ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.073.02, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО УЧРЕЖДЕНИЯ «ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ИНФОРМАТИКА И УПРАВЛЕНИЕ» РОССИЙСКОЙ АКАДЕМИИ НАУК», ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от «27» декабря 2021 г. протокол № 4

О присуждении СМИРНОВУ ДМИТРИЮ ВЛАДИМИРОВИЧУ, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методы поиска признаков инсайдера в Big Data» по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность, в виде рукописи принята к защите 22.10.2021, протокол № 3 диссертационным советом Д 002.073.02, созданным на базе Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) (119333, г. Москва, ул. Вавилова, д. 44, корп. 2; приказ Министерства образования и науки РФ от 24.06.2016 №771/нк).

Соискатель Смирнов Дмитрий Владимирович, 1984 года рождения, в 2008 году окончил факультет микроприборов и технической кибернетики в Государственном образовательном учреждении высшего профессионального образования «Московский государственный институт электронной техники (технический университет)» по специальности «Комплексная защита объектов информатизации». С 2006 по 2012 года работал на инженерных должностях компаний ООО «СТЭЛКОМ», ЗАО «Корпорация ЮНИ», ЗАО «Банк Кредит Свисс (Москва). С 2012 по настоящее время работает в ПАО «Сбербанк», в службе информационной безопасности. В 2020 году был прикреплен (с 27.11.2020, приказ № 3-73) к ФИЦ ИУ РАН для подготовки кандидатской диссертации.

Диссертация выполнена в отделе №53 «Информационная безопасность в информационных, управляющих и телекоммуникационных системах» отделения №5 ФИЦ ИУ РАН.

Научный руководитель – доктор физико-математических наук, член-корреспондент Академии криптографии Российской Федерации, профессор Грушо Александр Александрович, главный научный сотрудник ФИЦ ИУ РАН.

Официальные оппоненты:

1. Зегжда Петр Дмитриевич, гражданин Российской Федерации, доктор технических наук (специальность 05.13.19), профессор, ФГАОУ ВО «Санкт-Петербургский политехнический университет»;
2. Смирнов Сергей Николаевич, гражданин Российской Федерации, доктор технических наук (специальность 05.13.19), профессор ФГБОУ ВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)»,

дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное бюджетное образовательное учреждение «Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР)» – в своем положительном заключении, подписанном доктором технических наук А.А. Шелупановым и утвержденном В.М. Рулевским, доктором технических наук, доцентом, ректором ТУСУР, указала, что диссертация Смирнова Дмитрия Владимировича является законченной научно-квалификационной работой, в которой содержится решение актуальной задачи поиска инсайдеров в системах распределенной обработки данных, характеризующийся несколькими тысяч серверов, петабайтными объемами данных и числом пользователей в несколько тысяч; диссертационная работа полностью соответствует требованиям к диссертациям на соискание ученой степени кандидата наук, установленным Положением о порядке присуждения ученых степеней, а ее автор, Смирнов Дмитрий Владимирович, заслуживает присуждения искомой ученой степени кандидата технических наук.

Соискатель имеет 7 опубликованных работ, в том числе по теме диссертации – 7, из них в рецензируемых научных изданиях – 6. Общий объем публикаций по теме диссертации – 36 с.; вклад автора в них является определяющим. Сведения, представленные соискателем об опубликованных работах, в которых изложены основные научные результаты диссертации, являются достоверными. В них достаточно полно изложены материалы исследования.

Наиболее значимые работы по теме диссертации:

1. Смирнов Д.В., Грушо А.А., Забежайло М.И., Тимонина Е. Е. Система сбора и анализа информации из различных источников в условиях Big Data // International Journal of Open Information Technologies, 2021. V. 9. No 4. Pp. 64-71. http://injoit.org/index.php/j1/article/view/1099;

2. Грушо А.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е., Шоргин С.Я. Методы математической статистики в задаче поиска инсайдера // Информатика и ее применения, 2020. Т. 14. Вып. 3. С. 71-75;

3. Смирнов Д. В. Об одной методике проблемно-ориентированного анализа Big Data в режиме процессно-реального времени // International Journal of Open Information Technologies, 2021. V. 9. No 9. Pp. 88-94. http://www.injoit.org/index.php/j1/article/view/1169.

На автореферат дали положительные, не содержащие критических замечаний, отзывы:

1. Овчинский Анатолий Семенович, д.т.н., профессор, академик РАЕН, профессор кафедры Информационной безопасности Московского университета МВД РФ им. В.Я.Кикотя;
2. Ковалевский Артем Павлович, д.ф.-м.н., доцент, профессор кафедры высшей математики Новосибирского государственного технического университета;
3. Рабинович Борис Ильич, к.т.н., директор Департамента управления данными ПАО Сбербанк.

Выбор официальных оппонентов обосновывается их высокой квалификацией, наличием научных трудов, соответствующих теме оппонируемой диссертации, и следующими обстоятельствами:

– П.Д. Зегжда является крупным специалистом в области обнаружения инсайдеров и скрытых каналов, методов анализа и синтеза надежности и безопасности сложных систем;

– С.Н. Смирнов ведет активную деятельность в области качества информационных систем, технологий разработки больших программных систем и надежности программного обеспечения.

Выбор ведущей организации обосновывается тем, что ТУСУР активно занимается проблематикой по теме диссертационной работы Д.В. Смирнова, что подтверждается приоритетными направлениями работы и публикациями сотрудников.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– **решена** научно-техническая проблема поиска признаков вредоносной инсайдерской активности в Big Data информации о взаимодействии большого множества пользователей с большим хранилищем данных при допущении о пополнении новыми сведениями и в условиях жестких временных ограничений;

– **обоснованы** методы и алгоритмы интеллектуального анализа данных, обеспечивающие эффективный первичный поиск в «сырой» (неразмеченной) Big Data информации о взаимодействии большого множества пользователей с большим хранилищем данных сведений, релевантных идентификации признаков вредоносных инсайдерских активностей;

– **разработаны** методы и алгоритмы представления знаний об анализируемых угрозах в виде динамически пополняемого новыми данными профиля угроз, сформированного типовыми сценариями потенциально опасных действий инсайдеров, а также диаграммы сходств типовых сценариев угроз;

– **разработаны** методы идентификации и статистического анализа аномалий в поведении объектов мониторинга, а также метод выявления сговора инсайдеров, сочетающий методы кластеризации и статистических оценок;

– **разработаны** методы оценки качества\надежности формируемых статистическими средствами заключений о классификации аномалий в поведении объектов мониторинга, дающие дополнительные основания для принятия решений о приоритетности отработки соответствующих "подсвеченных" ситуаций;

– **разработаны** проблемно-ориентированные средства имитационного моделирования для оценки ряда эффектов и поддержки принятия управленческих решений;

– **реализован** набор оригинальных программных инструментов формирования и реконструкции диаграммы сходств типовых сценариев используемого профиля угроз;

– **разработан** программный комплекс, включающий в себя набор сервисных программных инструментов, поддерживающих нормализацию данных как в первичном, так и во вторичном поиске;

– **предложен** способ интеграции вновь разработанных программных инструментов интеллектуального анализа данных (ИАД) с уже имеющимися в организации промышленными программными инструментами обработки данных

– **получено** подтверждение работоспособности и результативности разработанных в диссертации методов в процессе промышленной реализации программных инструментов ИАД в деятельности крупной коммерческой организации.

Теоретическая значимость исследования обоснована тем, что найдены условия, при которых возможно идентифицировать признаки инсайдера в Big Data в ограниченное время. Разработанные алгоритмы позволяют ускорять перебор и обрабатывать большие объемы данных с необходимой полнотой и точностью.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что разработанные соискателем подходы и методы внедрены в практику в виде системы, которая работает в крупном коммерческом банке.

Оценка достоверности результатов исследования выявила, что оно обосновано теоретически и экспериментально, и это подтверждается их использованием в промышленной системе крупного коммерческого банка.

Основные результаты, представленные в диссертационной работе, получены соискателем лично. В опубликованных совместных работах постановка и исследование задач осуществлялись совместными усилиями соавторов при непосредственном участии соискателя.

На заседании 27 декабря 2021 года диссертационный совет принял решение присудить Смирнову Дмитрию Владимировичу ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 22 человек, из них 6 докторов наук по профилю защищаемой диссертации, участвовавших в заседании, из 32 человек, входящих в состав совета, проголосовали: за – 21, против – 1, недействительных бюллетеней – 0.

Председатель
диссертационного совета Д 002.073.02
академик И.А. Соколов

Ученый секретарь
диссертационного совета Д 002.073.02
к.ф.-м.н. Р.В. Разумчик

«27» декабря 2021 г.