

ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.073.02 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 «20» 03 2019 г., протокол № 3

О присуждении МАРТЪЯНОВУ ЕВГЕНИЮ АЛЕКСАНДРОВИЧУ, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Исследование и разработка методик оценки защищенности информационных объектов от потенциальных нарушителей» по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность, в виде рукописи принята к защите 26.12.2018, протокол № 8 диссертационным советом Д 002.073.02 на базе федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (119333, г. Москва, ул. Вавилова, д.44, корп.2; приказ Министерства образования и науки РФ от 24.06.2016 №771/нк).

Мартьянов Евгений Александрович, 22 сентября 1991 года рождения, гражданин Российской Федерации, в 2013 году с отличием окончил факультет Вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова» (отделение специалистов) по специальности «Прикладная математика и информатика». С 2013 по 2016 год обучался в аспирантуре факультета Вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова». В настоящее время работает в должности начальника отдела разработки приложений ООО «АгроТерра».

Диссертация выполнена на кафедре информационной безопасности факультета Вычислительной математики и кибернетики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова».

Научный руководитель – кандидат физико-математических наук, доктор технических наук Макаров-Землянский Николай Викулович, ведущий научный сотрудник лаборатории Компьютерной безопасности Научно-исследовательского вычислительного центра Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова».

Официальные оппоненты:

1. Зегжда Петр Дмитриевич, гражданин Российской Федерации, доктор технических наук (специальность 05.13.16 – Применение вычислительной техники, математического моделирования и математических методов в научных исследованиях (по отраслям наук)), профессор, заслуженный деятель науки РФ, директор Специализированного центра защиты информации Санкт-Петербургского политехнического университета Петра Великого,

профессор кафедры Информационной безопасности компьютерных систем Института компьютерных наук и технологий Санкт-Петербургского политехнического университета Петра Великого;

2. Лукин Владимир Николаевич, гражданин Российской Федерации, кандидат физико-математических наук (специальность 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»), доцент, доцент кафедры № 806 Вычислительная математика и программирование факультета Информационных технологий и прикладной математики Федерального государственного бюджетного образовательного учреждения высшего образования «Московский авиационный институт (национальный исследовательский университет)»

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное бюджетное учреждение науки «Институт проблем управления имени В.А. Трапезникова Российской академии наук» в своем положительном заключении, подписанным А.Г. Чхартишвили, доктором физико-математических наук, главным научным сотрудником, заведующим лабораторией №79 «Сложных сетей» Института проблем управления имени В.А. Трапезникова Российской академии наук и утвержденное М.В. Губко, и.о. директора Института проблем управления имени В.А. Трапезникова Российской академии наук, указала, что диссертация Мартьянова Евгения Александровича является законченной квалификационной научно-исследовательской работой, содержащей новые научные и практические результаты, связанные с решением актуальной задачи. В заключении ведущей организации указано, что диссертационная работа соответствует п.9 Положения о присуждении ученых степеней №842, утвержденного постановлением Правительства Российской Федерации от 24.09.2013г., а ее автор, Мартьянов Евгений Александрович заслуживает присуждения искомой ученой степени кандидата технических наук.

Соискатель имеет 6 опубликованных работ по теме диссертации, опубликованных в рецензируемых научных изданиях – 4. Общий объем публикаций 2.44 п.л. Авторский вклад в полной мере определяет научную ценность всех публикаций.

Наиболее значимые публикации:

1. Мартьянов Е.А. Возможность выявления инсайдера статистическими методами// Системы и средства информатики, Т.27, №2, 2017.С. 41-47. ISSN 0869-6527.
2. Мартьянов Е.А. Имитационная модель поиска инсайдера статистическими методами // Системы и средства информатики, Т.27, №2, 2017. С. 48-59. ISSN 0869-6527.
3. Мартьянов Е.А. Запреты вероятностных мер в задаче поиска инсайдера //Системы и средства информатики, Т.27, №4, 2017. С. 144-149. ISSN 0869-6527.
4. Мартьянов Е.А., Макаров-Землянский Н.В. Оценка защищенности информационных объектов от потенциальных нарушителей // Естественные и технические науки, №6, 2013. С. 442-444. ISSN 1684-2626.

На диссертацию и автореферат поступили положительные, не содержащие критических замечаний отзывы от:

1. Толчеев В.О., гражданин Российской Федерации, доктор технических наук (специальность 05.13.01 – Системный анализ, управление и обработка информации), профессор кафедры Управления и информатики Института автоматизации и вычислительной техники Московского энергетического института;
2. Шубинский И.Б., доктор технических наук (специальность 05.13.15 – Вычислительные машины, комплексы и компьютерные сети), профессор, генеральный директор ЗАО «ИБТранс».

Выбор официальных оппонентов обосновывается следующими обстоятельствами:

- д.т.н. П.Д. Зегжда является известным специалистом в области информационной безопасности, кибербезопасности и технологий моделирования информационных систем, что подтверждается имеющимся у него большим количеством научных трудов и публикаций в области информационной безопасности;
- к.ф.-м.н. В.Н. Лукин ведет активную работу по тематике оппонируемой диссертации в области качества информационных систем и является специалистом в области защиты информации, читает обязательный курс для студентов по обеспечению информационной безопасности.

Выбор ведущей организации обосновывается тем, что Федеральное государственное бюджетное учреждение науки «Институт проблем управления им. В.А. Трапезникова Российской академии наук» является признанной широкой научной общественностью организацией, обладающей компетенцией в вопросах информационной безопасности, и активно занимается проблематикой по теме диссертационной работы Е.А. Мартьянова, что подтверждается приоритетными направлениями работы и публикациями сотрудников.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

- **разработан и обоснован** новый научный подход, позволяющий проводить исследование защищенности информационного объекта, представляющего из себя хранилище данных, путем реализации технического контроля и автоматического анализа всех выборок пользователей на предмет выхода за разрешенные множества областей данных, содержащая методическую, алгоритмическую и программную составляющие;
- **предложена** обобщенная модель взаимодействия пользователя с рабочим хранилищем данных, позволяющая выявить признаки инсайдера во множестве работающих пользователей по его запросам к хранилищу;
- на имитационной модели **показана** перспективность использования разработанного подхода в практике повышения и выявления инцидентов информационной безопасности;
- **определена** новая конструкция – множество «запретов», позволяющая, применительно к описанной модели, решать задачу с нулевой вероятностью ложной тревоги и асимптотически достоверным выводом;

- изложены научно обоснованные программно-технические решения, способствующие повышению устойчивости функционирования компьютерных систем.

Теоретическая значимость исследования обоснована тем, что:

- **решена** задача по анализу работы большого числа пользователей хранилища данных и в условиях множества малых выборок минимизировать вероятность ошибки первого рода (вне зависимости от множества атрибутов, с которыми работают пользователи), которая, в свою очередь, позволила решить техническую задачу построения системы контроля получения информации из хранилища данных;
- **решена** техническая задача построения системы контроля получения информации из хранилища данных, которая позволяет при анализе работы большого количества пользователей и в условиях множества малых выборок минимизировать вероятность ошибки первого рода и не зависит от тех множеств атрибутов, с которыми они работают;
- **разработан** новый метод оценки защищенности информационного объекта, состоящий в оценке эффективности метода обнаружения инсайдера.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

- результаты исследования позволили **создать** программное средство для контроля деятельности пользователей, которое было использовано в практической деятельности организаций, что подтверждено соответствующими актами;
- **представлены** предложения по дальнейшему развитию и оптимизации метода в части исследования времени наблюдения за действиями пользователя;
- **разработаны** практические рекомендации по повышению информационной защищенности систем различного назначения, заключающиеся в своевременном определении признаков функционирования неизвестного инсайдера с требуемой точностью на определенном объеме и представлении входных данных.

Оценка достоверности результатов исследования выявила, что:

- результаты **получены** на основании использования современных программных технологий и проверенных программных решений;
- теория **построена** на известных, проверяемых данных и согласуется с экспериментальными данными по теме диссертации;
- модель нарушителя **базируется** на анализе и обобщении накопленного опыта в изучении угрозы инсайдера в информационной системе;
- **установлено** соответствие полученных автором результатов применения классических методов математической статистики на имитационной модели с результатами, представленными в независимых источниках по данной тематике;
- **установлена** непротиворечивость экспериментально полученных количественных оценок теоретическим результатам;

– разработанные и представленные автором модель и результаты **обоснованы** строгими доказательствами и апробированными математическими методами исследования. Примененные методы адекватны решаемой научной задаче.

Основные результаты, представленные в диссертационной работе, получены соискателем лично. В работе [4] Е.А. Мартьянову принадлежат результаты исследования по оценке защищенности информационных ресурсов, Н.В. Макарову-Землянскому принадлежит постановка задачи и проверка результатов. В работе [5], указанной в автореферате, Е.А. Мартьянову принадлежит постановка задачи исследования по оценке защищенности информационных ресурсов и методика оценки. Остальные работы по теме диссертационного исследования написаны Е.А. Мартьяновым единолично.

На заседании 20 марта 2019 года диссертационный совет принял решение присудить Е.А. Мартьянову ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 26 человек, из них 8 докторов наук по профилю защищаемой диссертации, участвовавших в заседании, из 33 человек, входящих в состав совета, проголосовали: за 24, против 0, недействительных бюллетеней 2.

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

«20» марта 2019 г.