ЗАКЛЮЧЕНИЕ ОБЪЕДИНЕННОГО ДИССЕРТАЦИОННОГО СОВЕТА Д 999.121.03, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» ФЕДЕРАЛЬНОГО АГЕНТСТВА СВЯЗИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ» МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ВОЕНМЕХ» ИМ. Д.Ф. УСТИНОВА» МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА ТЕХНИЧЕСКИХ НАУК

аттестационное дело № _____

решение диссертационного совета от 26 декабря 2018 г. № 10

О присуждении Коломойцеву Владимиру Сергеевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Модели и методы оценки эффективности систем защиты информации и обоснование выбора их комплектации» по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность принята к защите 24 октября 2018 года, протокол № 7 объединенным диссертационным советом Д 999.121.03 на базе федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» Федерального агентства связи, федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» Министерства образования и науки Российской Федерации, федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» Министерства образования и науки Российской Федерации, 191186, Санкт-Петербург, наб. реки Мойки, д. 61, приказ № 44/нк от 30 января 2017 года.

Соискатель Коломойцев Владимир Сергеевич, 1990 года рождения, работает инженером на кафедре вычислительной техники в федеральном государственном автономном образовательном учреждении высшего образования "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики".

В 2014 году соискатель окончил федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения».

В 2018 году окончил освоение программы подготовки научно-педагогических кадров в аспирантуре федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики».

Диссертация выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики» Министерства науки и высшего образования Российской Федерации на кафедре вычислительной техники.

Научный руководитель – доктор технических наук, профессор Богатырев Владимир Анатольевич, основное место работы: федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», факультет программной инженерии и компьютерной техники, профессор.

Официальные оппоненты: 1. Молдовян Николай Андреевич, доктор технических наук, профессор, основное место работы: Федеральное государственное бюджетное учреждение науки "Санкт-Петербургский институт информатики и автоматизации Российской академии наук", научно-исследовательская лаборатория безопасности информационных систем, главный научный сотрудник; 2. Овчинников Андрей Анатольевич, кандидат технических наук, доцент, основное место работы: Федеральное государственное автономное

образовательное учреждение высшего образования "Санкт-Петербургский государственный университет аэрокосмического приборостроения", кафедра безопасности информационных систем, заведующий кафедрой, дали положительные отзывы на диссертацию.

Ведущая организация ЗАО "ЭВРИКА", Санкт-Петербург, в своем положительном заключении, подписанном Гущиным М.В., канд. техн. наук, начальником ОВК, Кухианидзе С.А., канд. воен. наук, менеджером СО по ГОЗ, утвержденном Сухановым А.В., д-ром техн. наук, доц., заместителем генерального директора по научно-исследовательской работе указала, что диссертационная работа Коломойцева В.С. является законченной научно-квалификационной работой, содержащей решение научной задачи по разработке методов оценки эффективности систем защиты информации и выбора их комплектации средствами защиты информации. В работе предложен метод и разработана модель оценки вероятности обнаружения и устранения угроз информационной безопасности, позволяющий оценить информационную защищенность вычислительной системы. Используя данную модель, разработаны модели оценки надежности и задержек обслуживания, учитывающие снижение нагрузки на промежуточных узлах вычислительной системы в результате фильтрации потока запросов от некоторых угроз информационной безопасности. Результаты работы позволяют проводить оценку надежности, задержек обслуживания и информационной защищенности для построения высокоэффективных систем защиты информации, способных выдерживать большее число отказов при обеспечении требования стационарности режима обслуживания. Достоверность и обоснованность основных выводов и полученных результатов определяется корректным формированием набора частных и комплексных показателей эффективности систем защиты информации, а также использованием математического аппарата теорий надежности, вероятности, статистики и теории массового обслуживания и положительными результатами внедрения. Диссертация соответствует требованиям п. 9 «Положения о присуждении ученых степеней», а её автор заслуживает присуждения ученой

степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 35 опубликованных работ, в том числе по теме диссертации 35 работ, опубликованных в рецензируемых научных изданиях – 4. Диссертация не содержит недостоверных сведений об опубликованных соискателем работах. Помимо 4-х работ в рецензируемых научных изданиях, соискатель ученой степени имеет 4 публикации в изданиях, входящих в международные системы цитирования Scopus и Web of Science, 27 – в сборниках научных трудов, материалов конференций и иных научных изданиях. Общий объём авторского вклада в работы составляет 7,1 п.л. из общего количества 10,0 п.л.

Наиболее значительные научные работы по теме диссертации:

1. Коломойцев В.С., Богатырев В.А. Эффективность поэтапного применения средств защиты с пересечением областей обнаружения угроз // Программные продукты и системы. – 2018. – Т. 32. – № 3. – С. 557-564.

2. Коломойцев В.С., Богатырев В.А. Вероятностно-временные показатели при поэтапном применении средств защиты информации // Вестник компьютерных и информационных технологий. – 2017. – № 11(161). – С. 37-43.

3. Коломойцев В.С. Выбор варианта построения многоуровневого защищенного доступа к внешней сети // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16. – № 1(101). – С. 115-121.

4. Коломойцев В.С., Богатырев В.А. Оценка эффективности и обоснование выбора структурной организации системы многоуровневого защищенного доступа к ресурсам внешней сети // Информация и космос. – 2015. – № 3. – С. 71-79.

5. Kolomoitcev V.S., Bogatyrev V.A. The fault-tolerant structure of multilevel secure access to the resources of the public network // Communications in Computer and Information Science. 2016. Vol. 678, pp. 302-313.

6. Kolomoitcev V.S., Bogatyrev V.A. A Fault-tolerant Two-tier Pattern Of Secure Access 'Connecting Node' // ACSR-Advances in Computer Science Research. 2017. Vol. 72, pp. 271-274.

На диссертацию и автореферат поступили отзывы: официального оппонента Молдовяна Н.А.; официального оппонента Овчинникова А.А.; ведущей организации ЗАО "ЭВРИКА"; Уткина Л.В., д-ра техн. наук, проф., заведующего кафедрой "Телематика (при ЦНИИ РТК)" Санкт-Петербургского политехнического университета Петра Великого; Жаринова И.О., д-ра техн. наук, проф., руководителя учебно-научного центра – Ученого секретаря научно-технического совета АО "ОКБ "Электроавтоматика"; Татарниковой Т.М., д-ра техн. наук, доц., профессора кафедры информационных систем Санкт-Петербургского государственного электротехнического университета "ЛЭТИ" им. В.И. Ульянова (Ленина); Полещикова С.М., д-ра физ.-мат. наук, проф., заведующего кафедрой информационных систем Сыктывкарского лесного института (филиал) Санкт-Петербургского государственного лесотехнического университета имени С.М. Кирова; Ермолова М.А., канд. техн. наук, ассистента кафедры компьютерные системы автоматизации производства Московского государственного технического университета имени Н.Э. Баумана (национальный исследовательский университет); Алексанковв С.М., канд. техн. наук, главного специалиста АО "НИИ Масштаб"; Алексеева А.В., д-ра техн. наук, проф., профессора кафедры судовой автоматики и измерений Санкт-Петербургского государственного морского технического университета; Колбанева М.О., д-ра техн. наук, проф., профессора кафедры информационных систем и технологий Санкт-Петербургского государственного экономического университета; Ныркова А.П., д-ра техн. наук, проф., профессора кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова; Сидоркиной И.Г., д-ра техн. наук, проф., декана факультета информатики и вычислительной техники Поволжского государственного технологического университета; Лавреша И.И., канд. техн. наук, начальника отдела организации научно-технической и образовательной деятельности Центра информационных технологий Республики

Коми; Ивановой И.В., д-ра техн. наук, проф., профессора кафедры информационных систем и вычислительной техники Санкт-Петербургского горного университета; Кочнева В.В., канд. техн. наук, заместителя директора центра проектирования, разработки и внедрения АСУ специального назначения ЗАО "НИИ "Центрпрограммсистем". Все отзывы положительные, но имеют следующие критические замечания:

1. Недостаточное описание построенных математических моделей. В частности, в явном виде отсутствует формулировка системы допущений, на которой основаны построенные модели. Не рассмотрены вопросы сложности и вычислительной устойчивости предлагаемых моделей. Предложенные модели оценки задержек ориентированы на простейший поток запросов и экспоненциальное распределение времени их поэтапного обслуживания. Игнорирование ошибок контроля по обнаружению угроз второго рода в моделях оценки защищенности. Модели надежности не учитывают влияние системы контроля.

2. В работе присутствует недостаточное описание, обоснование или анализ построения исследуемой системы защиты. Например, не ясно как происходит балансировка нагрузки между средствами защиты, объединенными в одну логическую группу (кластер). В работе не исследованы варианты параллельного и конвейерного применения средств защиты информации. Не дается обоснования использования конкретных величин параметров системы защиты. Не ясна применимость предложенных моделей оценки задержек обслуживания, в системах, в которых существенное влияние может оказывать качество канала связи (например, облачные системы защиты). Не исследованы вопросы влияния на эффективность защиты программных и аппаратных средств, выполняющих сервисные функции.

3. Отсутствие сравнения полученных результатов с результатами от полученными другими методами исследований и/или на других типах объектов исследования. В частности, нет экспериментального подтверждения основных положений и подтверждения результатов аналитического моделирования имитационным моделированием. Нет сравнения предложенных методов оценки эффективности

систем защиты с другими методами. Эффективность предлагаемых решений показана только при последовательном использовании средств защиты.

4. Недостаточное обоснование моделей, их использования и применения. Например, отсутствует описание того, как можно вычислить накладываемые ограничения на обеспечение стационарности режима работы узлов. Не ясно, что подразумевается автором под вычислительными ресурсами узла, в чем они измеряются и какие функции обеспечивают. Нет обоснования того, что система защиты является системой массового обслуживания, где время обработки информации в узлах системы считается константой или случайной величиной, распределенной по экспоненциальному закону.

Выбор официальных оппонентов и ведущей организации обосновывается их широкой известностью своими достижениями в области информационной безопасности и связанных с проблематикой, представленной к защите диссертации, в частности, наличием значительного количества публикаций по тематике диссертации и способностью определить научную и практическую ценность работы.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований: разработаны модели и методы оценки защищенности вычислительных систем, надежности систем защиты информации и задержек, вносимых ими при различных вариантах их комплектации средствами защиты; система частных и комплексных показателей эффективности систем защиты информации; метод построения схем безопасного доступа узлов корпоративной сети к ресурсам внешней сети; предложен подход к оценке информационной защищенности, и методика оценки времени поиска угроз информационной безопасности, учитывающие возможную пересекаемость множеств обнаруживаемых и устраняемых угроз информационной безопасности для последовательно применяемых средств защиты информации; доказано наличие зависимости показателей защищенности вычислительной системы и времени обнаружения и устранения угроз от порядка применения средств защиты и пересекаемости множеств обнаруживаемых и устраняемых средствами защиты угроз информационной безопасности.

Теоретическая значимость исследования обоснована тем, что доказаны положения о влиянии: пересекаемости множеств угроз информационной безопасности обнаруживаемых и устраняемых средствами защиты информации, применяемых в составе систем защиты информации, и порядка их использования на информационную защищенность вычислительной системы и вносимые системой защиты информации задержки обслуживания; о снижении потока запросов в результате его фильтрации при работе средств защиты и комплектности системы защиты информации на задержки системы защиты информации и её функциональную надежность; применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) использованы методы теории вероятностей, надежности и массового обслуживания, методы сравнительного анализа и математического моделирования; изложены аргументы в пользу необходимости учета влияния: пересекаемости множеств угроз обнаруживаемых и устраняемых последовательно применяемыми средствами защиты на вероятность и время обнаружения и устранения угроз; порядка применения средств защиты и возможной фильтрации трафика в результате их последовательной работы на время обнаружения и устранения угроз; аргументы в пользу применения модельно ориентированного подхода к оценке эффективности систем защиты информации; стадии модернизации системы защиты информации, использующей поэтапное применение средств защиты информации; раскрыты проблемы применения в составе систем защиты информации элементов, осуществляющих взаимное подключение нескольких групп узлов вычислительной системы, к которым предъявляются разные требования информационной безопасности; изучены связи между задержками, вероятностью обнаружения и устранения угрозы, а также функциональной надежностью от интенсивности входного потока, порядка применения средств защиты и пересечения множеств угроз информационной безопасности; проведена модификация существующих математических моделей оценки задержек и функциональной надежности системы защиты, позволяющая учесть пересекаемость множеств обнаруживаемых и устраняемых угроз, а также

порядок применения средств защиты; существующих схем безопасного доступа узлов корпоративной сети к ресурсам внешней сети.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что: разработаны и внедрены методы оценки эффективности систем защиты информации, включающие в себя оценку функциональной надежности, средней задержки и вероятности обнаружения угроз. Указанные методы могут быть применены с целью обоснования выбора комплектации средствами защиты и порядка их применения. Результаты внедрены в научно-исследовательских работах ФГАОУ ВО "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики", в производственную деятельность ООО "Академия тепла" и International Police Association – Международная неправительственная организация с консультативным статусом «SPECIAL» при Экономическом и Социальном Совете ООН; определены пределы и перспективы практического использования предложенных методов, критериев и моделей оценки эффективности систем защиты; созданы метод построения высокоэффективных систем защиты информации; практические рекомендации по использованию разработанных моделей и методов оценки эффективности систем защиты, включая обоснование выбора их комплектации и организации систем защиты, при поэтапном обнаружении и устранении угроз; представлены предложения по дальнейшему совершенствованию разработанных моделей и методов оценки эффективности систем защиты информации, в частности, применение конвейерного и/или параллельного методов обнаружения угроз, учет неординарности потока запросов; рекомендации по модернизации схем безопасного доступа, использующих поэтапное применение средств защиты.

Оценка достоверности результатов исследования выявила: для экспериментальных работ результаты получены при использовании общедоступного и/или лицензированного программного обеспечения (в частности, система компьютерной математики MathCAD, программа для анализа и организации информации MS Excel); входные данные и настраиваемые параметры для всех проведенных исследований (экспериментов) отражены в

тексте диссертации, что дает воспроизводимость результатов диссертационного исследования; теория построена на известных, проверяемых данных, согласуется с опубликованными данными по теме диссертации, а также подтверждается экспериментальным применением методов оценки эффективности систем защиты информации; идея базируется на анализе практики и обобщении передового опыта в построении и оценке эффективности систем защиты информации; использованы статистические и аналитические данные по параметрам, характеристикам и опыту построения и использования современных средств защиты информации, в том числе при их консолидации в единую систему; установлено качественное совпадение авторских результатов с результатами, представленными в независимых источниках по данной тематике, а именно, характер роста вносимых задержек от интенсивности входного потока при экспоненциальном распределении времени обслуживания; использованы типовая модель нарушителя и методы противодействия угрозам информационной безопасности, возникающих при работе вычислительных систем; типовые структуры (схемы) безопасного доступа узлов корпоративной сети к ресурсам внешней сети; модели массового обслуживания и теории надежности.

Личный вклад соискателя состоит в: обобщении и систематизации существующих методов обеспечения информационной безопасности вычислительных систем и анализе существующих угроз, которым они могут быть подвержены; разработке модели и метода оценки информационной защищенности вычислительной системы, учитывающей взаимное пересечение множеств обнаруживаемых и устраняемых угроз информационной безопасности различными средствами защиты; построении моделей надежности и задержек, позволяющие учесть снижение интенсивности потока запросов в результате его поэтапной фильтрации средствами защиты; обосновании системы комплексных показателей эффективности систем защиты, учитывающих защищенность вычислительной системы, задержки и функциональную надежность системы защиты; формировании вариантов исследуемых структур (схем) безопасного доступа; разработке практических рекомендаций по использованию методов оценки эффективности систем защиты информации, полученных в диссертации, и

вариантов рассматриваемых схем безопасного доступа; непосредственном участии в обработке и интерпретации экспериментальных данных; личном участии в подготовке основных публикаций, выступлении на научных конференциях и семинарах, а также внедрении полученных в диссертации результатов.

Диссертация "Модели и методы оценки эффективности систем защиты информации и обоснование выбора их комплектации", соответствует требованиям п. 9 "Положения о присуждении ученых степеней" и пунктам 6 и 10 паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

На заседании 26 декабря 2018 года диссертационный совет принял решение присудить Коломойцеву В.С. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 17 человек, из них 4 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за – 14, против – 2, недействительных бюллетеней – 1.

Председатель диссертационного совета,
доктор технических наук, профессор Бачевский Сергей Викторович

Ученый секретарь диссертационного совета,
кандидат технических наук Владыко Андрей Геннадьевич

28 декабря 2018 года