ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА
доктора технических наук, доктора юридических наук, профессора
Стрельцова Анатолия 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. Актуальность исследования систем управления криптографической защитой (КЗСУ), построенных на основе инфраструктуры открытых ключей (ИОК) обусловлена двумя обстоятельствами. С одной стороны, активным развитием данной инфраструктуры как важной составляющей системы обеспечения информационной безопасности информационных и коммуникационных сетей различного назначения, а с другой – увеличением опасности злонамеренного использования информационно-коммуникационных технологий (ИКТ) и, соответственно, - необходимостью повышения безопасности использования ИКТ в условиях формирования цифровой экономики. Злонамеренное использование ИКТ стало фактором, угрожающим не только информационной безопасности Российской Федерации[1], но и международному миру[2].

Одним из важных способов противодействия этой угрозе является применение средств криптографической защиты цифровых данных, в том числе для обеспечения безопасности электронного документооборота в экономической сфере общества.

К числу наиболее распространённых средств обеспечения безопасности электронного документооборота относятся технологии так называемой «электронной подписи». Применение этих технологий поддерживается организационной инфраструктурой удостоверяющих центров и технологической инфраструктурой средств, используемых удостоверяющими центрами для осуществления функций по созданию и выдаче сертификатов ключей проверки электронных подписей. В состав средств технологической инфраструктуры входят, в частности, средства электронной подписи – «шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи»[3]. В основу технологии «цифровой подписи» положена инфраструктура открытых ключей (ИОК), обеспечивающая создание, хранение и распространение цифровых сертификатов, подтверждающих принадлежность открытого ключа определенному субъекту электронного взаимодействия.

Средства обеспечения безопасности электронного документооборота в информационно-телекоммуникационных сетях (ИТС), использующие криптографические методы защиты данных, могут объединяться в системы управления криптографической защитой (КЗСУ). Такие

---

[1] Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 12 апреля 2021 г.
[2] Резолюция Генеральной Ассамблеи ООН от 4 января 2021 г., A/RES/75/240
[3] Федеральный закон «Об электронной подписи», Федеральный закон от 06.04 2011 № 63-ФЗ.

КЗСУ являются важной составляющей систем обеспечения безопасности объектов и сегментов информационной инфраструктуры как технологической основы пространства использования ИКТ (ИКТ-среды).

КЗСУ на основе ИОК в современных информационных системах обладают архитектурой, проектирование которой, как показал автор, является сложной научно-технической задачей. В то же время количество работ, посвященных изучению проблем построения КЗСУ, способных противостоять угрозам нарушения безопасности использования систем электронного документооборота, явно недостаточно.

С этой точки зрения актуальность работы Мельникова Д.А, посвященная изучению проблем построения КЗСУ на основе ИОК для ИТС различного назначения, сомнения не вызывает.

Краткое содержание работы. Диссертация состоит из введения, шести глав основного материала, заключения и трёх приложений.

В введении обоснована актуальность темы диссертации, проведен краткий анализ проблем обеспечения информационной безопасности информационно-телекоммуникационной инфраструктуры (ИТИ) цифровой экономики, сформулирована научно-техническая проблема и проведен анализ ее состояния. Кроме того, в введении сформулирована цель исследования, определены решаемые задачи и общие подходы для достижения поставленной цели, а также приведены сведения о теоретической и практической значимости работы, методологии и методах проведения исследования и научные положения, выносимые на защиту.

В первой главе проведен общий анализ тенденций цифровой трансформации общества, реализации программы «Цифровая экономика Российской Федерации», а также угрозы информационной безопасности (ИБ) страны, возникающие на этом пути. По мнению автора, для достижения позитивного эффекта от выполнения программы «Цифровая экономика» представляется необходимым создание информационно-технологической структуры обеспечения ИБ, нацеленной на противодействие проявлению угроз нанесения ущерба интересам человека, общества и государства в информационной сфере.

Проведен анализ угроз безопасности использования ИТИ цифровой экономики и входящей в нее информационно-технологической структуры ИБ.

Кроме того, проведен анализ проблемы обеспечения доверия к ИТИ цифровой экономики. Показано, что, разработка и развитие концепции ИОК и создание на её основе системы доверия к ИТИ цифровой экономики РФ становится важной стратегической задачей.

Во второй главе разработана концепция «доверие» применительно к информационно-коммуникационной системе, построенная на основе имитационного моделирования отдельных фрагментов интеллектуальной деятельности человека. Формализация этой концепции осуществлена на основе математического аппарата субъективной логики (СЛ). Показано, что требования к обеспечению «доверия» отражают «сопротивляемость» ИТС к злонамеренным действиям (например, атакам). В работе на основе распространения понятия субъективного «доверия» на социальные взаимодействия приведены определения «доверенная сторона», «доверяющая сторона» и «преступное намерение», рассмотрены два класса «доверенных сторон» – «мыслящий субъект» и «логический объект».

В третьей главе исследована архитектура ИОК, упрощающая переход субъектов экономической деятельности к использованию электронного документооборота и предоставляющая этим субъектам комплекс услуг по обеспечению ИБ. Предложена новая архитектура ИОК, обеспечивающая «привязывание» открытых криптографических ключей к субъектам эконо-

мической деятельности и позволяющая взаимодействующим субъектам проверять существование такой «привязки». Проведен анализ основных существующих архитектур ИОК, в том числе архитектур ИОК, используемых в США и Западной Европе.

В четвертой главе осуществлен анализ проблемы обеспечения субъектов экономического взаимодействия параметрами подлинности (ПП) сертификата открытого ключа в системах аутентификации на основе ИОК. Возможность отображать и распознавать субъектов в ИТС имеет важное значение для систем организации электронного документооборота, а также для функционирования систем обеспечения ИБ ИТС.

Рассмотрены системы обеспечения пользователей ПП. Показано, что для устойчивой работы системы необходимо осуществлять обоюдную аутентификацию взаимодействующих субъектов. Кроме того, показано, что современные системы аутентификации при предоставлении электронных услуг не обеспечивают аутентификацию провайдеров электронных услуг. Обоснован вывод о том, что для ИОК в ИКИ цифровой экономики наиболее перспективной и востребованной является архитектура с центром подтверждения подлинности (ЦПП).

В пятой главе представлены основные понятия и определения СЛ, составляющие математический аппарат синтеза сетей субъективного доверия. Была синтезирована, а затем проанализирована модель системы субъективного доверия на основе ИОК. Предложено данную модель отображать в виде последовательно-параллельного орграфа. Кроме того, предложена усовершенствованная, функционально-структурная и географически-распределённая модель системы субъективного доверия, а также новая функция, которая отсутствует в известных моделях доверия - проверка законности (обоснованности) издания сертификата открытого ключа ($СЕРТ_{ОК}$). Представлены методы защиты пользователей ИОК ИТС от угроз нарушения достоверности сертификата ключа и описаны средства, реализующие указанные методы. Разработаны предложения по использованию международных стандартов для глобальной идентификации Интернет-пользователей и провайдеров коммуникационных услуг в Интернет-сети, реализация которых, по мнению автора, позволит существенно снизить уровень киберпреступности и обеспечить безопасность использования национальной ИТИ цифровой экономики.

В шестой главе представлены сведения о реализации полученных в работе результатов, а также сформулированы практические задачи построения системы субъективного доверия на основе объединения ИОК в интересах ИТИ цифровой экономики в Российской Федерации. Отмечено, что результаты исследований нашли своё отражение в четырёх учебниках и учебных пособиях, которые рекомендованы к использованию во многих ВУЗах России при подготовке специалистов по направлению «Информационная безопасность».

В заключении и основных выводах обобщены теоретические и практические результаты работы, а также намечены возможные направления дальнейших исследований.

В первом приложении представлена директива президента США «О государственном регулировании в области шифрования информации» («Public Encryption Management» 15(16).03.1993); во втором приложении – таблица операторов субъективной логики; в третьем приложении – копии актов о внедрении и использовании результатов исследований.

В целом диссертация написана корректным техническим языком и включает большое количество иллюстраций, хотя большое количество используемых сокращений затрудняет понимание логики рассуждений автора. Выводы по каждой главе и всей работе вполне корректно отражают полученные результаты.

Новизна и достоверность результатов и положений диссертации. *Научная новизна* результатов и положений диссертации, полученных лично автором, заключается в том, что

совокупность полученных научных результатов может рассматриваться как основа методологии построения специализированного структурного элемента ИТС цифровой экономики – системы управления криптографической защитой в информационно-телекоммуникационных системах различных уровней управления экономической деятельностью, базирующейся на рациональном выборе конкретных методов, принципов, способов и средств анализа структуры системы субъективного доверия к сертификатам открытых ключей и на научно обоснованных технических, технологических и организационных решениях, внедрение которых вносит значительный вклад в решение проблем обеспечения ИБ ИТС систем цифровой экономики.

Достоверность теоретических и прикладных результатов работы обеспечивается корректностью систематизации частных научных задач, решаемых в рамках научной проблемы, а также постановок и обоснованием условий решения частных научных задач, доказательствами формулируемых в работе утверждений, а также апробацией результатов при практическом внедрении полученных результатов по построению системы управления криптографической защитой в научно-исследовательской и практической деятельности ряда организаций.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации. Исследование опиралось на общенаучные и специальные методы познания и базировалось на общей методологии построения систем, общей теории систем, теории управления, теории информационно-телекоммуникационных систем и сетей, а также на российских ГОСТах и международных стандартах, подтверждено апробацией научных результатов в печати и на научных конференциях. Результаты исследования подтверждены корректными выводами основных утверждений, сформулированных в работе, использованием известных, проверенных на практике, методов и лучших практик, соответствием предложенных усовершенствований общим архитектурным принципам построения ИТКС, а также результатами их практического внедрения.

Ценность результатов работы для науки и практики. В диссертации сформулированы ***выносимые на защиту положения***, которые создают научную основу для развития системы управления криптографической защитой в ИТС цифровой экономики и, в частности, следующие:

1. Архитектура системы субъективного доверия к сертификатам открытых ключей в ИТС цифровой экономики, при синтезе которой использовался математический аппарат субъективной логики, а также предложена усовершенствованная версия этой архитектуры, базирующаяся ни концепции иерархического распределенного центра подтверждения подлинности сертификатов.

2. Функционально-структурная и географически-распределённая архитектура системы субъективного доверия к сертификатам открытых ключей в ИТС цифровой экономики.

3. Требование включения в состав системы субъективного доверия к сертификатам открытых ключей функции проверки правомерности выпуска сертификата.

4. Метод парирования угроз безопасности, связанных с выпуском удостоверяющим центром фальсифицированных сертификатов открытых ключей.

5. Метод распознавания поддельных (мошеннических) *Web*-сайтов.

6. Модель единой системы идентификации удостоверяющих центров на основе логической характеристики следующего поколения протокола Интернета - IPv6-протокола, реализация которой может повысить безопасность использования глобальной информационной инфраструктуры.

Теоретическая значимость работы состоит в том, что сформулированные в ней положения развивают теорию построения КЗСУ в современных ИТС, создавая основу для выявления уязвимостей в ИОК и противодействия злонамеренному использованию этих уязвимостей, а также для синтеза рациональной системы субъективного доверия к сертификатам открытых ключей в ИТС.

Разработанные в диссертационной работе Мельникова Д.А. результаты имеют существенную ***практическую ценность***. Она заключается в том, что применение научных положений, сформулированных лично автором, будет содействовать повышению защищенности от угроз злонамеренного использования ИКТ информационных и телекоммуникационных систем цифровой экономики.

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 ВУЗов (с грифами). Следовательно, можно заключить, что основные результаты и выводы диссертации строго обоснованы, являются новыми и получены автором самостоятельно и в соавторстве (автор указал свой личный вклад).

Соответствие содержания автореферата основным положениям диссертации. Автореферат достаточно полно и адекватно отражает содержание решаемой в диссертации научно-технической проблемы – построение системы доверия на основе ИОК для ИТИЦЭ с целью парирования угроз ИБ, связанных с переходом экономики Российской Федерации на «цифровые рельсы», и защиты прав и законных интересов личности, бизнеса и государства.

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

Замечания по диссертации. Следует отметить следующие основные недостатки работы:

1. Не рассмотрены проблемы получения исходных данных, необходимых для практического применения математической модели на основе операторов субъективной логики, что затрудняет оценку практической реализуемости предложенного автором метода синтеза рациональной архитектуры системы субъективного доверия.

2. В работе не приведены прогнозные оценки влияния реализации предложенных автором методических подходов к оптимизации архитектуры ИОК на динамику изменения опасности угроз ИБ ИТС цифровой экономики, например, на снижение темпов роста компьютерной преступности, равно как и на повышение безопасности использования ИКТ-среды, хотя интуитивно такое влияние представляется весьма вероятным.

Указанные замечания несколько снижают ценность отдельных положений диссертационного исследования, но не являются определяющими при оценке ее научно-квалификационного уровня в целом.

Заключение по работе:

Диссертационная работа Мельникова Дмитрия Анатольевича представляет собой законченную научно-квалификационную работу, в которой на основе выполненных автором ис-

следований *разработаны научно обоснованные теоретические положения по повышению доверия к сертификатам открытых ключей в информационно-телекоммуникационной системе цифровой экономики, совокупность которых можно квалифицировать как новое крупное научное достижение*, оформлена согласно ГОСТ Р 7.0.11-2011 и, таким образом, полностью удовлетворяет требованиям «Положения о присуждении учёных степеней», утверждённого Постановлением Правительства Российской Федерации № 842 от 24.09.2013 (ред. от 01.10.2018, с изм. от 26.05.2020), к диссертациям на соискание учёной степени доктора наук, а её автор – Мельников Дмитрий Анатольевич – заслуживает присуждения ему учёной степени доктора технических наук.

ОФИЦИАЛЬНЫЙ ОППОНЕНТ:

Стрельцов Анатолий Александрович
МГУ имени М.В. Ломоносова, факультет «Вычислительная математика и кибернетика», ведущий научный сотрудник Центра проблем информационной безопасности,
член-корреспондент Академии криптографии РФ, заслуженный деятель науки Российской Федерации, профессор,
доктор технических наук, 20.02.12 – Военная кибернетика (в настоящее время – Системный анализ, исследование операций, моделирование боевых действий и систем военного назначения, компьютерные технологии в военном деле).
доктор юридических наук, 05.13.19 – «Методы и системы защиты информации, информационная безопасность»,
Тел. +7(910)441-40-01, email: aa.strelstov@yandex.ru

_____ Стрельцов Анатолий Александрович

«1» августа 2022 г.

Подпись Стрельцова Анатолия Александровича удостоверяю.

и.о. Начальника отдела кадров факультета «Вычислительная математика и кибернетика»
МГУ имени М.В. Ломоносова

Ревина Альбина Андреевна

Сведения об организации:
Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В. Ломоносова» (МГУ имени М.В. Ломоносова)
119991, г. Москва, Ленинские горы, д. 1
+7 (495) 939-10-00, info@ rector.msu.ru