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 20 апреля 2022 № 4

О присуждении Козину Ивану Сергеевичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Метод обеспечения безопасности данных при их обработке в блокчейн-системе за счёт применения искусственных нейронных сетей» по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность принята к защите 31 января 2022 года, протокол № 1, 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 Козин Иван Сергеевич, 28 июня 1988 года рождения, работает в должности руководителя группы отдела технических решений департамента информационной безопасности в ООО «Бизкомм», ПАО «Интер РАО».

В 2012 году соискатель окончил Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения». С 2011 по 2014 годы являлся аспирантом Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения».

Диссертация выполнена на кафедре технологий защиты информации Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Министерство науки и высшего образования Российской Федерации.

Научный руководитель – доктор технических наук, Беззатеев Сергей Валентинович, основное место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», кафедра технологий защиты информации, заведующий кафедрой.

Оппоненты: 1. Татарникова Татьяна Михайловна, доктор технических наук, профессор, основное место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)», кафедра информационные системы, профессор кафедры; 2. Полтавцева Мария Анатольевна, доктор технических наук, доцент, основное место работы: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», институт кибербезопасности и защиты информации, доцент, дали положительные отзывы о диссертации.

Ведущая организация Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (СибГУТИ), г. Новосибирск, в своем положительном заключении, подписанном Нечта Иваном Васильевичем, доктором технических наук, доцентом, заведующим кафедрой прикладной математики и кибернетики, утверждённом Хаировым Бари Галимовичем, доктором экономических наук, доцентом, исполняющим обязанности ректора СибГУТИ, указала, что диссертация Козина Ивана Сергеевича «Метод обеспечения безопасности данных при их обработке в блокчейн-системе за счёт применения искусственных нейронных сетей» соответствует критериям, предъявляемым в отношении кандидатских диссертаций, которые установлены пп. 9–14 «Положения о присуждении учёных степеней» (утв. постановлением Правительства Российской Федерации от 24.09.2013 № 842), а её автор Козин Иван Сергеевич заслуживает присуждения ему учёной степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 11 опубликованных работ, в том числе по теме диссертации 11, из них в рецензируемых научных изданиях, рекомендованных ВАК, – 5, в том числе 4 по искомой специальности, а также: 5 статей в других научных журналах, сборниках научных статей, трудов и материалах конференций; 1 отчет о НИР. Из них 6 работ опубликовано соискателем без соавторства. Общий объём авторского вклада в работы (без результатов интеллектуальной собственности) составляет 15,87 печ.л. из общего количества 27,28 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. Козин И.С. Метод обеспечения безопасности персональных данных при их обработке в информационной системе при помощи искусственной нейронной сети // Информатизация и связь. 2021. № 4. С. 54–59.

2. Козин И.С. Метод обеспечения безопасности персональных данных при их обработке в информационной системе на основе анализа поведения пользователей // Информационно-управляющие системы. 2018. № 3. С. 69–78.

3. Козин И.С. Метод разработки автоматизированной системы управления информационной безопасностью распределённой информационной системы // Информация и космос. 2018. № 3. С. 80–88.

4. Козин И.С., Беззатеев С.В. Метод определения опасности угрозы персональным данным при их обработке в информационной системе // Известия СПбГЭТУ «ЛЭТИ». 2017. № 10. С. 19–26.

5. Козин И.С. Метод обеспечения безопасной обработки персональных данных на основе применения технологии блокчейн // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 5. С. 892–900.

Публикации в других изданиях:

6. Козин И.С. Метод защиты персональных данных на основе применения технологии цепочки блоков (блокчейн) // Fourth Conference on Software Engineering and Information Management (SEIM-2019) (Saint-Petersburg, April 13, 2019). P. 10–16.

7. Козин И.С. Метод разработки автоматизированной системы управления информационной безопасностью региональной информационной системы // Сборник трудов «Региональная информатика и информационная безопасность. Выпуск 3» Санкт-Петербург. СПОИСУ. СПб., 2017. С. 283–289.

8. Козин И.С., Рощин А.А. Метод обеспечения безопасности информации при её обработке в информационной системе на основе машинного обучения // Техника средств связи. 2019. № 4 (148). С. 70–82.

9. Козин И.С., Рощин А.А. Метод определения опасности угрозы персональным данным личного состава объекта // Техника средств связи: науч.-техн. сб. СПб.: Изд-во Политех. у-та, 2017. № 6. С. 123–131.

10. Козин И.С., Рощин А.А. Метод построения модели угроз критически важной информации военного назначения // Техника средств связи: науч.-техн. сб. СПб.: Изд-во Политех. у-та, 2016. № 5. С. 98–103.

На диссертацию и автореферат поступили отзывы: официального оппонента Татарниковой Т.М.; официального оппонента Полтавцевой М.А.; ведущей организации СибГУТИ; Архипова С.Н., к.т.н., доц., начальника отдела по управлению проектами, Травкина В.С., к.т.н., учёного секретаря НТС, Борисенко Н.П., к.т.н., заместителя председателя НТС, Сохена М.Ю., к.т.н. генерального директора АО «РЦЗИ «Форт»; Дементьева В.Е., д.т.н., доц. главного специалиста, Рощина А.А. к.т.н., доц., начальника отдела, Кулешова И.А., д.т.н., доц., заместителя генерального директора ПАО «Интелтех»; Бондаренко А.В. к.в.н., начальника группы испытательной лаборатории АО «Информакустика»; Сарычева Д.Ю., к.т.н., директора департамента е-Навигации АО «СИТРОНИКС КТ»; Дрягина Д.М., к.т.н., генерального директора АО «КТ-Беспилотные системы»; Лукашкова Г.А., к.п.н., доц., доцента кафедры высшей математики ФГБОУ ВО «МГТУГА»; Чернышёва В.А., к.т.н., начальника отдела, Язова Ю.К., д.т.н., профессора, главного научного сотрудника ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Все отзывы положительные. Высказаны следующие критические замечания: тема диссертации сформулирована так, что можно понять так: метод обеспечения безопасности данных при их обработке в блокчейн-системе предлагается за счет применения искусственных нейронных сетей. Кажется, что уместнее было бы употребить «метод … на основе», «метод ... с применением». Безопасность обеспечивается, скорее, благодаря применению искусственных нейронных сетей. Во втором положении, выносимом на защиту, автор предлагает метод обеспечения достоверности данных. Таким образом, возможно, было бы более уместно назвать диссертацию «Метод обеспечения достоверности данных при их обработке в блокчейн-системе …». Поскольку удаление, это частный случай модификации, то при построении таблицы «Уточнённые числовые значения опасности нарушения характеристик безопасности» необходимо было объяснить причину введения последней строки. Не ясно, каким образом предлагаемые механизмы защиты будут реагировать на вновь появившиеся угрозы информационной безопасности? Поскольку множество угроз (атак) не ограничено. Не понятно, какие факторы влияют на ранжирование и вербальную интерпретацию числовых показателей

опасности угроз. Цель работы, записанная в автореферате, состоит в обеспечении достоверности данных при их обработке в блокчейн-системе. Однако автор не ввёл для оценки достоверности персональных данных никакого показателя. Введённый автором коэффициент опасности воздействия, нарушающего «достоверность объекта», оценивается экспертно на основе нечётких суждений, но не является показателем достоверности, а упоминаемые далее «повышенная вероятность ввода недостоверных данных» и «вероятность компрометации персональных данных» никак не поясняются, при этом соотношений для их оценки в автореферате нет. Автором приведены определенные на основе аппарата нечётких множеств значения показателей опасности угроз, однако в работе отсутствуют критерии отнесения угроз к актуальным. Указание на то, что определение актуальности угроз должно осуществляться в порядке, определённом некими «ФОИВ ТЗИ», для диссертации некорректно. Из глав 3-5 неочевидно, для каких именно информационных систем персональных данных, с точки зрения масштаба, применим предложенный метод выявления недостоверных персональных данных при их вводе в блокчейн-систему за счёт искусственной нейронной сети, насколько приемлемыми являются значения ошибок 1-го и 2-го рода. В работе вынесены за рамки решаемых задач процедуры хеширования и шифрования. Однако, они окажут существенное влияние не только на оценку временных показателей, но и на организацию и условия эксплуатации предлагаемых элементов подсистемы защиты информации, а также на работу информационной системы в целом. В автореферате не представлены конкретные недостатки известных моделей, методов и методик защиты данных, применительно к блокчейн-системами и обрабатываемым в них данным. При описании выбранных нейронных сетей (главы 3 и 4) не приведено обоснование выбора конкретных архитектур нейронных сетей. В качестве нейронных сетей, предназначенных для выявления недостоверных данных (стр. 65) и аномалий в поведении пользователей (стр. 94), представляется более целесообразным применение автокодировщиков (AE, VAE). Нейронная сеть в работе – это основной инструмент обеспечения безопасности данных, сеть обучается по технологии обучения с учителем. В работе пишется о выборке обучения, о ее большой размерности, но не говорится о том, как получена

обучающая выбора: самостоятельно на макете, использовался ли готовый датасет, на сколько можно доверять этому датасету, какие методы применялись при формировании входных числовых значений кроме теории нечётких множеств, какой вид в результате имели обучающие вектора, и т.д. Следовало бы более наглядно представить описание порядка обучения нейронных сетей (стр. 76–78, 107–110) – указать графики обучения и значения ошибок на промежуточных эпохах. Как следствие, не в полной мере обоснованы предложенные гиперпараметры нейронных сетей. При подборе гиперпараметров нейронных сетей (стр. 73–75, 102, 104–106) следовало бы использовать методы, основанные на применении генетических алгоритмов. Не приведено обоснование выбора метрики для суждения о качестве обучения нейронной сети. Предложено использовать многопараметрическую метрику, включающую значение гармонически среднего между точностью и полнотой, значение разброса и значение смещения. Почему эти, а не просто среднюю ошибку обучения? В третьем положении, выносимом на защиту, автор пишет о методике анализа поведения пользователей информационной системы. Предложенное автором решение действительно предназначено для обеспечения безопасности данных, обрабатываемых в блокчейн-системе, но применимо скорее для информационных систем, сопряжённых и обеспечивающих функционирование блокчейн-системы (на автоматизированных рабочих местах операторов, вносящих новые данные в цепочки блоков блокчейн-системы). Автором указано, что применение предложенных в диссертационной работе решений позволит обеспечить систему защиты информации появлением новых функций и свойств, обеспечивающих безопасность данных. В третьем положении, выносимом на защиту, автор пишет о методике анализа поведения пользователей информационной системы. Предложенное автором решение действительно предназначено для обеспечения безопасности данных, обрабатываемых в блокчейн-системе, но применимо скорее для информационных систем, сопряжённых и обеспечивающих функционирование блокчейн-системы (на автоматизированных рабочих местах операторов, вносящих новые данные в цепочки блоков блокчейн-системы). Из автореферата неясно, чем обоснован выбор конкретных архитектур нейронных сетей.

Выбор оппонентов и ведущей организации обосновывается тем, что оппоненты являются известными учёными в области защиты распределённых систем, мониторинга информационной безопасности (доц. института кибербезопасности и защиты информации ФГАОУ ВО СПбПУ, д.т.н., доцент Полтавцева М.А.) и применения методов машинного обучения в решении задач защиты информации (проф. каф. информационных систем СПбГЭТУ «ЛЭТИ», д.т.н., профессор Татарникова Т.М.), что подтверждается анализом их публикаций в ведущих международных и российских периодических научных изданиях. Ведущая организация – СибГУТИ характеризуется проведением масштабных исследований в области применения нейронных сетей для обеспечения безопасности информации. Учёные СибГУТИ внесли большой вклад в развитие методов машинного обучения и криптографии (Морозова К.И., Ракитский А.А., Рябко Б.Я., Новиков С.Н.). Заведующий кафедрой прикладной математики и кибернетики Нечта И.В., д.т.н., проф. является ведущим специалистом в области стеганографии.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований: разработаны новые численные методы определения опасности нарушения характеристик безопасности информации, позволяющие расчётным путём получить числовые значения опасности реализации угроз; **предложены** состав потенциальных угроз блокчейн-системе; архитектура нейронной сети, предназначенной для автоматизированной оценки достоверности вносимых в блокчейн-систему данных; архитектура нейронной сети, предназначенной для выявления аномалий в поведении пользователей информационной системы; **доказана** возможность выявления аномалий в поведении пользователя информационной системы при помощи искусственной нейронной сети; **введено понятие** санкционированного поведения пользователя.

Теоретическая значимость исследования обоснована тем, что: доказана возможность выявления аномалий в поведении пользователя при помощи искусственных нейронных сетей; **применительно к проблематике диссертации результативно использованы** методы вычислительной математики (теории нечётких множеств и теории искусственных нейронных сетей); **изложены**

основные положения и требования по созданию систем защиты информации на примере нормативной базы России, фактические недостатки применяемых в настоящее время решений по защите информации, идеи о расширении функций и свойств систем защиты информации; **раскрыты** противоречия и недостатки применяемых в настоящее время решений по обеспечению безопасности данных, обрабатываемых в блокчейн-системах; **изучены** зависимости между угрозами, актуальными для данных, обрабатываемых в блокчейн-системе, ущербом от потенциальных угроз блокчейн-системе, степенью опасности нарушения отдельных характеристик безопасности (в т.ч. достоверности), составом деструктивных воздействий, степенью важности данных; **проведена модернизация** существующих методических указаний по определению актуальных угроз данным, а также функциональных возможностей системы защиты данных, обрабатываемых в блокчейн-системе, обеспечивающих получение новых результатов по теме диссертации.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что: разработаны и внедрены в опытно-конструкторскую деятельность ООО «СИГМА» проектные решения по определению актуальных угроз, анализу поведения пользователей и процессов, в образовательный процесс ФГАОУ ВО ГУАП при чтении лекций, проведении практических занятий и лабораторных работ; **определены** возможности определения опасности угроз, обеспечения достоверности и анализа поведения пользователей при защите данных, обрабатываемых в блокчейн-системе; **созданы** численные методы, позволяющие определять опасность угроз данным, достоверность данных, а также выявлять аномалии в поведении пользователей; **представлены** рекомендации по дальнейшему совершенствованию предложенной модели угроз и численным методам, что позволит повысить границы применимости и повысить точность работы предложенных решений.

Оценка достоверности результатов исследования выявила: для экспериментальных работ результаты получены с использованием программного комплекса, разработанного на языке программирования Python с применением библиотеки Keras; **идея базируется** на критическом анализе известных

источников, опубликованных по теме диссертации; **использованы** сравнение авторских данных и данных, полученных ранее по рассматриваемой тематике; **установлено** качественное совпадение авторских результатов с результатами, представленными в независимых источниках по данной тематике; **использованы** современные методики защиты информации и методы вычислительной математики.

Личный вклад соискателя состоит в том, что основные результаты диссертационной работы получены автором самостоятельно.

В ходе защиты диссертации были высказаны следующие критические замечания: нет обоснования выбора алгоритма обучения и необходимо обосновать выбор конкретной архитектуры нейронной сети.

Соискатель Козин И.С. в ходе заседания согласился с замечаниями и привёл собственную аргументацию о том, что необходимо было дополнить предложенные решения результатами сравнительного анализа различных алгоритмов обучения и необходимо было представить обоснование выбора конкретной архитектуры нейронной сети. Более того, исследования, продолженные после написания диссертационной работы, показали, что более целесообразным является применение нейросетей, основанных на архитектуре автокодировщиков.

Диссертационный совет установил, что диссертация «Метод обеспечения безопасности данных при их обработке в блокчейн-системе за счёт применения искусственных нейронных сетей» является законченной научно-квалификационной работой и соответствует требованиям п. 9 Положения о присуждении ученых степеней, предъявляемым к кандидатским диссертациям, а также пунктам 1–3, 5, 7, 9, 13, 14 паспорта научной специальности Методы и системы защиты информации, информационная безопасность.

На заседании 20 апреля 2022 года объединенный диссертационный совет принял решение присудить Козину И.С. ученую степень кандидата технических наук за решение научных задач по разработке модели выявления актуальных угроз, метода обеспечения достоверности данных и методики анализа санкционированного поведения пользователей, позволяющих обеспечить

достоверность данных при их обработке в блокчейн-системе, и имеющих важное значение для развития систем защиты информации в Российской Федерации.

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 – 17, против – нет, недействительных бюллетеней – нет.

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

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

22 апреля 2022 года