Отзыв официального оппонента

Полтавцевой Марии Анатольевны

на диссертацию Козина Ивана Сергеевича на тему

«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

Актуальность темы исследования

Цифровизация различных областей человеческой деятельности обеспечила развитие информационных технологий во всех отраслях современной экономики и промышленности. Блокчейн-системы становятся неотъемлемой частью информационных систем различного назначения. В числе основных задач таких систем можно выделить задачи обработки большого количества данных и обеспечения их достоверности. Увеличение объёмов информации поступающей из различных источников и необходимость её обработки обуславливает востребованность и распространение соответствующих средств и методов защиты информации.

Блокчейн-системы, как закономерный этап эволюции информационных систем, занимают нишу в финансовом и банковском секторе, промышленности, системах электронного государства и других. Потому существенно возрастает как ценность обрабатываемой в таких системах информации, так и требования по её защите. В настоящее время обеспечение безопасности блокчейн-систем является одной из важных задач обеспечения информационной безопасности.

Современные исследования не в полной мере рассматривают угрозы, актуальные для блокчейн-систем, а также методы защиты таких систем, в том числе, основанные на применении машинного обучения.

Основные результаты

Представленные в диссертационной работе результаты включают в свой состав следующие материалы, составляющие научную **новизну**:

1) представление угроз, отличное от классического (предложенного ФСТЭК России) учётом: 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 (составом входных характеристик нейронной сети) и параметрами нейронной сети.

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.

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 (в т.ч. достоверности); 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 за счёт искусственной нейронной сети.

3. Формализовано поведение пользователя и доказана возможность выявления аномалий в поведении пользователя при помощи 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 путём обмана (УБИ.127);

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

Результаты научных исследований были использованы при проведении научно-исследовательской и опытно-конструкторских работ на предприятиях ПАО «Интелтех», ООО «СИГМА». Также результаты диссертационной работы использованы в учебном процессе ФГАОУ ВО «СПбГУАП».

Рекомендации по использованию результатов

Результаты и выводы, представленные в диссертационной работе, могут найти применение:

– при определении актуальных угроз блокчейн-системам;

– при разработке средств защиты информации, предназначенных для обеспечения достоверности данных, вводимых в блокчейн-систему, а также анализа поведения пользователей информационной системы.

Общая оценка диссертационной работы

В целом, содержание и оформление диссертации и автореферата соответствуют принятым для научных квалификационных работ нормам и требованиям. Автореферат адекватно и в полной мере отражает основные научные результаты и положения, сформулированные в тексте диссертации.

Основные результаты работы были опубликованы в 11 научных работах (в т.ч. в 5 из Перечня ВАК России), обсуждались на двух конференциях, были апробированы при проведении научно-исследовательской работы, при проектировании двух информационных систем, а также использованы в учебном процессе.

В диссертационной работе были выявлены следующие **недостатки**:

1. В главах 3 и 4 не представлен сравнительный анализ различных архитектур нейронных сетей и, как следствие, не в полной мере представлено обоснование предложенных архитектур.

2. В главах 3 и 4 не в полной мере представлено описание процесса обучения нейронных сетей и, как следствие, не в полной мере обоснованы предложенные гиперпараметры нейронных сетей.

3. 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.

4. В работе присутствуют стилистические недочеты, в частности, связанные с переводом и использованием специфической терминологии в области блокчейн и машинного обучения.

Заключение

Выявленные недостатки не снижают ценности диссертационной работы в целом. Диссертация является законченной научно-квалификационной работой, вносящей вклад в развитие методов защиты информации, связанных с технологиями распределённой обработки данных и машинного обучения, а также содержит новые результаты, представляющие научную и практическую ценность. Работа хорошо оформлена, имеет продуманную структуру, содержит обобщённое описание современных методов решения рассматриваемых задач.

Основные результаты, выносимые на защиту, прошли апробацию на значимых российских конференциях, а также при разработке информационных систем, и в полной мере опубликованы, в т.ч. в изданиях, рекомендованных ВАК России. Апробация подтверждена актами внедрения. Содержание диссертации соответствует пунктам 1–3, 5, 7, 9, 13, 14 Паспорта специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность. Автореферат адекватно отражает содержание диссертационной работы и её основные результаты.

На основании изложенного считаю, что диссертация Козина Ивана Сергеевича «Метод обеспечения безопасности данных при их обработке в блокчейн-системе за счёт применения искусственных нейронных сетей» соответствует требованиям п. 9 Положения о присуждении учёных степеней,

утверждённого Постановлением Правительства Российской Федерации от 24.09.2013 года № 842, а её автор, Козин Иван Сергеевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

«23» марта 2022 года.

Доцент института кибербезопасности
и защиты информации
доктор технических наук, доцент [redacted] Полтавцева
Мария Анатольевна

Почтовый адрес:

ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого»
195251, Россия, Санкт-Петербург,
ул. Политехническая, д. 29.
Тел.: (812) 552-76-32.
e-mail: kafedra@ibks.spbstu.ru

[redacted]