ОТЗЫВ

официального оппонента, доктора технических наук, профессора
Синещука Юрия Ивановича
на диссертационную работу Змеева Анатолия Анатольевича
«Модели и метод разграничения доступа в образовательных информационных системах на основе виртуальных машин»,
представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность»

1. Актуальность избранной темы диссертации

Процессы цифровизации, характеризующие современное состояние информационного общества, нацелены на полную цифровую трансформацию всех сфер жизнедеятельности государства за счёт внедрения информационных систем и информационных(цифровых) технологий. Это в полной мере относится и к сфере образования. Образовательные информационные системы, в рамках формирования специальных компетенций, практических умений и навыков, взаимодействуют с различными физическими объектами(или их модельными аналогами – тренажерами), при этом они предоставляют обучаемым различной квалификации и, в ряде случаев, различной государственной принадлежности доступ ко всем необходимым ресурсам в виде технического и программного обеспечения.

Это позволяет классифицировать такого рода системы как сложные социо-киберфизические, функционирование которых характеризуется высокой степенью динамичности и нечеткостью, неопределенностью многих исходных данных, необходимых для решения одной из базовых задач обеспечения информационной безопасности – задачи разграничения доступа. Указанные особенности обуславливают возможность рассматривать методы и технологии искусственного интеллекта как перспективный инструментарий решения заявленной научной задачи. Добавление «социо» подразумевает вовлечение в эту систему человека, а применение принципа «исключения привилегий» в процессе обеспечения информационной безопасности, позволяет рассматривать в качестве потенциальных нарушителей все категории обучаемых (пользователей) получающих возможность взаимодействовать с информационной системой.

Применение хорошо известных и широко используемых, в своем классическом виде, политик разграничения доступа (дискреционная, мандатная), при условии большого количества(групп) обучаемых, с разными потребностями и метками конфиденциальности приводит к большим временным затратам, что, зачастую, не позволяет выполнить конфигурирование системы за отведённое время.

В то же время в образовательных информационных системах имеется возможность использования технологии тонкого клиента, обеспечивающей настройки виртуальных машин под конкретную решаемую задачу. Однако такой подход даёт возможность подготовленным пользователям (слушателям) осуществлять несанкционированный доступ к гипервизору через виртуальные машины.

Таким образом, **актуальность** темы диссертационной работы обусловлена необходимостью решения противоречия между практической потребностью оперативного переконфигурирования системы разграничения доступа с учётом быстро меняющегося контингента слушателей с различными уровням компетенций и отсутствием моделей, алгоритмов, методов, обеспечивающих формирование профилей по разграничению доступа к информации с имеющимся программным и техническим обеспечением, применительно к технологии «тонкий клиент».

2. Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации, их достоверность

Степень обоснованности научных положений, выводов и рекомендаций, представленных автором в диссертационной работе, определяется корректным использованием известных научных методов, теоретических подходов, а также частными результатами, полученными другими авторами, исследующими системы разграничения доступа в образовательных информационных системах с использованием технологии «тонкий клиент».

При этом автор эффективно применил, к решаемым в диссертации задачам, методы теории математического моделирования, теории нечёткой логики, теории нейронных сетей и теории оценки устойчивости на основе метода бифуркаций и метода Ляпунова.

Практическая эффективность разработанной нечёткой модели определения значимости команд, формальной модели нарушителя, а также нечёткой модели оценивания возможности для реализации угроз НСД к гипервизору через виртуальные машины подтверждается результатами обработки экспертных данных в условиях их априорной неопределённости.

Решение заявленных автором научных задач позволяет обеспечить необходимую степень защищённости образовательных информационных систем от несанкционированного доступа к гипервизору через виртуальные машины и сократить время на реконфигурирование систем разграничения доступа без снижения качества их функционирования в реальном масштабе времени.

Таким образом, приведенные в работе положения позволяют сделать вывод, что результаты теоретического исследования Змеева Анатолия Анатольевич, а также выводы и рекомендации являются обоснованными.

3. Новизна научных положений, выводов и рекомендаций.

В диссертационном исследовании получены следующие основные результаты, характеризующиеся научной новизной:

1. Нечёткая модель для определения значимости команд при реализации угроз несанкционированного доступа к гипервизору через виртуальную машину в образовательных информационных системах, отличающаяся использованием нового подхода для формирования границ функций принадлежности по обработке экспертных оценок и обеспечивающая снижение неопределённости исходных данных.

Предложенная в работе формальная модель нарушителя, учитывающая специфику технологии «тонкого клиента» на основе использования в образовательных информационных системах виртуальных машин, позволяет учитывать качественные и количественные параметры с их взаимосвязями в виде оценённых компетенций потенциального нарушителя.

2. Нечёткая модель оценивания возможности для реализации угроз несанкционированного доступа в образовательных информационных системах к гипервизору через виртуальные машины со встроенными в неё правилами нечёткой логики и использованием метода центра сумм, отличающаяся введённым критерием осведомлённости слушателей, позволяет учитывать результаты оценки неформализованных ответов экспертов и осуществлять ранжирование слушателей по трём группам: сильная, средняя, слабая.

3. Нейронечёткая модель оценивания динамики состояния системы разграничения доступа образовательной информационной системы в условиях угроз несанкционированного доступа к гипервизору через виртуальные машины описывает динамику каждого отдельного этапа и их взаимодействие, 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

4. Методика(алгоритм) применения разработанных моделей 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 его этапов с учётом определения устойчивости в автоматизированном режиме.

Совокупность представленных моделей и методика(алгоритм) в совокупности представляю собою содержание метода разграничения доступа в образовательных информационных системах на основе виртуальных машин.

Все приведенные результаты, полученные в рамках диссертационной работы, являются новыми, достоверными, научно обоснованными и соответствуют существующим требованиям Положения о присуждении ученых степеней.

4. Общая оценка диссертационной работы

Работа выполнена на высоком научно-техническом уровне, достаточном для кандидатских диссертаций, и оформлена в соответствии с требованиями, предъявляемыми Минобрнауки РФ. Диссертационная работа хорошо структурирована, материал изложен четко и грамотно. По разделам диссертации и по работе в целом приведены соответствующие выводы, отражающие полученные научные и практические результаты. К достоинствам диссертационной работы следует отнести обоснованную теоретическую и практическую оценку полученных результатов, глубину проработки рассматриваемой предметной области, применительно к образовательным информационным системам с технологией «тонкий клиент».

Основные положения диссертации достаточно иллюстрированы. Текст диссертации изложен на 166 страницах машинописного текста с рисунками и таблицами, содержит введение, 4 раздела, заключение и список литературы из 176 наименований источников. В дополнение к основной части оформлено 4 приложения. Содержание диссертации в целом соответствует содержанию работ, опубликованных по тематике диссертации. На чужие материалы, использованные в диссертации, имеются ссылки. Краткое содержание глав диссертационной работы, основные выводы и результаты представлены в автореферате диссертации, содержание которого соответствует содержанию диссертации.

По результатам диссертационного исследования опубликовано 58 научных работ, отражающих основные положения исследования, в т.ч. 3 статьи в журналах из «Перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук». Имеется 5 свидетельств о государственной регистрации программы для ЭВМ.

5. Теоретическая и практическая значимость полученных результатов

Теоретическая значимость работы заключается в новом подходе по формированию границ функций принадлежности для лингвистических значений, позволяет снизить неопределенность 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, а также в обосновании использования метода Ляпунова и метода бифуркации для оценки устойчивости динамики процессов защиты информации

Введённый автором критерий осведомлённости слушателей, который базируется на основе теории нечёткой логики, позволяет учитывать результаты экспертной оценки неформализованных ответов, а предложенная формальная модель нарушителя позволяет учитывать релевантные параметры этапов несанкционированного доступа к гипервизору через виртуальные машины применительно к технологии «тонкий клиент.

Практическая значимость исследования заключается в разработке математического и программного обеспечения для оценки устойчивости процессов несанкционированного доступа к гипервизору через виртуальные машины на основе использования нейронечёткой модели и методов бифуркации и метода Ляпунова. Разработанные модели и алгоритмы могут быть использованы для встраивания в уже существующие системы разграничения доступа с целью повышения степени защищенности информации в образовательных информационных системах. На элементы программных средств получены свидетельства о государственной регистрации.

6. Замечания и рекомендации

Несмотря на вышеперечисленные достоинства, представленная диссертационная работа не лишена некоторых недостатков:

1. По тексту диссертации отсутствует ссылка к детальному описанию предложенного метода разграничения доступа, которое представлено в Приложении Б.

2. Из текста диссертации не совсем понятна первичность использования нечёткой модели определения значимости команд к гипервизору через виртуальные машины или нечёткой модели оценки возможности для реализации угроз НСД.

3. Во втором разделе диссертационного исследования автором сделан выбор функции принадлежности в пользу трапециевидной форме, что позволяет снизить неопределённость от лингвистических терм-множеств переменной входа к лингвистическому терм-множеству переменной выхода. Что изменится в модели, если использовать другие формы функции принадлежности?

4. В третьем разделе диссертационной работы на рисунке 3.14(стр.113) представлены компоненты нейронечёткой модели для оценивания возможностей реализации угроз НСД к гипервизору через виртуальные машины в образовательных

информационных системах, однако ссылка на детальное её описание в Приложении Б отсутствует, что усложняет процесс восприятия modelUgrSZI.mdl.

5. В четвёртом разделе автором приведены результаты, определяющие устойчивую к НСД образовательную информационную систему, использующую технологию «тонкий клиент». Хотелось бы увидеть вариант неустойчивой системы к НСД.

6. В процессе анализа предметной области исследования ограничено представлены переводные и зарубежные публикации.

7. В работе используются ссылки(стр.25) на проект методики определения угроз безопасности информации ФСТЭК 2015г., хотя в настоящее время действует методика 2021г.

8. Работа не лишена отдельных грамматических ошибок и стилистических неточностей:

— «Своевременность формирования профилей разграничения доступа с использованием предложенного метода возросло на…» (стр.124);

— «Несвоевременность настройки параметров СРД……за весь период проводимых исследований не выявлено» (стр.124);

— «……для автоматизации процесса создания профилей по разграничению профилей на основе технологии «тонкий клиент»(стр.3,114,115).

Данные замечания не ставят под сомнение научную новизну, достоверность, теоретическую и практическую значимость результатов диссертации Змеева Анатолия Анатольевича.

5. Заключение о соответствии диссертации критериям

Диссертация Змеева Анатолия Анатольевича является завершенной научно-квалификационной работой. В ней представлены решения научной задачи, заключающиеся в разработке моделей и метода разграничения доступа в образовательных информационных системах на основе использования математического аппарата нечёткой логики и нейронных сетей для оценки устойчивости к НСД к гипервизору через виртуальные машины и имеющие значение для развития соответствующей области знаний. Разработанные соискателем модели и алгоритм метода могут быть использованы для встраивания в уже существующие системы разграничения доступа образовательных информационных систем, использующих технологии «тонкий клиент».

Диссертация Змеева Анатолия Анатольевича «Модели и метод разграничения доступа в образовательных информационных системах на основе виртуальных машин» полностью соответствует требованиям пунктов 9-14 «Положения о

присуждении учёных степеней», утверждённого Постановлением Правительства РФ от 24.09.2013 года №842, предъявляемым к кандидатским диссертациям, а её автор, Змеев Анатолий Анатольевич, заслуживает присуждения учёной степени кандидата технических наук по научной специальности 2.3.6 — «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент

доктор технических наук, профессор, профессор ФГКОУ ВО «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»

«31» марта 2023 г. Синещук Юрий Иванович

Сведения о составителе отзыва:
ФИО: Синещук Юрий Иванович
Учёная степень: доктор технических наук
Место работы: Федеральное государственное казённое образовательное учреждение высшего образования «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»
Должность: профессор
Почтовый адрес: 198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1.
Телефон: +7 (911) 213-81-84
Эл. почта: sinegal53@mail.ru