«УТВЕРЖДАЮ»
Начальник Военной академии связи
кандидат физико-математических наук, доцент
генерал-лейтенант
С.Костарев
«22» марта 2023г.

ОТЗЫВ

ведущей организации

на диссертационную работу Змеева Анатолия Анатольевича «Модели и метод разграничения доступа в образовательных информационных системах на основе виртуальных машин», представленную к защите на соискание учёной степени кандидата технических наук по научной специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

1. Актуальность темы диссертации

Диссертационная работа Змеева Анатолия Анатольевича посвящена исследованию процессов разграничения доступа в образовательных информационных системах в условиях жесткого ограничения времени на реализацию их настройки и конфигурирования. В диссертационной работе решена задача оценивания системы разграничения доступа в образовательных информационных системах с технологией «тонкий клиент» от несанкционированного доступа к гипервизору через виртуальные машины применительно к отдельным группам пользователей с разными уровнями подготовки.

Основным направлением исследований автора является совершенствование моделей и метода разграничения доступа применительно к образовательным информационным системам на основе виртуальных машин с целью снижения возможностей осуществления несанкционированного доступа к гипервизору и сокращения времени на формирования профилей разграничения доступа, что подтверждает актуальность темы диссертации, а решаемая в диссертационной работе научная задача имеет как теоретическую, так и практическую значимость.

2. Личное участие автора и апробация полученных результатов

Личное участие автора в проведенных исследованиях заключается в разработке нечёткой модели определения значимости команд при реализации уязвимостей, связанных с несанкционированным доступом к гипервизору через виртуальные машины; разработке формальной модели нарушителя, учитывающей особенности технологии тонкого клиента на основе использования качественных и количественных параметров оценки компетенций слушателей для формирования профилей системы разграничения доступа; разработке нечёткой модели в соответствии с предложенными правилами нечёткой логики с использованием метода центра сумм; разработке нейронечёткой модели, для описания процессов изменения состояний образовательной информационной системы в условиях различного уровня угроз несанкционированного доступа. Теоретической основой решения научной задачи автором использовался математический аппарат нечёткой логики и нейронных сетей.

Автором самостоятельно разработано и зарегистрировано программное обеспечение, основанное на моделях, разработанных в ходе диссертационных исследований.

Положения, выносимые на защиту, и результаты работы базируются на теории нечёткой логики, теории нейронных сетей, математического моделирования и теории информационной безопасности.

Результаты работы докладывались и обсуждались на 22 всероссийских и международных научно-технических конференциях.

По результатам диссертационного исследования автором опубликовано 58 работ, из них статей 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» – 3, в прочих изданиях – 47, свидетельств о государственной регистрации программы для ЭВМ – 5.

3. Новизна исследования и полученных результатов, выводов и рекомендаций

В отличие от ранее проводимых исследований, предложен новый подход для формирования границ функций принадлежности по обработке

экспертных оценок; введён критерий осведомлённости слушателей, позволяющий ранжировать слушателей и распределять их в соответствии с предложенными правилами нечёткой логики с использованием метода центра сумм; предложена система уравнений для описания процессов изменения состояний образовательной информационной системы в условиях различного уровня угроз несанкционированного доступа к гипервизору через виртуальные машины и учитывающая релевантные параметры предложенной формальной модели; разработан алгоритм для реализации метода разграничения доступа с использованием виртуальных машин применительно к образовательным информационным системам.

На основе предложенного подхода диссертантом определены направления для минимизации времени по формированию адаптации профилей настройки систем разграничения доступа и их совершенствованию на основе разработанных моделей.

Основные научные результаты и положения диссертации являются новыми. Решены научные задачи, расширяющие подходы реализации систем разграничения доступа в образовательных информационных системах, использующих технологию тонкого клиента, на основе разработанных моделей нечёткой логики и нейронных сетей, учитывающих нечёткие релевантные параметры для оценки устойчивости к несанкционированному доступу к гипервизору.

В диссертационной работе Змеева Анатолия Анатольевича получены следующие основные результаты, обладающие научной новизной:

Основными результатами диссертации можно считать следующее.

1. Разработан новый подход для формирования границ функций принадлежности по обработке экспертных оценок на основе разработанной нечёткой модели определения значимости команд при реализации уязвимостей, связанных с несанкционированным доступом к гипервизору через виртуальные машины.

2. Предложена формальная модель нарушителя, учитывающая особенности технологии тонкого клиента на основе использования качественных и количественных параметров оценки компетенций слушателей для формирования профилей системы разграничения доступа.

3. Введён критерий осведомлённости слушателей, позволяющий ранжировать слушателей и распределять их на основе разработанной не-

чёткой модели в соответствии с предложенными правилами нечёткой логики с использованием метода центра сумм.

4. Предложена система уравнений, используемая в разработанной нейронечёткой модели, для описания процессов изменения состояний образовательной информационной системы в условиях различного уровня угроз несанкционированного доступа к гипервизору через виртуальные машины и учитывающая релевантные параметры предложенной формальной модели.

5. Доказана возможность применения метода бифуркаций и метода Ляпунова для автоматизации процесса оценивания устойчивости к несанкционированному доступу к гипервизору через виртуальные машины.

6. Разработан алгоритм для реализации метода разграничения доступа с использованием виртуальных машин применительно к образовательным информационным системам.

Указанные научно обоснованные технические и технологические решения способствуют повышению уровня защищенности информации в образовательных информационных системах с технологиями «тонкий клиент», а предлагаемый метод позволяет повысить оперативность и сократить время на формирование профилей системы разграничения доступа.

4. Значимость полученных автором диссертации результатов для науки и практики

Полученные в диссертации научные результаты расширяют подходы к формированию профилей разграничения доступа к информации в образовательных информационных системах, использующих технологии «тонкий клиент» на основе оценки устойчивости к несанкционированному доступу к гипервизору через виртуальные машины.

Теоретическая значимость исследования обоснована тем, что использован математический аппарат нейронных сетей для оценки устойчивости к НСД к гипервизору через виртуальные машины, вносящие вклад в расширение границ применимости полученных результатов на системы разграничения доступа, а также проведена модернизация существующих алгоритмов для её конфигурирования.

Практическую значимость результатов диссертационной работы составляют разработанные нечёткие модели, формальная модель злоумышленника, нейронечёткая модель, метод разграничения доступа с использованием виртуальных машин применительно к образовательным информационным системам за счёт чего своевременность формирования профилей разграничения доступа возросло на 19,65% без снижения устойчивости к НСД к гипервизору через виртуальные машины, а также сокращено время для определения состояния системы разграничения доступа до 10^{-2} с и исключения несвоевременности настройки её параметров.

Разработанные модели и метод представляют собой основу научно-методической и практической реализации профилей разграничения доступа к информации в образовательных информационных системах, использующих технологии «тонкий клиент».

5. Достоверность и обоснованность полученных результатов

Обоснованность и достоверность полученных научных результатов определяется:

- научной обоснованностью приводимых выкладок и математических преобразований;
- использованием теории нечёткой логики, нейронных сетей, теории информационной безопасности, включая теорию устойчивости с использованием метода Ляпунова и метода бифуркаций;
- системным анализом объекта исследования, дискреционной политики безопасности и опыта использования систем разграничения доступа в образовательных информационных системах с технологиями «тонкий клиент»;
- проведением сравнительного анализа результатов предложенных нечётких моделей и результатами экспериментов;
- непротиворечивостью полученных результатов известным решениям.

Использование в диссертации современных методик сбора и обработки исходной информации об уязвимостях, дающих возможности несанкционированного доступа к гипервизору через виртуальные машины, подтверждают оценку достоверности результатов исследования, где отмечено непосредственное участие соискателя в получении исходных дан-

ных и научных экспериментах, а также личное участие в апробации результатов исследования.

Достоверность результатов дополнительно подтверждается пятью свидетельствами о регистрации программ для ЭВМ, использующих полученные соискателем теоретические и практические результаты диссертационных исследований.

6. Рекомендации по использованию результатов и выводов

Проведенные в диссертации результаты исследования целесообразно развивать в направлении расширения практических возможностей разработанных моделей и метода разграничения доступа на основе виртуальных машин для образовательных информационных систем.

Полученные в диссертационной работе научные результаты, выводы и практические рекомендации могут найти применение в системах разграничения доступа информационных и инфокоммуникационных системах силовых министерств и ведомств РФ.

Предложенные модели формируют дополнительные средства по осуществлению разграничения доступа в условиях априорной неопределённости об осведомлённости слушателей.

Представленные в диссертации результаты будут востребованы в дальнейших изысканиях, связанных с расширением возможностей по использованию введённого критерия оценки устойчивости для более широкого спектра угроз (применительно к внутренним и внешним угрозам информационной безопасности в целом).

7. Соответствие содержания диссертации и автореферата

Автореферат отражает содержание диссертационной работы и содержит введение, четыре раздела, заключение, список литературы из 176 источников и четырёх приложений. Объём диссертации составляет 166 страниц.

Содержание диссертации в полной мере соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Автореферат и диссертация строго структурированы, материал логически связан, имеется хорошая доказательная база. Следует отметить,

что полученные в диссертации результаты имеют логическую взаимосвязь и последовательно изложены, а также обладают внутренним единством.

По предоставленному библиографическому списку и прилагаемому перечню собственных публикаций автора можно сделать вывод о том, что основные положения диссертации достаточно полно изложены в печатных работах и апробированы на профильных научных и технических конференциях.

8. Основные замечания по диссертации

Вместе с тем работа не лишена некоторых недостатков:

1. В работе приведена нечёткая модель NSD_SV_0.fis с использованием Fuzzy Logic среды MATLAB, которая учитывает параметры формальной модели нарушителя, а также, правила и параметры о результатах знания команд слушателями, позволяющая осуществлять их ранжирование по трём группам. Тем не менее, в работе приводится пример только для двух групп (сильной и средней).
2. В работе не отмечена прямая связь вида функций принадлежности, указывающей на разброс уверенности в ответе (таблица 2.4), с видом функции принадлежности в нечёткой модели NSD_SV_0.fis.
3. На странице 106 автором отмечается «Седьмая формула…», хотя правильно – это седьмое выражение (уравнение) в системе уравнений, представленной в (3.2).
4. На странице 114 имеется ссылка на приложение, однако не указано на какое конкретно. Кроме того, нет ссылки на приложение Б. Реализация алгоритма метода разграничения доступа, что затрудняет своевременность перехода к ознакомлению с методом, предложенным в диссертации.

Перечисленные замечания и недостатки не снижают научный уровень проведенных исследований и не влияют на общий положительный вывод о качестве представленной к защите диссертации.

9. Заключение по диссертационной работе

Представленная диссертация соответствует требованиям, предъявляемым к кандидатским диссертациям, обладает научной новизной и практической значимостью.

Диссертационное исследование Змеева Анатолия Анатольевича является законченной самостоятельной научно-квалификационной работой, которая вносит значительный вклад в решение актуальной задачи, повышающей эффективность настройки профилей систем разграничения доступа в образовательных информационных системах с технологией «тонкий клиент», что позволяет на практике использовать модели для оценки устойчивости к несанкционированному доступу к гипервизору через виртуальные машины.

Содержание и основные научные результаты соответствуют паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность». Автореферат диссертации достаточно полно отражает основное содержание диссертационной работы. По оформлению работа соответствует требованиям, предъявляемым к диссертациям.

На основании вышеизложенного можно заключить, что диссертационная работа «Модели и метод разграничения доступа в образовательных информационных системах на основе виртуальных машин», содержащая решение актуальной научно-технической задачи оценивания эффективности систем разграничения доступа в образовательных информационных системах с технологией «тонкий клиент» по защите информации от несанкционированного доступа к гипервизору через виртуальные машины, соответствует критериям, изложенным в пунктах 9–14 Положения «О порядке присуждения ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 года № 842 (в редакции Постановлений Правительства РФ от 11.09.2021 года № 1539), предъявляемым к кандидатским диссертациям, а её автор Змеев Анатолий Анатольевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Диссертационная работа Змеева Анатолия Анатольевича обсуждена на заседании кафедры безопасности инфокоммуникационных систем спе-

циального назначения Федерального государственного казённого образовательного учреждения высшего образования «Военная орденов Жукова и Ленина Краснознамённая академия связи имени Маршала Советского Союза С.М. Будённого», присутствовали 18 чел., из них 3 доктора технических и военных наук, протокол № 12 от «22» марта 2023 года.

Отзыв составил профессор кафедры безопасности инфокоммуникационных систем специального назначения, д.в.н., профессор Стародубцев Юрий Иванович.

Профессор кафедры безопасности инфокоммуникационных систем
специального назначения
доктор военных наук, профессор

Ю.Стародубцев

Начальник кафедры безопасности инфокоммуникационных систем
специального назначения
кандидат технических наук, доцент
полковник

М.Митрофанов

Федеральное государственное казённое образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознамённая академия связи имени Маршала Советского Союза С.М. Будённого»
Адрес:194064, г. Санкт-Петербург, Тихорецкий проспект, д.3
тел: +7 (812) 247-98-35
e-mail: vas@mil.ru
сайт: https://vas.mil.ru/