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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Тверь – 2022

Работа выполнена в Федеральном государственном казённом образовательном учреждении высшего образования «Военная академия воздушно-космической обороны имени Г.К. Жукова» (г. Тверь)

Научный руководитель	**Лавлинский Валерий Викторович**, доктор технических наук, доцент, исполняющий обязанности заведующего кафедрой вычислительной техники и информационных систем ФГБОУ ВО «ВГЛТУ им. Морозова»
Официальные оппоненты:	**Синещук Юрий Иванович**, доктор технических наук, профессор, профессор, ФГКОУ ВО «Санкт-Петербургский университет Министерства Внутренних Дел Российской Федерации», г. Санкт-Петербург
	Мельников Александр Владимирович, доктор технических наук, доцент, Центральный филиал ФГБОУ ВО «Российский государственный университет правосудия», заведующий кафедрой правовой информатики, информационного права и естественнонаучных дисциплин, г. Воронеж
Ведущая организация	Федеральное государственное казённое военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С.М. Будённого» Министерства обороны Российской Федерации, г. Санкт-Петербург

Защита состоится «20» апреля 2023 года в 14 часа 00 минут на заседании диссертационного совета 24.1.206.01, созданного на базе Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) по адресу: 199178, Санкт-Петербург, 14-линия В.О., 39, каб. 401, e-mail dc@spcras.ru. Факс: (812)328-44-50, тел: (812)328-33-11.

С диссертацией можно ознакомиться в отделе аспирантуры (каб. 402а) Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» и на сайте http://www.spiiras.nw.ru/dissovet

Автореферат разослан «17» февраля 2023 г.

Ученый секретарь
диссертационного совета 24.1.206.01,
кандидат технических наук М.В. Абрамов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. 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 обусловливает 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 исследования. Интерес, связанный с анализом процессов разграничения доступа, широко изучается во всём мире (Zhi Wang, Xuxian 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 диссертационного 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 меняющихся 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.

Соответствие диссертации научной специальности. Представленные результаты соответствуют специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность».

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: 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 [26–31] — вероятностные модели информационных процессов в интегрированных системах безопасности в условиях обеспечения защиты информации от НСД; в [47–55] — математическая модель нейронной сети для описания взаимодействия информационных потоков на примере доступа к гипервизору через виртуальную машину в [82–86] количественный показатель защищённости автоматизированных систем.

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 (рис. 1).

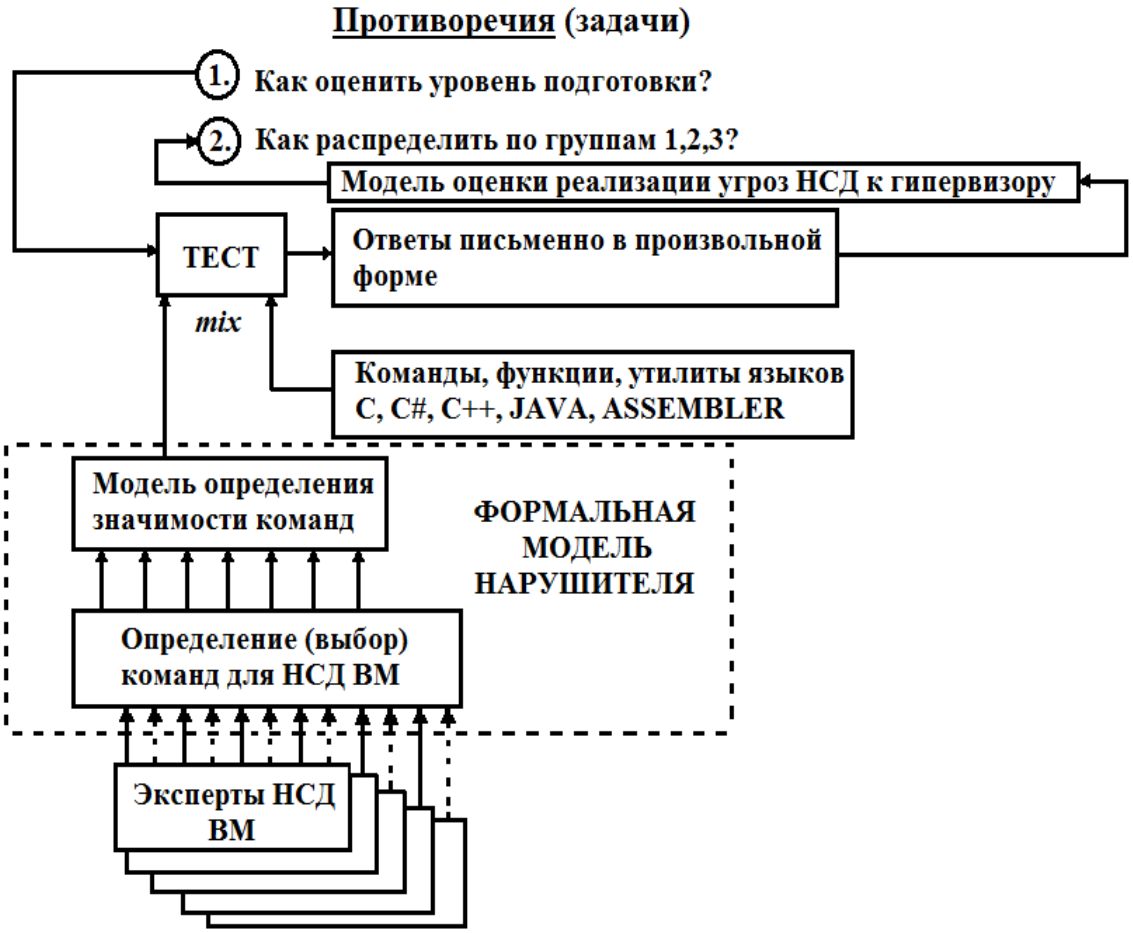


Рисунок 1 – Место нечёткой модели определения значимости команд NSD_SV.fis и формальной модели нарушителя в процессе исследования

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».**

Так в ходе эксперимента выбран набор из 11 команд, предложенный 20 экспертами. Каждый эксперт определил каждую команду к категории **«не важна»**. Согласно теории нечёткой логики было получено следующее уравнение:

x1 = (0|20+1|16+2|0+3|0+4|0+5|0+6|0+7|0+8|0+9|0+10|0)/(20+16)=
=(0·20+1·16+2·0+3·0+4·0+5·0+6·0+ +7·0+8·0+9·0+10·0)/36 =16/36=0,444.

«слабо важна»

x2=(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)=39/29=1,345.

«важна»

x3=(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)=
=246/59=4,169.

«очень важна»

x4=(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) = 7,441.

Разработанная формальная модель нарушителя представлена на рисунке 2.

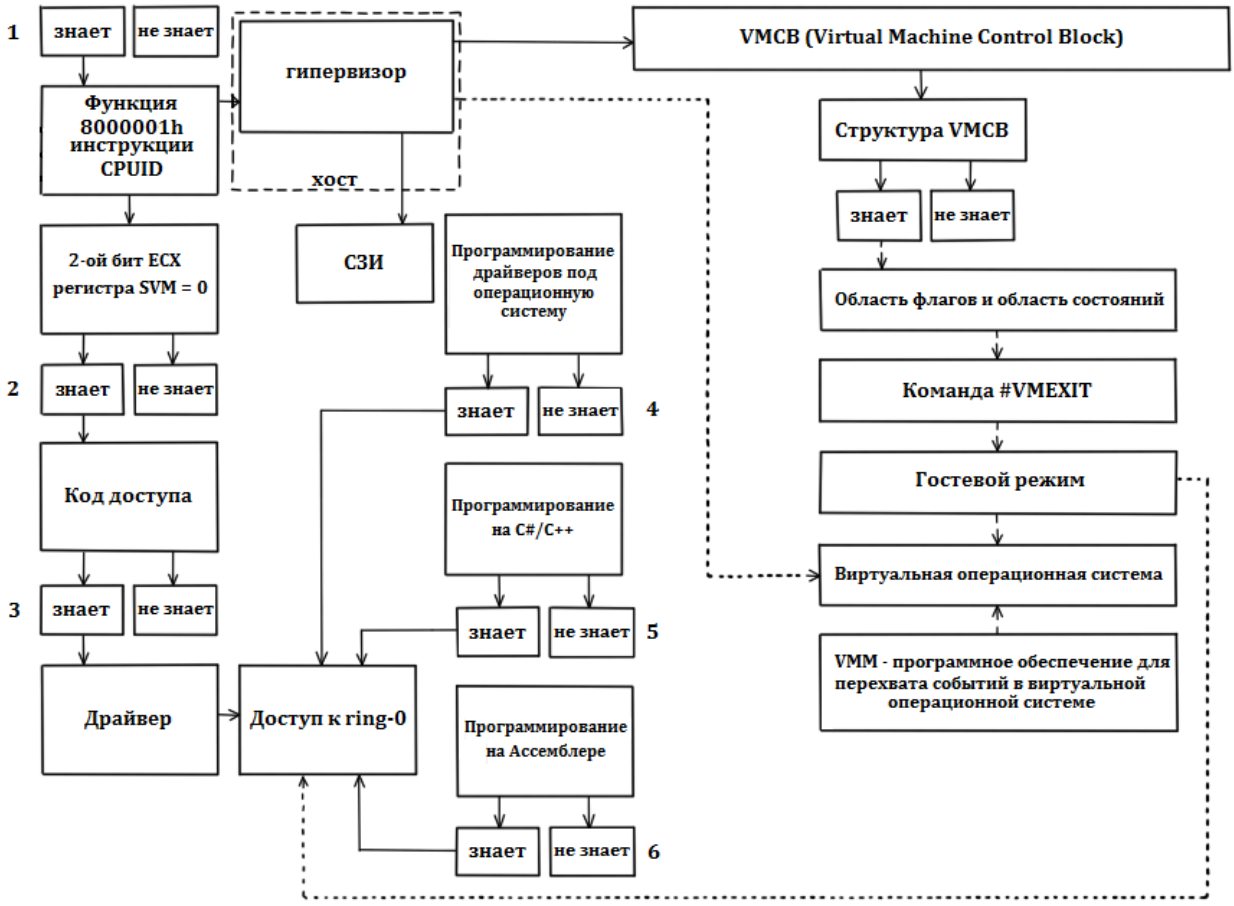


Рисунок 2 – Формальная модель нарушителя

Полученные числовые значения были нормированы, что позволило определить левую и правую граничные значения функций принадлежности в диапазоне [0,1]. Ввиду этого для каждого **лингвистического значения входа** получены следующие граничные значения: «не важна» [0, 0.06]; «слабо важна» [0.06,0.18]; «важна» [0.18, 0.56]; «очень важна» [0.56, 1]. Следовательно, для определения значимости команд в нечёткой модели NSD_SV.fis среды MATLAB сформированы функции принадлежности вида mf1→trampf→[0 0 0.06 0.06]; mf2→ trampf →[0.06 0.06 0.18 0.18]; mf3→ trampf →[0.18 0.18 0.56 0.56]; mf4→ trampf →[0.56 0.56 1 1], что позволяет снизить неопределённость при выборе команд для формальной модели нарушителя для НСД к гипервизору через виртуальную машину. Модель NSD_SV.fis представлена на рис.3.

В предложенной модели для определения важности команд использован метод центра сумм. На основе обработки экспертных оценок**,** и основанная на ней **формальная модель нарушителя,** в отличии 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.

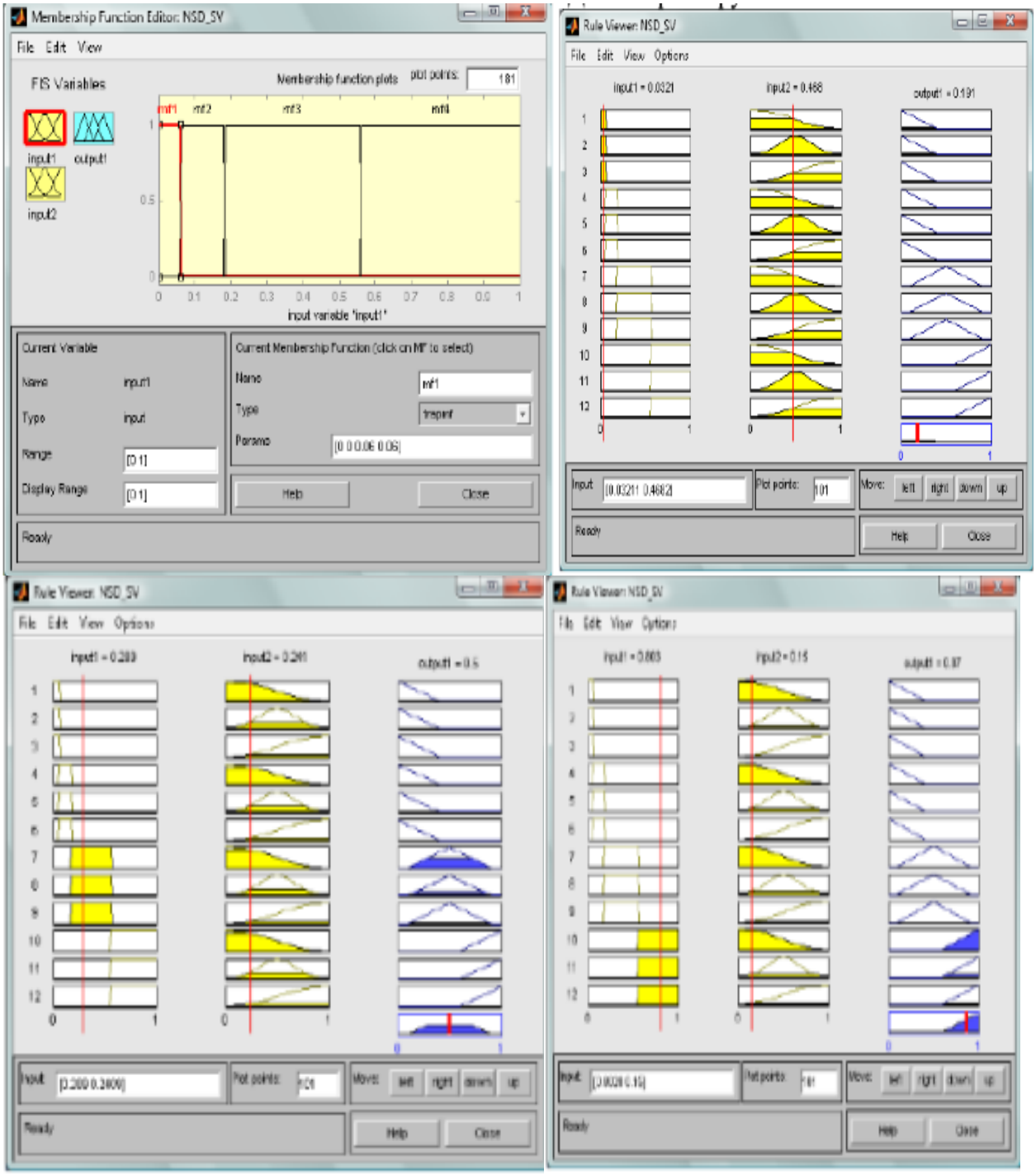


Рисунок 3– Входные функции принадлежности и результаты моделирования NSD_SV.fis

Также во второй главе предложена **нечёткая модель оценивания возможности для реализации угроз НСД в ОИСИСН к гипервизору через виртуальные машины** и её место в диссертационных исследованиях (рис. 4).

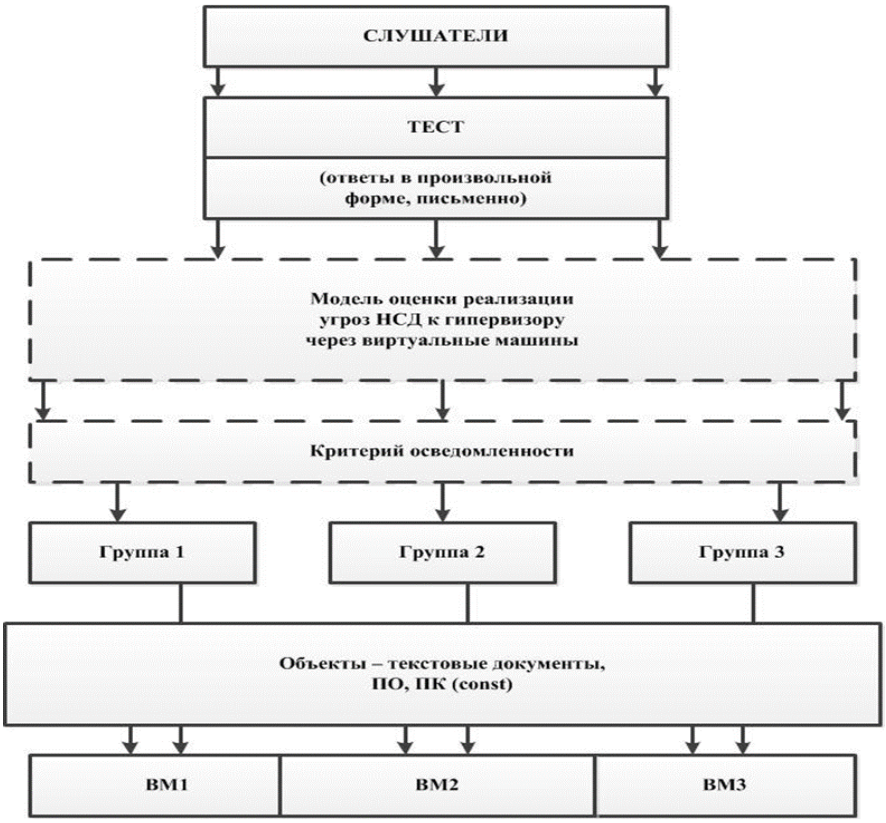
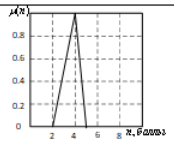
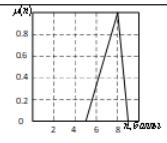


Рисунок 4 – Место нечёткой модели оценивания возможности для реализации угроз НСД в ОИСИСН к гипервизору через виртуальные машины NSD_SV_0.fis

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 (табл. 1), которые в дальнейшем обрабатываются экспертами на основе предложенных правил принятия решений.

Таблица 1 – Фрагмент результатов обработки ответов слушателей на вопросы теста

№	Вопрос	Характеристика ответа	Оценка ответа в баллах (по десятибалльной шкале)	Вид функции принадлежности, указывающая на разброс уверенности в ответе
1	Назначение регистра ECX 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	8	
		Ответа нет	0	-

Также описаны L-R правила нечёткой логики с суммированием нечетких

чисел и использованием дефаззификации результирующего показателя методом центра, на основе которого определяется **уровень осведомлённости слушателя** и осуществляется **ранжирование по трём группам** слушателей (табл. 2). Кроме того, представлены результаты формирования групп слушателей на основе функционирования моделей с использованием критерия осведомлённости.

Таблица 2 – Правило ранжирования слушателей по группам

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

Исходя из результатов исследования разработана нечеткая модель NSD_SV_0.fis с использованием Fuzzy Logic среды MATLAB, где учтены все правила и параметры оценивания самих слушателей Пример ранжирования в сильную (первую) и среднюю (вторую) группы представлены на рис. 5.

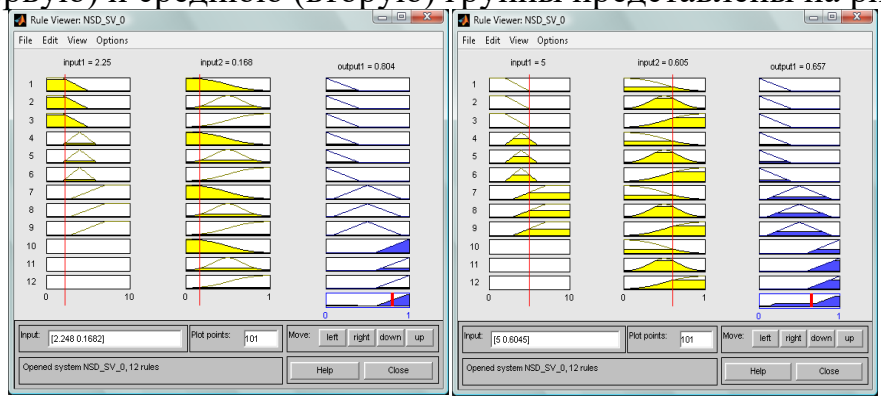


Рисунок 5 – Результаты ранжирования в сильную группу (критерий осведомлённости 0,804 (выше 0,7) и в среднюю группу (критерий осведомлённости 0,657 (в пределах 0,3- 0,69) соответственно

Третья глава посвящена **нейронечёткой модели оценивания динамики состояния образовательных информационных систем с ИСН в условиях угроз НСД к гипервизору через виртуальные машины** с учётом профилей настроек разграничения доступа при технологии «тонкий клиент» для групп слушателей при автоматизации этого процесса. 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 (1).

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

Представлена реализация системы уравнений (1) в виде нейронечёткой модели в среде MATLAB (рис. 6).

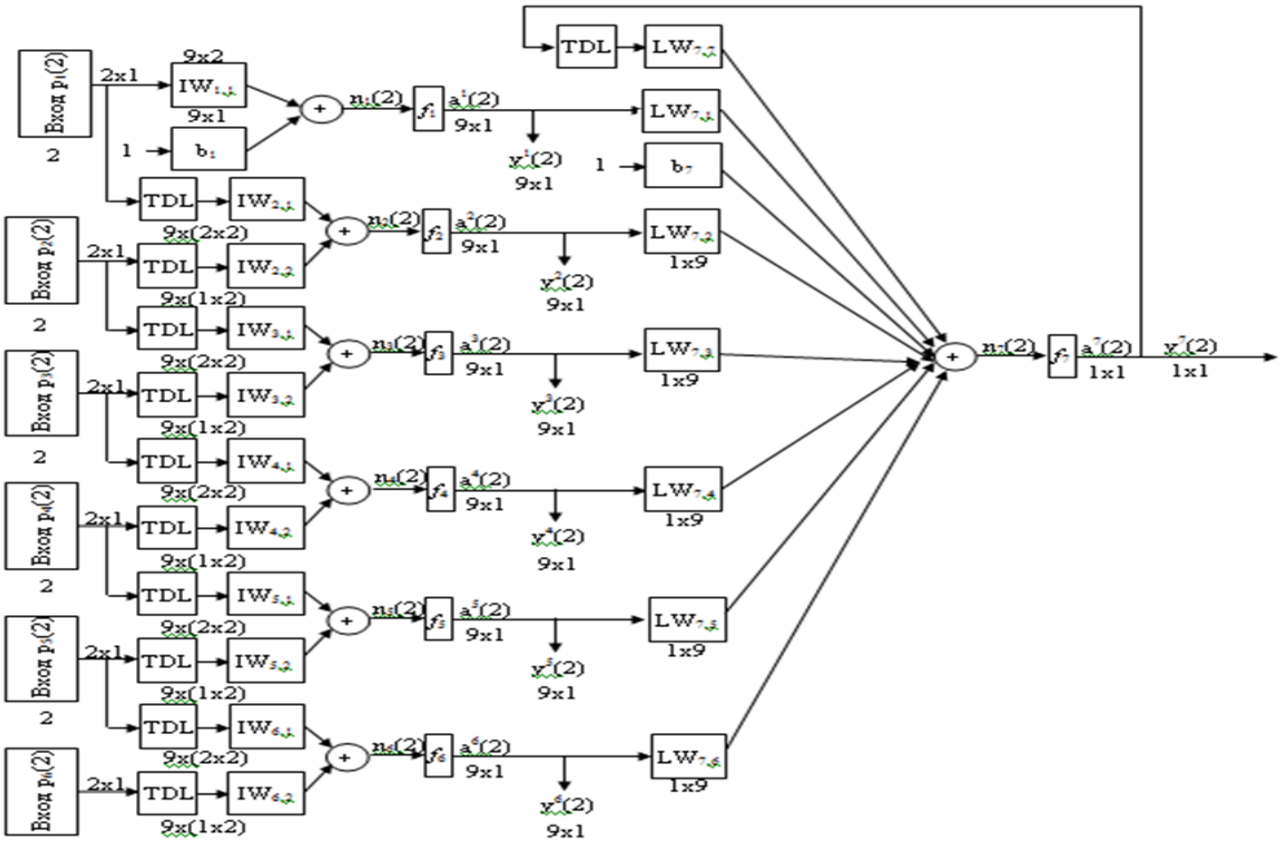


Рисунок 6 – Детализация компонентов нейронечёткой модели (modelUgrSZI.mdl) оценивания динамики состояния образовательных информационных систем на основе оценки устойчивости к НСД к гипервизору через виртуальные машины

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 6) 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. 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**, то, следовательно, система состояний **устойчива** к НСД к гипервизору через виртуальную машину в ОИСИСН на основе метода Ляпунова. Также разработан алгоритм функционирования средства оценки состояния ОИСИСН в условиях угроз НСД на основе технологии «тонкий клиент» и рассчитаны корни характеристического уравнения, где 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 (рис. 7).

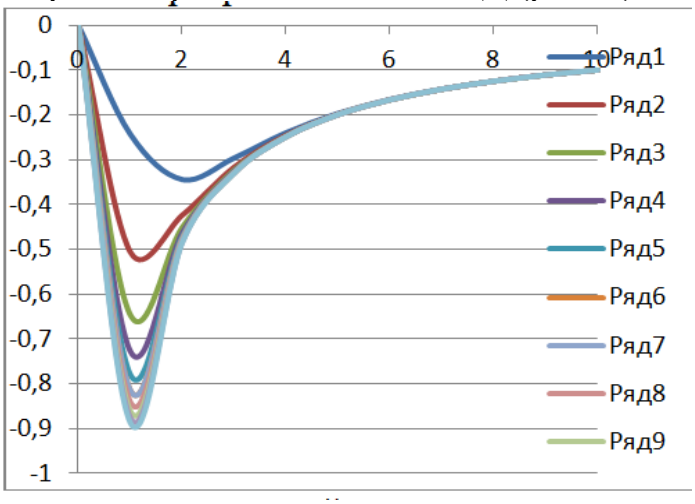


Рисунок 7 - Рассчитанные значения корней характеристического уравнения дифференциальной системы уравнений с использованием метода Ляпунова

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 для реализации метода разграничения доступа на основе виртуальных машин при использовании образовательных информационных систем (рис. 8).

Результаты оценки устойчивости состояний ОИСИСН в условиях угроз НСД на каждом этапе по методу бифуркаций (y_1-y_5) и методу Ляпунова (y_6) представлены на рис. 9.

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

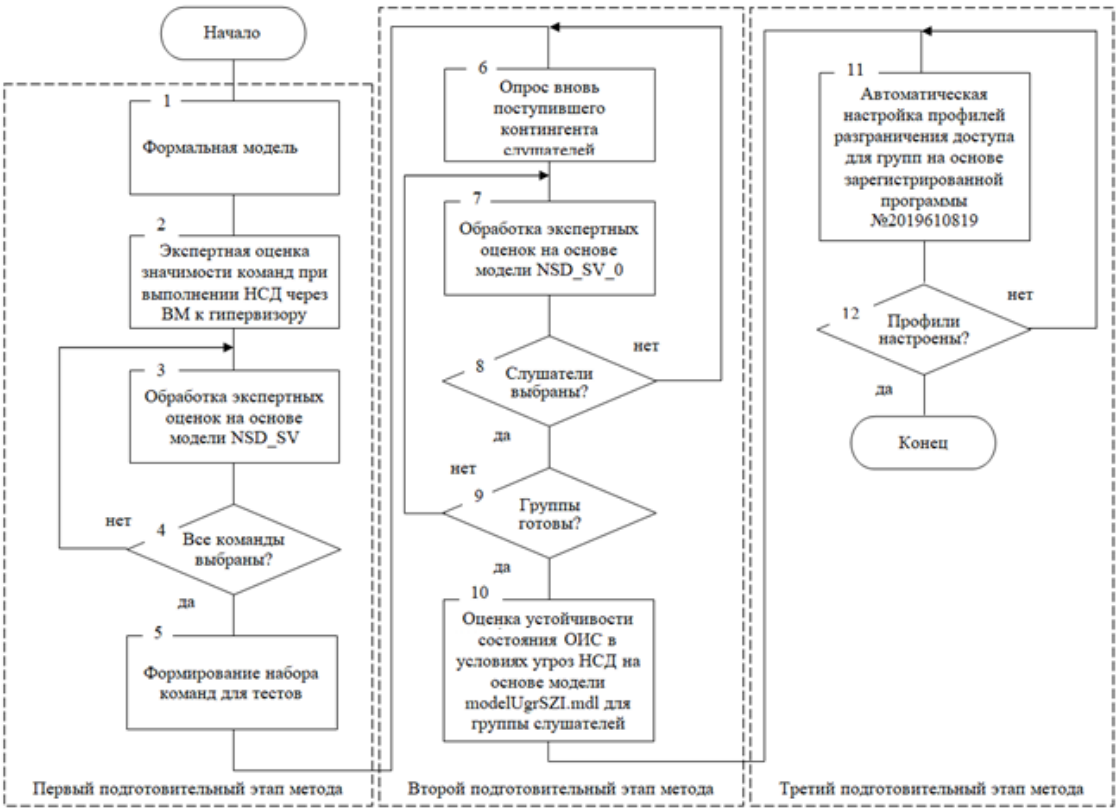


Рисунок 8 – Алгоритм для реализации **метода разграничения доступа** на основе виртуальных машин при использовании образовательных информационных систем

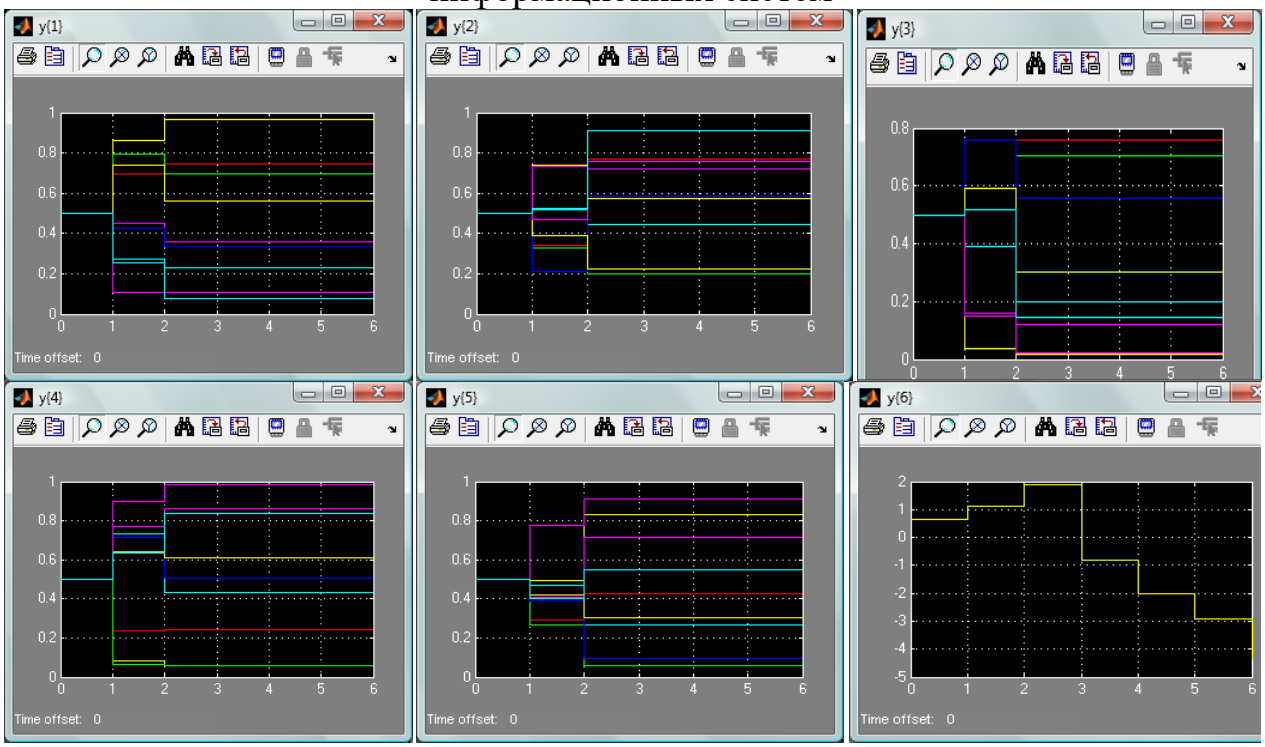


Рисунок 9 – Результаты оценки устойчивости состояний ИСО с ИСН в условиях угроз НСД на каждом этапе по методу бифуркаций (y_1-y_5) и методу Ляпунова (y_6)

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 меняющихся 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 разграничения 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 [1–5]. 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 22 научно-технических конференциях. Основные результаты, полученные автором, опубликованы в 58 научных работах.

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

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ:

Статьи, опубликованные в рецензируемых изданиях, определенных «Перечнем ВАК РФ»

1. 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, 2015. - № 3. - С. 82-86.
2. 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.
3. 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 - 2019. - № 4. - С. 47-55.

Патенты и свидетельства

4. Змеев, А.А. Свидетельство о государственной регистрации программы для ЭВМ «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» №2019610819; заявл. 06.11.2018; опубл. 18.01.2019.

Монографии

5. 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: Воронежский институт МВД России, 2012. № 2. С. 60-64.
6. 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. - 2016. - № 1. - С. 91-95.
7. 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.
8. 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.

9. 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.

Кроме того, были опубликованы 29 докладов и тезисов на научных мероприятиях (из которых 4 единоличных), получены 5 свидетельств о регистрации программ для ЭВМ (РОСПАТЕНТ). Полный перечень публикаций соискателя по теме исследования представлен в приложении А диссертационной работы

Автореферат диссертации

ЗМЕЕВ
Анатолий Анатольевич

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

Текст автореферата размещён на сайтах:
Высшей аттестационной комиссии при Министерстве науки и высшего образования Российской Федерации
https://vak.minobrnauki.gov.ru/
Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский цент Российской академии наук» (СПб ФИЦ РАН)
http://www.spiiras.nw.ru/dissovet/

Подписано в печать ___.___.20___г.
Усл. печ. л. 1,0.Тираж 100.
Заказ № ____