# ОТЗЫВ

официального оппонента Татарниковой Татьяны Михайловны на диссертацию Козина Ивана Сергеевича на тему «Метод обеспечения безопасности данных при их обработке в блокчейн-системе за счет применения искусственных нейронных сетей» по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

**Актуальность темы диссертации**

Обеспечение безопасности данных при их обработке в блокчейн-системе в настоящее время является актуальной задачей. Возрастающий интерес к этой области обусловлен возможностями, которые открывает применение распределенной обработки данных.

Необходимость обработки данных в блокчейн-системах предполагает новый эволюционный этап обеспечения безопасности информации, обусловленный появлением дополнительных требований к информационным системам, новыми технологиями обработки информации и специфическими задачами, такими как использование вычислительных ресурсов мобильных устройств, а также непрерывным расширением спектра потенциальных угроз и, как следствие, устареванием существующих методов защиты данных.

В настоящее время в недостаточной степени изучены модели выявления актуальных угроз нарушения информационной безопасности данных в блокчейн-системе, методы обеспечения безопасности данных в блокчейн-системах, а также методики анализа санкционированного поведения пользователей. Данные обстоятельства находятся в противоречии с объективной потребностью обеспечения безопасности данных при их обработке в блокчейн-системе и обусловливают актуальность темы диссертации.

**Новизна научных положений, выводов и рекомендаций**

Научная новизна диссертационной работы Козина И.С. определяется предметом исследования – методами обеспечения безопасности данных при их обработке в блокчейн-системе, в большей степени задачами определения актуальных угроз данным, обрабатываемым в блокчейн-системе и анализа поведения пользователей. Конкретные результаты, обладающие научной новизной, состоят в следующем:

1) представление угроз, отличное от классического, предложенного ФСТЭК России учетом специфических угроз данным, обрабатываемым в блокчейн-системе, числовых значений степени опасности нарушения отдельных характеристик безопасности (конфиденциальности, целостности, доступности, достоверности);

2) концептуально новым подходом к достижению консенсуса, включающим процедуру автоматизированной оценки рисков внесения и обработки недостоверных данных, разработанную с использованием теории искусственных нейронных сетей и теории нечетких множеств;

3) уникальным составом формализованных характеристик поведения пользователя, которые являются входными характеристиками нейронной сети и параметрами нейронной сети.

**Общая структура и содержание диссертационной работы**

В целом, содержание и оформление диссертации и автореферата соответствуют с принятыми для научных квалификационных работ нормами и требованиями. Диссертация состоит из введения, пяти глав, с выводами по каждой, заключения, списка литературы и четырех приложений.

В работе содержится обзор основных современных требований к разработке и защите информационных систем, выделены ключевые недостатки существующих мер защиты, а также предложены решения, направленные на устранение выявленных недостатков, а именно: модель выявления актуальных угроз нарушения информационной безопасности данных, обрабатываемых в блокчейн-системе; метод обеспечения достоверности персональных данных, обрабатываемых в блокчейн-системе; методика анализа санкционированного поведения пользователей информационной системы.

В работе представлены сведения о внедрении полученных результатов, а также проект приложения к Заявлению на полезную модель автоматизированной системы управления защитой информации в территориально распределенной информационной системе.

**Теоретическая и практическая значимость**

Теоретическая значимость диссертационной работы состоит в следующем:

1) Установлена и формализована зависимость между: угрозами, актуальными для данных, обрабатываемых в блокчейн-системе; ущербом от потенциальных угроз блокчейн-системе; степенью опасности нарушения отдельных характеристик безопасности; составом деструктивных воздействий; степенью важности данных.

2) Расширен класс методов обеспечения достоверности данных в части выявления недостоверных персональных данных при их вводе в блокчейн-систему благодаря применению искусственной нейронной сети.

3) Формализовано поведение пользователя и доказана возможность выявления аномалий в поведении пользователя с применением искусственных нейронных сетей.

Практическая значимость диссертационной работы состоит в том, что ее результаты позволяют:

а) определить угрозы, актуальные для блокчейн-систем, а также оказывающие влияние на достоверность данных;

б) обеспечить достоверность данных при их обработке в блокчейн-системе как на уровне организаций различных форм собственности, так и на уровне государства в целом;

в) оперативно выявлять аномалии в поведении пользователей;

г) в частности в России:

1) обеспечить выполнение требований государственных стандартов в части определения актуальных угроз;

2) выполнить требования ФСТЭК России:

– по контролю ошибочных действий пользователей при вводе персональных данных в части анализа зарегистрированных событий безопасности и реагирования на них (РСБ.5);

– при защите от угроз, представленных в банке данных угроз ФСТЭК

России, связанных с подменой доверенного пользователя (УБИ.128) и его действий путем обмана (УБИ.127);

3) дополнить метод определения актуальных угроз, предложенный ФСТЭК России.

Результаты и выводы, представленные в диссертационной работе, могут найти применение при определении актуальных угроз блокчейн-системам и при разработке средств защиты информации, предназначенных для обеспечения достоверности данных, вводимых в блокчейн-систему, а также анализа поведения пользователей информационной системы.

**Степень обоснованности и достоверности научных положений, выводов и результатов, сформулированных в диссертационной работе**

Обоснованность и достоверность выносимых на защиту полученных новых положений, выводов и рекомендаций обусловлены и подтверждаются корректностью математического обоснования проведенных исследований и системным подходом к решению поставленных задач, в том числе: математическими доказательствами и результатами экспериментальной проверки, анализом работ и согласованностью с известными решениями в данной предметной области, обсуждением в открытой печати и апробацией на российских конференциях.

**Полнота публикации научных результатов диссертации**

Основные результаты работы опубликованы в 11 научных работах, в том числе в 5 работах из Перечня ВАК России, обсуждались на двух конференциях, апробированы при проведении научно-исследовательской и опытно-конструкторских работ на предприятиях ПАО «Интелтех», ООО «СИГМА», использованы в учебном процессе ФГАОУ ВО «СПбГУАП».

**Замечания по диссертационной работе**

1) 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.

2) При описании выбранных нейронных сетей (главы 3 и 4) не приведено обоснование выбора конкретных архитектур нейронных сетей, а также описание порядка обучения нейронных сетей.

3) Методика анализа поведения пользователей (глава 4) в целом применима скорее не для блокчейн-системы, а для информационных систем, поддерживающих работу блокчейн-систем.

4) 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 и т.д.

5) 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?

**Выводы**

Отмеченные недостатки не снижают ценности результатов диссертации для теории и практики. Диссертационная работа Козина Ивана Сергеевича «Метод обеспечения безопасности данных при их обработке в блокчейн-системе за счёт применения искусственных нейронных сетей» является законченной научно-квалификационной работой. Диссертация соответствует следующим пунктам паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность: 1–3, 5, 7, 9, 13, 14.

В диссертации решена научная задача разработки методов обеспечения безопасности данных при их обработке в блокчейн-системе, имеющая важное значение в условиях перевода информационных систем и информационных ресурсов на облачные платформы. Диссертация отвечает критериям, изложенным в п. 9 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842 в редакции от 11.09.2021. Автореферат полностью отражает основное содержание диссертационной работы.

Диссертационная работа «Метод обеспечения безопасности данных при их обработке в блокчейн-системе за счёт применения искусственных нейронных сетей» заслуживает положительной оценки, а ее автор – Козин Иван Сергеевич присвоения ученой степени кандидата технических наук по специальности 2.3.6. – Методы и системы защиты информации, информационная безопасность

Профессор кафедры Информационные системы
Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина)
доктор технических наук, профессор Татарникова Т.М.

ПОДПИСЬ ЗАВЕРЯЮ
НАЧАЛЬНИК ОДС
Т. В. РУСЯЕВА
10.03.2022

Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
197022, Россия, Санкт-Петербург, ул. Профессора Попова, дом 5
Тел: +7 812 234-27-46
E-mail: info@etu.ru