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 01 декабря 2021 г. № 9

О присуждении Жуку Роману Владимировичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Методика и алгоритмы определения актуальных угроз информационной безопасности в информационных системах персональных данных» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 29 сентября 2021 года, протокол № 8 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 Жук Роман Владимирович, 03.10.1990 года рождения, работает начальником отдела информационной безопасности Краснодарского регионального производственного управления в Филиале "Макрорегион Юг" ООО ИК "Сибинтек".

В 2012 году соискатель окончил Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Кубанский государственный технологический университет". С 01.11.2012 по 31.10.2016 являлся аспирантом Федерального государственного бюджетного образовательного учреждения высшего образования "Кубанский государственный технологический университет", Министерство науки и высшего образования Российской Федерации.

Диссертация выполнена на кафедре компьютерных технологий и информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования "Кубанский государственный технологический университет", Министерство науки и высшего образования Российской Федерации.

Научный руководитель – кандидат технических наук, Власенко Александра Владимировна, основное место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования "Кубанский государственный технологический университет", кафедра компьютерных технологий и информационной безопасности, заведующий кафедрой.

Оппоненты: 1. Ажмухамедов Искандар Маратович, доктор технических наук, профессор, основное место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Астраханский государственный университет», факультет цифровых технологий и кибербезопасности, декан; 2. Аникин Игорь Вячеславович, доктор технических наук, профессор, основное место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ», кафедра систем информационной безопасности, заведующий кафедрой,

дали положительные отзывы о диссертации.

Ведущая организация Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва, в своем положительном заключении, подписанном Поликарповым Евгением Сергеевичем, канд. техн. наук, начальником кафедры и Минаевым Владимиром Александровичем, д-ром техн. наук, проф., профессором кафедры специальных информационных технологий учебно-научного комплекса информационных технологий, утвержденном Зиборовым Олегом Валентиновичем, д-ром юрид. наук, доц., первым заместителем начальника университета, указала, что диссертационная работа Жука Романа Владимировича «Методика и алгоритмы определения актуальных угроз информационной безопасности в информационных системах персональных данных» является научно-квалификационной работой, в которой содержится решение задач, связанных с построением взаимосвязи между нарушителем информационной безопасности, активом информационной системы персональных данных и уязвимостью программного обеспечения в процессе определения актуальных угроз информационной безопасности. Диссертация соответствует пп. 9–14 «Положения о присуждении учёных степеней», утверждённого Постановлением Правительства РФ от 24.09.2013 № 842, а её автор, Жук Роман Владимирович, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 12 опубликованных работ, в том числе по теме диссертации 12, из них в рецензируемых научных изданиях, рекомендованных ВАК, – 9, в том числе 9 по искомой специальности, а также: 1 статья в изданиях, индексируемых в международных базах цитирования; 1 результат интеллектуальной деятельности; 1 статья в других научных журналах, сборниках научных статей, трудов и материалах конференций. Из них 1 работа опубликована соискателем без соавторства. Общий объём авторского вклада в работы (без результатов интеллектуальной собственности) составляет 4,34 печ.л.

из общего количества 8,97 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. Жук Р.В., Власенко А.В., Чебанов А.С., Сазонов С.Ю. Методический подход к выбору и разработке моделей оценки эффективности комплексной системы объектов защиты // Известия Юго-Западного государственного университета. – 2012. – № 6 (45). – С. 038-040;

2. Жук Р.В., Власенко А.В., Титенко Е.А. Системы противодействия Инсайдерам //Известия Юго-Западного государственного университета. – 2012. – №6 (45). – С. 30-33;

3. Жук Р.В., Власенко А.В., Титенко Е.А. Классификация информационных систем персональных данных: вчера, сегодня, завтра // Известия Юго-Западного государственного университета. – 2013. – № 1. – С. 87-90,

4. Жук Р.В., Власенко А.В. Модель нарушителя комплексной системы обеспечения информационной безопасности объектов защиты // Известия Юго-Западного государственного университета. – 2013. – № 1. – С. 171-173;

5. Жук Р.В., Власенко А.В., Дзьобан П.И. Защита персональных данных при авторизации пользователя в распределенных информационных системах, построенных на основе Web-технологий// Вестник Адыгейского государственного университета. – 2017. – С. 120-128.

6. Власенко А.В., Дзьобан П.И., Жук Р.В. Обзор инструментов машинного обучения и их применения в области кибербезопасности // Прикаспийский журнал: управление и высокие технологии. – 2020. – С.144-155,

7. Жук Р.В., Дзьобан П.И., Власенко А.В. Построение взаимосвязи между нарушителем информационной безопасности и уязвимостями информационных активов в информационных системах обработки персональных данных // Прикаспийский журнал: управление и высокие технологии. – 2020. – С.162-169.

8. Жук Р.В., Дзьобан П.И., Власенко А.В. Определение актуальности угроз информационной безопасности в информационных системах обработки персональных данных с использованием математического аппарата нейронных

сетей // Прикаспийский журнал: управление и высокие технологии. – 2020. – С.169-178;

9. Жук Р.В. Способ определения потенциала нарушителя безопасности информации и реализуемых им уязвимостей программного обеспечения // Труды учебных заведений связи. – 2021. Т. 7. № 2. – С. 95-101.

Публикации в изданиях, индексируемых в МБЦ:

10. Roman Zhuk, Alexandra Vlasenko Article, Definition of the Method of Determination of the Violator of Information Security in Process of Modeling the Threats of Information Security in the Information Systems of Processing Personal Data // Journal of Engineering and Applied Sciences, №12, 2017, с. 7776-7778.

Результаты интеллектуальной деятельности:

11. Жук Р.В., Власенко А.В. Программа определения степени возможности реализации угрозы информационной безопасности в информационных системах персональных данных // Свидетельство о регистрации государственной программы для ЭВМ 2018613024. Зарегистрировано в реестре баз данных 11.01.2018 г.

Публикации в других изданиях:

12. Жук Р.В., Власенко А.В. Анализ характеристик определения нарушителя при моделировании угроз информационной безопасности в информационных системах персональных данных // Научные труды КубГТУ, № 16, 2016, с 99-104.

На диссертацию и автореферат поступили отзывы: официального оппонента Ажмухамедова И.М.; официального оппонента Аникина И.В.; ведущей организации Московского университета МВД России; Хашировой Т.Ю., д.т.н., проф., заведующего кафедрой компьютерных технологий и информационной безопасности Института информатики Кабардино-Балкарского государственного университета им. Х.М. Бербеков; Алисултановой Э.Д., д.п.н., к.ф.-м.н., проф., директора института прикладных информационных технологий Грозненского государственного нефтяного технического университета имени академика М.Д. Миллионщикова; Давидюк Н.В., к.т.н., доц., заведующего кафедрой информационной безопасности, Астраханского государственного технического университета; Луценко Е.В., д.э.н., к.т.н., проф., профессора кафедры компьютерных технологий и систем Кубанского государственного аграрного

университета имени И.Т. Трубилина; Емельянова В.А., д.т.н., проф., профессора департамента бизнес-информатики факультета информационных технологий и анализа больших данных Финансового университета при Правительстве Российской Федерации; Титенко Е.А., к.т.н., доц., доцента кафедры программной инженерии Юго-Западного государственного университета; Еськова А.В., д.т.н., проф., начальника кафедры информационной безопасности Краснодарского университета Министерства внутренних дел Российской Федерации; Больных А.А., к.т.н., начальника административно-коммерческого управления ООО «ЭКОН Технологии».

Все отзывы положительные, но имеются критические замечания. В тексте диссертации не указано каковы преимущества использования разработанной методики и в чем заключаются существенные отличия от сценарного подхода определения актуальных угроз ИБ. Из текста диссертации не ясно для чего было произведено разбиение на типы актуальных угроз ИБ в ИСПДн. Не достаточно полно описан механизм формирования обучающей выборки для нейронной сети, определяющей актуальность угрозы ИБ. Во введении диссертационной работы не сформулирован перечень задач, решаемых для достижения поставленной цели, что несколько нарушает логическую стройность изложения. Перечень данных задач вынесен в раздел 1.4 диссертации, а также представлен в соответствующем разделе автореферата, однако более логично было бы их привести после формулирования цели диссертационного исследования. Для решения отдельных задач в диссертационной работе (в частности, присвоения потенциала нарушителя ИБ) автором использован метод анализа иерархий (МАИ). Однако, в диссертационной работе не сказано, производилась ли оценка согласованности матриц парных сравнений. При описании МАИ в формуле (2.1) присутствует опечатка, запись должна быть представлена в виде $x_{ji} = 1/x_{ij.}$ Матрицы парных сравнений желательно было бы вынести в приложение диссертационной работы. Необходимо большее внимание уделить вопросу подготовки обучающей выборки для искусственной нейронной сети, представленной в Главе 3, например, оценить насколько обучающая выборка (табл. 49) является репрезентативной. В тексте диссертационной работы отсутствует сравнение сценарного подхода определения актуальных угроз ИБ с авторской методикой и алгоритмами. В первой главе

повествовательный уклон сделан на анализ отечественных методик определения УБИ, международная методическая база в области УБИ раскрыта не полностью. Несмотря на периодическое упоминание в диссертационной работе во второй главе отсутствует перечень нарушителей, предлагаемый для использования в сценарном подходе определения УБИ. Во второй главе необходимо акцентировать внимание на подходе выбора количественной градации потенциала нарушителей ИБ, а также проецирования значений метрик уязвимостей ПО на параметры потенциала нарушителя ИБ. В третьей главе недостаточно внимания уделено подготовке, обучающей и проверочной выборкам ИНС. В четвертой главе отсутствует детальное описание требований к группе экспертов по ИБ, которые были созваны для проведения эксперимента сравнения времени затраченного на подготовку перечня актуальных УБИ с применением разработанной методики и существующих методик моделирования УБИ. Отсутствует сравнение разрабатываемой методики с предлагаемым методическими документами отечественных регуляторов в области защиты информации сценарным подходом определения актуальных угроз информационной безопасности в информационных системах. В автореферате не приведены перечни угроз информационной безопасности, подготовленные с помощью существующих и авторской методики. В автореферате не указан способ классификации активов информационной системы персональных данных. В разделе 2.2 приведены возможности нарушителя информационной безопасности для информационных систем на этапе проектирования, заимствованные из проекта методического документа «Методика определения угроз безопасности информации в информационных системах», однако не приведено объяснение причин, по которым выбраны именно эти параметры, а не статистическая информация о нарушителях предлагаемая для информационных систем на этапах эксплуатации. Из текста диссертации недостаточно понятно каким образом и в каких целях используются типы актуальных угроз информационной безопасности. Не достаточно подробно приведен анализ международной нормативно-методической базы анализа рисков и определения угроз информационной безопасности в информационных системах В автореферате не приведены выборки угроз информационной безопасности, подготовленные с

помощью разработанной методики. Не в полной мере приведено формирование обучающей выборки для аппарата нейронной сети, определяющей актуальность угрозы безопасности информации. Раздел посвященный международной практике оценки рисков написан достаточно сжато, однако менеджмент рисков информационной безопасности широко распространен и регламентирован в иностранных организациях. В разделе 2 приведены продукционные правила для определения актуальных уязвимостей программного обеспечения и актуальных типов угроз безопасности информации, однако, в работе не описана продукционная база знаний. В автореферате не приведены критерии сравнения и унификации перечня нарушителей информационной безопасности. Категорию нарушителя информационной безопасности «недобросовестные партнеры» стоить включить в категорию «Внешние субъекты». Отсутствует перечень источников формирования обучающей выборки нейронной сети. Недостаточно развернуто проведен анализ стандартов определения и оценки информационных активов, а также различных банков уязвимостей программного обеспечения. В разделе 3 не приведено описание источников, принимаемых для обучающей выборки ИНС. Не указано согласно какой градации сопоставлены качественные и количественные значения параметров потенциала нарушителя ИБ. Не приведен этап оценки рисков от реализации угрозы ИБ.

Выбор оппонентов и ведущей организации обосновывается известностью, компетентностью, ведущей ролью и значимой позицией в научных кругах крупнейших специалистов по информационной безопасности, связанных с профилем диссертационной работы, значительным количеством публикаций в рецензируемых изданиях по тематике диссертационного исследования. Официальные оппоненты также известны своими публикациями в области диссертационной работы, д.т.н., профессор, Ажмухамедов И.М. автор ряда работ по анализу защищённости информационных систем и моделирования угроз информационной безопасности, д.т.н., профессор, Аникин И.В. активно занимается исследованиями по тематике определения нарушителей информационной безопасности и оценке рисков информационной безопасности чему посвящены публикации в ведущих научных журналах. Кафедра специальных информационных технологий учебно-научного комплекса

информационных технологий внесла значительный вклад в исследования процессов определения угроз информационной безопасности, в частности, силами таких ученных, как Поликрапов Е.С, Минаев В.А, Цимбал В.Н. Проведено большое количество исследований по определению и оценке уязвимостей программного обеспечения, и выбору нарушителей информационной безопасности применительно к решению прикладных задач.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований: разработаны методика и алгоритмы, позволяющие установить связь между потенциалом нарушителя информационной безопасности и уязвимостями программного обеспечения, а также осуществить выбор актуальных угроз информационной безопасности в информационных системах персональных данных; **предложены** способ присвоения количественной оценки потенциалу нарушителя информационной безопасности в информационных системах персональных данных и способ определения типа актуальных угроз в информационных системах персональных данных; **доказана** перспективность использования разработанных методики и алгоритмов в рамках подготовки перечня актуальных угроз безопасности информации в организция – операторах персональных данных, а также в процессе выбора защитных мер для различных уровней защищенности информационных систем персональных данных; **введены** новая классификация нарушителей информационной безопасности, а также градация количественной оценки потенциала нарушителя информационной безопасности .

Теоретическая значимость исследования обоснована тем, что: доказана эффективность применения продукционных правил для подготовки алгоритмов определения актуальных уязвимостей программного обеспечения и типов актуальных угроз для информационных систем персональных данных, вносящих вклад в расширение представлений о процессе подготовки перечней угроз безопасности информации; **применительно к проблематике диссертации результативно использованы** методы анализа иерархий, экспертных оценок, продукционное моделирование и математический аппарат искуственных нейронных сетей; **изложены** идеи проецирования метрик вектора уязвимости программного обеспечения на возможности нарушителя информационной

безопасности, а также взаимосвязи типа актуальзых угроз при определении уровня защищенности информационной системы персональных данных с метрикой наличия и детализации информации об уязвимости программного обеспечения; **раскрыты** противоречия в существующих методических документах регламентирующих определение актуальных угроз информационной безопасности, выявление проблемы построения взаимосвязи уязвимостей программного обеспечения с нарушителями информационной безопасности и угрозами безопасности информации; противоречия в процессах определения угроз безопасности информации, предлагаемых различными методическими документами, а также способа приминения банка угроз данными методиками; **проведена модернизация** существующего перечня нарушителей информационной безопасности, а также показателей уровня защищенности при определении возможности реализации угрозы информационной безопасности.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что: разработаны и внедрены модели угроз информационной безопасности информационных систем обработки персональных данных на предприятиях топливно-энергетического комлекса: филиал ООО «РН-Учет» в г. Краснодаре, ООО «РН-Краснодарнефтегаз» и ООО «Базовый Авиатопливный Оператор» в г. Краснодар; **определены** перспективы использования предложенной методики и алгоритмов в составе автоматизированных комплексов систем менеджмента информационной безопасности и сканеров уязвимостей; **создана** модель разработанной методики и алгоритмов, позволяющая сократить время на подготовку перечня актуальных угроз информационной безопасности; **представлены** методические рекомендации для последующего сбора обучающей выборки исскуственной нейровнной сети, что позволит сократить вероятность возникновения ошибок при ее функционирвоании.

Оценка достоверности результатов исследования выявила: для экспериментальных работ произведено сравнение временных затрат при использовании разработанных методики и алгоритмов с применением средств их автоматизации с существующими методиками определения угроз информационной безопасности в информационных системах персональных

данных; **теория** базируется на общеизвестных способах оценки уязвимостей программного обеспечения, методиках определения активов и нарушителей информационной безопасности, а также подготовки перечней угроз информационной безопасности; **идея базируется** на анализе методик определения угроз информационной безопасности и менеджмента рисков информационной безопасности и использовании актуальных средств автоматизации процессов, таких как аппарат искусственных нейронных сетей; **использованы** результаты сравнения временных затрат при подготовке перечня актуальных угроз информационной безопасности по разработанной методике с учетом существующих; **установлено** совпадение качественных параметров алгоритмов авторской методики с методиками определения угроз информационной безопасности, представленными в независимых источниках по данной тематике, в части выбора параметров активов и возможностей нарушиетелей информационной безопасности в информационных системах персональных данных; **использованы** современные методики сбора и анализа данных с применением метода анализа иерархий и метода экспертных оценок.

Личный вклад соискателя состоит в разработке способа количественной оценки потенциала нарушителя информационной безопасности, алгоритма выбора уязвимостей программного обеспечения, которые могут быть реализованы нарушителем информационной безопасности с заданным потенциалом, способа определения типа актуальных угроз и алгоритма определения актуальных угроз информационной безопасности в информационных системах персональных данных.

В ходе защиты диссертации были высказаны следующие критические замечания: о возможности создания обучающей выборки данных для информационной системы, используемой в данной работе; о необходимости разделения задач исследования № 4 "Разработка способа выбора типа актуальных УБИ для установления уровня защищенности ИСПДн" и № 5 "Разработка способа определения актуальности УБИ в ИСПДн", а также задан вопрос: в чем специфика и отличие построения систем безопасности для информационных систем с персональными данными от других информационных систем?.

Соискатель Жук Р.В. в ходе заседания: **ответил** на задаваемые ему вопросы и привел собственную аргументацию, что тип актуальных угроз приведен в Постановлении Правительства 1119 при установлении уровня защищенности. И это абстрактное понятие, которое позволяет выбрать уровень защищенности и определить в дальнейшем защитные меры согласно 21-му приказу ФСТЭК. А актуальные угрозы, это те угрозы, которые могут реализоваться в информационной системе выбранным нарушителем за счет существующих уязвимостей. Это немного два разных понятия; **согласился с замечаниями** и привел собственную аргументацию, что в данном случае используется понятие программное обеспечение, которое конкретно занимается обработкой персональных данных, то есть это компьютеры, сервера и так далее, на которых крутится конкретная информация, конкретный тип и вид информации; что экспертным путем на базе данных учреждений, где внедрялись результаты работы подготовил обучающую выборку, но в своей дальнейшей научной работе. Я бы хотел заострить на это внимание и предложить уже в дальнейших статьях механизм, который бы собирал обезличенные данные о моделях угроз, разрабатываемых у операторов, как реестр информационных систем персональных данных у Роскомнадзора. Сделать такой же реестр моделей угроз, но обезличено на базе какого-либо из регуляторов, допустим, того же ФСТЭКа.

Диссертационный совет установил, что диссертация «Методика и алгоритмы определения актуальных угроз информационной безопасности в информационных системах персональных данных» является законченной научно-квалификационной работой и соответствует требованиям п. 9 Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а также пунктам 3 и 7 паспорта научной специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

На заседании 01 декабря 2021 года объединенный диссертационный совет принял решение присудить Жуку Р.В. ученую степень кандидата технических наук за решение научной задачи имеющей значение для отрасли информационной безопасности, а именно сокращение временных затрат на процесс определения актуальных угроз информационной безопасности в информационных систем, а также разработку способа оценки потенциала нарушителя информационной

безопасности для организации взаимосвязи с активами информационной системы персональных данных и уязвимостями программного обеспечения активов.

При проведении тайного голосования объединенный диссертационный совет в количестве 17 человек, из них 5 докторов наук по научной специальности рассматриваемой диссертации, участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за – 15, против – нет, недействительных бюллетеней – 2.

Председатель диссертационного совета,
доктор технических наук, профессор [redacted] Бачевский Сергей Викторович

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

03 декабря 2021 года