Предисловие

В настоящее время национальная программа «Цифровая экономика» активно реализуется на территории нашей страны. Цифровизацией охвачены практически все сферы жизнедеятельности общества, государства и личности. Очевидным для многих стал неоспоримый факт появления практически ежедневных новых решений в информационной сфере, управлении экономикой страны, сложными техническими объектами и пр. Интернет вещей, искусственный интеллект, Большие данные, облачные вычисления вошли в привычный словесный обиход. Однако появление новых информационных технологий неразрывно связано с увеличением числа противоправных действий злоумышленников и увеличением количества преступлений в информационной сфере. Следует признать факт необходимости создания отечественных решений в противодействие этим атакам, создание надежных и доверенных отечественных систем, элементов и программных продуктов, обеспечивающих взаимодействие участников информационного обмена в цифровой среде с заданным уровнем безопасности. Особенно это важно, когда речь идет о цифровизации деятельности объектов критической инфраструктуры, поскольку к ней предъявляются повышенные требования по кибербезопасности. Например, по данным Европейского агентства по кибербезопасности (ENISA), из-за кибератак экономика Евросоюза ежегодно теряет около $400 млрд. На повестке дня остро стоит вопрос обеспечения цифрового суверенитета страны. Достижение целей Программы «Цифровая экономика» и, в частности, решение проблематики, связанной с информационной безопасностью, невозможно достичь без обоснованных научных исследований, апробированных подходов, методологий и решений.

Именно развитию теории и практики идентификации и аутентификации в цифровом мире как одного из ключевых элементов технологии доверенного взаимодействия посвящена эта книга. Авторы убедительно показывают, что идентификация и аутентификация в цифровом мире являются основой доверия при переходе к цифровому государству.

В книге авторы предлагают оригинальную методологию построения иерархии уровней доверия к результатам идентификации и аутентификации субъектов доступа, в том числе при удаленном электронном взаимодействии. На основе анализа рисков и учета специфики процессов идентификации и аутентификации предложена методика формирования уровней доверия к результатам идентификации и аутентификации в информационных системах различного назначения с целью повышения доверия к результатам идентификации и аутентификации в составе систем управления доступом пользователей.

Авторам удалось предложить не только критерии и показатели доверия к результатам идентификации и аутентификации, но и методику оценки рисков, а также методы и модели по совершенствованию способов и средств защиты информации применительно к задаче идентификации и аутентификации участников удаленного электронного взаимодействия.

Например, для оценки рисков идентификации и аутентификации разработаны многоуровневые модели анализа рисков нарушения информационной безопасности, которые дают возможность определить вероятностные характеристики разнородных по длительности и повторяемости процедур идентификации и аутентификации в корпоративных и открытых ИС. Это позволило доказать, что высокий уровень рисков аутентификации наиболее вероятен при регистрации нового пользователя информационной системы, генерации, хранении и предъявлении аутентификационной информации, а также ее обмене при взаимодействии сторон в процессе аутентификации.

В книге предложен интересный математический аппарат оценки функциональной надежности и безопасности процессов аутентификации с учетом надежности не аппаратной части, а услуг, предоставляемых информационной системой, а также оценки достоверности результатов идентификации при удаленном электронном взаимодействии, что позволяет формировать заданные уровни надежности результатов идентификации и аутентификации в информационных системах различного назначения.

Особого внимания заслуживает факт рассмотрения авторами вопросов обеспечения юридической силы и значимости электронных документов. Показано, что аналогом реквизитов бумажных документов являются сервисы безопасности, применяемые для создания, оформления и подписи электронного документа, а необходимым и достаточным для большинства операций с электронными документами является набор сервисов безопасности, состоящий из аутентификации ав-

тора подписи, электронной подписи, меток доверенного времени, валидации сертификата ключа проверки электронной подписи, проверки полномочий на подпись и гарантированной доставки документов и сообщений. Перспективным направлением развития цифрового общества и цифровой экономики является практическое развитие этих сервисов безопасности в доверенном состоянии, что позволит обеспечивать электронным документам юридическую силу и возможность перехода от бумажного документооборота к электронному документообороту с сохранением заданного, как и для бумажных документов, уровня доверия к электронным документам.

Рассмотрена роль идентификации и аутентификации при построении платежных систем, систем Интернета вещей, а также защиты персональных данных при переходе к облачным вычислениям. Проводимые авторами изыскания синхронизированы с современным уровнем международных и российских научных исследований в области идентификации и аутентификации, проводимых в том числе Академией криптографии Российской Федерации. Автором книги представлено современное состояние стандартов национальной системы ГОСТ Р по идентификации и аутентификации.

Уверен, что книга будет интересна и полезна не только специалистам в области обеспечения кибербезопасности, защиты информации, но и широкому кругу читателей, аспирантам и студентам, которые интересуются вопросами информационной безопасности.

Президент Академии криптографии РФ,
действительный член Академии криптографии РФ,
доктор физико-математических наук
Шойтов Александр Михайлович