ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 002.073.02, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО УЧРЕЖДЕНИЯ «ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ИНФОРМАТИКА И УПРАВЛЕНИЕ» РОССИЙСКОЙ АКАДЕМИИ НАУК», ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ ДОКТОРА НАУК

аттестационное дело № _____

решение диссертационного совета от «07» сентября 2022 г. протокол № 9

О присуждении МЕЛЬНИКОВУ ДМИТРИЮ АНАТОЛЬЕВИЧУ, гражданину Российской Федерации, ученой степени доктора технических наук.

**Диссертация** «Методы и средства построения системы управления криптографической защитой на основе инфраструктуры открытых ключей для широкомасштабных информационно-телекоммуникационных систем» по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность, в виде рукописи принята к защите 06.04.2022, протокол № 2 диссертационным советом Д 002.073.02, созданным на базе Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) (119333, г. Москва, ул. Вавилова, д. 44, корп. 2; приказ Министерства образования и науки РФ от 24.06.2016 №771/нк).

**Соискатель** Мельников Дмитрий Анатольевич, 1959 года рождения, диссертацию на соискание ученой степени кандидата технических наук защитил в 1992 году в диссертационном совете, созданном на базе Военной академии связи им. С.М. Будённого. В настоящее время работает в ФИЦ ИУ РАН в должности ведущего научного сотрудника отдела №63 «Методы и программные средства накопления и обработки данных» отделения №6 .

Диссертация выполнена в отделе №63 ФИЦ ИУ РАН.

Научный консультант – доктор технических наук, Будзко Владимир Игоревич, академик Академии криптографии РФ, заместитель директора по научной работе Института проблем информатики ФИЦ ИУ РАН.

Официальные оппоненты:

1. Лось Владимир Павлович, гражданин Российской Федерации, доктор военных наук, профессор, директор Центра исследования проблем кадрового

обеспечения отрасли информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «МИРЭА – Российский технологический университет» (РТУ МИРЭА);

2. Сизов Валерий Александрович, гражданин Российской Федерации, профессор, доктор технических наук, профессор кафедры «Прикладная информатика и информационная безопасность» Российского экономического университета имени Г.В. Плеханова;

3. Стрельцов Анатолий Александрович, гражданин Российской Федерации, доктор технических наук, доктор юридических наук, профессор, ведущий научный сотрудник Центра проблем информационной безопасности МГУ имени М.В. Ломоносова

дали положительные отзывы на диссертацию.

Ведущая организация Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО «СПбПУ») в своем положительном заключении, подписанном Е.Б. Александровой, доктором технических наук, доцентом, профессором Института кибербезопасности и защиты информации, и утверждённом Ю.С. Клочковым, доктором технических наук, доцентом, проректором по научно-организационной деятельности ФГАОУ ВО «СПбПУ», указала, что диссертация Мельникова Дмитрия Анатольевича является законченной научно-квалификационной работой, в которой решена актуальная научно-техническая проблема – разработка и реализация модели системы управления криптографической защитой (системы доверия) на основе инфраструктуры открытых ключей (ИОК) для широкомасштабных информационно-телекоммуникационных систем (ИТС), образующих информационно-телекоммуникационную инфраструктуру цифровой экономики (ИТИЦЭ) РФ, и создание единой системы доверия с целью парирования угроз информационной безопасности (ИБ), связанных с цифровой трансформацией экономики РФ, и защиты прав и законных интересов личности, бизнеса и государства; диссертационная работа полностью соответствует требованиям к диссертациям на соискание учёной степени доктора технических наук, установленным Положением о порядке присуждения учёных степеней, а её автор, Д.А. Мельников, заслуживает присуждения ему учёной степени доктора технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность.

Соискатель имеет 89 опубликованных работы, в том числе по теме диссертации – 35, из них в рецензируемых научных изданиях – 20. Общий объем публикаций по теме диссертации – 20.46 п.л.; вклад автора в них является определяющим. Сведения, представленные соискателем об опубликованных работах, в которых изложены основные научные результаты диссертации, являются достоверными. В них достаточно полно изложены материалы исследования.

Наиболее значимые работы по теме диссертации:

1. Мельников Д.А. и др. К вопросу об использовании свойств логической характеристики IPv6-протокола в целях повышения уровня защищённости национальной информационно-технологической инфраструктуры Российской Федерации // Безопасность информационных технологий. – 2014. – №1. с. 30-35.
2. Мельников Д.А. и др. Базовые требования к подсистемам обеспечения криптоключами в информационно-технологических системах высокой доступности //Системы высокой доступности. – 2016. Т.12, № 3. С. 73-81.
3. Мельников Д.А. и др. Практическая реализация различных моделей инфраструктуры открытых ключей // Безопасность информационных технологий. Т. 23, № 1. 2016. С. 100 – 114.
4. Melnikov D.A., et al. Russian model of public keys and validation infrastructure as base of the cloud trust. In the Proceedings of the 4th International Conference on Future Internet of Things and Cloud (FiCloud 2016). 2016. P. 123–130.
5. Мельников Д.А. и др. Основы организации обеспечения информационной безопасности и киберустойчивости в централизованных информационно-телекоммуникационных системах высокой доступности. // Системы высокой доступности. – 2019. Т. 15. № 1. С. 70-77.
6. Мельников Д.А. и др. Модель доверия для цифровой экономики Российской Федерации // Безопасность информационных технологий. – 2020. – Т. 27, № 2. С. 47 – 64.
7. Мельников Д.А. О проблеме доверия к удостоверяющим центрам в Российской Федерации. // Системы высокой доступности. – 2022. Т. 18. № 1. С. 5-15.
8. Мельников Д.А. К вопросу распознавания мошеннических Web-сайтов. // Системы высокой доступности. – 2022. Т. 18. № 1. С. 16-25.

На автореферат дали положительные, не содержащие критических замечаний, отзывы:

– Крылов Г.О., профессор, д.ф.-м.н., профессор департамента «Информационная безопасность» Финансового университета при Правительстве РФ;

– Мазепа Р.Б., профессор, к.т.н., заведующий кафедрой 402 «Радиосистемы и комплексы управления, передачи информации и информационная безопасность» Московского авиационного института (национального исследовательского университета).

Выбор официальных оппонентов обосновывается их высокой квалификацией, наличием научных трудов, соответствующих теме оппонируемой диссертации, и следующими обстоятельствами:

– В.П. Лось – президент Ассоциации защиты информации, является известным специалистом в области ИБ, включая вопросы подготовки специалистов, разработки архитектур управления ИБ и процессов управления инцидентами ИБ;

– В.А. Сизов ведёт активную научно-педагогическую деятельность в области подготовки специалистов по защите информации в экономических системах; является разработчиком программы магистерской подготовки «Защита информационного пространства субъектов экономической деятельности» в РЭУ имени Г.В. Плеханова;

– А.А. Стрельцов является крупным специалистом в области правовых аспектов ИБ и построения систем управления; заслуженный деятель науки РФ; член-корреспондент Академии криптографии РФ.

Выбор ведущей организации обосновывается тем, что ФГАОУ ВО «СПбПУ» является крупным научным центром и активно занимается проблематикой по теме диссертационной работы Д.А. Мельникова, что подтверждается приоритетными направлениями работ и публикациями сотрудников.

**Диссертационный совет отмечает, что на основании выполненных соискателем исследований:**

– **Разработаны** две новые модели ложно-доверительных взаимосвязей: первая – модель взаимодействия с поддельным сайтом; вторая – модель компьютерного шпионажа.

– впервые была **разработана** модель системы управления криптографической защитой (системы доверия) на основе ИОК для ИТС, образующих ИТИЦЭ РФ.

– был впервые **разработан** метод (алгоритм) определения обоснованности выпуска сертификата открытого ключа ($СЕРТ_{ОК}$).

– впервые **разработан** метод обнаружения злонамеренных провайдеров электронных услуг.

– впервые **предложена** модель единой системы идентификации Интернет

пользователей и провайдеров электронных услуг на основе логической характеристики IPv6-протокола.

– достоверность и результативность проведённых научных исследований **подтверждена** практическими внедрениями их результатов.

**Теоретическая значимость исследования обоснована тем, что:**

– на основе аппарата субъективной логики (СЛ) была **синтезирована** новая модель системы доверия и **сформулировано** основное требование к ней;

– **определена** новая функция, реализуемая разработанной системой доверия – определение обоснованности выпуска $СЕРТ_{ОК}$. Таким образом, **расширены** научные представления о возможностях ИОК, выполняющих функции инфраструктуры обеспечения безопасности.

– впервые **обнаружена** глобальная уязвимость системы доверия на основе ИОК – совмещение всеми российскими УЦ функций центров сертификации и регистрации. Следствием этого является невозможность системы доверия на основе ИОК предотвратить выпуск поддельных $СЕРТ_{ОК}$, являющихся источниками рисков и угроз.

**Значение полученных соискателем результатов исследования для практики подтверждается тем, что:**

– была **предложена** усовершенствованная модель, в которой концепция единого центра подтверждения подлинности (ЦПП) заменена на концепцию распределённого ЦПП. Усовершенствованная модель включает единую иерархическую систему ЦПП, являющуюся ядром системы доверия на основе ИОК;

– **разработана** функционально-структурная модель системы доверия. Также была **разработана** географически-распределённая модель единой иерархической системы ЦПП;

– **сформулировано главное требование** к системе доверия на основе ИОК, заключающееся в реализации 3-х основных функций: проверка электронной подписи и целостности подписанного документа; подтверждение подлинности предоставленного $СЕРТ_{ОК}$; проверка обоснованности выпуска $СЕРТ_{ОК}$;

– впервые **разработан** метод распознавания фальсифицированных $СЕРТ_{ОК}$. **Предложен** алгоритм и вариант реализации указанного метода,

предусматривающий участие специализированного субъекта, который регистрирует и подтверждает наличие заявки на получение $СЕРТ_{ОК}$;

– **разработан** метод распознавания поддельных (мошеннических) *Web*-сайтов, который включает проверку и подтверждение подлинности $СЕРТ_{ОК}$ провайдера электронных услуг;

– **предложен** комплекс мероприятий по созданию и реализации единой системы идентификации на основе логической характеристики IPv6-протокола;

– практическая значимость результатов исследования **подтверждена** пятью актами о внедрении.

**Оценка достоверности результатов исследования выявила, что:**

– достоверность результатов исследования, интерпретации результатов моделирования, выносимых на защиту научных положений, новизны и выводов **подтверждается** тем, что выявленные в работе уязвимости и закономерности, разработанные методы и выводы не противоречат основным целям, задачам и международным стандартам обеспечения ИБ;

– **основными методами** диссертационного исследования являются анализ, синтез и структурное (системное) моделирование с последующим анализом синтезированных моделей. Исследование **основано** на функционально-ориентированном и предметно-ориентированном подходах;

– основные результаты исследований были **получены** на основе применения математического аппарата СЛ;

– при исследовании понятия «доверия» был проведён **анализ** известных теоретических работ по данной тематике и на основе результатов этого анализа были **предложены** новые структурные модели доверительных взаимосвязей/взаимоотношений;

– достоверность и реализуемость результатов исследования **подтверждены** широкой апробацией в открытой печати и на международных и национальных научных конференциях, а также практикой их внедрения в крупных организациях и образовательных учреждениях России.

**Основные результаты, представленные в диссертационной работе, получены соискателем лично.** В совместно опубликованных работах постановка и

исследование задач осуществлялись совместными усилиями соавторов при непосредственном участии соискателя.

На заседании 07 сентября 2022 года диссертационный совет принял решение присудить Мельникову Дмитрию Анатольевичу ученую степень доктора технических наук за решение научно-технической проблемы построения системы доверия на основе инфраструктур открытых ключей информационно-телекоммуникационных систем, имеющей важное социально-экономическое значение для парирования угроз информационной безопасности и защиты прав и законных интересов личности, бизнеса и государства.

При проведении тайного голосования диссертационный совет в количестве 22 человек, из них 6 докторов наук по профилю защищаемой диссертации, участвовавших в заседании, из 32 человек, входящих в состав совета, проголосовали: за - 17, против - 4, недействительных бюллетеней - 1.

Председатель
диссертационного совета Д 002.073.02
академик И.А. Соколов

Ученый секретарь
диссертационного совета Д 002.073.02
к.ф.-м.н. Р.В. Разумчик

«07» сентября 2022 г.