РЕШЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА УрФУ 2.3.05.13 ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

от «16» ноября 2021 г. № 18

о присуждении Гибилинде Роману Владимировичу, гражданство Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Разработка автоматизированных методов анализа воздействий на файлы в задаче расследования инцидентов информационной безопасности» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите диссертационным советом УрФУ 2.3.05.13 «07» октября 2021 г., протокол № 14.

Соискатель, Гибилинда Роман Владимирович, 1991 года рождения;

в 2014 г. окончил ФГАОУ ВПО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» по специальности 090106 Информационная безопасность телекоммуникационных систем;

с 01.01.2017 г. по 01.07.2017 г. и с 11.03.2021 г. по 10.08.2021 г. был прикреплен в качестве экстерна по направлению 10.06.01 Информационная безопасность (Методы и системы защиты информации, информационная безопасность) для сдачи кандидатских экзаменов;

с 01.04.2020 г. прикреплен к ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» для подготовки диссертации на соискание ученой степени кандидата технических наук без освоения программ подготовки научно-педагогических кадров в аспирантуре по направлению 10.06.01 Информационная безопасность (Методы и системы защиты информации, информационная безопасность), предполагаемый срок окончания прикрепления 31.03.2023 г.;

является военнослужащим (г. Екатеринбург); по совместительству работает в должности ассистента Учебно-научного центра «Информационная безопасность» Института радиоэлектроники и информационных технологий-РТФ

ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина».

Диссертация выполнена в Учебно-научном центре «Информационная безопасность» Института радиоэлектроники и информационных технологий-РТФ ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», Минобрнауки России.

Научный руководитель – кандидат технических наук, доцент, Синадский Николай Игоревич, ФГАОУ ВО «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина», Институт радиоэлектроники и информационных технологий-РТФ, Учебно-научный центр «Информационная безопасность», доцент.

Официальные оппоненты:

Баранкова Инна Ильинична – доктор технических наук, доцент, ФГБОУ ВО «Магнитогорский государственный технический университет им. Г.И. Носова», г. Магнитогорск, кафедра «Информатика и информационная безопасность», заведующая кафедрой;

Титов Сергей Сергеевич – доктор физико-математических наук, профессор, ФГБОУ ВО «Уральский государственный университет путей сообщения», г. Екатеринбург, кафедра «Информационные технологии и защита информации», главный научный сотрудник;

Соколов Александр Николаевич – кандидат технических наук, доцент, ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», г. Челябинск, Высшая школа электроники и компьютерных наук, кафедра «Защита информации», заведующий кафедрой

дали положительные отзывы на диссертацию.

Соискатель имеет 8 опубликованных работ, в том числе по теме диссертации – 8 работ, из них 4 статьи, опубликованные в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ, включая 1 ста-

тью в издании, входящем в международную реферативную базу Scopus; 2 свидетельства о государственной регистрации программы для ЭВМ. Общий объем опубликованных работ – 3,11 п.л., авторский вклад – 1,64 п.л.

Основные публикации по теме диссертации:

статьи, опубликованные в рецензируемых научных изданиях, определенных ВАК РФ и Аттестационным советом УрФУ:

1. Гайдамакин Н.А. Метод экспресс-анализа событий, связанных с воздействиями на файлы, предназначенный для расследования инцидентов информационной безопасности / Н.А. Гайдамакин, **Р.В. Гибилинда**, Н.И. Синадский // Вестник СибГУТИ. — 2020. — № 4. — С.3-13. (0,68 п.л. / 0,23 п.л.).

2. Gaidamakin N.A. File Operations Information Collecting Software Package Used in the Information Security Incidents Investigation / Nikolay A Gaidamakin, **Roman V Gibilinda** and Nikolay I Sinadskiy // 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – 2020. – № 9117671. – pp. 559-562. (0,25 п.л. / 0,08 п.л.) (Scopus).

3. Гайдамакин Н.А. Событийная модель процесса идентификации воздействий на файлы при расследовании инцидентов информационной безопасности, основанная на математическом аппарате сетей Петри / Н.А. Гайдамакин, **Р.В. Гибилинда**, Н.И. Синадский // Вестник СибГУТИ. — 2020. — № 1. — С.73-88. (1 п.л. / 0,33 п.л.).

4. **Гибилинда Р.В.** Кластеризационный метод идентификации воздействий на файлы с применением алгоритма k-средних, используемый при расследовании инцидентов информационной безопасности / **Р.В. Гибилинда** // Вестник УрФО. Безопасность в информационной сфере. — 2020. — Вып. 35 — № 1. — С. 35-47. (0,81 п.л.).

Свидетельства о государственной регистрации программ для ЭВМ:

5. Свидетельство № 2020616110 Российская Федерация. Свидетельство о государственной регистрации программы для ЭВМ «Программное средство обнаружения событий информационной безопасности, использующее шаблоны

воздействий на файлы» / **Р.В. Гибилинда**. – Заявка № 2020613614 от 26.03.2020; дата гос. регистрации в Реестре 09.06.2020. – Реестр программ для ЭВМ. – 1 с.

6. Свидетельство № 2020616109 Российская Федерация. Свидетельство о государственной регистрации программы для ЭВМ «Программное средство генерации шаблонов воздействий на файлы, используемое при расследовании инцидентов информационной безопасности» / **Р.В. Гибилинда**. – Заявка № 2020613613 от 26.03.2020; дата гос. регистрации в Реестре 09.06.2020. – Реестр программ для ЭВМ. – 1 с.

На автореферат поступили отзывы:

1. Королькова Юрия Дмитриевича, доктора физико-математических наук, профессора, профессора кафедры радиофизики и радиоэлектроники физического факультета ФГБОУ ВО «Иркутский государственный университет», г. Иркутск. Содержит замечания по алгоритмам и рисункам автореферата.

2. Затонского Андрея Владимировича, доктора технических наук, профессора, заведующего кафедрой «Автоматизация технологических процессов» Березниковского филиала ФГБОУ ВО «Пермский национальный исследовательский политехнический университет», г. Березники. Содержит замечания по рисункам автореферата и вопрос об оптимизации временных затрат.

3. Пономарева Олега Павловича, доктора технических наук, доцента, заместителя генерального директора по НТР – главного конструктора АО «Уральское производственное предприятие «Вектор», г. Екатеринбург. Содержит вопросы о полноте множества приведенных типов операций и используемых законах распределения, и замечание по рисункам.

4. Поляковой Елены Николаевны, кандидата педагогических наук, доцента, директора Института математики и интеллектуальных систем ФГБОУ ВО «Курганский государственный университет», г. Курган. Содержит вопросы об используемых шаблонах в разработанном модуле.

5. Тимакова Алексея Анатольевича, кандидата технических наук, доцента, доцента базовой кафедры № 252 – информационной безопасности Инсти-

тута кибернетики ФГБОУ ВО «МИРЭА – Российский технологический университет», г. Москва. Содержит замечания по приведенным алгоритмам и тексту автореферата.

6. Фадеева Михаила Михайловича, кандидата юридических наук, доцента кафедры финансового мониторинга (№ 75) Института финансовых технологий и экономической безопасности ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», г. Москва. Содержит замечания по тексту и рисункам автореферата.

7. Ручая Алексея Николаевича, кандидата физико-математических наук, доцента, заведующего кафедрой компьютерной безопасности и прикладной алгебры ФГБОУ ВО «Челябинский государственный университет», г. Челябинск. Содержит замечания по используемым обозначениям, формулировкам приведенных метрик и описаниям на рисунках.

8. Богданова Валентина Викторовича, кандидата технических наук, Генерального директора ООО «Уральский центр систем безопасности», г. Екатеринбург. Содержит замечания по отсутствию достаточных пояснений к рисункам и алгоритмам.

9. Гильмиярова Романа Владимировича, Генерального директора ООО «Институт радиоэлектронных систем», г. Екатеринбург. Содержит замечания о недостаточности пояснений на рисунках и вопрос о проверке системы в условиях высокой нагрузки.

Выбор официальных оппонентов обосновывается широкой известностью их достижений и исследований в области информационной безопасности и практического применения методов и систем защиты информации. Это подтверждается соответствующими публикациями в рецензируемых российских и международных научных изданиях.

Диссертационный совет отмечает, что представленная диссертация на соискание ученой степени кандидата технических наук соответствует п. 9 Положения о присуждении ученых степеней в УрФУ, является научно-квалификационной рабо-

той, в которой на основании выполненных автором исследований разработаны новые научно обоснованные технические решения для идентификации событий нарушения информационной безопасности (ИБ) на основе автоматизированных методов анализа последовательностей внешних воздействий на файлы, размещаемые на электронных носителях. Представленные разработки имеют существенное значение для развития методов компьютерной криминалистики, применяемых в Российской Федерации при расследовании инцидентов ИБ.

Диссертация представляет собой самостоятельное законченное исследование, обладающее внутренним единством. Положения, выносимые на защиту, содержат новые научные результаты и свидетельствуют о личном вкладе автора в науку:

1. Разработана событийная модель процесса идентификации воздействий на файлы, позволяющая выделить ключевой набор признаков, необходимых для анализа и мониторинга в рамках расследования инцидентов информационной безопасности.

2. Разработан метод автоматизации процесса идентификации внешних воздействий на файлы, направленных на нарушение используемой политики ИБ, на основе выделенного набора признаков, включая способы предварительной обработки данных, обеспечивающие повышение точности работы алгоритма в целом.

3. Разработана методика, позволяющая проводить экспресс-анализ событий ИБ, связанных с внешними воздействиями на файлы, а также специальное программное обеспечение, предназначенное для автоматизации процессов выявления фактов нарушений действующей политики ИБ и оперативного реагирования на специалистов в области ИБ.

Диссертационная работа Гибилинды Романа Владимировича ориентирована на решение актуальной проблемы автоматизации процессов обнаружения, идентификации и классификации внешних воздействий на файлы, являющихся неотъемлемой частью расследований инцидентов ИБ. Разработанные автором диссертации автоматизированные методы и алгоритмы используются в ООО «Уральский центр систем безопасности» (г. Екатеринбург); в ОКБ «Новатор» (г. Екатеринбург); и в

Институте информационных технологий и радиоэлектроники-РТФ УрФУ при изучении дисциплины «Программно-аппаратные средства обеспечения информационной безопасности».

На заседании 16 ноября 2021 г. диссертационный совет УрФУ 2.3.05.13 принял решение присудить Гибилинде Р.В. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет УрФУ 2.3.05.13 в количестве 14 человек, в том числе 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 19 человек, входящих в состав совета, проголосовали: за – 14, против – нет, недействительных бюллетеней – нет.

Председатель
диссертационного совета
УрФУ 2.3.05.13 Поршнев Сергей Владимирович

Ученый секретарь
диссертационного совета
УрФУ 2.3.05.13 Сафиуллин Николай Тахирович

16.11.2021 г.