Экз. № 1

ОТЗЫВ

специалистов ФАУ «ГНИИИ ПТЗИ ФСТЭК России» на автореферат диссертации КОЗИНА Ивана Сергеевича на тему: «Метод обеспечения безопасности данных при их обработке в блокчейн-системе за счет применения искусственных нейронных сетей», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы диссертации

В числе наиболее перспективных методов обеспечения хранения, обработки и защиты данных выделяются методы с применением технологии «блокчейн» на облачных платформах. В целях реализации национальной программы «Цифровая экономика Российской Федерации» и повышения эффективности использования информационно-технологической и коммуникационной инфраструктуры, созданной для предоставления государственных и муниципальных услуг в электронной форме, Правительство Российской Федерации даже постановило провести эксперимент по переводу информационных систем и ресурсов федеральных органов исполнительной власти и государственных внебюджетных фондов в государственную единую облачную систему.

Вместе с тем применение технологии «блокчейн» обусловило появление новых угроз безопасности обрабатываемой с использованием этой технологии данных. Однако до сих пор исследования, направленные на анализ таких угроз и, тем более, на разработку методов их парирования, практически не проводились.

Поэтому тема работы, направленной на разработку методов обеспечения безопасности данных при их обработке в блокчейн-системе за счет применения искусственных нейронных сетей является актуальной.

Возникшее противоречие, заключающееся в необходимости защиты данных в блокчейн-системах и отсутствии соответствующих моделей и методик обоснования способов и средств такой защиты привели к необходимости решения автором соответствующей научной задачи и формулирования цели исследований, заключающейся, на наш взгляд, в обеспечении безопасности данных от преднамеренных угроз при их обработке в блокчейн-системе.

В результате решения научной задачи автором лично получен ряд

новых научных результатов, выносимых им на защиту:

1. Модель выявления актуальных угроз нарушения безопасности данных, обрабатываемой в блокчейн-системе.

2. Метод обеспечения достоверности персональных данных, обрабатываемых в блокчейн-системе.

3. Методика анализа санкционированного поведения пользователей информационной системы.

Научная новизна работы заключается, на наш взгляд, в следующем:

1. Модель выявления актуальных угроз нарушения безопасности данных, обрабатываемых в блокчейн-системе, отличается от известных моделей выявления актуальных угроз в информационных системах, во-первых, введением связей угроз с показателем важности данных, с составом возможных деструктивных воздействий на обрабатываемые в блокчейн-системе данные, с нечеткой оценкой возможного ущерба от них и степени опасности таких действий.

2. Метод обеспечения достоверности персональных данных, обрабатываемых в блокчейн-системе, отличается от известных применением алгоритма построения архитектуры распределенного реестра персональных данных, процедурами автоматизированной оценки рисков нарушения безопасности данных, разработанными с использованием теории искусственных нейронных сетей и теории нечетких множеств, а также составом входных характеристик нейронной сети, обеспечивающим учет формализованных характеристик поведения пользователя.

Теоретическая значимость результатов исследований заключается в том, что:

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 счет искусственной нейронной сети.

3. Формализовано поведение пользователя и доказана возможность выявления аномалий в поведении пользователя при помощи искусственных нейронных сетей.

Практическая значимость результатов подтверждается тем, что результаты работы позволяют:

определить угрозы, актуальные для блокчейн-систем, а также

оказывающие влияние на достоверность данных;

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

оперативно выявлять аномалии в поведении пользователей.

Достоверность результатов подтверждается математическими доказательствами и результатами экспериментальной проверки работоспособности предложенного метода анализа поведения пользователей на реальных исходных данных.

Установлена согласованность авторских результатов с известными решениями в данной предметной области.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации, подтверждены: корректностью математического обоснования проведенных исследований и системным подходом к решению поставленных задач.

Оценка содержания диссертации, ее завершенности

Судя по автореферату, результаты диссертационных исследований прошли апробацию на 2 научно-технических конференциях различного уровня, реализованы при выполнении одной научно-исследовательской работы, а также в достаточной степени опубликованы в 5 изданиях из Перечня ВАК при Министерстве науки и высшего образования РФ или приравненных к ним.

Замечания и недостатки

Однако, судя по автореферату, в работе имеются следующие недостатки:

1. Цель работы, записанная в автореферате, состоит в обеспечении достоверности данных при их обработке в блокчейн-системе. Однако автор не ввел для оценки достоверности персональных данных никакого показателя. Введенный автором коэффициент опасности воздействия, нарушающего «достоверность объекта», оценивается экспертно на основе нечетких 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.

2. Автором приведены определенные на основе аппарата нечетких 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, определенном некими «ФОИВ ТЗИ», для диссертации некорректно.

Несмотря на отмеченные недостатки, представленная диссертационная работа является законченным научно-квалификационным трудом, имеющим научную новизну и практическую значимость.

Содержание работы соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» и отрасли – технические науки.

Вывод

Диссертация Козина Ивана Сергеевича соответствует критериям, установленным для диссертации на соискание ученой степени кандидата технических наук в пп. 9-11 «Положения о присуждении ученых степеней», а ее автор заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Главный научный сотрудник управления
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
доктор технических наук, профессор Язов Ю.К.

«31» марта 2022 г.

Начальник отдела
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
кандидат технических наук Чернышов В.А.

«31» марта 2022 г.

Подпись Язова Ю.К. и Чернышова В.А. заверяю.

Ученый секретарь
ФАУ «ГНИИИ ПТЗИ ФСТЭК России»
кандидат технических наук,
старший научный сотрудник Паринов И.В.

«31» марта 2022 г.

Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»)
Почтовый адрес: 394030, г. Воронеж, ул. Студенческая, д. 36
Тел.:8(473) 257-92-58
e-mail: gniii@fstec.ru