Предисловие

Книга предназначена учёным и специалистам в области информационной безопасности и инфраструктур открытых ключей, занимающихся разработкой и построением систем обеспечения информационной безопасности и доверия в интересах цифровой экономики Российской Федерации. Также она будет интересна научно-педагогическим работникам, аспирантам и студентам старших курсов государственных образовательных учреждений высшего профессионального образования, обучающимся по направлениям подготовки 10.00.00 «Информационная безопасность» и 38.00.00 «Экономика и управление».

Первая глава посвящена анализу Национальной Программы «Цифровая экономика Российской Федерации» (далее — Программа). В частности, показано, что современное развитие российского общества направлено на *цифровизацию* (*цифровую трансформацию*) всех его сфер, включая экономику, науку, здравоохранение, образование, культуру и т. д. Вместе с тем цели, содержащиеся в Программе, никак не конкретизируются, т. е. не определены. Более того, Программа исходит не из того, чтобы что-то производить, уметь, создавать новое, а из приоритета предоставления услуг по сравнению с производством и интересов «квалифицированного потребителя». Также представлен анализ угроз национальной безопасности Российской Федерации в связи с цифровой трансформацией, рассмотрены возможные пути их нейтрализации и проанализированы информационно-технологическая инфраструктура цифровой экономики (ИТИЦЭ) и российская инфраструктура открытых ключей (ИОК), которая *не способна парировать различные киберпреступления*!

Вторая глава посвящена общетеоретическим аспектам доверия. Она сфокусирована на фундаментальной проблеме точного понимания доверия в реальном мире, и в частности в информационно-технологических системах/сетях (ИТС). Эта тема лежит на стыке двух научных направлений теории распределённых

вычислений и ИБ. Было проанализировано доверие в условиях ограниченных знаний в области психологии и поведенческой науки. Сделан вывод о том, что появление нового научного направления — *субъективной логики* (СЛ) — послужило прорывом в исследовании доверия в ИТС и, что очень важно, проблем обеспечения ИБ. Аргументы в СЛ называются *субъективными мнениями* (или просто *мнениями*). При этом мнение может содержать *множество неопределённости* в смысле неопределённости вероятностей.

В **третьей главе** рассмотрены основные различия между бумажным и электронным документооборотом (БДО и ЭДО). Электронные и бумажные документы способны выполнять абсолютно разные функции в юриспруденции и бизнесе. Глобальная информатизация позволила «перевести» БДО в ИТС («на электронные рельсы»), реализующие ЭДО, а ИОК способна их ускорить и упростить. Современные «электронные коммерческие системы и системы предоставления услуг» зависят от целостности и подлинности данных. Эти оба свойства данных могут быть реализованы ИОК на основе привязки электронной подписи (ЭП) к автору ЭП и обеспечения гарантий того, что ЭП не может быть подделана (сфальсифицирована). Рассмотрены основные архитектуры ИОК и форматы данных, используемые в ИОК, а также североамериканская и западноевропейская модели организации ИОК.

Также проанализированы проблемы и риски функционирования ИОК и её пользователей. Кроме того, сделан вывод, что системы электронной коммерции и предоставления электронных услуг нуждаются в ИОК.

В **четвёртой главе** рассмотрены проблемы обеспечения параметрами подлинности. Показано, что одним из фундаментальных понятий, используемых в системах аутентификации на основе ИОК, является *параметр подлинности* (ПП). Наличие возможности отображать и распознавать объекты в ИТС имеет основополагающее значение для систем электронного взаимодействия и сотрудничества и является функциональным фундаментом практически всех систем обеспечения безопасности. Далее рассмотрены системы обеспечения пользователей и провайдеров электронных услуг (ПЭУ) параметрами подлинности.

Также проанализированы структуры (системы) доверия на основе инфраструктуры открытых ключей. ИОК позволяет распространять доверие оттуда, где оно существует, туда, где оно

необходимо. Рассмотрены различные модели архитектур ИОК. Для каждой из них указаны проблемы обеспечения доверия, их преимущества и недостатки. Сделан вывод о том, что в современных условиях модель с центром подтверждения подлинности (ЦПП) является наиболее перспективной и востребованной. Также определены основные направления развития и совершенствования ИОК.

В **пятой главе** представлены элементы СЛ, составляющие математический аппарат синтеза сетей субъективного доверия (ССД). Также представлены алгоритмы синтеза и анализа ССД. Были определены исходные условия, количественные и качественные показатели, необходимые для синтеза модели национальной системы доверия на основе ИОК. Используя аппарат СЛ и эвристический метод поиска сети доверия, *была синтезирована модель национальной системы доверия на основе ИОК*. С эвристической точки зрения, было определено, что использование единого ЦПП для всех российских удостоверяющих центров (УЦ) — наиболее приемлемое решение для создания национальной системы доверия на основе ИОК.

На основании синтезированной модели были разработаны функционально-структурная и географически-распределённая модели национальной системы доверия на основе ИОК. Также было сформулировано главное требование к национальной системе доверия на основе ИОК.

В рамках исследований разработаны методы защиты пользователей ИОК, а также метод решения проблемы обеспечения глобальными идентификаторами в мировом киберпространстве на основе использования логической характеристики IPv6-протокола.

Авторы выражают глубокую благодарность академику Академии криптографии РФ В.И. Будзко, члену-корреспонденту Академии криптографии РФ А.А. Стрельцову, профессору В.П. Лосю и профессору С.А. Сизову за их критический и скрупулёзный анализ рукописи, позволивший, несомненно, повысить её качество.

При подготовке рукописи к изданию большую поддержку авторам оказали В.А. Григорьев, В.С. Горбатов, В.Н. Захаров, В.И. Королёв, А.И. Костогрызов, Г.О. Крылов, Н.Г. Милославская, Р.В. Разумчик, В.М. Фомичёв. Высказанные ими советы, замечания и предложения были с благодарностью приняты и учтены.