ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

доктора военных наук, профессора Лося Владимира Павловича 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 исследований определяется недостаточной способностью национальной инфраструктуры обеспечения безопасности парировать современные угрозы, связанные с переходом РФ на «цифровые рельсы» и созданием информационно-телекоммуникационной инфраструктуры цифровой экономики (ИТИЦЭ), объединяющей широкомасштабные информационно-телекоммуникационные системы (далее – ИТС), которые решают различные социально-экономические задачи и задачи информационного и иных видов обеспечения. Современные ИТС включают системы обеспечения информационной безопасности (СОИБ), в состав которых входит система управления криптографической защитой информации (КЗСУ). ИТС, образующие ИТИЦЭ, должны обладать очень высоким уровнем защищённости, а СОИБ каждой ИТС должна противостоять реальным нарушениям информационной безопасности (ИБ).

Ввиду широкомасштабности распределённых ИТС, КЗСУ базируются на инфраструктурах открытых ключей (ИОК), также входящих в ИТС. Очевидно, что КЗСУ должна способствовать формированию доверия между субъектами ИТС, т.е. выступать в роли системы доверия. Вместе с тем, анализ ИОК ИТС в РФ показывает, что они требуют своей глубокой модернизации и обновления, и только после их совершенствования можно обеспечить высокий уровень защищённости ИТИЦЭ. Поэтому, актуальная научно-техническая проблема – это построение системы доверия на основе ИОК ИТС с целью парирования угроз ИБ в условиях создания цифровой экономики Российской Федерации, и защиты прав и законных интересов личности, бизнеса и государства.

Целью работы является разработка с использованием математического аппарата субъективной логики системы управления криптографической защитой (системы доверия) на основе инфраструктуры открытых ключей с целью повышения уровня защищённости ИТС, образующих ИТИЦЭ РФ.

Содержание работы по главам. Диссертационная работа Мельникова Д.А. состоит из введения, шести глав, заключения, выводов по диссертации, перечня сокращений и обозначений, словаря терминов, списка литературы и трёх приложений.

Во введении содержится краткий анализ проблем ИБ, связанных с цифровизацией экономики РФ, и современного состояния решаемой научной проблемы, обоснована актуальность темы диссертации, сформулирована цель исследования, определён круг решаемых задач, обозначены общие подходы к достижению поставленной цели, а также приведены основные результаты, выносимые на защиту, показана их роль и сформулирована научная новизна.

В Главе 1 представлен анализ проблем обеспечения безопасности цифровой экономики РФ. В частности, представлен анализ угроз национальной безопасности Российской Федерации в связи с цифровой трансформацией и рассмотрены возможные пути их нейтрализации.

В данной главе рассмотрена модель ИТИЦЭ. Обязательной подсистемой ИТИЦЭ должна быть информационно-технологическая инфраструктура обеспечения безопасности (ИТИБ), которая должна решать задачи предоставления услуг ИБ и формирования единой системы доверия. Основа такого доверия – высокий уровень защищённости ИТС.

Современные ИТИБ представляют собой ИОК, на основе которых строятся различные модели систем доверия в киберпространстве. Таким образом, разработка и реализация модели ИОК в РФ и создание на её основе системы доверия в интересах цифровой экономики РФ становится стратегической задачей, решение которой носит безотлагательный характер.

В заключительной части главы сформулирована цель диссертационной работы, а также научно-технические задачи, которые должны быть решены в диссертационной работе.

Глава 2 посвящена общетеоретическим аспектам доверия. Смысл доверия заключается в том, что требования к обеспечению доверия напрямую коррелируют с влиянием риска. С другой стороны, показано, что доверие, затрагивающее безопасность ИТС, отражает её сопротивляемость (резистивность) по отношению к злонамеренным действиям (например, атакам).

В работе проанализированы концептуальные понятия «доверенная сторона», «доверяющая сторона» и «преступное намерение». В работе определены два класса «доверенных сторон» – «мыслящий субъект» и «логический объект».

Кроме того, представлен обзор основных типов доверительных взаимосвязей с точки зрения участвующих субъектов (сторон). Доверие в ИТС предусматривает участие трёх сторон: мыслящего доверяющего субъекта, логического доверенного

объекта и мыслящего внешнего угрожающего (злонамеренного) субъекта. Показано, что злонамеренное поведение никогда не может быть абсолютным, а может быть определено только на основе политики безопасности, морально-этических норм, контрактов/договоров и законодательства.

Также исследована концепция доверия в ИТС на основе математического аппарата субъективной логики (СЛ).

В Главе 3 показано, что ИОК способна ускорить и упростить переход к электронному документообороту, и предоставить целый комплекс услуг по обеспечению ИБ.

Далее рассмотрены организация и компоненты ИОК. ИОК привязывает открытые криптографические ключи к субъектам и позволяет другим субъектам проверять привязки открытых ключей. Также представлен анализ основных архитектур ИОК, а также форматы данных, используемых в ИОК. Показано, что североамериканская и западноевропейская модели ИОК по своей сути неприемлемы для их реализации в Российской Федерации.

Кроме того, проанализированы проблемы и риски функционирования ИОК. Показаны несостоятельность и уязвимости модели удостоверяющего центра, которая характерна для УЦ в Российской Федерации.

Глава 4 посвящена исследованию проблемы обеспечения параметрами подлинности (ПП), которые используются в системах аутентификации на основе ИОК. Наличие возможности отображать и распознавать объекты в компьютерных сетях имеет основополагающее значение для систем электронного взаимодействия и сотрудничества, и является функциональным фундаментом практически всех систем обеспечения безопасности. Кроме того, рассмотрены системы обеспечения пользователей параметрами подлинности.

Показано, что для обоюдной аутентификации необходимо персональное устройство аутентификации. Однако, современные системы аутентификации при предоставлении электронных услуг не обеспечивают аутентификацию провайдеров электронных услуг (ПЭУ). Был сделан вывод о том, что в современных условиях модель с центром подтверждения подлинности (ЦПП) является наиболее перспективной и востребованной.

В главе 5 представлены элементы СЛ, составляющие математический аппарат синтеза сетей субъективного доверия (ССД). Используя аппарат СЛ и эвристический метод поиска сети доверия, была синтезирована модель системы доверия на основе ИОК для ИТИЦЭ, и сформулировано основное требование к ней – это должна быть ССД, отображаемая в последовательно-параллельный орграф (ППОГ). Затем был проведён анализ полученной системы доверия.

На основе синтезированной модели системы доверия были предложены её усовершенствованная, функционально-структурная и географически-распределённая модели. Была определена новая и ранее не реализованная в рамках существующих моделей доверия функция: проверка обоснованности (законности) выпуска СЕРТ$_{ОК}$.

Также представлены методы защиты пользователей ИОК ИТС и описаны средства, реализующие указанные методы. Рассмотрена модель (метод) глобальной идентификации Интернет-пользователей и ПЭУ в Интернет-сети, которая позволит существенно снизить уровень киберпреступности и защитить национальные ИТИЦЭ государств.

В Главе 6 рассмотрены проблемы внедрения и реализации полученных в диссертационном исследовании результатов, а также практические задачи построения объединённой КЗСУ (системы доверия) на основе интеграции ИОК для ИТС, образующих ИТИЦЭ РФ.

Кроме того, результаты исследований нашли своё отражение в учебниках и учебных пособиях, которые рекомендованы к использованию во многих ВУЗах России при подготовке специалистов по направлению «Информационная безопасность».

Заключение и основные выводы отражают результаты диссертационного исследования и дальнейшие перспективы исследований в данном направлении.

Словарь терминов содержит основные понятия и определения, относящиеся к области обеспечения ИБ.

Список литературы включает 201 источник, из которых 55 отечественных и 146 зарубежных авторов.

В трёх приложениях представлены: *а*) директива президента США от 15 (16) апреля 1993 года «О государственном регулировании в области шифрования информации», *б*) таблица операторов СЛ, *в*) копии актов о внедрении и использовании результатов исследований.

В целом диссертация написана хорошим литературным языком и достаточно полно проиллюстрирована. Выводы по каждой главе и всей работе вполне корректно отражают полученные результаты.

Достоверность и новизна результатов. Достоверность результатов исследования, интерпретации результатов моделирования, выносимых на защиту научных положений, новизны и выводов подтверждается тем, что выявленные в работе уязвимости и закономерности, разработанные способы и выводы не противоречат основным целям, задачам, национальным и международным стандартам обеспечения ИБ,

а все аналитические результаты получены с использованием математического аппарата субъективной логики. Корректность синтезированных моделей систем доверия была подтверждена результатами последующего вероятностного анализа, а также практическим внедрением полученных результатов научных исследований.

Основным научным результатом следует считать синтезированную и проанализированную с использованием математического аппарата субъективной логики систему управления криптографической защитой (системы доверия) на основе инфраструктуры открытых ключей с целью повышения уровня защищённости ИТС, образующих ИТИЦЭ РФ, а также методы и средства защиты граждан и бизнеса от использования фальсифицированных сертификатов открытых ключей и мошеннических *Web*-сайтов всемирной гипертекстовой информационно-технологической системы. Полученные результаты характеризуются научной новизной, которая состоит в следующем:

– представлены новые модели (структурные блок-схемы) ложно-доверительных взаимосвязей: первая – модель взаимодействия Интернет-пользователя с поддельным (мошенническим) *Web*-сайтом; вторая – модель взаимодействия субъекта с управляемым им логическим объектом в условиях компьютерного шпионажа;

– разработана новая модель системы доверия на основе ИОК для ИТС, формирующих ИТИЦЭ РФ;

– впервые для анализа ИОК (КЗСУ) был использован математический аппарат субъективной логики;

– установлено, что все российские УЦ построены на основе модели «Центр сертификации + Центр регистрации», которая обладает серьёзными уязвимостями, т.е. является источником многочисленных угроз и рисков;

– разработан метод определения обоснованности (законности) выпуска сертификата открытого ключа ($СЕРТ_{ОК}$), что представляет собой новую для ИОК задачу, которая не была решена ни одной из известных на сегодняшних день систем доверия (КЗСУ) на основе различных архитектур ИОК;

– разработан метод обнаружения злонамеренного ПЭУ на основе проверки собственника $СЕРТ_{ОК}$;

– предложена модель единой системы идентификации Интернет-пользователей и ПЭУ на основе логической характеристики IPv6-протокола.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации. В диссертационной работе использовались анализ, синтез и структурное (системное) моделирование с последующим анализом синтезированных моделей. Исследование основано на функционально-ориентированном и предметно-ориентированном подходах. При первом подходе применялась

последовательная декомпозиция проблемы на отдельные, достаточно простые составляющие, обладающие функциональной определённостью. При втором подходе формировались абстрактные модели реальных объектов, которые позволили создать субоптимальные системы, устанавливающие взаимосвязи между функциональными объектами (субъектами). Исследование также опиралось на российские ГОСТы и международные стандарты, материалы научно-практических конференций и публикаций в периодической печати, лучшие отечественные и международные методики обеспечения ИБ, что доказывает высокую степень обоснованности полученных научных результатов.

Подтверждение опубликования основных результатов диссертации в научной печати. Основные результаты диссертационной работы были апробированы на 10-ти всероссийских и международных научных и научно-практических конференциях. Они с достаточной полнотой изложены в 31 печатной работе, из них в 20 публикациях в изданиях, рекомендованных ВАК для опубликования основных научных результатов диссертаций на соискание учёной степени доктора наук. Кроме того, отдельные результаты диссертации отражены в 4 учебниках и учебных пособиях для образовательных организаций высшего образования (с грифами соответствующих ФУМО). Таким образом, можно заключить, что основные результаты и выводы диссертации строго обоснованы, являются новыми и получены автором самостоятельно и в соавторстве (автор обозначил свой личный вклад).

Ценность результатов работы для науки и практики. Теоретическая ценность работы заключается в том, что была синтезирована новая (ранее не известная) модель КЗСУ (системы доверия) на основе ИОК и сформулировано основное требование к ней – она должна представлять собой ССД, отображаемую в форму ППОГ; была определена новая функция (задача), реализуемая (решаемая) разработанной системой доверия на основе ИОК – определение обоснованности (законности) выпуска $СЕРТ_{ОК}$, что расширило научные представления о возможностях различных архитектур ИОК; была обнаружена и проанализирована глобальная уязвимость системы доверия на основе российской ИОК – чрезвычайно уязвимая модель построения всех без исключения российских УЦ, реализующих одновременно функции центров сертификации и регистрации.

Полученные в диссертационной работе Мельникова Д.А. результаты имеют существенную практическую ценность. Она заключается в том, что разработаны система доверия на основе ИОК, которая была усовершенствована за счёт создания распределённого ЦПП; функционально-структурная и географически-распределённая модели системы доверия на основе ИОК; функции, реализуемые системой до-

верия на основе ИОК; способы парирования угроз безопасности, связанных с выпуском фальсифицированных сертификатов удостоверяющим центром, и метод распознавания поддельных (мошеннических) *Web*-сайтов. В диссертации предложен комплекс международных и национальных мероприятий по созданию и реализации глобальной системы идентификации на основе логической характеристики IPv6-протокола.

Замечания по работе.

Следует отметить следующие недостатки в работе:

1. В работе нет обоснования, какой из подходов построения (анализа) сети доверия в форме последовательно-параллельного орграфа наиболее предпочтителен (комплексный или эвристический).

2. В работе не совсем явно определены средства построения системы доверия на основе ИОК для ИТИЦЭ.

3. В работе не определены, какие, отечественные или зарубежные, асимметричные криптографические системы будут использоваться в разработанной системе доверия, и как такая система будет взаимодействовать с зарубежными инфраструктурами открытых ключей при трансграничном взаимодействии.

4. В работе не рассмотрены проблемы внедрения предложенного способа идентификации на основе логической характеристики IPv6-протокола.

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

Соответствие содержания автореферата основным положениям диссертации. Автореферат достаточно полно и адекватно отражает основные результаты диссертации.

Соответствие диссертации требованиям, предъявляемым к диссертациям на соискание учёной степени доктора наук. Считаю, что диссертация Мельникова Д.А. является законченной научно-квалификационной работой, имеющей несомненную научную и практическую значимость при решении задач коренной модернизации и обновления существующей общероссийской ИОК и построении на её основе системы доверия в интересах цифровой экономики Российской Федерации. Полученные результаты обладают актуальностью, научной новизной и практической ценностью. Тема диссертационной работы соответствует паспорту специальности 05.13.19 – методы и системы защиты информации, информационная безопасность. Содержание диссертации соответствует отрасли наук, по которой присуждается учёная степень, – «технические науки».

Заключение по работе. Таким образом, диссертация Мельникова Д.А. оформлена согласно ГОСТ Р 7.0.11-2011, полностью соответствует критериям «Положения о порядке присуждения учёных степеней» к диссертациям 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:

Лось Владимир Павлович
РТУ МИРЭА, Центр исследования проблем кадрового обеспечения отрасли информационной безопасности, директор.
Президент Ассоциации защиты информации, профессор, доктор военных наук. 20.01.03 – «Оперативное искусство в целом, по видам Вооружённых Сил, родам войск и специальным войскам», 20.02.12 – Военная кибернетика (в настоящее время – Системный анализ, исследование операций, моделирование боевых действий и систем военного назначения, компьютерные технологии в военном деле).
Тел. +7(903)740-32-61, email: los-vladimir@yandex.ru

_____ Лось Владимир Павлович

«12» августа 2022 г.

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет» (РТУ МИРЭА), 119454, г. Москва, пр-т Вернадского, д. 78
+7 (499) 215-65-65, rector@mirea.ru

(подпись руки) Лось В.П.
Достоверяю
Проректор по инновационному развитию
А.В. Рагуткин