ЗАКЛЮЧЕНИЕ ОБЪЕДИНЕННОГО ДИССЕРТАЦИОННОГО СОВЕТА 99.2.038.03, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «БАЛТИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ «ВОЕНМЕХ» ИМ. Д.Ф. УСТИНОВА» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» МИНИСТЕРСТВА ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА ТЕХНИЧЕСКИХ НАУК

аттестационное дело № _____

решение диссертационного совета от 21 декабря 2022 г. № 12

О присуждении Пестову Игорю Евгеньевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методика автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры с использованием безагентного метода сбора метрик» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 19 октября 2022 года, протокол № 9 объединенным диссертационным советом 99.2.038.03, созданным на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова» Министерства науки и высшего образования Российской Федерации, Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения» Министерства науки и высшего образования Российской Федерации, Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, 191186, Санкт-Петербург, наб. реки Мойки, д. 61, приказ № 44/нк от 30 января 2017 года.

Соискатель Пестов Игорь Евгеньевич, 31 марта 1992 года рождения, работает старшим преподавателем в Федеральном государственном бюджетном образовательном учреждении высшего образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича", Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. В 2020 году окончил освоение программы подготовки научных и научно-педагогических кадров в аспирантуре Федерального государственного бюджетного образовательного учреждения высшего образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича".

Диссертация выполнена на кафедре защищенных систем связи Федерального государственного бюджетного образовательного учреждения высшего образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича", Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

Научный руководитель – кандидат технических наук, Красов Андрей Владимирович, основное место работы: Федерального государственного бюджетного образовательного учреждения высшего образования "Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича", кафедра защищенных систем связи, заведующий кафедрой.

Оппоненты: 1. Беззатеев Сергей Валентинович, доктор технических наук, доцент, основное место работы: Санкт-Петербургский государственный университет аэрокосмического приборостроени, кафедра информационной безопасности, заведующий кафедрой; 2. Павленко Евгений Юрьевич, кандидат технических наук, доцент, основное место работы: Санкт-Петербургский политехнический университет Петра Великого, институт кибербезопасности и защиты информации, доцент, дали положительные отзывы о диссертации.

Ведущая организация Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», г. Санкт-Петербург, в своем положительном заключении, подписанном Саенко Игорем Борисовичем, доктором технических наук, профессором, ведущим научным сотрудником; Новиковой Евгенией Сергеевной, кандидатом технических наук, доцентом, старшим научным сотрудником лаборатории проблем компьютерной безопасности, утвержденном Кулешовым Сергеем Викторовичем, доктором технических наук, заместителем директора СПб ФИЦ РАН по научной работе, указала, что диссертационная работа соответствует критериям, предъявляемым в отношении кандидатских диссертаций, которые установлены пунктами 9-14 «Положения присуждении ученых степеней», утвержденным постановлением Правительства Российской Федерации от 24.09.2013 г. № 842. Автор Пестов Игорь Евгеньевич заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 25 опубликованных работ, в том числе по теме диссертации 15, из них в рецензируемых научных изданиях, рекомендованных ВАК, – 5, в том числе 4 по искомой специальности, а также: 2 работы в изданиях, индексируемых в международных базах цитирования; 3 результата интеллектуальной деятельности; 5 статей в других научных журналах, сборниках научных статей, трудов и материалах конференций. Из них 2 работы опубликованы соискателем без соавторства. Общий объём авторского вклада в работы (без результатов интеллектуальной собственности) составляет 2,88 печ.л. из общего количества 8,38 печ.л. Диссертация не содержит недостоверных сведений об опубликованных соискателем ученой степени работах.

Наиболее значительные научные работы по теме диссертации.

Публикации в рецензируемых научных изданиях, рекомендованных ВАК:

1. Пестов И.Е., Шемякин С.Н., Ильин М.В., Рудченко Н.А. Теоретическая оценка использования математических методов прогнозирования загрузки ресурсов элементов виртуальной инфраструктуры OpenStack. // Научно

аналитический журнал «Наукоемкие технологии в космических исследованиях Земли». – 2021. – Том 13, № 4. – С. 66-75.

2. Пестов И.Е., Шемякин С. Н. Федоров П.О., Кошелева С.А., Использование теории графов для моделирования безопасности облачных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2021. – № 2. – С. 31-35.

3. Пестов И.Е. Методика разработки управляющего воздействия на инстансы облачной инфраструктуры. // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 4. – С. 72-76.

4. Пестов И. Е., Фёдоров П.О. Кошелева С.А. Алехин Р.В. Метод передачи метрик загруженности инстансов облачной инфраструктуры в кластер обработки средствами и методами больших данных для защиты информации и обеспечения информационной безопасности // I-METHODS – 2022. Т. 14. № 1. С. 1-14.

Публикации в изданиях, индексируемых в МБЦ:

5. Pestov I., Krasov A., Vitkova L. Behavioral analysis of resource allocation systems in cloud infrastructure // 2019 International Russian Automation Conference (RusAutoCon). – IEEE, 2019. – С. 1-5.

Результаты интеллектуальной деятельности:

6. Свидетельство 2020619716. «Программное обеспечение для сбора данных метрик и выявлений аномалий облачной инфраструктуры open stack»: программа для ЭВМ / И.Е. Пестов, А.В. Красов, Д.В. Рыжаков Г.А. Орлов (RU); правообладатель СПбГУТ. № 2020618952; заявл. 10.08.2020; опубл. 21.08.2020.

7. Свидетельство 2022660102. «Программа по выявлению вредоносного управляющего воздействия (атаки) на инстансы облачной инфраструктуры» программа для ЭВМ / И.Е. Пестов, (RU); правообладатель СПбГУТ. № 2022617589; заявл. 26.05.20222; опубл. 31.05.2022.

Публикации в других изданиях:

8. Пестов И.Е., Кошелева С.А. Атаки на облачную инфраструктуру // Инновационные решения социальных, экономических и технологических проблем современного общества. – 2021. – С. 113-115.

9. Пестов И.Е., Сахаров Д.В., Сергеева И.Ю., Чернобородов И.С. Выявление угроз безопасности информационных систем // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). – 2017. – С. 525-527.

На диссертацию и автореферат поступили отзывы: официального оппонента Беззатеева С.В.; официального оппонента Павленко Е.Ю.; ведущей организации СПб ФИЦ РАН; Шакина Д.Н., к.в.н., доц., заместителя руководителя управления ФСТЭК России по СЗФО; Потехина И.Ю., к.ф.-м.н., заместителя руководителя управление Роскомнадзора по СЗФО; Соколова С.С., д.т.н., доц., заведующего кафедрой комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова; Корниенко А.А., д.т.н., проф., профессора кафедры информатика и информационная безопасность Петербургского государственного университета путей сообщения Императора Александра I; Бурлова В.Г., д.т.н., проф., и.о. заведующего кафедрой информационных технологий и систем безопасности Российского государственного гидрометеорологического университета; Билятдинова К.З., к.в.н., доц., доцента факультета инфокоммуникационных технологий, Национального исследовательского университета ИТМО; Киселева О.Н., к.т.н., доц., доцента кафедры информационных технологий и организации расследования киберпреступлений Санкт-Петербургской академии следственного комитета Российской Федерации; Душина С.Е., д.т.н., проф., профессора кафедры автоматики и процессов управления Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина).

Все отзывы положительные, но имеются критические замечания. В автореферате недостаточно полно рассмотрены релевантные работы зарубежных ученых; в автореферате не в полной мере отражено описание методики проведения экспериментов по выявлению несанкционированных управляющих

воздействий; приводится краткий обзор отзывов, с обязательным отображением содержащихся в них критических замечаний; отсутствуют структурные схемы облачной инфраструктуры, на которой проводились эксперименты, а элементы представлены лишь кратким описанием; отсутствуют описание работы программных продуктов используемых при экспериментальной проверке методик; автореферат не отражает затрачиваемые вычислительные ресурсы, при реализации предложенных методов и методики, не указаны количественные характеристики уменьшения временных затрат на выработку и применение управляющего воздействия для противодействия атаке злоумышленника; в автореферате не обосновывается взаимосвязь между наличием вредоносного воздействия и показателями CPU, RAM, Storage, Network (формула (2) автореферата), лежащими в основе метрик, используемых в предлагаемом методе; автор в качестве научной новизны второго научного результата (пункт 4 стр. 5 автореферата) указывает на отсутствие пороговых критериев в предлагаемой методике, тогда как при анализе результатов на рисунках 1 и 2 использует пороговые значения; в автореферате явно не указываются управляющие воздействия, применяемые при проведении экспериментов, при анализе эффективности методики типизированной рефлексии на вредоносные управляющие воздействия; автореферат не содержит подробного описания процесса создания модели нормального поведения инстанса, при оценке эффективности методики выявления вредоносного управляющего воздействия; из текста автореферата не ясно какая именно модель угроз безопасности информации использовалась в диссертационном исследовании и применялся ли автором методический документ ФСТЭК России «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 5 февраля 2021 года; автореферат поверхностно отражает анализ релевантных работ в области обеспечения информационной безопасности облачных инфраструктур и инстансов; в автореферате не в полной мере раскрыт принцип выбора типовых управляющих воздействий в рамках описания третьего научного результата; в описании методики автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры не

включены типовые контрмеры; в автореферате отсутствуют примеры графа состояния при различных несанкционированных воздействиях.

Выбор оппонентов и ведущей организации обосновывается тем, что д.т.н., доцент, Беззатеев С.В. является автором весомых работ, посвященных разработке методов и подходов к обеспечению информационной безопасности. К.т.н., Павленко Е.Ю. провел ряд исследований по оценке устойчивости киберфизических систем на основе теории графов, а также анализом информационной безопасности цифрового производства. СПб ФИЦ РАН, в частности лаборатория проблем компьютерной безопасности, занимается исследованиями в области кибербезопасности, разработке моделей и методов противодействия компьютерным атакам, управлением политиками безопасности, обнаружением компьютерных атак, многоагентными системами, мягкими и эволюционными вычислениями, машинным обучением, интеллектуальными системами поддержки принятия решений, а также методами оценки эффективности систем защиты информации. СПб ФИЦ РАН внес значительный вклад в создание подходов к обеспечению информационной безопасности, в частности силами таких ученых, как Котенко И.В., Саенко И.Б., Юсупова Р.М., Кулешова С.В., Молдовяна Н.А., Молдовяна А.А. и т.д.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований: разработаны метод сбора метрик инстансов облачной инфраструктуры, для оценки состояния информационной безопасности, позволяющий сократить время сбора и первичной обработки метрик виртуальных машин и контейнеров облачной инфраструктуры; методика выявления вредоносного управляющего воздействия (атаки) на виртуальные машины и контейнеры облачной инфраструктуры, позволяющая автоматизированно учитывать экзогенные параметры; **предложена** методика типизированного автоматизированного противодействия на вредоносные управляющие воздействия в отличии от известных комплексной оценкой состояния виртуальных машин и контейнеров; анализируется набор метрик MCPU, MRAM, MStorage, MNetwork, позволяющий полностью описать состояние инстанса; **доказана** возможность и целесообразность использования безагентного метода

сбора метрик виртуальных машин и контейнеров облачной инфраструктуры; **введена** система критериев автоматизированного противодействия открытого типа на вредоносные управляющие воздействия на виртуальные машины и контейнеры облачной инфраструктуры.

Теоретическая значимость исследования обоснована тем, что: доказана возможность и целесообразность использование безагентного метода сбора метрик инстансов облачной инфраструктуры, также расширен класс методов динамического моделирования в части моделирования нормального поведения виртуальных машин и контейнеров облачной инфраструктуры; **применительно к проблематике диссертации результативно использованы** методы обработки больших данных, теории вероятности и математической статистики, бинартных классификаций и сравнительного анализа; **изложены** теоретические и экспериментальные доказательства возможности и целесообразности использования безагентного метода сбора метрик инстансов облачной инфраструктуры, системы критериев автоматизированного противодействия открытого типа на вредоносные управляющие воздействия.; **раскрыты** проблемы при построении модели нормального поведения виртуальной машины, контейнера облачной инфраструктуры; **изучены** связи метрик вычислительных ресурсов виртуальных машин или контейнеров облачной инфраструктуры с вредоносными управляющими воздействиями; **проведена модернизация** класса методов динамического моделирования в части моделирования нормального поведения инстансов облачной инфраструктуры.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что: разработаны и внедрены – метод сбора метрик инстансов облачной инфраструктуры, для оценки состояния информационной безопасности (ИБ), методика выявления вредоносного управляющего воздействия (атаки) на инстансы облачной инфраструктуры, методика типизированной автоматизированного противодействия на вредоносные управляющие воздействия, использованы в ГК ПАО "Ростелеком", для предупреждения и предотвращения угроз информационной безопасности инфраструктуры ПАО "Ростелеком", также использованы ГАУ КО КГ НИЦ в

мероприятиях по выработке перспективных подходов к защите информационно-телекоммуникационной сети Правительства Калининградской области. Разработана программа для ЭВМ «Программное обеспечение для сбора данных метрик и выявлений аномалий облачной инфраструктуры Open Stack», реализующая метод безагентного сбора метрик загруженности виртуальных машин и контейнеров. Разработана программа для ЭВМ «Программа по выявлению вредоносного управляющего воздействия (атаки) на инстансы облачной инфраструктуры», реализующая методику выявления вредоносного управляющего воздействия на инстансы облачной инфраструктуры. Результаты работы были внедрены в учебный процесс СПбГУТ на старших курсах обучения бакалавров по направлению подготовки 10.03.01 «Информационная безопасность» по дисциплинам «Защита операционных систем», «Защита информации в центрах обработки данных» при чтении курсов лекций, проведении практических занятий и лабораторных работ; **определены** перспективы практического использования результатов диссертационного исследования при обеспечинии информационной безопасности виртуальных машин и контейнеров облачной инфраструктуры; **создана** научно-обоснованая методика типизированного автоматизированного противодействия на вредоносные управляющие воздействия, направленные на нарушения конфеденциальности, целостности, доступности виртуальных машин и контейнеров облачной инфраструктуры; **представлены** рекомендации для дальнейших научных исследований по теме диссертационного исследования.

Оценка достоверности результатов исследования выявила: для экспериментальных работ показана воспроизводимость результатов исследования при работе различного программного обеспечения, в том числе разработанного автором, на сформированных наборах данных российских базах данных, произведена верификация математических рассчетов, результаты расчетов применены в реальных условиях эксплутации виртуальных машин и контейнеров облачной инфраструктуры; **теория** построена на известных, проверяемых данных, в т.ч. для предельных случаев, согласуется с опубликованными экспериментальными данными по теме диссертации; **идея**

базируется на анализе российских и международных лучших практик, стандартов и методических документов в области обеспечения информационной безопасности; **использованы** сравнение авторских данных, полученных по результатам диссертационного иссследования и данных, полученных ранее по определению угроз информационной безопасности виртикальных машин и контейнеров облачной инфраструктуры; **установлено** качественное и количественное совпадение результатов математического моделирования и результатов инструментальных расчетов; **использованы** современные методики сбора и обработки информации с применением технологий Data Science, современные методы моделирования систем и средства разработки программного обеспечения.

Личный вклад соискателя состоит в том, что все основные результаты диссертационного исследования получены автором лично, а именно: проведен анализ известных методов и методик обеспечения иформационной безопсности виртуальых машин и контейнеров облачных инфраструктур. Автор принимал активное участие в формировании наборов данных и формировании экспертных оценок для предложенных методики и метода. Автором определены необходимые и достаточные показатели определения вредоносного воздействия на инстансы облачной инфраструктуры, осуществлял проведение экспериментов и обработку их результатов, разработал алгоритмы работы программ для ЭВМ, реализующие предложенные методы и методики. Автором были внедрены результаты работы в учебный процесс СПбГУТ. Подготовка публикаций по результатам диссертационного исследования выполнялась автором лично или при его значительном участии.

В ходе защиты диссертации было высказано критическое замечание об использовании общепринятых оценок для валидации разработанного метода.

Соискатель Пестов И.Е. в ходе заседания ответил на задаваемые ему вопросы и привел собственную аргументацию, а также согласился с замечаниями.

Диссертационный совет установил, что диссертация «Методика автоматизированного противодействия несанкционированным воздействиям на инстансы облачной инфраструктуры с использованием безагентного метода сбора

метрик» является законченной научно-квалификационной работой и соответствует требованиям п. 9 Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а также пунктам 15, 5, 6 паспорта научной специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

На заседании 21 декабря 2022 года объединенный диссертационный совет принял решение присудить Пестову И.Е. ученую степень кандидата технических наук за решение научной задачи по созданию новых и повышению эффективности существующих средств противодействия угрозам виртуальных машин и контейнеров облачной инфраструктуры, предложив методику выявления вредоносного управляющего воздействия, а также методику типизированного автоматизированного противодействия, имеющей важное значение для развития науки и страны в период цифровой трансформации.

При проведении тайного голосования объединенный диссертационный совет в количестве 17 человек, из них 4 докторов наук по научной специальности рассматриваемой диссертации, участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за – 17, против – нет, недействительных бюллетеней – нет.

И.о. председателя диссертационного совета,
доктор технических наук, профессор [redacted] Бабук Валерий Александрович

Ученый секретарь диссертационного совета,
кандидат технических наук, доцент [redacted] Владыко Андрей Геннадьевич

23 декабря 2022 года