ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 212.268.03, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР) МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____
решение диссертационного совета от 28 декабря 2021 г. № 16

О присуждении Егошину Николаю Сергеевичу, гражданину Российской Федерации, учёной степени кандидата технических наук.

Диссертация «Модели угроз нарушения безопасности информационных потоков в киберпространстве» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 28 октября 2021 г. (протокол № 12) диссертационным советом Д 212.268.03, созданным на базе ТУСУРа (634050, г. Томск, пр. Ленина, 40), приказ № 105/нк от 11.04.2012.

Соискатель Егошин Николай Сергеевич, 15 февраля 1992 года рождения, в 2015 году окончил ТУСУР. С 2015 по 2019 годы обучался в аспирантуре ТУСУРа по специальности «Методы и системы защиты информации, информационная безопасность» (05.13.19.). Работает в должности старшего преподавателя кафедры комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) и младшего научного сотрудника лаборатории безопасных биомедицинских технологий центра технологий безопасности кафедры КИБЭВС.

Диссертация выполнена на кафедре КИБЭВС ТУСУРа.

Научный руководитель – Шелупанов Александр Александрович, доктор технических наук, профессор, президент ТУСУРа.

Официальные оппоненты: Ложников Павел Сергеевич, доктор технических наук, профессор, заведующий кафедрой «Комплексная защита информации» Омского государственного технического университета; Золотарев Вячеслав Владимирович, кандидат технических наук, заведующий кафедрой «Безопасность информационных технологий» Сибирского государственного университета науки

и технологий имени академика М.Ф. Решетнева (г. Красноярск), дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ» (г. Москва), в своем положительном отзыве, составленном Толстым А.И., к.т.н., доц., и.о. зав. кафедрой «Информационная безопасность банковских систем», утвержденном Нагорновым О.В. д.ф.-м.н., и.о. первого проректора», указала, что диссертация Егошина Н.С. является законченной научно-квалификационной работой, в которой на основании выполненных автором исследований решена научно-техническая задача, имеющая важное хозяйственное значение. Полученные результаты вносят определенный вклад в развитие таких областей ИБ как методы и модели идентификации и классификации УБИ объектов различного вида и класса, а также модели и методы управления ИБ. Таким образом, диссертационная работа удовлетворяет требованиям «Положения о порядке присуждении ученых степеней», а ее автор – Егошин Николай Сергеевич – заслуживает присуждения ему ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 10 опубликованных работ, все по теме диссертации, из них в рецензируемых научных изданиях, рекомендованных ВАК – 4, в изданиях Scopus и WoS – 2. Общий объем – 7,4 п.л., авторский вклад – 4,1. Наиболее значимые работы:

1. Егошин Н.С. Модель типовых угроз безопасности информации, основанная на модели информационных потоков // Доклады ТУСУРа. – 2021 – Т. 24. – №3. – С. 21-25

2. Егошин Н.С. Модель угроз безопасности информации, передаваемой через интернет / Н.С. Егошин, А.А. Конев, А.А. Шелупанов // Информация и безопасность. – 2018. – Т. 21. – №4. – С. 530-533.

3. Егошин Н.С. Формирование модели нарушителя / Н.С. Егошин, А.А. Конев, А.А. Шелупанов // Безопасность информационных технологий. – 2017. – Т. 24. – №4. – С. 19–26. – DOI: 10.26583/bit.2017.4.02

4. Egoshin N.S., Konev A.A., Shelupanov A.A. A Model of Threats to the Confidentiality of Information Processed in Cyberspace Based on the Information Flows Model // Symmetry. – 2020. – Volume 12. – Issue 11. – 1840. – pp. 1-18

5. Egoshin N.S., Konev A.A., Shelupanov A.A. Functional scheme of the process of access control: Methodology for the formation of normative documents on the access control // 2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC), DOI: 10.1109/RPC.2018.8482179

На диссертацию и автореферат поступило 9 положительных отзывов из следующих организаций: Уральский государственный университет путей сообщения, г. Екатеринбург (Зырянова Т.Ю., к.т.н., доцент кафедры информационных технологий и защиты информации); Северо-Кавказский федеральный университет, г. Ставрополь (Петренко В.И., к.т.н., зав. кафедрой организации и технологии защиты информации); Тамбовский государственный технический университет (Громов Ю.Ю., д.т.н., проф., директор института автоматики и информационных технологий); Нижегородский государственный университет им. Н.И. Лобачевского (Ротков Л.Ю., к.т.н. доц., зав. кафедрой безопасности информационных систем); Самарский университет (Осипов М.Н., к.ф.-м.н., доц., зав. кафедрой безопасности информационных систем); АО «Аладдин Р. Д.» (Сабанов А.Г., д.т.н., проф., зам. генерального директора); ФГАНУ НИИ «Спецвузавтоматика» (Мкртичян В.В, к.т.н., старший научный сотрудник лаборатории телекоммуникационных технологий; Хади Р.А., к.т.н., директор); РТУ МИРЭА, г. Москва (Григорьев В.Р., к.т.н., доц., зам. директора Института кибербезопасности и цифровых технологий), Академия ФСО РФ, г. Орел (Цибуля А.Н., к.т.н., доц., сотрудник).

В отзывах на автореферат указаны следующие основные замечания: не представлены ограничения на применимость разработанной модели, поскольку ни одна модель не может отражать абсолютно все свойства моделируемого объекта; не представлена как таковая методика формирования политики разграничения доступа даже сокращенном варианте; нет достаточного обоснования полноты множества элементарных информационных потоков; бальная система модели нарушителя не соответствует итоговым уровням нарушителя; на модель

информационных потоков вводится 4 дополнительных ограничения, но они никак не обосновываются; не совсем понятно, почему угрозу контроля канала нельзя представить как добавление несанкционированного канала; автор выделяет три типа несанкционированного воздействия на информацию (уничтожение, искажение, подмена), однако не обосновывает такой выбор; во всем тексте автореферата подразумевается автономность системы мандатного управления правами доступа от ИС, модель угроз которой рассматривается; по тексту не ясно, какие противоречия заложены в основу выбранной темы; не дано четкое обоснование разделению типов нарушителей при реализации ими функции поиска и использования уязвимостей; при прочтении возникают вопросы, что же является объектом исследований; в автореферате написано «Объектом исследований данной работы является информация, защищаемая и обрабатываемая в информационной системе...», а названия и положения, выносимые на защиту, утверждают, что исследуются информационные потоки; в автореферате нет достаточного обоснования полноты множества элементарных информационных потоков.

Выбор официальных оппонентов обосновывается тем, что д.т.н. проф. Ложников П.С. является известным специалистом в области информационной безопасности, защиты информации, математического моделирования и математических методов; к.т.н. Золотарев В.В. является признанным специалистом в области информационной безопасности и разработки автоматизированных систем.

Выбор ведущей организации обосновывается тем, что «НИЯУ «МИФИ» имеет общепризнанные достижения в области управления информационной безопасностью, безопасности компьютерных сетей и облачных вычислений.

Официальные оппоненты и ведущая организация имеют значительный объём публикаций по тематике диссертации в ведущих изданиях и способны аргументированно обосновать научную и практическую ценность диссертационной работы Егошина Н.С.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– **разработаны** модель информационных потоков в информационной си-

стеме, модель угроз безопасности информации, новая модель нарушителя ИБ, методика формирования политики разграничения доступа к информации;

– **предложена** оригинальная классификация угроз безопасности информации, в основе которой лежит модель информационных потоков;

– **предложена** мультиграфовая модель потоков данных в информационной системе, отличающаяся учетом гетерогенности каналов передачи информации;

– **доказана** эффективность применения полученных результатов при решении научно-прикладных задач, связанных с составлением перечней типовых угроз безопасности информации и перспективность их использования для решения актуальных практических задач.

Теоретическая значимость исследования обоснована тем, что:

– **применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) использован** математический аппарат теории графов для описания информационных потоков применительно к разработке модели информационных потоков, применяемой для описания информационной системы.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что сравнение разработанной модели угроз безопасности информации с аналогом позволило дополнительно выделить 13 типовых угроз. Разработанная модель угроз была внедрена в деятельность ООО «НПФ «ИСБ», г. Томск. Применение модели угроз позволило получить полный перечень типовых угроз безопасности информации, обрабатываемой в Информационной системе персональных данных (ИСПДн). Полученный список был учтен при определении перечня актуальных угроз, что показало необходимость внедрения в систему дополнительных механизмов защиты. Результатом внедрения работы в деятельность ООО «НПФ «ИСБ» стал перечень из 43 угроз безопасности информации в ИСПДн, что на 14 % больше, чем количество угроз, выявленных экспертами ранее. Разработанная методика формирования политики разграничения доступа, использующая упомянутую ранее модель элементарных информационных потоков, позволила разграничить доступ к каналам передачи данных как к само-

стоятельным структурным единицам системы. Предложенная методика была внедрена в деятельность ООО «УЦ Сибири», г. Томск. Результатом внедрения стало уменьшение времени, необходимого для формирования политики разграничения доступа на 19 %. Внедрение модели угроз и методики формирования политики разграничения доступа в учебный процесс кафедры КИБЭВС ТУСУРа в рамках курсов «Управление информационной безопасностью» и «Разработка и эксплуатация защищенных автоматизированных систем» позволило студентам ознакомиться с процессами применения моделей угроз безопасности информации, обрабатываемой в информационной системе и построения политики разграничения доступа к ресурсам системы.

Оценка достоверности результатов исследования выявила:

– **теория** построена на известных методах теории множеств, системного анализа, теории защиты информации и теории графов;

– **идея базируется** на анализе практики и обобщении передового опыта моделирования угроз безопасности информации;

– **использовано** сравнение авторского перечня типов угроз с угрозами из банка данных ФСТЭК России.

Личный вклад соискателя: в диссертационной работе использованы результаты, в которых автору принадлежит определяющая роль. Постановка задачи исследования и верификация результатов в процессе выполнения работы осуществлялась научным руководителем д.т.н., проф. Шелупановым А. А.

В ходе защиты диссертации были высказаны следующие критические замечания: в работе нет подробного описания внедрения, не указано кто именно и какие конкретно методики оценки результатов внедрения использовал; при формировании модели информационных потоков в системе учитывается множество носителей информации и множество программных процессов, но игнорируется множество программно-аппаратных средств; в работе отсутствует обоснованность применения полного перебора состояний элементарного информационного потока, которые обуславливаются компрометацией его элементов, для доказа-

тельства полноты разработанной модели угроз безопасности информации; в работе нет подробного описания применяемых методов системного анализа.

Соискатель Егошин Н.С. ответил на заданные вопросы и согласился с озвученными в рамках заседания критическими замечаниями.

На заседании 28 декабря 2021 г. диссертационный совет принял решение, что полученные Егошиным Н.С. результаты вносят определенный вклад в развитие таких областей ИБ как методы и модели идентификации и классификации угроз безопасности информации, а также модели и методы управления ИБ. За решение научно-технической задачи, имеющей важное хозяйственное значение, присудить Егошину Н.С. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 18 человек, из них 9 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за – 18, против – 0, недействительных бюллетеней – 0.

Заместитель председателя
диссертационного совета Шурыгин Юрий Алексеевич

Ученый секретарь
диссертационного совета Костюченко Евгений Юрьевич

29 декабря 2021 г.