ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.199.01, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ САНКТ-ПЕТЕРБУРГСКОГО ИНСТИТУТА ИНФОРМАТИКИ И АВТОМАТИЗАЦИИ РОССИЙСКОЙ АКАДЕМИИ НАУК МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 02.07.2020 г. № 2

О присуждении Ушакову Игорю Александровичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных» по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» принята к защите 27 февраля 2020 г., протокол № 1 диссертационным советом Д 002.199.01 на базе Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, Министерства науки и высшего образования Российской Федерации, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Рособрнадзора номер 2472-618 от 8 октября 2010 года (с изменениями согласно приказам Минобрнауки России №105/нк от 11 апреля 2012 г. №574/нк от 15 октября 2014 г., № 386/нк от 27 апреля 2017 г., №748/нк от 12 июля 2017 г., №301/нк от 23 ноября 2018 г.).

Соискатель Ушаков Игорь Александрович, 1988 года рождения, в 2010 г. с отличием окончил Государственное образовательное учреждение высшего профессионального образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ) по специальности «Защищенные системы связи» (диплом № ВСА 0847253), в 2013 г. окончил очную аспирантуру в той же организации. Справка о сдаче кандидатских экзаменов №56003010/рег №199, выдана в 2019 г. Федеральным государственным бюджетным образовательным учреждением высшего образования «Санкт-

Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича».

В настоящее время Ушаков Игорь Александрович работает младшим научным сотрудником лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук, Министерства науки и высшего образования Российской Федерации и старшим преподавателем кафедры защищенные системы связи федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» Федерального агентства связи.

Диссертация выполнена в лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук Министерства науки и высшего образования РФ.

Научный руководитель – доктор технических наук, профессор КОТЕНКО Игорь Витальевич, основное место работы: Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук, главный научный сотрудник лаборатории проблем компьютерной безопасности.

Официальные оппоненты:

СИНЕЩУК Юрий Иванович, доктор технических наук, профессор, Федеральное государственное казенное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет Министерства внутренних дел Российской Федерации», кафедра специальных информационных технологий, профессор;

ЕФИМОВ Вячеслав Викторович, кандидат технических наук, доцент, акционерное общество «Научно-исследовательский институт «Масштаб», советник генерального директора, начальник научно-системного центра, дали положительные отзывы на диссертацию.

Ведущая организация – акционерное общество «Научно-исследовательский институт «Рубин», г. Санкт-Петербург в своем положительном отзыве, подписанном Шерстюком Юрием Михайловичем, доктором технических наук, доцентом, главным научным сотрудником научно-исследовательского отдела, Олимпиевым Алексеем Александровичем, кандидатом технических наук, инженером отдела РКД, Смирновым Константином Алексеевичем, кандидатом технических наук, начальником научно-исследовательского отдела и утвержденном Степановым Сергеем Степановичем, генеральным директором, указала, что диссертационная работа Ушакова И.А. является законченной научно-квалификационной работой, в которой решена актуальная задача исследования, заключающаяся в разработке модельно-методического аппарата для обнаружения инсайдеров в сети на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных, и имеющая существенное значение для построения устойчивых сетей связи ведомственного назначения.

Соискателем предложены

- модель представления больших данных об инсайдерских атаках в формате NoSQL, обеспечивающая хранение и анализ признаков пользователей в компьютерных сетях в различные моменты времени, отличается возможностью обеспечения хранения и анализа признаков пользователей, полученных на базе UBA/UEBA-аналитики и характеризующих потенциальную инсайдерскую деятельность в компьютерных сетях, а также возможностью учета динамики изменения этих признаков;
- модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак отличаются применением комплексного подхода к решению задачи обнаружения инсайдеров с учетом признаков и свойств пользователей, устройств, приложений, сервисов, включая параметр времени;
- методика обнаружения инсайдеров в компьютерных сетях с использованием комбинированных экспертных правил, методов машинного обучения и обработки больших данных отличается использованием предложенной модели представления больших данных об инсайдерских атаках, а также предложенных модели и алгоритмов комбинированного применения

экспертных правил, методов машинного обучения и обработки больших данных;

- архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных отличаются использованием предложенной методики обнаружения инсайдеров, обеспечивающей комбинированное применение технологий обработки больших данных, экспертных правил и методов машинного обучения.

Отличительной особенностью разработанных автором предложений является строго аргументированное обоснование системотехнических решений, направленных на повышение информационной безопасности компьютерных сетей. Достоверность полученных научных результатов подтверждается наличием ряда свидетельств о регистрации программ для ЭВМ.

Полученные соискателем результаты целесообразно использовать в специальных службах органов внутренних дел, осуществляющих специальные технические мероприятия по противодействию преступлениям в сфере инфотелекоммуникаций (например, Управление специальными техническими мероприятиями ГУВД г. Санкт-Петербург), а также подразделениях защиты от иностранных технических разведок предприятий оборонно-промышленного комплекса Санкт-Петербурга (например, АО «НИИ «Рубин», АО «НИИ «Масштаб», ПАО «Интелтех», АО «НИИ «Вектор» и др.).

Текст автореферата соответствует содержанию диссертации. Содержание диссертации соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». В целом диссертационная работа соответствует требованиям п.п. 9, 10, 11 и 14 “Положения о присуждении ученых степеней” и предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук.

Соискатель имеет 69 опубликованных работ, в том числе по теме диссертации 40 работ, опубликованных в рецензируемых научных изданиях 40 работ, из них опубликованных в изданиях, рекомендуемых ВАК – 9, индексируемых в WoS/Scopus – 2, имеется 3 свидетельства о государственной регистрации программы для ЭВМ.

Основные научные результаты опубликованы в 40 научных трудах общим объемом 16,44 п.л., из которых объем личного вклада соискателя составляет 6,58 п.л.

Наиболее значимые работы по теме диссертации:

1. **Ушаков, И.А.** Обнаружение инсайдеров в корпоративной компьютерной сети на основе технологий обработки больших данных. / И.А. Ушаков // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2019. – № 4. – С. 38-43.
2. **Ушаков, И.А.** Гибридная модель базы данных NoSQL для анализа сетевого трафика. / И.В. Котенко, И.А. Ушаков, Д.В. Пелёвин, А.Ю. Овраменко // Защита информации. Инсайд. – 2019. – № 1 (85). – С. 46-54. *Личный вклад соискателя – 55%.*
3. **Ушаков, И.А.** Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack / И.В. Котенко, А.А. Кулешов, И.А. Ушаков // Труды СПИИРАН. – 2017. – № 5 (54). – С. 5-34. *Личный вклад соискателя – 65%.*
4. **Ушаков, И.А.** Технологии больших данных для мониторинга компьютерной безопасности / И.В. Котенко, И.А. Ушаков // Защита информации. Инсайд. – 2017. – № 3 (75) – С. 23-33. *Личный вклад соискателя – 65%.*
5. **Ушаков, И.А.** Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA / И.В. Котенко, И.А. Ушаков, Пелевин Д.В., Преображенский А.И., Овраменко А.Ю. // Защита информации. Инсайд. – 2019. – № 5 (89). – С. 2-11. *Личный вклад соискателя – 55%.*
6. **Ushakov, I.** Aggregation of Elastic Stack Instruments for Collecting, Storing and Processing of Security Information and Events / I. Kotenko, A. Kuleshov, I. Ushakov // 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) 2017. – Pp. 1-8. *Личный вклад соискателя – 65%.*

Оригинальность содержания диссертации составляет не менее 89% от общего объёма текста; цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник

заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На автореферат диссертации поступило 6 отзывов, все отзывы положительны:

1) Управление федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Северо-Западному федеральному округу. Отзыв составили заместитель руководителя Управления Роскомнадзора по СЗФО, к.ф-м.н. Потехин И.Ю., заместитель руководителя Управления Роскомнадзора по СЗФО Парсон И.М., помощник руководителя Управления Роскомнадзора по СЗФО к.филос.н. Скакун А.А. Замечания: в автореферате автор использует размытые понятия «инсайдер» и «компьютерная сеть», не давая четких определения данных терминов; второй основной научный результат состоит из множества – модель и алгоритмы; возможно, имело бы смысл или дать иное название (комплекс алгоритмов на базе модели), или разбить их на несколько (модель и комплекс алгоритмов); не приводится анализ влияния количества исследуемых записей на результаты. Не ясен критерий выбора количества в 100 тыс. записей; в Таблице 1 используются буквенные обозначения «мер» без их расшифровки.

2) Акционерное общество «Лаборатория противодействия промышленному шпионажу». Отзыв составил заместитель генерального директора по научной работе АО «Лаборатория ППШ» к.т.н., доцент Лысов А.В. Замечания: в автореферате модель инсайдера раскрыта на концептуальном уровне, в частности не понятны критерии определения атрибутов инсайдера, уровни доступа, квалификация инсайдера, цель инсайдера; согласно рисунку 4 – сбор информации осуществляется с серверов AAA, AD, DNS, DHCP однако, в автореферате не указывается, каким образом осуществляется сбор информации и с использованием каких протоколов, а также не указывается – используются ли при этом протоколы Syslog, SNMP и Netflow/SFlow; не раскрыто понятие кибербезопасности применительно к тематике исследования.

3) Управление ФСТЭК России по Северо-Западному федеральному округу. Отзыв составил заместитель руководителя Управления ФСТЭК России по СЗФО к.воен.н., доцент Шакин Д.Н. Замечания: представленный текст автореферата не дает полного представления об архитектуре предлагаемой автором системы обнаружения инсайдеров в компьютерных сетях, что позволяет лишь на концептуальном уровне иметь суждения об организации системы, а также принципах ее проектирования и эволюции;. из текста автореферата (с.13) неясно какие существенные признаки использованы автором при определении понятия «атака инсайдеров» и его соотношение с другими понятиями специфической предметной области, например, «компьютерная атака», или «компьютерный инцидент».

4) ООО «Ниеншанц-защита». Отзыв составил начальник производственно-технического отдела, к.т.н. Мурашов С.В. Замечания: из автореферата не понятна роль применяемого MapReduce алгоритма во втором этапе разработанной методики; не ясно отличие используемых терминов «инсайдер КС» и «внутренний нарушитель КС»; на рисунке 1 на блок-схеме определения аномалий в качестве проверки используется критерий «нестандартное устройство», однако отсутствует описание методики классификации устройств на стандартные и нестандартные.

5) УФСБ России по г. Санкт-Петербургу и Ленинградской области. Отзыв составил сотрудник УФСБ России по г. СПб и ЛО к.т.н., доцент Башмаков А.В. Замечания: в автореферате в качестве типовых сценариев атак инсайдеров были выбраны семь сценариев, однако автор не поясняет о причинах выбора именно этих сценариев, а также не аргументирует выбор именно такого количества сценариев; не до конца понятна роль обработки больших данных во втором научном результате – «Модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак»; на рисунке 2 не указаны буквенные обозначения изображенных сущностей (I_0, I_{RB}, I_{ML}).

6) Акционерное общество «Эврика». Отзыв составил советник генерального директора АО «Эврика» д.т.н., доцент Суханов А.В. Замечания: в автореферате при описании алгоритма, основанного на экспертных правилах указано, что правила

создаются экспертами с учетом собственного накопленного опыта и существующих «лучших практик». Однако, непонятно какой квалификацией должны обладать эксперты и по какому принципу они выбирались; в тексте автореферата не раскрыты атрибуты пользователей, входящих в кортеж $Users_i$.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., профессор Синещук Ю.И. является известным ученым в области автоматизированных систем управления и безопасности информационных систем; к.т.н., доцент Ефимов В.В. – известный специалист в области защиты информационно-вычислительных систем; ведущая организация, акционерное общество «Научно-исследовательский институт «Рубин», является известной как в России, так и за рубежом организацией в области разработки, внедрения и эксплуатации современных защищенных сетей связи и автоматизации, а ее сотрудники являются признанными специалистами в области обеспечения защиты компьютерных сетей.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны:

- оригинальная методика обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных, которая отличается от существующих использованием предложенных моделей, алгоритмов комбинированного применения экспертных правил, методов машинного обучения и обработки больших данных;
- архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных, которая отличается от известных архитектур и программных средств использованием предложенной методики обнаружения инсайдеров, обеспечивающей комбинированное применение технологий обработки больших данных, экспертных правил и методов машинного обучения.

предложены:

модель представления больших данных об инсайдерских атаках в формате NoSQL, обеспечивающая хранение и анализ признаков пользователей в компьютерных сетях в различные моменты времени, которая отличается от существующих возможностью обеспечения хранения и анализа признаков пользователей, полученных на базе UBA/UEBA-аналитики и характеризующих потенциальную инсайдерскую деятельность в компьютерных сетях, а также возможностью учета динамики изменения этих признаков;

модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак, которые отличаются от существующих применением комплексного подхода к решению задачи обнаружения инсайдеров с учетом признаков и свойств пользователей, устройств, приложений, сервисов, включая параметр времени.

экспериментально **доказана** перспективность использования предложенного подхода и методики на его основе для решения задачи обнаружения инсайдеров в компьютерных сетях.

введены:

- новые классификации атрибутов, необходимые для обнаружения инсайдеров;
- требования к программно-аппаратному обеспечению, необходимому для установки и корректного функционирования разработанной системы обнаружения инсайдеров в компьютерных сетях.

Теоретическая значимость исследования обоснована тем, что:

сформулированные в работе теоретические утверждения **доказаны** на основе результатов проведенных экспериментов с использованием разработанного программного прототипа, реализующего предложенные модели, алгоритмы и методику. Эти утверждения составляют основу разработанной методики обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных.

применительно к проблематике диссертации результативно использованы теория вероятностей, теория множеств, функциональный и структурный синтез;

изложены методологические и методические основы использования аналитического моделирования для задачи обнаружения инсайдеров в компьютерных сетях;

раскрыты основные проблемы применения существующих методов обнаружения инсайдеров в компьютерных сетях;

изучены существующие модели, алгоритмы и методики для обнаружения инсайдеров в компьютерных сетях, предложенные различными исследователями, при этом отдельное внимание уделено рассмотрению вопросов их применения в рамках систем мониторинга безопасности и управления инцидентами;

проведена модернизация существующих методов, методик и алгоритмов обнаружения инсайдеров в компьютерных сетях.

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

разработаны и внедрены следующие результаты диссертационной работы:

- модель представления больших данных об инсайдерских атаках в формате NoSQL, обеспечивающая хранение и анализ признаков пользователей в компьютерных сетях в различные моменты времени;
- модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак;
- методика обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных;
- архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных

внедрены в учебный процесс на кафедре «Защищенные системы связи» СПбГУТ при подготовке специалистов по направлению подготовки 10.03.01

«Информационная безопасность»; использованы при разработке мероприятий по технической защите информации в распределенной информационно-вычислительной сети Управления Роскомнадзора по СЗФО; использованы в рамках рабочего процесса при организации безопасности компьютерной сети организации ООО «Фаст Лейн»; использованы в рамках ФЦП 2019-2020 гг. в соответствии с соглашением № 05.607.21.0322 (идентификатор RFMEFI60719X0322) с Минобрнауки России по теме: «Разработка методов, моделей, алгоритмов и программных средств, основанных на выявлении отклонений в эвристиках трафика сверхвысоких объемов, для обнаружения сетевых атак и защиты от них»;

- методика обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных;
- архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных

внедрены в учебный процесс на кафедре «Интеллектуальных систем и защиты информации» СПбГУПТД при подготовке специалистов по направлению подготовки 10.03.01 «Информационная безопасность»;

определены возможности и перспективы практического использования полученных результатов диссертации при разработке систем обнаружения аномалий в компьютерных сетях;

создана система обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных;

представлены предложения и направления для дальнейших научных исследований, в основу которых могут быть положены разработанные модели, алгоритмы и методика.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ достоверность полученных результатов подтверждена проведением предварительного анализа существующих

исследований в данной предметной области, корректным применением научно-методического аппарата, апробацией основных результатов диссертации в печатных трудах и докладах на международных и всероссийских конференциях, положительными результатами экспериментальных исследований алгоритмов, моделей и методики и сравнительного анализа предложенной методики с существующими аналогами;

теория построена на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методов исследования, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области обнаружения инсайдеров в компьютерных сетях;

использованы полученные характеристики для сравнения с данными, приведенными в современной научной литературе по обнаружению инсайдеров в компьютерных сетях;

установлено качественное и количественное соответствие результатов решения задачи разработки модельно-методического аппарата для обнаружения инсайдеров в сети на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных, при этом подтверждены преимущества предложенного подхода перед результатами, полученными другими авторами;

использованы современные методики, обеспечивающие сбор и обработку исходной информации о пользователях больших объемов, характеризующей потенциальную инсайдерскую деятельность в компьютерных сетях.

Личный вклад соискателя состоит в:

- анализе современного состояния дел в области обнаружения инсайдеров в компьютерных сетях (КС);
- исследовании и классификации существующих подходов к обнаружению инсайдеров в компьютерных сетях, моделей, методик и алгоритмов обнаружения инсайдеров в КС на основе методов машинного обучения и обработки больших данных;

- постановке задачи разработки методики обнаружения инсайдеров в КС с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных;
- разработке модели представления больших данных об инсайдерских атаках в формате NoSQL (включая модель инсайдера);
- разработке алгоритма обнаружения инсайдеров в КС, основанного на экспертных правилах;
- разработке модели и алгоритмов комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак;
- разработке методики обнаружения инсайдеров в КС с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных;
- построении архитектуры и реализации программного комплекса системы обнаружения инсайдеров в КС на базе предложенной методики;
- экспериментальной оценке предложенных моделей, алгоритмов и методики, и сравнении их с существующими аналогами.
- подготовке основных публикаций по выполненной работе.

Диссертационный совет считает, что в соответствии с требованиями п. 9 «Положения о присуждении ученых степеней», предъявляемыми к кандидатским диссертациям, и пп. 1, 2, 4, 7 и 9 паспорта научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность, Ушаков И.А. в своей диссертационной работе решил научную задачу разработки модельно-методического аппарата для обнаружения инсайдеров в сети на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных, имеющую важное значение для развития теории и практики обеспечения информационной безопасности компьютерной сети организации.

На заседании 02.07.2020 г. диссертационный совет принял решение присудить Ушакову И.А. ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 20 человек, из них 4 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 26 человек, входящих в состав совета, проголосовали: за 20, против нет, недействительных бюллетеней нет.

Председатель диссертационного совета
доктор техниче
член-корреспо Юсупов Рафаэль Мидхатович

Ученый секретарь диссертационного совета
кандидат техн Зайцева Александра Алексеевна

02.07.2020 г.