документ. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — М.: Воениздат, 1997.

116. Гостехкомиссия РФ. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. — М.: Воениздат, 1992.

117. ГОСТ Р 50992-2006. Защита информации. Основные термины и определения. – М.: Госстандарт России, 2008. — 5 с.

118. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения. — М.: Госстандарт России. — 12 с.

119. ГОСТ Р ИСО/МЭК 15408-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. — М.: ИПК Издательство стандартов, 2014. — 40 с.

120. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К): нормативно-методический документ; утв. приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

121. Змеев, А.А. Алгоритм анализа решений на множестве Парето большой мощности / С.В. Белокуров, А.П. Сидельников, А.А. Змеев: сб. матер. 43-ей воен.-науч. конф. – Тверь: Военная академия ВКО, 2014. – С. 8-9.

122. Змеев, А.А. Алгоритм нормирования требований к информационной безопасности автоматизированной системы / В.А. Хвостов, Р.А. Родин, А.А. Змеев: межвуз. сб. науч. тр. – Воронеж: Воронежский государственный технический университет, 2012. – С. 27-30.

123. Змеев, А.А. Анализ архитектуры и кластеризация структуры организационно-технических систем биологической деятельности при обосновании требований к ним по защите информации/ И.Г. Дровникова, Е.А. Рогозин, В.А. Алферов, А.А. Змеев // Интернет-журнал «Технологии техносферной безопасности». – 2016. – Вып. № 1 (65) (февраль). – <http://ipb.mos.ru/ttb/2016-1>.

124. **Змеев, А.А.** Анализ программных средств системы защиты информации от несанкционированного доступа в интегрированных систем безопасности / Н.А. Андреева, О.В. Багринцева, А.А. Змеев // Пожарная безопасность: проблемы и перспективы: сб. матер. IV Всеросс. науч.-практич. конф. с междунар. участием. – Воронеж: Воронежский институт ГПС МЧС России, 2013. – С. 101-103.

125. **Змеев, А.А.** Анализ эффективности работы подсистемы защиты информационной системы / С.В. Белокуров, Д.Г. Зыбин, А.А. Змеев: сб. матер. 43 воен.-науч. конф. ВА ВКО. – Тверь: Военная академия ВКО, 2014. – С. 6-8.

126. **Змеев, А.А.** Задача оптимального распределения временного резерва для оптимизации антивирусной защиты в инфокоммуникационных системах УИС / Д.Г. Зыбин, Н.В. Роцин, А.А. Змеев. – Воронеж: Научн. книга, 2013. – Т. 1. – С. 31-34.

127. **Змеев, А.А.** Информационные технологии в технике / А.А. Змеев, О.Ю. Макаров, Е.А. Рогозин // Детальные алгоритмы реализации угроз безопасности информации информационных систем персональных данных. «Интеллектуальные информационные системы»: матер. Всеросс. конф. – Воронеж: Воронежский государственный технический университет, 2015. – С. 3-4.

128. **Змеев, А.А.** Использование новых информационных технологий при задании требований к системам защиты информации автоматизированных систем с целью идентификации и предупреждения компьютерных преступлений / И.Г. Дровникова, Е.А. Рогозин, А.А. Змеев // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: сб. матер. Всеросс. науч.-практич. конф. ППС, сотрудников правоохран. органов (Воронеж, 27 апреля 2017 г.). – Воронеж: Воронежский институт МВД России, 2017. – С. 69-71.

129. **Змеев, А.А.** Методический подход к обоснованию требований к показателям качества функционирования систем защиты информации при разработке автоматизированных систем / Е.А. Рогозин, А.А. Змеев, В.П. Алферов // Моделирование систем и процессов: науч.-технич. журнал ВГЛТА. – Воронеж, 2015. – № 1. – С. 42-46.

130. **Змеев, А.А.** Нормирование требований к основным элементам автоматизированной системы информационной безопасности / В.А. Хвостов, Р.А. Родин, А.А. Змеев // Проблемы обеспечения надёжности и качества приборов, устройств и систем: межвуз. сб. науч. тр. – Воронеж: Воронежский государственный технический университет, 2012. – С. 25-27.

131. **Змеев, А.А.** Нормирование требований устойчивого функционирования систем управления специального назначения на основе методов эволюционного моделирования / А.А. Змеев, Е.А. Рогозин // Системы управления и информационные технологии. – М., 2016. – № 1. – С 91-95.

132. **Змеев, А.А.** Нормы безопасности информации автоматизированных систем на основе использования методов эволюционного моделирования / И.Г. Дровникова, Е.А. Рогозин, Д.И. Коробкин, А.А. Змеев // Интернет-журнал «Технологии техносферной безопасности». – 2015. – Вып. № 2 (60) (апрель). – [http:// ipb.mos.ru/ttb/2015-2](http://ipb.mos.ru/ttb/2015-2).

133. **Змеев, А.А.** Обоснование требований к системам защиты информации автоматизированных систем на основе эволюционных методов / И.Г. Дровникова, Е.А. Рогозин, А.А. Змеев // Охрана, безопасность и связь. сб. матер. Междунар. науч.-практич. конф. — Воронеж: Воронежский институт МВД России, 2016. – С. 185-188.

134. **Змеев, А.А.** Организация инфокоммуникационных систем УИС в условиях воздействия вредоносных программ / И.Е. Мирошина, А.А. Змеев // Проблемы безопасности при ликвидации последствий чрезвычайных ситуаций: сб. матер. II Всеросс. науч.-практич. конф. с междунар. участием. – Воронеж: Воронежский институт ГПС МЧС России, 2013. – С. 61-64.

135. **Змеев, А.А.** Особенности построения и функционирования инфокоммуникационных систем УИС в условиях воздействия вредоносных программ / Д.Г. Зыбин, А.А. Мытницкий, А.А. Змеев. – Воронеж: Научн. книга, 2013. – Т. 1. – С. 27-30.

136. **Змеев, А.А.** Особенности реализации символьного генетического алгоритма обоснования требований безопасности информации персональных данных / А.А. Змеев, О.Ю. Макаров, Е.А. Рогозин, В.А. Хвостов // «Интеллектуальные информационные системы»: матер. Всеросс. конф. – Воронеж: Воронежский государственный технический университет, 2015. – С. 138-141.

137. **Змеев, А.А.** Особенности реализации символьного генетического алгоритма обоснования требований к безопасности информации персональных данных / А.А. Змеев, Е.А. Рогозин // Проблемы создания и перспективы развития единой (объединенной) системы противовоздушной и противоракетной обороны организации договора о коллективной безопасности: матер. Междунар. воен.-науч.конф. ВА ВКО, апрель, 2015 г. – Тверь: Военная академия ВКО, 2015. – С. 71-75.

138. **Змеев, А.А.** Порядок использования эволюционных методов обоснования требований к безопасности информации автоматизированных систем / Е.А. Рогозин, А.А. Змеев, В.П. Алферов // Моделирование систем и процессов: науч.-технич. журнал Воронежской Государственной Лесотехнической Академии. – Воронеж, 2015. – № 1. – С. 47-50.

139. **Змеев, А.А.** Принципы оптимизации технологий защиты информации в инфокоммуникационных системах УИС / Д.Г. Зыбин, Д.Г. Антипенко, А.А. Змеев // Проблемы создания и применения Войск и сил ВКО: сб. матер. 42-ой воен.-науч. конф. – Тверь: Военная академия ВКО, 2013. – С. 8-13.

140. **Змеев, А.А.** Принятие решений в системах защиты информации в случае конфликтности множества показателей защищённости / А.В. Душкин,

В.В. Цветков, А.А. Змеев // Вестник Воронежского института МВД России. – Воронеж: ВИ МВД России, 2012. – № 2. – С. 60-64.

141. **Змеев, А.А.** Проблематика обеспечения информационной безопасности инновационных проектов: оценки и рекомендации / С.В. Белокуров, О.В. Багринцева, А.А. Змеев: сб. матер. 43-ей воен.-науч. конф. – Тверь: Военная академия ВКО, 2014. – С. 2-5.

142. **Змеев, А.А.** Системы контроля и управления доступом в интегрированных системах безопасности / С.В.Скрыль, Д.В. Волков, А.А. Змеев. — М.: Энергоатмиздат, 2013. – Ч. 2. – С. 27-29.

143. **Змеев, А.А.** Система контроля и управления доступом в интегрированных системах безопасности / О.В. Радченко, О.В. Багринцева, А.А. Змеев // Охрана, безопасность и связь. сб. матер. Междунар. науч.-практич. конф. – Воронеж: Воронежский институт МВД России, 2013. – С. 110-113.

144. **Змеев, А.А.** Способ оценки эффективности функционирования системы обнаружения несанкционированного доступа к информации / А.А. Змеев // Проблемы создания и применения Войск и сил ВКО: сб. матер. 42-ой воен.-науч. конф. – Тверь: Военная академия ВКО, 2013. – С. 3-8.

145. **Змеев, А.А.** Способ реализации антивирусной защиты в инфокоммуникационных системах УИС / Д.Г. Зыбин, А.А. Змеев // Математические методы и информационно-технические средства: матер. IX Всеросс. науч.-практич. конф. – Краснодар: Краснодарский университет МВД России, 2013. – С. 54-56.

146. **Змеев, А.А.** Структурная модель показателей защищенности в системах управления критического применения / С.В. Белокуров, О.А. Кондратов, А.А. Змеев: сб. матер. 43-ей воен.-науч. конф. – Тверь: Военная академия ВКО, 2014. – С. 10-12.

147. **Змеев, А.А.** Технологии защиты информации в инфокоммуникационных системах / И.Е. Мирошина, А.А. Змеев // Математические методы и информационно-технические средства: матер. IX

Всеросс. науч.-практич. конф. – Краснодар: Краснодарский университет МВД России, 2013. – С. 57-59.

148. **Змеев, А.А.** Управление доступом в системах защиты информации на основе комплексной оценки качества их функционирования / Д.Г. Зыбин, А.А. Змеев // *Общественная безопасность, законность и правопорядок в III тысячелетии: сб. матер. Междунар. науч.-практич. конф.* – Воронеж: Воронежский институт МВД России, 2013. – С. 90-93.

149. **Змеев, А.А.** Эволюционная модель обоснования требований к программным системам защиты информации персональных данных / А.А. Змеев, Е.А. Рогозин // *Проблемы создания и перспективы развития единой (объединенной) системы противовоздушной и противоракетной обороны организации договора о коллективной безопасности: матер. Междунар. воен.-науч. конф. ВА ВКО, апрель 2015 г.* – Тверь: Военная академия ВКО, 2015. – С. 75-79.

150. **Змеев А.А.** Эволюционные методы обоснования требований к системам безопасности информации автоматизированных систем / И.Г. Дровникова, Е.А. Рогозин, Д.И. Коробкин, А.А. Змеев // *Интернет-журнал «Технологии техносферной безопасности».* – 2015. – Вып. № 3 (61) (июнь). – [http:// ipb.mos.ru/ttb/2015-3](http://ipb.mos.ru/ttb/2015-3).

151. **Змеев, А.А.** Способ вычисления количественного показателя защищённости автоматизированных систем на основе требований ГОСТ Р ИСО/МЭК 15408-1-2013/ И.Г. Дровникова, А.А. Никитин, А.А. Змеев // *Вестник Воронежского института МВД России.* - Воронеж: Воронежский институт МВД России, 2015. - № 3. - С. 82-86.

152. **Змеев, А.А.** Вероятностные модели информационных процессов в интегрированных системах безопасности в условиях обеспечения защиты информации от несанкционированного доступа / С.В. Скрыль, А.М. Сычев, В.В. Корчагин, А.А. Змеев, О.В. Багринцева // *Телекоммуникации.* 2015. № 6. С. 26-31.

153. **Змеев, А.А.** Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем/ А.А. Змеев [и др.] // Вестник Воронежского Государственного университета инженерных технологий. - Воронеж: Воронежский Государственный университет инженерных технологий, 2015. - Вып. № 2 (64). - С. 86-92.

154. **Змеев, А.А.** Анализ архитектуры и кластеризация структуры автоматизированных систем при обосновании требований к информационной безопасности / И.Г. Дровникова, Е.А. Рогозин, А.В. Хвостов, А.А. Змеев // Интернет-журнал «Технологии техносферной безопасности». – 2016. – Вып. № 3 (67) (июнь). – [http:// ipb.mos.ru/ttb/2016-3](http://ipb.mos.ru/ttb/2016-3).

155. **Змеев, А.А.** Математическая модель нейронной сети для описания взаимодействия информационных потоков на примере доступа к гипервизору через виртуальную машину / В.В. Лавлинский, А.А. Змеев // Приборы и системы. Управление, контроль, диагностика – М., 2019. – № 4. – С. 47-55.

156. **Змеев, А.А.** Оценки взаимосвязи между значимостью команд для реализации НСД к гипервизору через виртуальную машину на основе методов нечеткой логики / А.А. Змеев // Моделирование систем и процессов. – М., 2020. – Т. 13. – № 2. – С. 78-85.

157. **Свидетельство на государственную регистрацию программы для ЭВМ № 2019610819** 18.01.2019. Программное средство разработки моделей и метода для анализа рисков нарушения информационной безопасности в информационных системах специального назначения / Лавлинский В.В., Змеев А.А. // РОСПАТЕНТ «Федеральная служба по интеллектуальной собственности» – 2018. – 1с.

158. **Змеев, А.А.** Методы и средства повышения защищенности автоматизированных систем: монография / А.А. Змеев [и др.]; под общ. ред. д-ра техн. наук, проф. Е.А. Рогозина. – Воронеж: Воронежский институт МВД России, 2013. – 108с.

159. **Змеев, А.А.** Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного документооборота: монография / А.А. Змеев [и др.]. – Воронеж: ГОУВПО ВГТУ, 2015. – 106 с.

160. **Змеев, А.А.** Методы и средства эволюционного моделирования при обосновании требований к программным системам защиты информации: монография / А.А. Змеев [и др.]; под ред. д-ра техн. наук, проф. Е.А. Рогозина. - Воронеж: Воронежский институт МВД России, 2015. – 98 с.

161. **Змеев, А.А.** Защита информации от несанкционированного доступа в интегрированных системах безопасности / О.В. Багринцева, А.А. Змеев // Вестник Воронежского института ГПС МЧС России. - Воронеж: Воронежский институт ГПС МЧС России: сб. науч. тр., 2012. – № 4. – С. 27-30.

162. **Змеев, А.А.** Анализ подсистем программных средств защиты информации от несанкционированного доступа для интегрированных систем безопасности / Ю.В. Щербакова, А.А. Змеев. – Курск: ЮЗГУ, 2013. – Т. 1. – С. 53-56.

163. **Змеев, А.А.** Интегрированные системы безопасности в условиях защиты информации от несанкционированного доступа / Ю.В. Щербакова, Д.Е. Лопатин, А.А. Змеев. – М.: Энергоатмиздат, 2013. – Ч. 2. – С. 25-27.

164. **Змеев, А.А.** Структурная модель противодействия угрозам информационной безопасности в системах управления критического применения / Д.Г. Зыбин, И.М. Тегенцев, А.А. Змеев. – Воронеж: Научн. книга, 2013. – С. 98- 100.

165. **Змеев, А.А.** К вопросу о нормах безопасности информации автоматизированных систем на основе использования методов эволюционного моделирования / Е.А. Рогозин, А.А. Змеев, В.П. Алферов // Моделирование систем и процессов: науч.-технич. ВГЛУ. – Воронеж, 2015. – № 1. – С. 39-42.

166. **Змеев, А.А.** Анализ программных средств системы защиты информации от несанкционированного доступа в интегрированных системах

безопасности / Н.А. Андреева, О.В. Багринцева, А.А. Змеев // Пожарная безопасность: проблемы и перспективы: сб. матер. IV Всеросс. науч.-практич. конф. с междунар. участием. Воронеж: Воронеж. ин-т ГПС МЧС России, 2013. – С. 101-103.

167. **Змеев, А.А.** Детальный алгоритм реализации угроз безопасности информации информационных систем персональных данных / А.А. Змеев // Проблемы создания и перспективы развития единой (объединенной) системы противовоздушной и противоракетной обороны организации договора о коллективной безопасности: матер. Междунар. воен.-науч. конф. ВА ВКО, апрель 2015 г. – Тверь: Военная академия ВКО, 2015. – С. 79-83.

168. **Змеев, А.А.** Анализ методов для оценки угроз несанкционированного доступа в информационных системах специального назначения / А.А. Змеев // Моделирование систем и процессов. – М., 2017. – № 4. – С. 30-38.

169. **Змеев, А.А.** Сравнительный анализ архитектур нейронных сетей для использования их на практике / Лавлинский В.В., Змеев А.А., Яньшин С.Н. // Моделирование систем и процессов. – М., 2017. – Т. 10. – № 4. – С. 18-26

170. **Змеев, А.А.** Модель нейронной сети системы несанкционированного доступа в информационных системах специального назначения / А.А. Змеев, В.В. Лавлинский // Моделирование систем и процессов. – М., 2018. – № 1. – С. 33-41.

171. **Змеев, А.А.** Метод анализа рисков информационной безопасности в информационных системах специального назначения / А.А. Змеев, В.В. Лавлинский // Моделирование систем и процессов. – М., 2018. – № 1. – С. 42-51.

172. **Змеев, А.А.** Имитационная модель оценки стойкости шифрования методом анализа криптографических алгоритмов с позиций виртуализации 8-битных идентификаторов / Лавлинский В.В., Березнев А.С., Змеев А.А. // Моделирование систем и процессов. – М., 2018. – Т. 11. – № 4. – С. 71-78.

173. **Змеев, А.А.** Сравнительный анализ методов шифрования для разработки имитационной модели / Лавлинский В.В., Березнев А.С., Змеев А.А. // Моделирование систем и процессов. – М., 2018. – Т. 11. – № 4. – С. 78-85.

174. **Змеев, А.А.** Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем / А.А. Змеев и др. // Вестник Воронежского Государственного университета инженерных технологий. – Воронеж, 2015. – Вып. № 2 (64). – С. 86-92.

175. **Пегат, А.** Нечёткое моделирование и управление / А. Пегат: пер. с англ. – 2-е изд. – М.: БИНОМ. Лаборатория знаний, 2013. – 798 с.

176. **Фомичев, А.В.** Элементы теории бифуркаций и динамических систем. Часть 1: уч.-метод. Пособие. – М.: МФТИ, 2019. – 42 с.

Приложение А. Публикации соискателя по теме диссертации

Монографии

1. **Змеев, А.А.** Методы и средства повышения защищенности автоматизированных систем: монография / А.А. Змеев [и др.]; под общ. ред. д-ра техн. наук, проф. Е.А. Рогозина. — Воронеж: Воронежский институт МВД России, 2013. - 108с.

2. **Змеев, А.А.** Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного документооборота: монография / А.А. Змеев [и др.]. - Воронеж: ГОУВПО ВГТУ, 2015. - 106 с.

3. **Змеев, А.А.** Методы и средства эволюционного моделирования при обосновании требований к программным системам защиты информации: монография / А.А. Змеев [и др.]; под ред. д-ра техн. наук, проф. Е.А. Рогозина. - Воронеж: Воронежский институт МВД России, 2015. - 98 с.

Статьи, опубликованные в журналах из перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук.

4. **Змеев, А.А.** Способ вычисления количественного показателя защищённости автоматизированных систем на основе требований ГОСТ Р ИСО/МЭК 15408-1-2013/ И.Г. Дровникова, А.А. Никитин, А.А. Змеев // Вестник Воронежского института МВД России. - Воронеж: Воронежский институт МВД России, 2015. - № 3. - С. 82-86.

5. **Змеев, А.А.** Вероятностные модели информационных процессов в интегрированных системах безопасности в условиях обеспечения защиты информации от несанкционированного доступа / С.В. Скрыль, А.М. Сычев, В.В.

Корчагин, А.А. Змеев, О.В. Багринцева // Телекоммуникации. 2015. № 6. С. 26-31.

6. **Змеев, А.А.** Математическая модель нейронной сети для описания взаимодействия информационных потоков на примере доступа к гипервизору через виртуальную машину / В.В. Лавлинский, А.А. Змеев // Приборы и системы. Управление, контроль, диагностика – М., 2019. – № 4. – С. 47-55.

Зарегистрированные программы для ЭВМ

7. **Свидетельство на государственную регистрацию программы для ЭВМ № 2019610819 18.01.2019.** Программное средство разработки моделей и метода для анализа рисков нарушения информационной безопасности в информационных системах специального назначения / Лавлинский В.В., Змеев А.А. // РОСПАТЕНТ «Федеральная служба по интеллектуальной собственности» – 2018. –1с.

8. **Свидетельство на государственную регистрацию программы для ЭВМ № 2021615168 05.04.2021.** Программный комплекс оценки безопасности сервера / Деревяннов А.М., Змеев А.А. // РОСПАТЕНТ «Федеральная служба по интеллектуальной собственности» – 2021. –1с.

9. **Свидетельство на государственную регистрацию программы для ЭВМ № 2021615666 12.04.2021.** Программный комплекс анализа и оценки коэффициента готовности программных систем защиты информации в АСУ специального назначения / Щеберев И.А., Змеев А.А. // РОСПАТЕНТ «Федеральная служба по интеллектуальной собственности» – 2021. –1с.

10. **Свидетельство на государственную регистрацию программы для ЭВМ № 2022617810 26.04.2022.** Программа контроля целостности программного обеспечения / Афандеев А.С., Змеев А.А. // Калинин А.В./// РОСПАТЕНТ «Федеральная служба по интеллектуальной собственности» – 2022. –1с.

11. **Свидетельство на государственную регистрацию программы для ЭВМ № 2022617745 25.04.2022.** Программа расчета средней наработки на отказ СЗИ от НСД / Ветохин О.Д., Змеев А.А. // Калинин А.В./// РОСПАТЕНТ «Федеральная служба по интеллектуальной собственности» – 2022. –1с.

Статьи в иных рецензируемых изданиях

12. **Змеев, А.А.** Нормирование требований устойчивого функционирования систем управления специального назначения на основе методов эволюционного моделирования / А.А. Змеев, Е.А. Рогозин // Системы управления и информационные технологии. – М., 2016. – № 1. – С 91-95.

13. **Змеев, А.А.** Принятие решений в системах защиты информации в случае конфликтности множества показателей защищённости / А.В. Душкин, В.В. Цветков, А.А. Змеев // Вестник Воронежского института МВД России. – Воронеж: ВИ МВД России, 2012. – № 2. – С. 60-64.

14. **Змеев, А.А.** Оценки взаимосвязи между значимостью команд для реализации НСД к гипервизору через виртуальную машину на основе методов нечеткой логики / А.А. Змеев // Моделирование систем и процессов. – М., 2020. – Т. 13. – № 2. – С. 78-85.

15. **Змеев, А.А.** Анализ методов для оценки угроз несанкционированного доступа в информационных системах специального назначения / А.А. Змеев // Моделирование систем и процессов. – М., 2017. – № 4. – С. 30-38.

16. **Змеев, А.А.** Сравнительный анализ архитектур нейронных сетей для использования их на практике / Лавлинский В.В., Змеев А.А., Яньшин С.Н. // Моделирование систем и процессов. – М., 2017. – Т. 10. – № 4. – С. 18-26

17. **Змеев, А.А.** Модель нейронной сети системы несанкционированного доступа в информационных системах специального назначения / А.А. Змеев, В.В. Лавлинский // Моделирование систем и процессов. – М., 2018. – № 1. – С. 33-41.

18. **Змеев, А.А.** Метод анализа рисков информационной безопасности в информационных системах специального назначения / А.А. Змеев, В.В. Лавлинский // Моделирование систем и процессов. – М., 2018. – № 1. – С. 42-51.

19. **Змеев, А.А.** Защита информации от несанкционированного доступа в интегрированных системах безопасности / О.В. Багринцева, А.А. Змеев // Вестник Воронежского института ГПС МЧС России. - Воронеж: Воронежский институт ГПС МЧС России: сб. науч. тр., 2012. – № 4. – С. 27-30.

20. **Змеев, А.А.** Анализ подсистем программных средств защиты информации от несанкционированного доступа для интегрированных систем безопасности / Ю.В. Щербакова, А.А. Змеев. – Курск: ЮЗГУ, 2013. – Т. 1. – С. 53-56.

21. **Змеев, А.А.** Интегрированные системы безопасности в условиях защиты информации от несанкционированного доступа / Ю.В. Щербакова, Д.Е. Лопатин, А.А. Змеев. – М.: Энергоатмиздат, 2013. – Ч. 2. – С. 25-27.

22. **Змеев, А.А.** Анализ архитектуры и кластеризация структуры организационно-технических систем биологической деятельности при обосновании требований к ним по защите информации/ И.Г. Дровникова, Е.А. Рогозин, В.А. Алферов, А.А. Змеев // Интернет-журнал «Технологии техносферной безопасности». – 2016. – Вып. № 1 (65) (февраль). – [http:// ipb.mos.ru/ttb/2016-1](http://ipb.mos.ru/ttb/2016-1).

23. **Змеев, А.А.** Нормы безопасности информации автоматизированных систем на основе использования методов эволюционного моделирования / И.Г. Дровникова, Е.А. Рогозин, Д.И. Коробкин, А.А. Змеев // Интернет-журнал «Технологии техносферной безопасности». – 2015. – Вып. № 2 (60) (апрель). – <http:// ipb.mos.ru/ttb/2015-2>.

24. **Змеев А.А.** Эволюционные методы обоснования требований к системам безопасности информации автоматизированных систем / И.Г. Дровникова, Е.А. Рогозин, Д.И. Коробкин, А.А. Змеев // Интернет-журнал «Технологии

техносферной безопасности». – 2015. – Вып. № 3 (61) (июнь). – <http://ipb.mos.ru/ttb/2015-3>.

25. **Змеев, А.А.** Анализ архитектуры и кластеризация структуры автоматизированных систем при обосновании требований к информационной безопасности / И.Г. Дровникова, Е.А. Рогозин, А.В. Хвостов, А.А. Змеев // Интернет-журнал «Технологии техносферной безопасности». – 2016. – Вып. № 3 (67) (июнь). – <http://ipb.mos.ru/ttb/2016-3>.

26. **Змеев, А.А.** К вопросу о нормах безопасности информации автоматизированных систем на основе использования методов эволюционного моделирования / Е.А. Рогозин, А.А. Змеев, В.П. Алферов // Моделирование систем и процессов: науч.-технич. ВГЛТУ. – Воронеж, 2015. – № 1. – С. 39-42.

27. **Змеев, А.А.** Имитационная модель оценки стойкости шифрования методом анализа криптографических алгоритмов с позиций виртуализации 8-битных идентификаторов / Лавлинский В.В., Березнев А.С., Змеев А.А. // Моделирование систем и процессов. – М., 2018. – Т. 11. – № 4. – С. 71-78.

28. **Змеев, А.А.** Сравнительный анализ методов шифрования для разработки имитационной модели / Лавлинский В.В., Березнев А.С., Змеев А.А. // Моделирование систем и процессов. – М., 2018. – Т. 11. – № 4. – С. 78-85.

29. **Змеев, А.А.** Порядок использования эволюционных методов обоснования требований к безопасности информации автоматизированных систем / Е.А. Рогозин, А.А. Змеев, В.П. Алферов // Моделирование систем и процессов: науч.-технич. журнал Воронежской Государственной Лесотехнической Академии. – Воронеж, 2015. – № 1. – С. 47-50.

30. **Змеев, А.А.** Задача оптимального распределения временного резерва для оптимизации антивирусной защиты в инфокоммуникационных системах УИС / Д.Г. Зыбин, Н.В. Рощин, А.А. Змеев. – Воронеж: Научн. книга, 2013. – Т. 1. – С. 31-34.

31. **Змеев, А.А.** Методический подход к обоснованию требований к показателям качества функционирования систем защиты информации при

разработке автоматизированных систем / Е.А. Рогозин, А.А. Змеев, В.П. Алферов // Моделирование систем и процессов: науч.-технич. журнал ВГЛТА. – Воронеж, 2015. – № 1. – С. 42-46.

32. **Змеев, А.А.** Особенности построения и функционирования инфокоммуникационных систем УИС в условиях воздействия вредоносных программ / Д.Г. Зыбин, А.А. Мытницкий, А.А. Змеев. – Воронеж: Научн. книга, 2013. – Т. 1. – С. 27-30.

33. **Змеев, А.А.** Системы контроля и управления доступом в интегрированных системах безопасности / С.В.Скрыль, Д.В. Волков, А.А. Змеев. — М.: Энергоатмиздат, 2013. – Ч. 2. – С. 27-29.

34. **Змеев, А.А.** Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем/ А.А. Змеев [и др.] // Вестник Воронежского Государственного университета инженерных технологий. - Воронеж: Воронежский Государственный университет инженерных технологий, 2015. - Вып. № 2 (64). - С. 86-92.

35. **Змеев, А.А.** Структурная модель противодействия угрозам информационной безопасности в системах управления критического применения / Д.Г. Зыбин, И.М. Тегенцев, А.А. Змеев. – Воронеж: Научн. книга, 2013. – С. 98- 100.

36. **Змеев, А.А.** Способы оценки угроз безопасности конфиденциальной информации для информационно-телекоммуникационных систем / А.А. Змеев и др. // Вестник Воронежского Государственного университета инженерных технологий. – Воронеж, 2015. – Вып. № 2 (64). – С. 86-92.

37. **Змеев, А.А.** Способ оценки эффективности функционирования системы обнаружения несанкционированного доступа к информации / А.А. Змеев // Проблемы создания и применения Войск и сил ВКО: сб. матер. 42-ой воен.-науч. конф. – Тверь: Военная академия ВКО, 2013. – С. 3-8.

38. **Змеев, А.А.** Структурная модель показателей защищенности в системах управления критического применения / С.В. Белокуров, О.А. Кондратов,

А.А. Змеев: сб. матер. 43-ей воен.-науч. конф. – Тверь: Военная академия ВКО, 2014. – С. 10-12.

39. **Змеев, А.А.** Анализ программных средств системы защиты информации от несанкционированного доступа в интегрированных системах безопасности / Н.А. Андреева, О.В. Багринцева, А.А. Змеев // Пожарная безопасность: проблемы и перспективы: сб. матер. IV Всеросс. науч.-практич. конф. с междунар. участием. Воронеж: Воронеж. ин-т ГПС МЧС России, 2013. – С. 101-103.

40. **Змеев, А.А.** Алгоритм нормирования требований к информационной безопасности автоматизированной системы / В.А. Хвостов, Р.А. Родин, А.А. Змеев: межвуз. сб. науч. тр. – Воронеж: Воронежский государственный технический университет, 2012. – С. 27-30.

41. **Змеев, А.А.** Алгоритм анализа решений на множестве Парето большой мощности / С.В. Белокуров, А.П. Сидельников, А.А. Змеев: сб. матер. 43-ей воен.-науч. конф. – Тверь: Военная академия ВКО, 2014. – С. 8-9.

42. **Змеев, А.А.** Анализ программных средств системы защиты информации от несанкционированного доступа в интегрированных систем безопасности / Н.А. Андреева, О.В. Багринцева, А.А. Змеев // Пожарная безопасность: проблемы и перспективы: сб. матер. IV Всеросс. науч.-практич. конф. с междунар. участием. – Воронеж: Воронежский институт ГПС МЧС России, 2013. – С. 101-103.

43. **Змеев, А.А.** Анализ эффективности работы подсистемы защиты информационной системы / С.В. Белокуров, Д.Г. Зыбин, А.А. Змеев: сб. матер. 43 воен.-науч. конф. ВА ВКО. – Тверь: Военная академия ВКО, 2014. – С. 6-8.

44. **Змеев, А.А.** Информационные технологии в технике / А.А. Змеев, О.Ю. Макаров, Е.А. Рогозин // Детальные алгоритмы реализации угроз безопасности информации информационных систем персональных данных. «Интеллектуальные информационные системы»: матер. Всеросс. конф. –

Воронеж: Воронежский государственный технический университет, 2015. – С. 3-4.

45. **Змеев, А.А.** Использование новых информационных технологий при задании требований к системам защиты информации автоматизированных систем с целью идентификации и предупреждения компьютерных преступлений / И.Г. Дровникова, Е.А. Рогозин, А.А. Змеев // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений: сб. матер. Всеросс. науч.-практич. конф. ППС, сотрудников правоохран. органов (Воронеж, 27 апреля 2017 г.). – Воронеж: Воронежский институт МВД России, 2017. – С. 69-71.

46. **Змеев, А.А.** Нормирование требований к основным элементам автоматизированной системы информационной безопасности / В.А. Хвостов, Р.А. Родин, А.А. Змеев // Проблемы обеспечения надёжности и качества приборов, устройств и систем: межвуз. сб. науч. тр. – Воронеж: Воронежский государственный технический университет, 2012. – С. 25-27.

47. **Змеев, А.А.** Обоснование требований к системам защиты информации автоматизированных систем на основе эволюционных методов / И.Г. Дровникова, Е.А. Рогозин, А.А. Змеев // Охрана, безопасность и связь. сб. матер. Междунар. науч.-практич. конф. — Воронеж: Воронежский институт МВД России, 2016. – С. 185-188.

48. **Змеев, А.А.** Организация инфокоммуникационных систем УИС в условиях воздействия вредоносных программ / И.Е. Мирошина, А.А. Змеев // Проблемы безопасности при ликвидации последствий чрезвычайных ситуаций: сб. матер. II Всеросс. науч.-практич. конф. с междунар. участием. – Воронеж: Воронежский институт ГПС МЧС России, 2013. – С. 61-64.

49. **Змеев, А.А.** Особенности реализации символического генетического алгоритма обоснования требований безопасности информации персональных данных / А.А. Змеев, О.Ю. Макаров, Е.А. Рогозин, В.А. Хвостов //

«Интеллектуальные информационные системы»: матер. Всеросс. конф. – Воронеж: Воронежский государственный технический университет, 2015. – С. 138-141.

50. **Змеев, А.А.** Особенности реализации символического генетического алгоритма обоснования требований к безопасности информации персональных данных / А.А. Змеев, Е.А. Рогозин // Проблемы создания и перспективы развития единой (объединенной) системы противовоздушной и противоракетной обороны организации договора о коллективной безопасности: матер. Междунар. воен.-науч. конф. ВА ВКО, апрель, 2015 г. – Тверь: Военная академия ВКО, 2015. – С. 71-75.

51. **Змеев, А.А.** Принципы оптимизации технологий защиты информации в инфокоммуникационных системах УИС / Д.Г. Зыбин, Д.Г. Антипенко, А.А. Змеев // Проблемы создания и применения Войск и сил ВКО: сб. матер. 42-ой воен.-науч. конф. – Тверь: Военная академия ВКО, 2013. – С. 8-13.

52. **Змеев, А.А.** Проблематика обеспечения информационной безопасности инновационных проектов: оценки и рекомендации / С.В. Белокуров, О.В. Багринцева, А.А. Змеев: сб. матер. 43-ей воен.-науч. конф. – Тверь: Военная академия ВКО, 2014. – С. 2-5.

53. **Змеев, А.А.** Система контроля и управления доступом в интегрированных системах безопасности / О.В. Радченко, О.В. Багринцева, А.А. Змеев // Охрана, безопасность и связь. сб. матер. Междунар. науч.-практич. конф. – Воронеж: Воронежский институт МВД России, 2013. – С. 110-113.

54. **Змеев, А.А.** Способ реализации антивирусной защиты в инфокоммуникационных системах УИС / Д.Г. Зыбин, А.А. Змеев // Математические методы и информационно-технические средства: матер. IX Всеросс. науч.-практич. конф. – Краснодар: Краснодарский университет МВД России, 2013. – С. 54-56.

55. **Змеев, А.А.** Технологии защиты информации в инфокоммуникационных системах / И.Е. Мирошина, А.А. Змеев // Математические методы и

информационно-технические средства: матер. IX Всеросс. науч.-практич. конф. – Краснодар: Краснодарский университет МВД России, 2013. – С. 57-59.

56. **Змеев, А.А.** Управление доступом в системах защиты информации на основе комплексной оценки качества их функционирования / Д.Г. Зыбин, А.А. Змеев // *Общественная безопасность, законность и правопорядок в III тысячелетии: сб. матер. Междунар. науч.-практич. конф.* – Воронеж: Воронежский институт МВД России, 2013. – С. 90-93.

57. **Змеев, А.А.** Эволюционная модель обоснования требований к программным системам защиты информации персональных данных / А.А. Змеев, Е.А. Рогозин // *Проблемы создания и перспективы развития единой (объединенной) системы противовоздушной и противоракетной обороны организации договора о коллективной безопасности: матер. Междунар. воен.-науч. конф. ВА ВКО, апрель 2015 г.* – Тверь: Военная академия ВКО, 2015. – С. 75-79.

58. **Змеев, А.А.** Детальный алгоритм реализации угроз безопасности информации информационных систем персональных данных / А.А. Змеев // *Проблемы создания и перспективы развития единой (объединенной) системы противовоздушной и противоракетной обороны организации договора о коллективной безопасности: матер. Междунар. воен.-науч. конф. ВА ВКО, апрель 2015 г.* – Тверь: Военная академия ВКО, 2015. – С. 79-83.

Приложение Б. Реализация алгоритма метода разграничения доступа

Реализация алгоритма метода разграничения доступа на основе виртуальных машин при использовании информационных систем обучения с информацией специального назначения, правила интерпретации модели для оценки динамики состояния ИСО с ИСН в условиях угроз несанкционированного доступа к гипервизору через виртуальные машины и описание системы уравнений на основе аппарата нейронных сетей.

Согласно формальной модели нарушителя, представленной на рис. 2.6, необходимы следующие правила формирования модели для оценки состояния информационной системы обучения с информацией специального назначения в условиях угроз несанкционированного доступа к гипервизору через виртуальные машины:

1. Первым входом для нейронной сети должен быть вектор размерностью 2×1 (на рис. 3.14 обозначен $p_1(2)$), который позволяет моделировать два состояния о знании или незнании работы злоумышленника со специализированной функцией (например, CPUID) и активировать процесс выполнения первого необходимого им действия первого этапа НСД.

2. Значения первого входного вектора определяются двумя начальными величинами: 0 (соответствует значению – не знает) и 1 (соответствует значению – знает).

3. Вторым входом для нейронной сети должен быть вектор размерностью 2×1 (на рис. 3.14 обозначен $p_2(2)$), моделирующий два состояния злоумышленника о знании или незнании кода доступа и формирующий процесс выполнения необходимых действий второго этапа НСД.

4. Значения второго входного вектора должны определяться двумя величинами: 0 (соответствует значению – не знает) и 1 (соответствует значению – знает).

5. Необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

6. Третьим входом для нейронной сети должен быть вектор размерностью 2×1 (на рис. 3.14 обозначен $p_3(2)$), моделирующий два состояния злоумышленника о знании или незнании возможности доступа к ring-0 и формирующий процесс выполнения необходимых действий третьего этапа НСД.

7. Значения третьего входного вектора должны определяться двумя величинами: 0 (соответствует значению – не знает) и 1 (соответствует значению – знает).

8. Необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

9. Четвёртым входом для нейронной сети должен быть вектор размерностью 2×1 (на рис. 3.14 обозначен $p_4(2)$), моделирующий состояния злоумышленника о знании или незнании программирования драйверов под операционную систему и формирующий процесс выполнения четвёртого необходимого действия.

10. Значения четвёртого входного вектора должны определяться двумя крайними величинами в диапазоне значений: 0 (соответствует значению – не знает) и 10 (соответствует значению – знает в полном объёме). Моделирование величин в диапазоне от 0 до 10 определяет критерий осведомлённости слушателя.

11. Необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

12. Пятым входом для нейронной сети должен быть вектор размерностью 2×1 (на рис. 3.14 обозначен $p_5(2)$), моделирующий состояния

злоумышленника о знании или незнании программирования на языке C#/C++ и формирующий процесс выполнения необходимых действий пятого этапа НСД.

13. Значения пятого входного вектора должны определяться двумя крайними величинами в диапазоне значений: 0 (соответствует значению – не знает) и 10 (соответствует значению – знает в полном объёме). Моделирование величин в диапазоне от 0 до 10 определяет критерий осведомлённости слушателя.

14. Необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

15. Шестым входом для нейронной сети должен быть вектор размерностью 2×1 (на рис. 3.14 обозначен $p_6(2)$), моделирующий состояния злоумышленника о знании или незнании программирования на языке Ассемблер и формирующий процесс выполнения необходимых действий шестого этапа НСД.

16. Значения шестого входного вектора должны определяться двумя крайними величинами в диапазоне значений: 0 (соответствует значению – не знает) и 10 (соответствует значению – знает в полном объёме). Моделирование величин в диапазоне от 0 до 10 определяет критерий осведомлённости слушателя.

17. Необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

18. Первый входной слой нейронной сети должен формировать входные веса $IW_{1,1}$ для него размерностью 9×2 , соответственно описывающие 9 слушателей одной группы согласно этапам НСД (их 6) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для первого слоя.

19. Первый входной слой должен иметь b_1 вектор 9×1 величин смещений, которые характеризуют скорость выполнения действий каждым слушателем группы (их 9) на первом этапе НСД или ,другими словами, b_1 определяет пороговые значения величины срабатывания (выполнения) слушателем конкретных действий первого этапа (b_1 в данной работе выбран в интервале 0,7-1.0 в соответствии с таблицей 2.5, где показаны правила ранжирования слушателей и определения их в группы).

20. Второй входной слой нейронной сети должен формировать входные веса $IW_{2,1}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно второму этапу НСД (из 6) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает – не знает) первого слоя в виде двух векторов первого входа $p_1(2)$.

21. Для слоя $IW_{2,1}$ необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

22. Второй входной слой нейронной сети должен формировать входные веса $IW_{2,2}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно второму этапу НСД (из 6) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает – не знает) третьего слоя в виде двух векторов второго входа $p_2(2)$.

23. Третий входной слой нейронной сети должен формировать входные веса $IW_{3,1}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно третьему этапу НСД (из 6) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает - не знает) второго слоя в виде двух векторов второго входа $p_2(2)$.

24. Для слоя $IW_{3,1}$ необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

25. Третий входной слой нейронной сети должен формировать входные веса $IW_{3,2}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно третьему этапу НСД (из б) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает - не знает) четвёртого слоя в виде двух векторов третьего входа $p_3(2)$.

26. Четвёртый входной слой нейронной сети должен формировать входные веса $IW_{4,1}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно четвёртому этапу НСД (из б) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает – не знает) третьего слоя в виде двух векторов третьего входа $p_3(2)$.

27. Для слоя $IW_{4,1}$ необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

28. Четвёртый входной слой нейронной сети должен формировать входные веса $IW_{4,2}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно четвёртому этапу НСД (из б) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает – не знает) пятого слоя в виде двух векторов четвёртого входа $p_4(2)$.

29. Пятый входной слой нейронной сети должен формировать входные веса $IW_{5,1}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно пятому этапу НСД (из б) к гипервизору

через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает – не знает) четвёртого слоя в виде двух векторов четвёртого входа $p_4(2)$.

30. Для слоя $IW_{5,1}$ необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

31. Пятый входной слой нейронной сети должен формировать входные веса $IW_{5,2}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно пятому этапу НСД (из 6) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает – не знает) шестого слоя в виде двух векторов пятого входа $p_5(2)$.

32. Шестой входной слой нейронной сети должен формировать входные веса $IW_{6,1}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно шестому этапу НСД (из 6) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает – не знает) пятого слоя в виде двух векторов пятого входа $p_5(2)$.

33. Для слоя $IW_{6,1}$ необходимо выполнение соответствующей последовательности действий с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

34. Шестой входной слой нейронной сети должен формировать входные веса $IW_{6,2}$ для него размерностью $9 \times (2 \times 2)$, соответственно описывающие 9 слушателей одной группы согласно шестому этапу НСД (из 6) к гипервизору через виртуальные машины в виде взаимосвязи нейронов для двух состояний (знает – не знает) седьмого слоя в виде двух векторов шестого входа $p_6(2)$.

35. Для седьмого (скрытого) слоя нейронной сети должны формироваться веса $LW_{7,1}$, $LW_{7,2}$, $LW_{7,3}$, $LW_{7,4}$, $LW_{7,5}$, $LW_{7,6}$ для каждого

размерностью 1×9 , соответственно описывающие 9 слушателей одной группы в виде взаимосвязи нейронов для выходов слоёв a_1 - a_6 согласно выполнению каждого этапа НСД к гипервизору через виртуальные машины.

36. Для седьмого (скрытого) слоя нейронной сети должны формироваться веса $LW_{7,7}$ из a_7 с учётом задаваемой (требуемой) временной линии задержки TDL, которая моделирует время реализации критерия осведомлённости слушателя.

37. Для седьмого (скрытого) слоя нейронной сети должно формироваться смещение b_7 , которое характеризует скорость протекания процессов при осуществлении каждого конкретного шага НСД или, другими словами, b_7 определяет пороговые значения величины срабатывания (выполнения) слушателем конкретных действий всех этапов (b_7 в данной работе выбран в интервале 0,7-1.0 в соответствии с таблицей 2.5, где показаны правила ранжирования слушателей и определения их в группы).

38. Выходами нейронной сети должны быть шесть выходов $u_1, u_2, u_3, u_4, u_5, u_6$, которые показывают взаимодействие процессов на каждом шаге НСД, а также u_7 , который определяет возможность достижения цели в виде несанкционированного доступа или его невозможности.

Эта детализация компонентов модели (modelUgrSZI.mdl) для оценки возможностей реализации угроз НСД к гипервизору через ВМ в ИСО с ИСН представлена на рис. 3.14. Уравнения для описания отдельных этапов процесса несанкционированного доступа к гипервизору через виртуальные машины в информационных системах обучения с информацией специального назначения представлены в виде следующей системы, интерпретируемой согласно описанной модели нейронной сети (3.2). Первое уравнение моделирует возможность использования НСД через виртуальную машину к гипервизору, где определяющим моментом служит b_1 , который определяет пороговые значения величины срабатывания (выполнения) слушателем конкретных действий первого этапа (b_1 в данной работе выбран в интервале 0,7-1.0 в

соответствии с таблицей 2.5, где показаны правила ранжирования слушателей и определения их в группы). Второе уравнение моделирует возможность использования НСД через виртуальную машину к гипервизору и определяет вероятности угроз НСД при оценке состояния информационной системы обучения с информацией специального назначения при возможности выполнения ими действий по второму этапу (соответствует значению y_1 на рис. 4.6). Третье уравнение моделирует возможность использования НСД через виртуальную машину к гипервизору и определяет вероятности угроз НСД при оценке состояния информационной системы обучения с информацией специального назначения при возможности выполнения ими действий по третьему этапу (соответствует значению y_2 на рис. 4.7). Четвертое уравнение моделирует возможность использования НСД через виртуальную машину к гипервизору и определяет вероятности угроз НСД при оценке состояния информационной системы обучения с информацией специального назначения при возможности выполнения ими действий по четвертому этапу (соответствует значению y_3 на рис. 4.8). Пятое уравнение моделирует возможность использования НСД через виртуальную машину к гипервизору и определяет вероятности угроз НСД при оценке состояния информационной системы обучения с информацией специального назначения при возможности выполнения ими действий по пятому этапу (соответствует значению y_4 на рис. 4.9). Шестое уравнение моделирует возможность использования НСД через виртуальную машину к гипервизору и определяет вероятности угроз НСД при оценке состояния информационной системы обучения с информацией специального назначения при возможности выполнения ими действий по шестому этапу (соответствует значению y_5 на рис. 4.10). Седьмое уравнение оценивает состояние информационной системы обучения с информацией специального назначения и определяет количество пройденных этапов в зависимости от возможности конкретной группы (соответствует положительному значению y_6 на рис. 4.11 и определяет номер группы при

формируемом профиле разграничения доступа по технологии «тонкий клиент»). На рис. 4.12 показан пример, демонстрирующий возможность осуществления группой с уровнем подготовленности 2 (ось ординат) лишь до третьего этапа НСД (ось абсцисс) на основе критерия устойчивости по Ляпунову. Отрицательные значения u_b определяют невозможность преодоления выбранной СЗИ по технологии «тонкий клиент» начиная с 4 этапа, то есть свидетельствуют, что все критерии Ляпунова отрицательны и СРД в целом устойчива к НСД к гипервизору через виртуальную машину в информационной системе обучения с информацией специального назначения.

Приложение В. Акты внедрения



АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»
(АО «НИИИТ»)

Россия, 170100, г. Тверь, ул. Андрея Дементьева, дом 3,
Тел. (4822) 34-52-17, 35-79-80, факс (4822) 35-79-80
<http://www.niit.tver.ru>, E-mail: niit@niit.tver.ru,
ОКПО 07551973, ОГРН 1126952002825, ИНН/КПП 6950145750/695001001

Экз. № 1

УТВЕРЖДАЮ

Генеральный директор
АО «НИИИТ»
доктор технических наук, доцент



И.Б. Бреслер

«03» декабря 2021 г.

АКТ

реализации научных результатов, полученных в диссертационном исследовании ЗМЕЕВА Анатолия Анатольевича на соискание учёной степени кандидата технических наук на тему «Модели и метод разграничения доступа на основе виртуальных машин при обучении с использованием информации специального назначения»

Комиссия в составе: председателя - заместителя генерального директора по режиму и безопасности А.П. Пугина; членов комиссии: начальника отдела по противодействию иностранным техническим разведкам и техническим средствам защиты С.Н. Гончарова, старшего научного сотрудника отдела системного проектирования научно-исследовательского управления, кандидата технических наук, доцента А.Н. Зарубина составила настоящий акт в том, что разработанные в рамках диссертационного исследования Змеева Анатолия Анатольевича на тему «Модели и метод разграничения доступа на основе виртуальных машин при обучении с использованием информации специального назначения» модель оценки устойчивости информационной системы обучения с информацией

специального назначения к угрозам НСД и модель оценки реализации угроз НСД к гипервизору через виртуальные машины в информационную систему обучения с информацией специального назначения реализованы в рамках СЧ ОКР «Селекция-НИИИТ».

Председатель комиссии:

Заместитель генерального директора по режиму и безопасности



А.П. Пугин

Члены комиссии:

Начальник отдела по противодействию иностранным
техническим разведкам и техническим средствам защиты



С.Н. Гончаров

Старший научный сотрудник отдела системного проектирования
научно-исследовательского управления
кандидат технических наук, доцент



А.Н. Зарубин

УТВЕРЖДАЮ

Заместитель начальника Военной академии ВКО
по учебной и научной работе

полковник



2021г.

В.Тикшаев

о реализации основных результатов диссертационной работы на тему
«Модели и метод разграничения доступа на основе виртуальных машин при
обучении с использованием информации специального назначения»
подполковника Змеева в Военной академии воздушно-космической
обороны им. Г.К. Жукова.

Комиссия в составе: председателя – начальника учебно-методического отдела, кандидата военных наук, доцента полковника Дрешина А.И. и членов комиссии: начальника кафедры №8, кандидата военных наук, полковника Байбакова А.В., доцента кафедры № 8, кандидата военных наук профессора Моренкова В.А. составила настоящий акт о том в рамках своего диссертационного исследования Змеев А.А. предложил формальную модель нарушителя, учитывающую специфику технологии тонкого клиента на основе виртуальных машин и позволяющую формировать качественные и количественные параметры с их взаимосвязями, что позволяет в некоторых случаях снижать параметры неопределённости до нуля для дальнейшего обеспечения ранжирования слушателей по отдельным группам на основе оценённых компетенций для формирования профилей СРД.

Разработанная модель оценки возможности для реализации угроз НСД в информационных системах обучения с информацией специального назначения к гипервизору через виртуальные машины, опирающаяся на результаты экспертной оценки неформализованных ответов слушателей по тесту знаний различных команд для определения осведомлённости слушателей на основе критериев, базируемых на правилах нечёткой логики в соответствии с методом суммирования нечетких чисел с L - R правилом и использованием результирующего показателя методом центра сумм, дающая возможность ранжирования на три группы. Это даёт возможность повысить эффективность системы разграничения доступа и сократить время настройки профилей, а также осуществлять смену профилей в минимально короткое время.

Экономический эффект данной работы определяется ценностью защищаемой информации и определяется высокой устойчивостью к НСД через виртуальную машину к гипервизору с минимальной (порядка 10^{-2} с) скоростью мониторинга системы разграничения доступа.

При проведении занятий по дисциплине «Защита информации» на кафедре Автоматизированных систем управления (и связи).

Председатель комиссии:

Начальник учебно-методического отдела,
кандидат военных наук, доцент
полковник



А. Дрешин

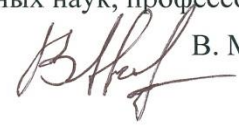
Члены комиссии:

Начальника кафедры № 8,
кандидат военных наук
полковник



А. Байбаков

Доцент кафедры № 8,
кандидат военных наук, профессор



В. Моренков

УТВЕРЖДАЮ
ректор ФГБОУ ВО
ВГЛТУ им. Г.Ф. Морозова

д.т.н.

Драпалюк М.В.

«24» 12 2021 г.

Акт внедрения

результатов диссертации Змеева Анатолия Анатольевича на тему: «Модели и метод разграничения доступа на основе виртуальных машин при обучении с использованием информации специального назначения» (Специальность 2.3.6 — «Методы и системы защиты информации, информационная безопасность»)

В рамках диссертационной работы Змеев А.А. предложил оригинальный метод разграничения доступа, включающий возможность распределения обучаемых по группам на основе использования виртуальных машин, что сокращает время, связанное с настройкой параметров системы перед проведением занятий. Такой метод совместно с разработанными автором моделями позволяют повысить эффективность защиты информации от несанкционированного доступа через виртуальные машины к гипервизору.

Данный метод и модели были использованы для осуществления разграничения доступа к информации в процессе обучения студентов в ФГБОУ ВО «ВГЛТУ имени Г.Ф. Морозова», осуществляемого сотрудниками Центра информационных технологий, что сократило расходы по восстановлению информации более чем на 30%, а также была полностью устранена несвоевременность настройки параметров СРД при подготовке к занятиям.

Также метод и модели, разработанные в ходе диссертационной работы Змеева А.А., используются при обучении студентов на кафедре вычислительной техники и информационных систем по дисциплинам «Администрирование информационных систем» и «Безопасность информационных технологий и систем».

Разработанный метод и предложенные математические модели позволяют сократить время на определение состояния СРД до 10^{-2} с, что даёт выигрыш в экономии средств около миллиона рублей в год за счёт использования программного обеспечения для ЭВМ №2019610819, а также повышает эффективность СРД от НСД через виртуальные машины к гипервизору.

И.о. заведующего кафедрой
вычислительной техники и
информационных систем, к.т.н.

Е.А. Аникеев

Приложение Г. Свидетельства на программное обеспечение

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО
о государственной регистрации программы для ЭВМ
№ 2021615168

«Программный комплекс оценки безопасности сервера»

Правообладатель: *Федеральное государственное казенное
военное образовательное учреждение высшего
образования «Военная академия воздушно-космической
обороны имени Маршала Советского Союза Г.К. Жукова»
Министерства обороны Российской Федерации (RU)*

Авторы: *Дервяннов Андрей Михайлович (RU), Змеев
Анатолий Анатольевич (RU)*

Заявка № **2021614133**
Дата поступления **26 марта 2021 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ **05 апреля 2021 г.**

*Руководитель Федеральной службы
по интеллектуальной собственности*


Г.П. Ивлиев



РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ
№ 2021615666

**«Программный комплекс анализа и оценки
коэффициента готовности программных систем защиты
информации в АСУ специального назначения»**

Правообладатель: *Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия воздушно-космической обороны имени Маршала Советского Союза Г.К. Жукова» Министерства обороны Российской Федерации (RU)*

Авторы: *Щеберев Игорь Алексеевич (RU), Змеев Анатолий
Анатольевич (RU)*

Заявка № 2021614836

Дата поступления 06 апреля 2021 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 12 апреля 2021 г.



*Руководитель Федеральной службы
по интеллектуальной собственности*

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2019610819

Программное средство разработки моделей и метода для анализа рисков нарушения информационной безопасности в информационных системах специального назначения

Правообладатель: **Змеев Анатолий Анатольевич (RU)**

Авторы: **Змеев Анатолий Анатольевич (RU),
Лавлинский Валерий Викторович (RU)**



Заявка № **2018662774**

Дата поступления **06 ноября 2018 г.**

Дата государственной регистрации

в Реестре программ для ЭВМ **18 января 2019 г.**

*Руководитель Федеральной службы
по интеллектуальной собственности*

Г.П. Ивлиев

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022617810

Программа контроля целостности программного обеспечения

Правообладатель: *Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия воздушно-космической обороны имени Маршала Советского Союза Г.К. Жукова» Министерства обороны Российской Федерации (RU)*

Авторы: *Афандеев Александр Сергеевич (RU), Змеев Анатолий Анатольевич (RU), Калинин Артемий Викторович (RU)*

Заявка № 2022616644

Дата поступления 12 апреля 2022 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 26 апреля 2022 г.



Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ



СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022617745

**Программа расчета средней наработки на отказ СЗИ от
НСД**

Правообладатель: **Федеральное государственное казенное
военное образовательное учреждение высшего
образования «Военная академия воздушно-космической
обороны имени Маршала Советского Союза Г.К. Жукова»
Министерства обороны Российской Федерации (RU)**

Авторы: **Ветохин Олег Денисович (RU), Змеев Анатолий
Анатольевич (RU), Калинин Артемий Викторович (RU)**

Заявка № 2022616589

Дата поступления 12 апреля 2022 г.

Дата государственной регистрации

в Реестре программ для ЭВМ 25 апреля 2022 г.



Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов