ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора технических наук, профессора Сизова Валерия Александровича на диссертацию Мельникова Дмитрия Анатольевича на тему: «Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных систем», представленную на соискание учёной степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы. Диссертационная работа Мельникова Дмитрия Анатольевича направлена на решение актуальной научно-технической проблемы построения эффективной системы управления криптографической защитой (КЗСУ) на основе инфраструктур открытых ключей (ИОК) широкомасштабных информационно-телекоммуникационных систем (ИТС) с учетом формирования и использования механизмов доверия с целью парирования угроз информационной безопасности (ИБ) в условиях цифровой трансформации экономики Российской Федерации и защиты прав и законных интересов личности, бизнеса и государства.

Анализ ИОК ИТС в РФ показывает, что они требуют модернизации и реструктуризации с учетом возросших требований к доверию между субъектами ИТС, требований к высокому уровню защищённости и необходимости противостояния реальным нарушениям ИБ каждой из ИТС, объединенных в широкомасштабную систему.

В настоящее время методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей ИТС не в полной мере учитывают механизмы построения и применения эффективных систем доверия.

Поэтому тема диссертации Мельникова Д.А. «Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных систем» является актуальной.

Достоверность и новизна результатов диссертации

Достоверность теоретических и прикладных результатов работы определяется строгим следованием общенаучным методам и основным положениям, и системе понятий российских ГОСТов и международных стандартов, а также корректностью и формально-логическими доказательствами формулируемых утверждений и предложений, полученных с использованием математического аппарата субъективный логики (СЛ), который включает ряд новых операторов, позволяющих проанализировать различные сети субъективного доверия (ССД) и, соответственно, позволяет разработать механизмы построения и применения эффективных систем доверия.

Основными методами диссертационного исследования являются: анализ, синтез и математическое моделирование. Исследование основано на функционально-ориентированном и предметно-ориентированном подходах. При первом подходе применялась последовательная декомпозиция проблемы на отдельные, достаточно простые составляющие, об-

ладающие функциональной определённостью. При втором подходе формировались абстрактные модели реальных объектов, которые позволили создать рациональные системы, устанавливающие взаимосвязи между функциональными объектами.

Достоверность результатов работы также подтверждается положительными отзывами их успешного внедрения в крупные ведомства и организации.

В диссертационной работе на основе применения системного подхода при решении поставленной научно-технической проблемы получены следующие *новые выносимые на защиту результаты*.

1. Разработанная с помощью математического аппарата СЛ модель системы доверия (КЗСУ) на основе ИОК для ИТИЦЭ и её усовершенствованная версия, в которой предложена концепция распределённого центра подтверждения подлинности (ЦПП), представляющего собой единую иерархическую систему ЦПП, которая является ядром системы (формирования) доверия в ИТС, входящих в ИТИЦЭ РФ.

2. Функционально-структурная модель системы доверия на основе ИОК для ИТИЦЭ, в рамках которой были определены требования к ЦПП, входящих в единую иерархическую систему ЦПП ИТС. Географически-распределённая модель единой иерархической системы ЦПП, которая определяет географические места размещения ЦПП ИТС на каждом уровне иерархии.

3. Главное требование к системе доверия на основе ИОК для ИТИЦЭ, заключающееся в реализации следующих основных функций: предоставление (по запросу) услуг по проверке ЭП и целостности подписанного электронного документа; подтверждение подлинности (по запросу) предоставленного сертификата открытого ключа ($СЕРТ_{ОК}$); проверка обоснованности (законности) выпуска $СЕРТ_{ОК}$ с целью защиты прав и свобод гражданина, на имя которого (без его согласия) мог быть издан фальсифицированный сертификат.

4. Реализуемый системой доверия на основе ИОК для ИТИЦЭ метод парирования угроз безопасности, связанных с выпуском удостоверяющими центрами (УЦ) фальсифицированных $СЕРТ_{ОК}$, который основан на подтверждении подлинности и проверке законности выпуска $СЕРТ_{ОК}$, и предусматривает участие специализированного государственного органа, предназначенного для регистрации заявки пользователя ИОК на получение $СЕРТ_{ОК}$ и подтверждения наличие такой заявки.

5. Реализуемый системой доверия на основе (инфраструктуры) открытых ключей для ИТИЦЭ метод распознавания поддельных (мошеннических) *Web*-сайтов, который включает проверку и подтверждение подлинности $СЕРТ_{ОК}$ провайдера электронных услуг (ПЭУ) со стороны пользователя с целью предотвращения (блокирования) мошеннических транзакций.

6. Модель единой (глобальной) системы идентификации Интернет-пользователей и провайдеров электронных услуг на основе логической характеристики IPv6-протокола, реализация которой позволит существенно снизить киберпреступность в мировом информационном пространстве.

Научная новизна результатов и положений диссертации, полученных лично автором, заключается в следующем:

1. Разработаны модели (структурные блок-схемы) ложно-доверительных взаимосвязей субъектов, которые в отличие от существующих моделей позволяют распознать злонамеренные действия киберпреступников и предотвратить ложные транзакции, связанные с возможной потерей материально-финансовых средств.

2. Разработана модель системы доверия (КЗСУ) на основе ИОК для ИТИЦЭ, которая в отличие от известных моделей учитывает уязвимости существующей в РФ ИОК и реализует функцию проверки законности выпуска сертификатов открытых ключей.

3. Модифицирован математический аппарат СЛ для анализа и синтеза системы доверия на основе ИОК для ИТИЦЭ, который позволяет анализировать и исследовать состояние существующей в РФ ИОК на формализованном уровне.

4. На основе анализа системы доверия ИТИЦЭ методом поиска сетей субъективного доверия раскрыта уязвимость УЦ в РФ, которая является источником многочисленных угроз и рисков, и которая не характерна для существующих моделей доверия на основе ИОК.

5. Разработан метод определения обоснованности (законности) выпуска СЕРТОК для моделей систем доверия на основе различных архитектур ИОК, учитывающий все распространённые злонамеренные действия киберпреступников.

6. Разработан метод обнаружения злонамеренных действий провайдеров электронных услуг, включающий два алгоритма проверки собственника $СЕРТ_{ОК}$, которые не реализуется в рамках существующих моделей доверия на основе ИОК.

7. Разработана модель единой системы идентификации Интернет-пользователей и провайдеров электронных услуг на основе логической характеристики IPv6-протокола, которая существенным образом отличается от существующих систем идентификации, а её реализация позволяет существенным образом повысить уровень защищённости ИТИЦЭ.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Диссертант провёл большую работу по исследованию, анализу и творческому осмыслению фундаментальных и прикладных научных работ по проблематике диссертации и использовал большое число трудов отечественных и зарубежных авторов, нормативные и правовый документы. Это позволило автору сделать научно-обоснованные выводы и осуществить разработку практически значимых математических моделей и предложений. Обоснованность полученных результатов также доказывается структурой и логикой изложения. Сформулированные выводы и предложения, представленные на защиту, а также основные научные результаты полностью соответствуют поставленной цели.

Ценность результатов диссертации для науки и практики

Ценность работы для науки заключается в том, что автором разработан теоретический аппарат построения эффективной КЗСУ на основе ИОК широкомасштабных ИТС на основе использования методов субъективной логики, включающий ряд моделей и методов. В частности, разработанная модель системы доверия на основе ИОК по критерию отображения ССД в форме ППОГ позволила определить новую функцию этой системы – «опре-

деление обоснованности выпуска СЕРТОК», что не только расширило научные представления о возможностях различных архитектур ИОК, но позволило выявить и обосновать глобальную уязвимость системы доверия на основе российской ИОК, реализующей одновременно функции центров сертификации и регистрации.

Полученные в диссертационной работе Мельникова Д.А. результаты имеют существенную практическую ценность. Она заключается в том, что результаты работы были реализованы или использованы в научно-исследовательской и практической деятельности следующих организаций:

– Акционерном обществе «Газпромбанк»;

– Акционерном обществе «Научно-технический и сертификационный центр по комплексной защите информации» (АО Центр «Атомзащитаинформ»);

– Обществе с ограниченной ответственностью «Код безопасности»;

– Обществе с ограниченной ответственностью Фирма «АНКАД»;

– Группе компаний (ГК) «МАСКОМ»;

– в Центральном Банке Российской Федерации (НИР «Ключи – 2018», Договор № 569-27-и от 24.04.2018, выполненной в ФИЦ ИУ РАН).

Также материалы диссертационной работы используются в Национальном исследовательском ядерном университете «МИФИ» и Финансовом университете при Правительстве Российской Федерации при подготовке бакалавров, магистров и аспирантов по направлению «Информационная безопасность».

Подтверждение опубликования основных результатов диссертации в научной печати

Основные научные результаты работы с достаточной степенью полноты опубликованы в 35 печатных работах, среди которых:

– 1 статья в журнале, индексируемом в базах данных Scopus и/или Web of Science;

– 7 статей в сборниках трудов международных научных конференций, индексируемых в базах данных Scopus и/или Web of Science;

– 20 статей в рецензируемых российских журналах из списка ВАК;

– 3 статьи в сборниках трудов международных конференций (на английском языке);

– 4 учебника и учебных пособия.

Соответствие содержания автореферата основным положениям диссертации

Текст диссертации представлен на 350 страницах машинописного текста и включает введение, шесть глав, в каждой из которой решена своя задача исследования, заключение и выводы с основными результатами работы, список литературы из 201 источника, перечень сокращений, словарь терминов и три приложения (первое – директива президента США от 15 (16) апреля 1993 года «О государственном регулировании в области шифрования информации»; второе – таблица операторов СЛ, третье –копии пяти актов о внедрении и использовании результатов исследований). Материалы диссертации хорошо проиллюстрированы 13 таблицами и 100 рисунками. Автореферат полностью отражает основное содержание

диссертации и соответствует ей, раскрывая направление исследований, актуальность и содержание решаемой *научно-технической проблемы*, заключающейся в разработке методов и средств построения эффективной системы управления криптографической защитой (системы доверия) на основе инфраструктуры открытых ключей с использованием математического аппарата субъективной логики методов с целью повышения уровня защищённости ИТС, образующих ИТИЦЭ РФ.

Тема диссертационной работы соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность». Содержание диссертации соответствует отрасли «*технические науки*».

Замечания по работе

По диссертации можно отметить следующие *замечания*:

– автор предлагает использовать математический аппарат субъективной логики для анализа и синтеза системы доверия и при этом не рассматривает другие подходы (например, сети Петри, имитационное моделирование и др.), что сужает возможности оценки эффективности предлагаемых решений;

– в работе отсутствует обоснование адекватности разработанных моделей реальности, количественной оценки их эффективности.

– предложенный автором способ защиты от мошеннических *Web*-сайтов предусматривает использование ассиметричных криптографических систем и соответствующих средств (комплексов программного обеспечения) на стороне пользователей услугами провайдера. В работе не представлены требования к такому средству относительно его надёжности и защищённости, так как оно само может быть объектом различных компьютерных атак;

– в работе имеются некоторые некорректные представления смысловой информации (например, метод (алгоритм), служб (услуг), модель (блок-схема) и др.).

Отмеченные замечания не снижают научной ценности проведённого лично автором исследования и содержания основных положений, выносимых на защиту.

Заключение по работе:

Диссертационная работа Мельников Дмитрия Анатольевича является законченной научно-квалификационной работой, имеющей несомненную научную и практическую значимость при решении задач коренной модернизации и реструктуризации существующей ИОК в интересах цифровой экономики Российской Федерации. Автореферат диссертации полно и достоверно передаёт её основное содержание. Полученные результаты обладают актуальностью, научной новизной и практической ценностью. Работа оформлена в соответствии с ГОСТ Р 7.0.11-2011 и полностью соответствует требованиям «Положения о порядке присуждения учёных степеней», утверждённого Постановлением Правительства Российской Федерации № 842 от 24.09.2013 (ред. от 01.10.2018, с изм. от 26.05.2020), к диссерта-

циям на соискание учёной степени доктора наук, а её автор – Мельников Дмитрий Анатольевич – достоин присуждения ему учёной степени доктора технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

ОФИЦИАЛЬНЫЙ ОППОНЕНТ:

Сизов Валерий Александрович
профессор кафедры «Прикладная информатика и информационная безопасность» Российского экономического университета имени Г.В. Плеханова, профессор, доктор технических наук,
Тел. +7 (916) 810-38-63, email: sizov.va@rea.ru

_____ Сизов Валерий Александрович

«25» июля 2022 г.

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский экономический университет имени Г.В. Плеханова» (РЭУ им. Г.В. Плеханова),
117997, г. Москва, Стремянный пер. 36,
+7 (495) 958-25-56, rector@rea.ru

ПОДПИСЬ Сизова В.А.
удостоверяю
Специалист по работе с персоналом
25.07 2022 г.