СВЕДЕНИЯ О ПРИНЯТЫХ НАЦИОНАЛЬНЫХ И МЕЖДУНАРОДНЫХ СТАНДАРТАХ ЗА 1 КВАРТАЛ 2025 ГОДА

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Настоящие материалы подготовлены в целях информационного обеспечения организаций-членов технического комитета по стандартизации «Защита информации» (ТК 362) сведениями о принятых с января по март 2025 года национальных и международных стандартах в области защиты информации (ЗИ), а также об основных направлениях работ в рамках деятельности Международной организации по стандартизации (ИСО) и (или) Международной электротехнической комиссии (МЭК) по совершенствованию международной системы стандартов в области ЗИ.

Настоящие материалы включают:

сведения о принятых с января по март 2025 года стандартах;

обзор результатов деятельности (с января по март 2025 года) подкомитета 27 «Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности» совместного технического комитета 1 «Информационные технологии» ИСО/МЭК (ПК 27 СТК 1 ИСО/МЭК) в части совершенствования международных стандартов в области ЗИ за отчетный период.

Материалы подготовлены на основе данных Росстандарта, представленных на официальном сайте (www.rst.gov.ru) и в Федеральной государственной информационной системе Росстандарта ФГИС «Береста» (www.fgis.gost.ru), а также на официальных сайтах ИСО и МЭК (www.iso.org, www.iec.ch) и аннотированных переводов англоязычных версий стандартов с последующим сравнением номенклатуры действующих и разрабатываемых национальных стандартов (аналогов международным).

Обзор результатов деятельности ПК 27 СТК 1 ИСО/МЭК проведен на основе сбора данных, представленных на официальных сайтах ИСО и МЭК (www.iso.org, www.iec.ch), и аннотированных переводов англоязычных версий стандартов с последующим сравнением номенклатуры действующих и разрабатываемых национальных стандартов (аналогов международным). Результаты обзора деятельности ПК 27 СТК 1 ИСО/МЭК представлены в разделе 2.

1 Сведения о принятых национальных и международных стандартах за 1 квартал 2025 года

С января по март 2025 года Росстандартом утверждены два национальных стандарта в области ЗИ: ГОСТ Р 59453.3-2025 «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке» (далее – ГОСТ Р 59453.3), ГОСТ Р 59453.4-2025 «Защита информации. Формальная модель управления доступом. Часть 4. Рекомендации по верификации средства защиты информации, реализующего политики управления доступом, на основе формализованных описаний модели управления доступом» (далее – ГОСТ Р 59453.4) [1, 2], а ИСО/МЭК международные стандарты в области ЗИ не утверждались [3-5].

Вышеуказанные стандарты в соответствии с их назначением и содержанием относятся к следующей группе [6, 7] – стандарты, устанавливающие требования по безопасности информационных и коммуникационных технологий (ИКТ) (национальные стандарты ГОСТ Р 59453.3-2025, ГОСТ Р 59453.4-2025).

1.1 Стандарты, устанавливающие требования по безопасности информационных и коммуникационных технологий

С января по март 2025 года Росстандартом утверждены два национальных стандарта, устанавливающие требования по безопасности информационных и коммуникационных технологий (ИКТ).

1.1.1 Национальный стандарт ГОСТ Р 59453.3-2025 «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке» устанавливает рекомендации по разработке и описанию формальных моделей управления доступом, на основе которых разрабатываются средства защиты информации, реализующие политики управления доступом.

Разработка формальных моделей управления доступом в большинстве случаев является комплексным многоэтапным процессом, от качества выполнения

которого зависит эффективность реализации моделируемым средством защиты информации политик управления доступом.

Рекомендуются следующие этапы разработки и описания формальной модели управления доступом:

определение границ моделирования средства защиты информации;

определение видов политик управления доступом, рассматриваемых при моделировании и реализуемых средством защиты информации;

выбор технологий, инструментальных средств (при необходимости) и практических приемов разработки формальной модели;

описание формальной модели;

описание и доказательство выполнения условий безопасности, в том числе, при верификации формальной модели.

На этапе определения границ моделирования средства защиты информации, реализующего политики управления доступом, рекомендуется зафиксировать используемые при этом ограничения, допущения или исключения, при этом показать их влияние на снижение сложности описания формальной модели при обеспечении его соответствия моделируемому средству защиты информации, в том числе следует зафиксировать:

назначение формальной модели для существующего или проектируемого средства защиты информации, наличие или отсутствие возможности внесения изменений в средство защиты информации согласно разрабатываемой формальной модели;

политики управления доступом, реализуемые средством защиты информации и регламентирующие предоставление доступов между всеми компонентами среды функционирования средства защиты информации или только их подмножеством;

существенные особенности среды функционирования средства защиты информации (наличие сетевой инфраструктуры, применение технологий виртуализации или другие особенности), учитываемые при разработке

формальной модели.

При определении рассматриваемых при моделировании видов реализуемых средством защиты информации политик управления доступом рекомендуется использовать политики, определенные в ГОСТ Р 59453.1 «Защита информации. Формальная модель управления доступом. Часть 1. Общие положения» (далее – ГОСТ Р 59453.1) (политики дискреционного управления доступом, мандатного контроля целостности, мандатного управления доступом и ролевого управления доступом).

Для описания формальной модели управления доступом рекомендуется использовать математический и, как минимум, один из формализованных (машиночитаемых) языков. Это обусловлено тем, что применение математического описания формальной модели всегда допускает полную независимую от разработчика проверку корректности этого описания, заданных в формальной модели условий безопасности, а также всех выполненных в модели доказательств.

При выборе инструментальных средств разработки формальной модели управления доступом целесообразно исходить из возможности их использования для автоматической верификации модели. В связи с этим инструментальные средства, используемые для автоматической верификации формальной модели управления доступом, должны удовлетворять критериям, установленным в ГОСТ Р 59453.2 «Защита информации. Формальная модель управления доступом. Часть 2. Рекомендации по верификации формальной модели управления доступом» (далее – ГОСТ Р 59453.2).

Непосредственное описание формальной модели управления доступом рекомендуется начинать с состояний абстрактного автомата, которые должны включать элементы:

множество учетных записей пользователей;

множество субъектов доступа;

множество объектов доступа;

заданное на множестве объектов доступа отношение иерархии;

множество реализуемых доступов субъектов к объектам доступа и используемые для задания доступов множества;

множества информационных потоков;

условия внутренней и взаимной корректности (согласованности) используемых для описания состояний абстрактного автомата множеств.

При разработке формальной модели управления доступом должны быть описаны условия безопасности состояний абстрактного автомата и условия безопасности переходов из состояний в состояния абстрактного автомата согласно ГОСТ Р 59453.1. При этом следует формулировать условия безопасности так, чтобы проверка их выполнения являлась алгоритмически разрешимой задачей (для чего может потребоваться явно задавать необходимые допущения или исключения из этих условий).

В стандарте используются нормативные ссылки на национальные стандарты ГОСТ Р 59453.1, ГОСТ Р 59453.2 (в части соответствия терминологии и определения критериев, которым должны соответствовать описания формальных моделей управления доступом).

Стандарт предназначен для разработчиков средств защиты информации, реализующих политики управления доступом, а также для органов по сертификации и испытательных лабораторий при проведении сертификации средств защиты информации, реализующих политики управления доступом.

Национальный стандарт ГОСТ Р 59453.3-2025 разработан Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Институтом системного программирования им. В.П. Иванникова Российской академии наук (ИСП РАН), Обществом с ограниченной ответственностью «РусБИТех-Астра» (ООО «РусБИТех-Астра»), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») и утвержден приказом руководителя Росстандарта № 111-ст от 10 марта 2025 г. Дата введения в действие 31 марта 2025 г.

1.1.2 Национальный стандарт ГОСТ Р 59453.4-2025 «Защита информации. Формальная модель управления доступом. Часть 4. Рекомендации по верификации средства защиты информации, реализующего политики управления доступом, на основе формализованных описаний модели управления доступом» устанавливает рекомендации по верификации средств защиты информации, реализующих политики управления доступом, на основе формализованного описания модели управления доступом, а также доказательства или демонстрации того, что исследуемое средство защиты информации в действительности реализует формальную модель управления доступом.

Рекомендации стандарта по верификации средств защиты информации, реализующих политики управления доступом на основе формализованного описания модели управления доступом, направлены на обеспечение соответствия функционирования средства защиты информации формальной модели управления доступом, разработанной в соответствии с критериями и рекомендациями ГОСТ Р 59453.1, ГОСТ Р 59453.2, ГОСТ Р 59453.3.

Рекомендуются следующие этапы верификации средства защиты информации, реализующего политики управления доступом, на основе формализованного описания модели управления доступом:

проведение архитектурного анализа средства защиты информации и исследование наличия модуля безопасности или группы функций, которые могут рассматриваться как модуль безопасности (возможность определения интерфейсов взаимодействия такого модуля с его окружением);

принятие решения о проведении модульной верификации или отказе от нее;

выбор языков разработки формальных спецификации и инструментов разработки и верификации;

выбор критериев и методики оценки полноты верификации (оценки верификационного покрытия);

разработка формальной спецификации интерфейсов средства защиты информации, реализующих политики управления доступом, и ее верификация;

верификация средства защиты информации, проверка соответствия поведения средства защиты информации формальной модели управления доступом;

разработка формальной спецификации интерфейсов модуля безопасности (если ставится задача верификации модуля безопасности) и ее верификация;

верификация модуля безопасности (если ставится задача верификации модуля безопасности).

В описании результатов верификации должны быть представлены:

анализ архитектуры средства защиты информации, обоснование вывода о наличии или отсутствии возможности модульной верификации модуля безопасности;

описание формальной спецификации интерфейсов средства защиты информации;

сопоставление структуры формальной модели управления доступом и формальной спецификации средства защиты информации;

обоснование выбора способа демонстрации того, что формальная спецификация соответствует формальной модели управления доступом;

результаты проведения верификации.

Стандарт предназначен для разработчиков средств защиты информации, реализующих политики управления доступом, а также для органов по сертификации и испытательных лабораторий при проведении сертификации средств защиты информации, реализующих политики управления доступом.

Национальный стандарт ГОСТ Р 59453.4-2025 разработан Федеральной службой по техническому и экспортному контролю (ФСТЭК России), Институтом системного программирования им. В.П. Иванникова Российской академии наук (ИСП РАН), Обществом с ограниченной ответственностью «РусБИТех-Астра» (ООО «РусБИТех-Астра»), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России») и утвержден приказом руководителя Росстандарта № 112-ст от 10 марта 2025 г. Дата введения в действие 31 марта 2025 г.

2 Обзор результатов деятельности подкомитета 27 «Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности» совместного технического комитета 1 «Информационные технологии» Международной организации по стандартизации и Международной электротехнической комиссии в части совершенствования международных стандартов в области защиты информации

В настоящее время, в целях обеспечения технологического суверенитета Российской Федерации за счет импортозамещения по приоритетным направлениям, закрепленным в Указе Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года», работы по стандартизации в области защиты информации должны базироваться преимущественно на национальных нормативных правовых актах и методических документах в данной области. Однако в интересах учета при разработке национальных документов по стандартизации перспективных практик в области информационной безопасности, закрепленных в международных документах по стандартизации, необходимо своевременное отслеживание проводимых на международном уровне работ по стандартизации в области ЗИ и обеспечения безопасности ИТ.

Международная стандартизация в области ЗИ и обеспечения безопасности ИТ осуществляется в рамках деятельности ПК 27 СТК 1 ИСО/МЭК [3-5] по следующим основным направлениям [8]:

безопасность информации, обрабатываемой в автоматизированных системах (стандарт ISO/IEC TR 19791:2010);

безопасность информационных и коммуникационных технологий (стандарты серии 18000, 19000, 20000, 29000, 30000, а также стандарты 27031 и выше);

менеджмент ИБ (стандарты 27000-27023);

критерии безопасности ИТ (стандарты серии 15000, 19000).

В настоящее время в рамках указанных направлений стандартизации (по состоянию на март 2025 года) действуют 110 международных стандартов и документов, 23 из которых пересматриваются. Разрабатываются 12 международных стандартов и документов.

Пять международных стандартов и документов, на основе которых разработаны действующие национальные стандарты, отменены.

В рассматриваемый отчетный период основная деятельность ПК 27 СТК 1 ИСО/МЭК была направлена на развитие системы стандартов по следующим направлениям:

безопасность информационных и коммуникационных технологий;

менеджмент ИБ;

критерии безопасности ИТ.

Состояние разработки международных стандартов характеризуется стадиями работ, представленными в таблице 1.

Таблица 1 – Основные стадии работ по разработке международных стандартов

№ п/п	Наименование стадии	Обозначение стадии
1	Предложение новой темы для разработки	NP
2	Рабочий проект	WD
3	Проект комитета	CD
4	Проект международного стандарта	DIS
5	Окончательный проект международного стандарта	FDIS

По направлению *безопасность информационных и коммуникационных технологий* (в том числе по вопросам установления требований к таким технологиям, как: «Интернет вещей» (Internet of things), «Умные города» (Smart cities) и «Большие данные» (Big data), Искусственный интеллект» (Artificial intelligence) предложено шесть новых тем (NP) для разработки международных стандартов и документов, на стадии рабочего проекта (WD) ведется разработка (пересмотр) пяти международных стандартов, на стадии проекта комитета (CD) ведется разработка

(пересмотр) одного международного стандарта, на стадии проекта международного стандарта (DIS) ведется разработка (пересмотр) двух международных стандартов и документов, на стадии окончательного проекта международного стандарта (FDIS) ведется разработка (пересмотр) одного международного стандарта, готовятся к публикации четыре международных стандарта.

В качестве новых тем (NP) для разработки предложены проекты следующих международных стандартов и документов:

ISO/IEC 5689 «Структура безопасности и варианты использования киберфизических систем» («Security frameworks and use cases for cyber physical systems»);

ISO/IEC TS 7709 «Информационные технологии. Безопасность и конфиденциальность больших данных. Рекомендации по сохранению конфиденциальности и безопасности при обработке данных из множественных источников» («Information technology — Big data security and privacy - Security and privacy-preserving guidelines for multi-sourced data processing»);

ISO/IEC 25093-1 «Компьютерная безопасность. Конфиденциальные вычисления. Часть 1. Обзор и концепции» («Cybersecurity – Confidential computing – Part 1: Overview and concepts»);

ISO/IEC 27045 «Информационные технологии. Безопасность и конфиденциальность больших данных. Рекомендации по управлению рисками, связанными с большими данными» («Information technology – Big data security and privacy – Guidelines for managing big data risks»);

ISO/IEC 27046 «Информационная технология. Обеспечение безопасности и конфиденциальности больших данных. Рекомендации по реализации» («Information technology – Big data security and privacy – Implementation guidelines»);

ISO/IEC 27109 «Обучение и тренинг в сфере компьютерной безопасности» («Cybersecurity education and training»).

На стадии рабочего проекта (WD) ведется разработка следующих международных стандартов и документов:

ISO/IEC 24760-4 «Обеспечение безопасности и конфиденциальности ИТ. Основы управления идентичностью. Часть 4. Аутентификаторы, учетные данные и аутентификация» («IT Security and Privacy – A framework for identity management – Part 4: Authenticators, Credentials and Authentication»);

ISO/IEC 27091 «Компьютерная безопасность и обеспечение конфиденциальности. Искусственный интеллект. Обеспечение конфиденциальности» («Cybersecurity and Privacy – Artificial Intelligence – Privacy protection»);

ISO/IEC 27115 «Оценка компьютерной безопасности систем. Введение и общая структура». («Cybersecurity evaluation of complex systems – Introduction and framework overview»);

ISO/IEC TS 27564 «Конфиденциальность. Руководство по моделированию инженерии конфиденциальности» («Privacy – Guidance on the use of models for engineering»);

ISO/IEC 29115 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к аутентификации объектов и субъектов» («Information technology – Security techniques – Entity authentication assurance framework»).

На стадии проекта комитета (CD) ведется разработка одного международного стандарта – ISO/IEC 5181 «Информационные технологии. Безопасность и обеспечение конфиденциальности. Происхождение данных» («Information technology – Security and privacy – Data provenance»).

На стадии проекта международного стандарта (DIS) ведется разработка (пересмотр) следующих международных стандартов:

ISO/IEC 27028 «Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Руководство по атрибутам стандарта ISO/IEC 27002» («Information security, cyber security and privace protection – Guidance on ISO/IEC 27002 attributes»);

ISO/IEC TR 27103 «Информационная технология. Методы и средства обеспечения безопасности. Компьютерная безопасность и стандарты ИСО и МЭК»

(«Information technology – Security techniques – Cybersecurity and ISO and IEC Standards») (пересмотр ISO/IEC TR 27103:2018).

На стадии окончательного проекта международного стандарта (FDIS) ведется пересмотр одного международного стандарта ISO/IEC 27701 «Информационная технология. Методы и средства обеспечения безопасности. Применение ИСО/МЭК 27001 и ИСО/МЭК 27002 для обеспечения конфиденциальности идентификационных данных. Требования и рекомендации» («Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines») (пересмотр ISO/IEC 27701:2019).

Готовятся к публикации следующие международные стандарты:

ISO/IEC 24760-1 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции» («IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts») (пересмотр ISO/IEC 24760-1:2019);

ISO/IEC 24760-2 «Обеспечение безопасности и конфиденциальности ИТ. Основы управления идентичностью. Часть 2. Базовая архитектура и требования» («IT Security and Privacy – A framework for identity management – Part 2: Reference architecture and requirements») (пересмотр ISO/IEC 24760-2:2015);

ISO/IEC 24760-3 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы» («Information technology – Security techniques – A framework for identity management – Part 3: Practice») (пересмотр ISO/IEC 24760-3:2016);

ISO/IEC 27031 «Информационная технология. Компьютерная безопасность. Готовность информационно-коммуникационных технологий к обеспечению непрерывности бизнеса» («Information technology – Cybersecurity – Information and communication technology readiness for business continuity») (пересмотр ISO/IEC 27031:2011).

По направлению *менеджмент ИБ* на стадии проекта комитета (CD) ведется разработка (пересмотр) двух международных стандартов и документов, на стадии

проекта международного стандарта (DIS) ведется разработка (пересмотр) трех международных стандартов и документов, на стадии окончательного проекта международного стандарта (FDIS) ведется разработка (пересмотр) одного международного стандарта.

На стадии проекта комитета (CD) ведется пересмотр следующих международных стандартов и документов:

ISO/IEC 27000 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (««Information technology – Security techniques –Information security management systems – Overview and vocabulary»);

ISO/IEC TS 27008 «Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности» («Information technology – Security techniques – Guidelines for the assessment of information security controls»).

На стадии проекта международного стандарта (DIS) ведется разработка (пересмотр) следующих международных стандартов и документов:

ISO/IEC TS 27006-2 «Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Часть 2. Система менеджмента конфиденциальной информации» («Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy information management systems») (пересмотр ISO/IEC TS 27006-2:2021);

ISO/IEC 27017 «Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб» («Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services»);

ISO/IEC 29151 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил для защиты персональных данных (персональной идентификационной информации)» («Information technology – Security techniques –

Code of practice for personally identifiable information protection») (пересмотр ISO/IEC 29151:2017).

На стадии окончательного проекта международного стандарта (FDIS) ведется пересмотр одного международного стандарта ISO/IEC 27018 «Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки» («Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors») (пересмотр ISO/IEC 27018:2019).

По направлению *критерии безопасности ИТ* на стадии рабочего проекта (WD) ведется пересмотр одного международного стандарта, на стадии проекта международного стандарта (DIS) ведется пересмотр девяти международных стандартов.

На стадии рабочего проекта (WD) ведется пересмотр одного международного стандарта ISO/IEC 27004 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание» («Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation»).

На стадии проекта международного стандарта (DIS) ведется пересмотр следующих международных стандартов:

ISO/IEC 15408-1 «Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» («Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model» (пересмотр ISO/IEC 15408-1:2022);

ISO/IEC 15408-2 «Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности»

(«Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components») (пересмотр ISO/IEC 15408-2:2022);

ISO/IEC 15408-3 «Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» («Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components») (пересмотр ISO/IEC 15408-3:2022);

ISO/IEC 15408-4 «Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Основы определения (выбора) методов и способов проведения оценки» («Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 4: Framework for the specification of evaluation methods and activities») (пересмотр ISO/IEC 15408-4:2022);

ISO/IEC 15408-5 «Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Типовые пакеты требований безопасности» («Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 5: Pre-defined packages of security requirements») (пересмотр ISO/IEC 15408-5:2022);

ISO/IEC 18045 «Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Методология оценки безопасности информационных технологий» («Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation») (пересмотр ISO/IEC 18045:2022);

ISO/IEC 19896-1 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 1. Введение, основные понятия и общие требования» («IT security techniques – Competence requirements for information security testers and evaluators – Part 1: Introduction, concepts and general requirements») (пересмотр ISO/IEC 19896-1:2018);

ISO/IEC 19896-2 «Методы и средства обеспечения безопасности ИТ. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 2. Требования к знаниям, навыкам и эффективности деятельности специалистов по тестированию ИТ по ИСО/МЭК 19790» («IT security techniques – Competence requirements for information security testers and evaluators – Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers») (пересмотр ISO/IEC 19896-2:2018);

ISO/IEC 19896-3 «Методы и средства обеспечения безопасности ИТ. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 3. Требования к знаниям, навыкам и эффективности деятельности специалистов по оценке безопасности ИТ по ИСО/МЭК 15408» («IT security techniques – Competence requirements for information security testers and evaluators – Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators») (пересмотр ISO/IEC 19896-3:2018).

Сводный перечень действующих и разрабатываемых международных стандартов и документов в области ЗИ и обеспечения безопасности ИТ, а также национальных стандартов, разработанных на основе международных, приведен в таблице 2 и включает:

наименование действующих, разрабатываемых (пересматриваемых) международных стандартов и документов;

данные о наличии национальных стандартов, соответствующих международным стандартам, и их соответствии действующим версиям международных стандартов;

данные о сроках разработки и введения в действие международных стандартов и документов;

дополнительные сведения об актуальности национальных аналогов международных стандартов.

Таблица 2 – Сводный перечень действующих и разрабатываемых международных стандартов и документов в области защиты информации и обеспечения безопасности информационных технологий и их российских аналогов (национальных стандартов, разработанных на основе международных)

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
1	ISO/IEC 5181 «Information technology – Security and privacy – Data provenance» («Информационные технологии. Безопасность и обеспечение конфиденциальности. Происхождение данных») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	CD Проект комитета	2025	
2	ISO/IEC 5689 «Security frameworks and use cases for cyber physical systems» («Структура безопасности и варианты использования киберфизических систем») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	NP Предложен в качестве новой темы для разработки	2026	
3	ISO/IEC TR 5891:2024 «Information security, cybersecurity and privacy protection – Hardware monitoring technology for hardware security assessment» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Технология мониторинга для оценки безопасности аппаратных средств») *действует*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	

* Прочерк означает, что международный стандарт действует, работы по его пересмотру не проводятся

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
4	ISO/IEC TR 5895:2022 «Cybersecurity – Multi-party coordinated vulnerability disclosure and handling» («Компьютерная безопасность. Скоординированное несколькими сторонами обнаружение и обработка уязвимостей») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
5	ISO/IEC TR 6114:2023 «Cybersecurity – Security assurance throughout the product life cycle» («Компьютерная безопасность – Доверие к обеспечению безопасности в течение жизненного цикла изделия») *действует*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	
6	ISO/IEC TS 7709 «Information technology — Big data security and privacy - Security and privacy-preserving guidelines for multi-sourced data processing» («Информационные технологии. Безопасность и конфиденциальность больших данных. Рекомендации по сохранению конфиденциальности и безопасности при обработке данных из множественных источников») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	NP Предложен в качестве новой темы для разработки	2026	
7	ISO/IEC 13335-1:2004 «Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management»	ГОСТ Р ИСО/МЭК 13335-1-2006	-	-	ISO/IEC 13335-1:2004 отменен

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
	(«Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий») *отменен*				
8	ISO/IEC TR 13335-5:2001 «Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security» («Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети») *заменен на ISO/IEC 18028-1:2006*	ГОСТ Р ИСО/МЭК ТО 13335-5-2006	-	-	ISO/IEC 13335-5:2001 заменен на ISO/IEC 18028-1:2006

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
9	ISO/IEC 15408-1:2022 «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель») *старое название:* «Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model» («Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель») *пересматривается*	ГОСТ Р ИСО/МЭК 15408-1-2012	DIS Проект международного стандарта	2025	Национальный стандарт гармонизирован по версии ISO/IEC 15408-1:2009. В рамках деятельности ТК 362 выполнен перевод на русский язык ISO/IEC 15408-1:2022
10	ISO/IEC 15408-2:2022 «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности») *старое название:*	ГОСТ Р ИСО/МЭК 15408-2-2013	DIS Проект международного стандарта	2025	Национальный стандарт гармонизирован по версии ISO/IEC 15408-2:2008. В рамках деятельности ТК 362 выполнен перевод на русский язык ISO/IEC 15408-2:2022

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
	«Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components» («Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности») *пересматривается*				
11	ISO/IEC 15408-3:2022 «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности») *старое название:* «Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components» («Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности») *пересматривается*	ГОСТ Р ИСО/МЭК 15408-3-2013	DIS Проект международного стандарта	2025	Национальный стандарт гармонизирован по версии ISO/IEC 15408-3:2008. Целесообразно выполнить перевод на русский язык ISO/IEC 15408-3:2022

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
12	ISO/IEC 15408-4:2022 «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 4: Framework for the specification of evaluation methods and activities» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 4. Основы определения (выбора) методов и способов проведения оценки») *пересматривается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	DIS Проект международного стандарта	2025	
13	ISO/IEC 15408-5:2022 «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 5: Pre-defined packages of security requirements» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 5. Типовые пакеты требований безопасности») *пересматривается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	DIS Проект международного стандарта	2025	
14	ISO/IEC TR 15443-1:2012 «Information technology – Security techniques – Security assurance framework – Part 1: Introduction and concepts» («Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 1. Обзор и основы») *действует*	ГОСТ Р 54581-2011 / ISO/IEC TR 15443-1:2005	-	-	Национальный стандарт гармонизирован по версии ISO/IEC TR 15443-1:2005. Целесообразно выполнить перевод на русский язык ISO/IEC TR 15443-1:2012

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
15	ISO/IEC TR 15443-2:2012 «Information technology – Security techniques – Security assurance framework – Part 2: Analysis» («Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Анализ») *действует*	ГОСТ Р 54582-2011 / ISO/IEC TR 15443-2:2005	-	-	Национальный стандарт гармонизирован по версии ISO/IEC TR 15443-2:2005. Целесообразно выполнить перевод на русский язык ISO/IEC TR 15443-2:2012
16	ISO/IEC TR 15443-3:2007 «Information technology – Security techniques – A framework for IT security assurance – Part 3: Analysis of assurance methods» («Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия») *отменен*	ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007	-	-	ISO/IEC TR 15443-3:2007 отменен
17	ISO/IEC TR 15446:2017 «Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets» («Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности») *действует*	ГОСТ Р 57628-2017	-	-	Национальный стандарт разработан по версии ISO/IEC TR 15446:2009. Целесообразно выполнить перевод на русский язык ISO/IEC TR 15446:2017

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
18	ISO/IEC TR 18044:2004 «Information technology – Security techniques – Information security incident management» («Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности») *заменен на ISO/IEC 27035-1:2023*	ГОСТ Р ИСО/МЭК ТО 18044-2007	-	-	ISO/IEC TR 18044:2004 заменен на ISO/IEC 27035-1:2023
19	ISO/IEC 18045:2022 «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Methodology for IT security evaluation» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Критерии оценки безопасности информационных технологий. Методология оценки безопасности информационных технологий») *старое название:* «Information technology – Security techniques – Methodology for IT security evaluation» («Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий») *пересматривается*	ГОСТ Р ИСО/МЭК 18045-2013	DIS Проект международного стандарта	2025	Национальный стандарт гармонизирован по версии ISO/IEC 18045:2008. Целесообразно выполнить перевод на русский язык ISO/IEC 18045:2022
20	ISO/IEC 19086-4:2019 «Information technology – Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and of protection of PII» («Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 4. Компоненты	ГОСТ Р ИСО/МЭК 19086-4-2020	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
	информационной безопасности и защиты персональных данных») *действует*				
21	ISO/IEC TS 19249:2017 «Information technology – Security techniques – Catalogue of architectural and design principles for secure products, systems, and applications» («Информационная технология. Методы и средства обеспечения безопасности. Каталог архитектурных принципов и принципов проектирования безопасных продуктов, систем и приложений») *действует*	ГОСТ ISO/IEC TS 19249-2021	-	-	
22	ISO/IEC TS 19608:2018 «Guidance for developing security and privacy functional requirements based on ISO/IEC 15408» («Руководство по разработке функциональных требований по обеспечению безопасности и конфиденциальности идентификационных данных на основе ISO/IEC 15408») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
23	ISO/IEC TR 19791:2010 «Information technology – Security techniques – Security assessment of operational systems» («Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем») *действует*	ГОСТ Р ИСО/МЭК ТО 19791-2008	-	-	Национальный стандарт гармонизирован по версии ISO/IEC TR 19791:2006. Целесообразно выполнить перевод на русский язык ISO/IEC TR 19791:2010
24	ISO/IEC 19896-1:2018 «IT security techniques – Competence requirements for information security testers and evaluators – Part 1: Introduction, concepts and general requirements» («Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 1. Введение, основные понятия и общие требования») *пересматривается*	ГОСТ ISO/IEC 19896-1-2021	DIS Проект международного стандарта	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
25	ISO/IEC 19896-2:2018 «IT security techniques – Competence requirements for information security testers and evaluators – Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers» («Методы и средства обеспечения безопасности ИТ. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 2. Требования к знаниям, навыкам и эффективности деятельности специалистов по тестированию ИТ по ИСО/МЭК 19790») *пересматривается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	DIS Проект международного стандарта	2025	
26	ISO/IEC 19896-3:2018 «IT security techniques – Competence requirements for information security testers and evaluators – Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators» («Методы и средства обеспечения безопасности ИТ. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 3. Требования к знаниям, навыкам и эффективности деятельности специалистов по оценке безопасности ИТ по ИСО/МЭК 15408») *пересматривается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	DIS Проект международного стандарта	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
27	ISO/IEC TR 20004:2015 «Information technology – Security techniques – Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045» («Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045) *действует*	ГОСТ Р 58142-2018 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 1. Использование доступных источников для идентификации потенциальных уязвимостей»; ГОСТ Р 58143-2018 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения»	-	-	
28	ISO/IEC 20547-4:2020 «Information technology – Big data reference architecture – Part 4: Security and privacy» («Информационная технология. Эталонная архитектура больших данных. Часть 4. Безопасность и конфиденциальность») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
29	ISO/IEC 21827:2008 «Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®)» («Информационная технология. Методы и средства обеспечения безопасности. Проектирование безопасности систем. Модель зрелости процесса») *действует*	ГОСТ Р ИСО/МЭК 21827-2010	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
30	ISO/IEC 21878:2018 «Information technology – Security techniques – Security guidelines for design and implementation of virtualized servers» («Информационные технологии. Методы и средства обеспечения безопасности. Руководство по обеспечению безопасности при внедрении серверов виртуализации») *действует*	ГОСТ Р 59163-2020	-	-	
31	ISO/IEC TR 22216:2022 «Information security, cybersecurity and privacy protection – New concepts and changes in ISO/IEC 15408:2022 and ISO/IEC 18045:2022» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Новые принципы и изменения в положениях ISO/IEC 15408:2022 и ISO/IEC 18045:2022») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
32	ISO/IEC TS 23532-1:2021 «Information security, cybersecurity and privacy protection – Requirements for the competence of IT security testing and evaluation laboratories – Part 1: Evaluation for ISO/IEC 15408» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Требования к компетенции испытательных и проводящих оценку безопасности ИТ лабораторий. Часть 1: Оценка безопасности ИТ по ISO/IEC 15408») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
33	ISO/IEC TS 23532-2:2021 «Information security, cybersecurity and privacy protection – Requirements for the competence of IT security testing and evaluation laboratories –Part 2: Testing for ISO/IEC 19790» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Требования к компетенции испытательных и проводящих оценку безопасности ИТ лабораторий. Часть 2: Тестирование безопасности ИТ по ISO/IEC 19790») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
34	ISO/IEC 24392:2023 «Cybersecurity – Security reference model for industrial Internet platform (SRM - IIP)» («Компьютерная безопасность. Эталонная модель обеспечения безопасности для промышленной Интернет-платформы») *действует*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	
35	ISO/IEC 24760-1:2019 «IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts» («Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции») *пересматривается* *ISO/IEC 24760-1:2019/Amd 1:2023* *«IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts Amendment 1"*	ГОСТ Р 59381-2021	Подготовка к публикации	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
36	ISO/IEC 24760-2:2015 «Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements» («Информационные технологии Методы и средства обеспечения безопасности. Основы управления идентичностью Часть 2. Базовая архитектура и требования») *новое название:* «IT Security and Privacy – A framework for identity management – Part 2: Reference architecture and requirements» («Обеспечение безопасности и конфиденциальности ИТ. Основы управления идентичностью. Часть 2. Базовая архитектура и требования») *пересматривается*	ГОСТ ISO/IEC 24760-2-2021	Подготовка к публикации	2025	
37	ISO/IEC 24760-3:2016 «Information technology – Security techniques – A framework for identity management – Part 3: Practice» («Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы») *пересматривается* *ISO/IEC 24760-3:2016/Amd 1:2023* *Amendment 1: Identity Information Lifecycle processes* («Процессы жизненного цикла идентификационной информации»)	ГОСТ Р 59382-2021	Подготовка к публикации	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
38	ISO/IEC 24760-4 «IT Security and Privacy – A framework for identity management – Part 4: Authenticators, Credentials and Authentication» («Обеспечение безопасности и конфиденциальности ИТ. Основы управления идентичностью. Часть 4. Аутентификаторы, учетные данные и аутентификация») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	WD Рабочий проект	2025	
39	ISO/IEC 24762:2008 «Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services» («Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения») *отменен*	ГОСТ Р 53131-2008 / ISO/IEC TR 24762:2008	-	-	ISO/IEC 24762:2008 отменен
40	ISO/IEC 25093-1 «Cybersecurity – Confidential computing – Part 1: Overview and concepts» («Компьютерная безопасность. Конфиденциальные вычисления. Часть 1. Обзор и концепции») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	NP Предложен в качестве новой темы для разработки	2026	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
41	ISO/IEC 27000:2018 «Information technology – Security techniques – Information security management systems – Overview and vocabulary» («Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология») *пересматривается*	ГОСТ Р ИСО/МЭК 27000-2021	CD Проект комитета	2025	
42	ISO/IEC 27001:2022 «Information security, cybersecurity and privacy protection – Information security management systems – Requirements» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Системы менеджмента информационной безопасности. Требования») *старое название:* «Information technology – Security techniques – Information security management systems – Requirements» («Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования») */Amd 1:2024 (Изменение № 1)* *действует*	ГОСТ Р ИСО/МЭК 27001-2021	-	-	Национальный стандарт гармонизирован по версии ISO/IEC 27001:2013. В рамках деятельности ТК 362 выполнен перевод на русский язык ISO/IEC 27001:2022

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
43	ISO/IEC 27002:2022 «Information security, cybersecurity and privacy protection – Information security controls» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Меры обеспечения информационной безопасности») *старое название:* «Information technology – Security techniques – Code of practice for information security controls» («Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности») *действует*	ГОСТ Р ИСО/МЭК 27002-2021	-	-	Национальный стандарт гармонизирован по версии ISO/IEC 27002:2013. В рамках деятельности ТК 362 выполнен перевод на русский язык ISO/IEC 27002:2022
44	ISO/IEC 27003:2017 «Information technology – Security techniques – Information security management systems – Guidance» («Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации») *действует*	ГОСТ Р ИСО/МЭК 27003-2021	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
45	ISO/IEC 27004:2016 «Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation» («Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание») *пересматривается*	ГОСТ Р ИСО/МЭК 27004-2021	WD Рабочий проект	2025	
46	ISO/IEC 27005:2022 «Information technology – Security techniques – Information security risk management» («Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности») *новое название:* «Information security, cybersecurity and privacy protection – Guidance on managing information security risks» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Руководство по управлению рисками информационной безопасности») *действует*	ГОСТ Р ИСО/МЭК 27005-2010	-	-	Национальный стандарт гармонизирован по версии ISO/IEC 27005:2008. В рамках деятельности ТК 362 выполнен перевод на русский язык ISO/IEC 27005:2022

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
47	ISO/IEC 27006:2015 «Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems» («Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности») *Заменен на ISO/IEC 27006-1:2024* *«Requirements for bodies providing audit and certification of information security management systems – Part 1: General»* *(«Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Часть 1. Основные положения»)*	ГОСТ Р ИСО/МЭК 27006-2020	-	-	
48	ISO/IEC TS 27006-2:2021 «Requirements for bodies providing audit and certification of information security management systems – Part 2: Privacy information management systems» («Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Часть 2. Система менеджмента конфиденциальной информации») *пересматривается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	DIS Проект международного стандарта	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
49	ISO/IEC 27007:2020 «Information security, cybersecurity and privacy protection – Guidelines for information security management systems auditing» («Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности») *действует*	ГОСТ Р ИСО/МЭК 27007-2014	-	-	Национальный стандарт гармонизирован по версии ISO/IEC 27007:2011. Целесообразно выполнить перевод на русский язык ISO/IEC 27007:2020
50	ISO/IEC TS 27008:2019 «Information technology – Security techniques – Guidelines for the assessment of information security controls» («Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности») *пересматривается*	ГОСТ Р 56045-2021	CD Проект комитета	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
51	ISO/IEC 27010:2015 «Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications» («Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности при обмене информацией между отраслями и организациями») *действует*	ГОСТ Р ИСО/МЭК 27010-2020	-	-	
52	ISO/IEC 27011:2024 */Cor 1:2018 (Техническая поправка № 1*) «Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations» («Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002») *новое название:* «Information security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organizations» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Меры обеспечения информационной безопасности на основе ИСО/МЭК 27002 для телекоммуникационных организаций») *действует*	ГОСТ Р ИСО/МЭК 27011-2012	-	-	Национальный стандарт гармонизирован по версии ISO/IEC 27011:2008. Целесообразно выполнить перевод на русский язык ISO/IEC 27011:2016

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
53	ISO/IEC 27013:2021 «Information security, cybersecurity and privacy protection – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1») *старое название:* «Information technology – Security techniques – Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1» («Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1») *действует* *ISO/IEC 27013:2021/Amd 1* *Проект изменения к стандарту № 1* *(вносятся изменения)*	ГОСТ Р ИСО/МЭК 27013-2014	-	-	Национальный стандарт гармонизирован по версии ISO/IEC 27013:2012. Целесообразно выполнить перевод на русский язык ISO/IEC 27013:2021
54	ISO/IEC 27014:2020 «Information security, cybersecurity and privacy protection – Governance of information security» («Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности») *действует*	ГОСТ ISO/IEC 27014-2021	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
55	ISO/IEC TR 27016:2014 «Information technology – Security techniques – Information security management – Organizational economics» («Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации») *действует*	ГОСТ Р 59503-2021	-	-	
56	ISO/IEC 27017:2015 «Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services» («Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб») *пересматривается*	ГОСТ Р ИСО/МЭК 27017-2021	DIS Проект международного стандарта	2025	
57	ISO/IEC 27018:2019 «Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors» («Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки») *пересматривается*	ГОСТ Р ИСО/МЭК 27018-2020	FDIS Окончательный проект международного стандарта	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
58	ISO/IEC 27019:2024 «Information technology – Security techniques – Information security controls for the energy utility industry» («Информационные технологии. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности в энергетике (неатомной)») *новое название:* «Revision of Information technology – Security techniques – Information security controls for the energy utility industry» («Проверка информационных технологий. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности в энергетике (неатомной)») *действует*	ГОСТ Р ИСО/МЭК 27019-2021	-	-	
59	ISO/IEC 27021:2017 «Information technology – Security techniques – Competence requirements for information security management systems professionals» («Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетентности специалистов по системам менеджмента информационной безопасности») */Amd 1:2021* *«Information technology – Security techniques – Competence requirements for information security management systems professionals – Amendment 1: Addition of ISO/IEC 27001:2013 clauses or subclauses to competence requirements»*	ГОСТ Р ИСО/МЭК 27021-2021	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
	(«Информационная технология. Методы и средства обеспечения безопасности. Требования к компетентности специалистов по системам менеджмента информационной безопасности. Изменение № 1. Дополнение к разделам и подразделам стандарта ISO/IEC 27001:2013, относящимся к требованиям к компетентности») *действует*				
60	ISO/IEC TS 27022:2021 «Information technology – Guidance on information security management system processes» («Информационная технология. Руководство по осуществлению процессов системы менеджмента информационной безопасности») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
61	ISO/IEC 27028 «Information security, cyber security and privace protection – Guidance on ISO/IEC 27002 attributes («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Руководство по атрибутам стандарта ISO/IEC 27002») *разрабатывается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	DIS Проект международного стандарта	2025	
62	ISO/IEC 27031:2011 «Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity»	ГОСТ Р ИСО/МЭК 27031-2012	Подготовка к публикации	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
	(«Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса») *новое название:* «Information technology – Cybersecurity – Information and communication technology readiness for business continuity» («Информационная технология. Компьютерная безопасность. Готовность информационно-коммуникационных технологий к обеспечению непрерывности бизнеса») *пересматривается*				
63	ISO/IEC 27032:2023 «Cybersecurity – Guidelines for Internet Security» («Компьютерная безопасность. Рекомендации по обеспечению безопасности сети Интернет») *старое название:* «Information technology – Security techniques – Guidelines for cybersecurity» («Информационная технология. Методы и средства обеспечения безопасности. Рекомендации по компьютерной безопасности») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
64	ISO/IEC 27033-1:2015 «Information technology – Security techniques – Network security – Part 1: Overview and concepts» («Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции») *действует*	ГОСТ Р ИСО/МЭК 27033-1-2011	-	-	Национальный стандарт гармонизирован по версии ISO/IEC 27033-1:2009. Целесообразно выполнить перевод на русский язык ISO/IEC 27033-1:2015
65	ISO/IEC 27033-2:2012 «Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security» («Информационные технологии. Методы и средства обеспечения информационной безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей») *действует*	ГОСТ Р ИСО/МЭК 27033-2-2021	-	-	
66	ISO/IEC 27033-3:2010 «Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues» («Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления») *действует*	ГОСТ Р ИСО/МЭК 27033-3-2014	-	-	
67	ISO/IEC 27033-4:2014 «Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways»	ГОСТ Р ИСО/МЭК 27033-4-2021	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
	(«Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности») *действует*				
68	ISO/IEC 27033-5:2013 «Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Network (VPNs)» («Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС)») *действует*	ГОСТ Р ИСО/МЭК 27033-5-2021	-	-	
69	ISO/IEC 27033-6:2016 «Information technology – Security techniques – Network security – Part 6: Securing wireless IP network access» («Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей») *действует*	ГОСТ Р 59162-2020	-	-	
70	ISO/IEC 27033-7:2023 «Information technology – Network security – Part 7: Guidelines for network virtualization security»	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
	(«Информационная технология. Безопасность сетей. Часть 7. Рекомендации по безопасности виртуальных сетей») *действует*				
71	ISO/IEC 27034-1:2011 /*Cor 1:2014 (Техническая поправка № 1*) «Information technology – Security techniques – Application security – Part 1: Overview and concepts» («Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия») *действует*	ГОСТ Р ИСО/МЭК 27034-1-2014	-	-	
72	ISO/IEC 27034-2:2015 «Information technology – Security techniques – Application security – Part 2: Organization normative framework» («Информационные технологии. Методы и средства обеспечения информационной безопасности. Безопасность приложений. Часть 2. Нормативная структура организации») *действует*	ГОСТ Р ИСО/МЭК 27034-2-2021	-	-	
73	ISO/IEC 27034-3:2018 «Information technology – Security techniques – Application security – Part 3: Application security management process» («Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 3. Процесс менеджмента безопасности приложений») *действует*	ГОСТ Р ИСО/МЭК 27034-3-2021	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
74	ISO/IEC 27034-5:2017 «Information technology – Security techniques –Application security – Part 5: Protocols and application security controls data structure» («Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5. Структуры данных протоколов и мер обеспечения безопасности приложений») *действует*	ГОСТ Р ИСО/МЭК 27034-5-2020	-	-	
75	ISO/IEC TS 27034-5-1:2018 «Information technology – Application security – Part 5-1: Protocols and application security controls data structure, XML schemas» («Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5-1. Структуры данных протоколов и мер обеспечения безопасности приложений. XML-схемы») *действует*	ГОСТ Р 59494-2021	-	-	
76	ISO/IEC 27034-6:2016 «Information technology – Security techniques – Application security – Part 6: Case studies» («Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 6. Практические примеры») *действует*	ГОСТ Р ИСО/МЭК 27034-6-2021	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
77	ISO/IEC 27034-7:2018 «Information technology – Security techniques – Application security – Part 7: Assurance prediction framework» («Информационные технологии. Безопасность приложений. Часть 7. Основы прогнозирования доверия») *действует*	ГОСТ Р ИСО/МЭК 27034-7-2020	-	-	
78	ISO/IEC 27035-1:2023 «Information technology – Information security incident management – Part 1: Principles and process» («Информационная технология. Управление инцидентами информационной безопасности. Часть 1. Принципы и процесс») *старое название:* «Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management» («Информационная технология. Методы и средства обеспечения безопасности. Управление инцидентами информационной безопасности». Часть 1. Принципы управления инцидентами») «*действует*	По данной тематике приняты четыре национальных стандартов: ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения»; ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения»; ГОСТ Р 59711-2022 «Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами»; ГОСТ Р 59712-2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты»	-	-	
79	ISO/IEC 27035-2:2023 «Information technology – Information security incident management – Part 2: Guidelines to plan and prepare for incident response» («Информационная технология. Управление инцидентами информационной безопасности. Часть 2.		-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
	Рекомендации по планированию и подготовке к реагированию на инциденты») *старое название:* «Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response» («Информационная технология. Методы и средства обеспечения безопасности. Управление инцидентами информационной безопасности. Часть 2. Рекомендации по планированию и подготовке к реагированию на инциденты») *действует*				
80	ISO/IEC 27035-3:2020 «Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations» («Информационная технология. Управление инцидентами информационной безопасности. Часть 3. Рекомендации по операциям реагирования на инциденты ИКТ») *действует*		-	-	
81	ISO/IEC 27035-4:2024 «Information technology – Information security incident management – Part 4: Coordination» («Информационная технология. Управление инцидентами информационной безопасности. Часть 4. Координация») *действует*		-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
82	ISO/IEC 27036-1:2021 «Cybersecurity – Supplier relationships – Part 1: Overview and concepts» («Компьютерная безопасность. Взаимоотношения с поставщиками. Часть 1. Обзор и основные понятия») *старое название:* «Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts» («Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 1. Обзор и основные понятия») *действует*	ГОСТ Р ИСО/МЭК 27036-1-2021	-	-	Национальный стандарт гармонизирован по версии ISO/IEC 27036-1:2014. Целесообразно выполнить перевод на русский язык ISO/IEC 27036-1:2021
83	ISO/IEC 27036-2:2022 «Cybersecurity – Supplier relationships – Part 2: Requirements» («Компьютерная безопасность. Взаимоотношения с поставщиками. Часть 2. Требования») *старое название:* «Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements» («Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 2. Требования») *действует*	ГОСТ Р ИСО/МЭК 27036-2-2020	-	-	Национальный стандарт гармонизирован по версии ISO/IEC 27036-2:2014. Целесообразно выполнить перевод на русский язык ISO/IEC 27036-2:2022

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
84	ISO/IEC 27036-3:2023 «Cybersecurity – Supplier relationships – Part 3: Guidelines for hardware, software, and services supply chain security» («Компьютерная безопасность. Взаимоотношения с поставщиками. Часть 3. Рекомендации по обеспечению безопасности цепи поставок аппаратного, программного обеспечения и услуг») *старое название:* «Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security» («Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 3. Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий») *действует*	ГОСТ Р 59215-2020	-	-	
85	ISO/IEC 27036-4:2016 «Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services» («Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 4. Рекомендации по обеспечению безопасности облачных услуг») *действует*	ГОСТ Р ИСО/МЭК 27036-4-2020	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
86	ISO/IEC 27037:2012 «Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence» («Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме») *действует*	ГОСТ Р ИСО/МЭК 27037-2014	-	-	
87	ISO/IEC 27039:2015 «Information technology – Security techniques – Selection, deployment (and operations) of intrusion detection and prevention systems (IDPS)» («Информационная технология. Методы и средства обеспечения безопасности. Выбор, развертывание и функционирование систем обнаружения (и предотвращения) вторжения (СОПВ)») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
88	ISO/IEC 27040:2024 «Information technology – Security techniques – Storage security» («Информационная технология. Методы и средства обеспечения безопасности. Обеспечение безопасности хранения данных») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
89	ISO/IEC 27041:2015 «Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method» («Информационная технология. Методы и средства обеспечения безопасности. Руководство по обеспечению пригодности и адекватности метода расследования инцидентов») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
90	ISO/IEC 27042:2015 «Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence» «Информационная технология. Методы и средства обеспечения безопасности. Рекомендации по анализу и интерпретации цифровых свидетельств» *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
91	ISO/IEC 27043:2015 «Information technology – Security techniques – Incident investigation principles and processes» («Информационная технология. Методы и средства обеспечения безопасности. Принципы и процессы расследования инцидентов») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
92	ISO/IEC 27045 «Information technology – Big data security and privacy – Guidelines for managing big data risks» («Информационные технологии. Безопасность и конфиденциальность больших данных. Рекомендации по управлению рисками, связанными с большими данными») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	NP Предложен в качестве новой темы для разработки	2026	
93	ISO/IEC 27046 «Information technology – Big data security and privacy – Implementation guidelines» («Информационная технология. Обеспечение безопасности и конфиденциальности больших данных. Рекомендации по реализации») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	NP Предложен в качестве новой темы для разработки	2026	
94	ISO/IEC 27070:2021 «Information technology – Security techniques – Requirements for establishing virtualized roots of trust» («Информационная технология. Методы и средства обеспечения безопасности. Требования к установлению уровней доверия к средствам виртуализации») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
95	ISO/IEC 27071:2023 «Cybersecurity – Security recommendations for establishing trusted connections between devices and services» («Компьютерная безопасность. Рекомендации по безопасности установления доверенного соединения между устройством и сервисной службой») *действует*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
96	ISO/IEC 27091 «Cybersecurity and Privacy – Artificial Intelligence – Privacy protection» (Компьютерная безопасность и обеспечение конфиденциальности. Искусственный интеллект. Обеспечение конфиденциальности») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	WD Рабочий проект	2025	
97	ISO/IEC TS 27100:2020 «Information technology – Cybersecurity – Overview and concepts» («Информационная технология. Компьютерная безопасность. Обзор и концепции») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
98	ISO/IEC 27102:2019 «Information security management – Guidelines for cyber insurance» («Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности») *действует*	ГОСТ Р 59516-2021	-	-	
99	ISO/IEC TR 27103:2018 «Information technology – Security techniques – Cybersecurity and ISO and IEC Standards» («Информационная технология. Методы и средства обеспечения безопасности. Компьютерная безопасность и стандарты ИСО и МЭК») *пересматривается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	DIS Проект международного стандарта	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
100	ISO/IEC 27109 «Cybersecurity education and training» («Обучение и тренинг в сфере компьютерной безопасности») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	NP Предложен в качестве новой темы для разработки	2026	
101	ISO/IEC TS 27110:2021 «Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines» («Информационная технология, компьютерная безопасность и обеспечение конфиденциальности. Рекомендации по разработке инфраструктуры компьютерной безопасности») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
102	ISO/IEC TS 27115 «Cybersecurity evaluation of complex systems – Introduction and framework overview» («Оценка компьютерной безопасности систем. Введение и общая структура») *разрабатывается*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	WD Рабочий проект	2025	
103	ISO/IEC 27400:2022 «Cybersecurity – IoT security and privacy – Guidelines» («Компьютерная безопасность. Обеспечение безопасности и конфиденциальности идентификационных данных для Интернета вещей. Рекомендации») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
104	ISO/IEC 27402:2023 «Cybersecurity – IoT security and privacy – Device baseline requirements»	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
	(«Компьютерная безопасность. Обеспечение безопасности и конфиденциальности идентификационных данных для Интернета вещей. Основные требования по обеспечению безопасности») *действует*				
105	ISO/IEC 27403:2024 «Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics» («Компьютерная безопасность. Обеспечение безопасности и конфиденциальности идентификационных данных для Интернета вещей. Рекомендации для Интернета вещей: умный дом») *действует*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	
106	ISO/IEC TR 27550:2019 «Information technology – Security techniques – Privacy engineering for system life cycle processes» («Информационная технология. Методы и средства обеспечения безопасности. Обеспечение конфиденциальности идентификационных данных для процессов жизненного цикла системы») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
107	ISO/IEC 27551:2021 «Information security, cybersecurity and privacy protection – Requirements for attribute-based unlinkable entity authentication» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Требования по аутентификации, основанной на атрибутах несвязываемых объектов») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
108	ISO/IEC 27555:2021 «Information security, cybersecurity and privacy protection – Guidelines on personally identifiable information deletion» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Рекомендации по удалению персональной идентификационной информации») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
109	ISO/IEC 27556:2022 «Information security, cybersecurity and privacy protection – User-centric privacy preferences management framework» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Ориентированная на пользователя предпочтительная структура защищаемых идентификационных данных») *действует*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	
110	ISO/IEC 27557:2022 «Information security, cybersecurity and privacy protection – Application of ISO 31000:2018 for organizational privacy risk management» Organizational privacy risk management» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Применение ISO 31000 для менеджмента риска при обеспечении конфиденциальности идентификационных данных в организации») *действует*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
111	ISO/IEC 27559:2022 «Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework» («Информационная безопасность, компьютерная безопасность и обеспечение конфиденциальности. Обезличивание идентификационных данных») *действует*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	
112	ISO/IEC TR 27563:2023 «Security and privacy in artificial intelligence use cases – Best practices» («Обеспечение безопасности и конфиденциальности при использовании искусственного интеллекта. Лучшие практики») *действует*	Национальный стандарт по тематике разрабатываемого международного стандарта отсутствует	-	-	
113	ISO/IEC TS 27564 «Privacy – Guidance on the use of models for engineering» («Конфиденциальность. Руководство по моделированию инженерии конфиденциальности») *разрабатывается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	WD Рабочий проект	2025	
114	ISO/IEC TS 27570:2021 «Privacy protection – Privacy guidelines for Smart Cities» («Обеспечение конфиденциальности. Руководство по обеспечению конфиденциальности для Умных городов») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
115	ISO/IEC 27701:2019 «Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines» («Информационная технология. Методы и средства обеспечения безопасности. Применение ИСО/МЭК 27001 и ИСО/МЭК 27002 для обеспечения конфиденциальности идентификационных данных. Требования и рекомендации») *пересматривается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	FDIS Окончательный проект международного стандарта	2025	
116	ISO/IEC TS 29003:2018 «Information technology – Security techniques – Identity proofing» («Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности») *действует*	ГОСТ Р 59515-2021	-	-	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
117	ISO/IEC 29100:2024 «Information technology – Security techniques – Privacy framework» («Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных») */Amd 1:2018* *«Information technology - Security techniques - Privacy framework – Amendment 1: Clarifications»* *(«Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения конфиденциальности идентификационных данных (информации). Изменение № 1. Пояснения»)* *действует*	ГОСТ ISO/IEC 29100-2021	-	-	
118	ISO/IEC 29101:2018 «Information technology – Security techniques – Privacy architecture framework» («Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных») *действует*	ГОСТ Р 59407-2021	-	-	
119	ISO/IEC 29115:2013 «Information technology – Security techniques – Entity authentication assurance framework» («Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к аутентификации объектов и субъектов») *пересматривается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	WD Рабочий проект	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
120	ISO/IEC 29134:2023 «Information technology – Security techniques – Guidelines for privacy impact assessment» («Информационная технология. Методы и средства обеспечения безопасности. Рекомендации по анализу нарушений конфиденциальности») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
121	ISO/IEC 29146:2024 «Information technology – Security techniques – A framework for access management» («Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом») */Amd 1:2022 (Изменение № 1)* *действует*	ГОСТ Р 59383-2021	-	-	
122	ISO/IEC 29147:2018 «Information technology – Security techniques – Vulnerability disclosure» («Информационная технология. Методы и средства обеспечения безопасности. Предоставление сведений об уязвимостях») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
123	ISO/IEC 29151:2017 «Information technology – Security techniques – Code of practice for personally identifiable information protection» («Информационная технология. Методы и средства обеспечения безопасности. Свод правил для защиты персональных данных (персональной идентификационной информации)» *пересматривается*	Национальный стандарт по тематике действующего международного стандарта отсутствует	DIS Проект международного стандарта	2025	

Продолжение таблицы 2

№ п/п	Международный стандарт или документ	Национальный стандарт (на основе международного)	Стадия работ по разработке (пересмотру) международного стандарта*	Ожидаемый год введения в действие*	Примечание
124	ISO/IEC 29184:2020 «Information technology – Online privacy notices and consent» («Информационная технология. Методы и средства обеспечения безопасности. Уведомления и соглашения по обеспечению конфиденциальности идентификационных данных в режиме онлайн») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
125	ISO/IEC 29190:2015 «Information technology – Security techniques – Privacy capability assessment model» («Информационная технология. Методы и средства обеспечения безопасности. Модель оценки возможностей защиты персональных данных») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
126	ISO/IEC TS 30104:2015 «Information Technology – Security Techniques – Physical Security Attacks, Mitigation Techniques and Security Requirements» («Информационная технология. Методы и средства обеспечения безопасности. Атаки на физическую защиту, методы смягчения и требования безопасности») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	
127	ISO/IEC 30111:2019 «Information technology – Security techniques – Vulnerability handling processes» («Информационная технология. Методы и средства обеспечения безопасности. Процесс обработки уязвимостей») *действует*	Национальный стандарт по тематике действующего международного стандарта отсутствует	-	-	

В результате анализа данных, представленных в таблице 2, установлено следующее.

Из представленных в таблице 2 127 стандартов действуют 110 международных стандартов и документов (23 из которых пересматриваются), разрабатываются 12 международных стандартов и документов, 5 международных стандартов и документов отменены, но в Российской Федерации действуют соответствующие им национальные стандарты.

При этом в настоящее время в Российской Федерации действуют 59 национальных и 5 межгосударственных стандартов, разработанных (гармонизированных) на основе международных стандартов и документов, из которых 37 национальных и 5 межгосударственных стандартов разработаны на основе актуальных версий международных стандартов.

К числу национальных и межгосударственных стандартов, разработанных на основе актуальных версий международных стандартов и документов, относятся:

ГОСТ Р ИСО/МЭК 19086-4-2020 «Информационные технологии. Облачные вычисления. Структура соглашения об уровне обслуживания (SLA). Часть 4. Компоненты информационной безопасности и защиты персональных данных»;

ГОСТ ISO/IEC TS 19249-2021 «Информационная технология. Методы и средства обеспечения безопасности. Каталог архитектурных принципов и принципов проектирования безопасных продуктов, систем и приложений»;

ГОСТ ISO/IEC 19896-1-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 1. Введение, основные понятия и общие требования»;

ГОСТ Р ИСО/МЭК 21827-2010 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование безопасности систем. Модель зрелости процесса»;

ГОСТ ISO/IEC 24760-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования»;

ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»;

ГОСТ Р ИСО/МЭК 27003-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации»;

ГОСТ Р ИСО/МЭК 27004-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание»;

ГОСТ Р ИСО/МЭК 27010-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности при обмене информацией между отраслями и организациями»;

ГОСТ ISO/IEC 27014-2021 «Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности»;

ГОСТ Р ИСО/МЭК 27017-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб»;

ГОСТ Р ИСО/МЭК 27018-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки»;

ГОСТ Р ИСО/МЭК 27019-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности в энергетике (неатомной)»;

ГОСТ Р ИСО/МЭК 27021-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетентности специалистов по системам менеджмента информационной безопасности»;

ГОСТ Р ИСО/МЭК 27031-2012 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса»;

ГОСТ Р ИСО/МЭК 27033-2-2021 «Информационные технологии. Методы и средства обеспечения информационной безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей»;

ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления»;

ГОСТ Р ИСО/МЭК 27033-4-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности»;

ГОСТ Р ИСО/МЭК 27033-5-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС)»;

ГОСТ Р ИСО/МЭК 27034-1-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия»;

ГОСТ Р ИСО/МЭК 27034-2-2021 «Информационные технологии. Методы и средства обеспечения информационной безопасности. Безопасность приложений. Часть 2. Нормативная структура организации»;

ГОСТ Р ИСО/МЭК 27034-3-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 3. Процесс менеджмента безопасности приложений»;

ГОСТ Р ИСО/МЭК 27034-5-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5. Структуры данных протоколов и мер обеспечения безопасности приложений»;

ГОСТ Р ИСО/МЭК 27034-6-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 6. Практические примеры»;

ГОСТ Р ИСО/МЭК 27034-7-2020 «Информационные технологии. Безопасность приложений. Часть 7. Основы прогнозирования доверия»;

ГОСТ Р ИСО/МЭК 27036-4-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 4. Рекомендации по обеспечению безопасности облачных услуг»;

ГОСТ Р ИСО/МЭК 27037-2014 «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме»;

ГОСТ ISO/IEC 29100-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных»;

ГОСТ Р 56045-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности»;

ГОСТ Р 58142-2018 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 1. Использование доступных источников для идентификации потенциальных уязвимостей»;

ГОСТ Р 58143-2018 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения»;

ГОСТ Р 59162-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационно безопасности при использовании беспроводных IP-сетей»;

ГОСТ Р 59163-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Руководство по обеспечению безопасности при внедрении серверов виртуализации»;

ГОСТ Р 59215-2020 «Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 3. Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий»;

ГОСТ Р 59381-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции»;

ГОСТ Р 59382-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы»;

ГОСТ Р 59383-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом»;

ГОСТ Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных»;

ГОСТ Р 59494-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5-1. Структуры данных протоколов и мер обеспечения безопасности приложений. XML-схемы»;

ГОСТ Р 59503-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации»;

ГОСТ Р 59515-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности»;

ГОСТ Р 59516-2021 «Информационные технологии. Менеджмент информационной безопасности. Правила страхования рисков информационной безопасности».

Пять международных стандартов и документов отменены, но в Российской Федерации действуют следующие соответствующие им национальные стандарты:

ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»;

ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети»;

ГОСТ Р 54583-2011 / ISO/IEC TR 15443-3:2007 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия»;

ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности»;

ГОСТ Р 53131-2008 / ISO/IEC TR 24762:2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».

С учетом состояния работ по международной стандартизации, целесообразно на постоянной основе проведение работ по переводу на русский язык международных стандартов, для которых отсутствуют национальные аналоги.

Наиболее актуальным при проведении работ по подготовке переводов международных стандартов из вышеуказанного числа стандартов является перевод на русский язык международных стандартов, устанавливающих требования к обеспечению безопасности приложений, к процессам идентификации и аутентификации, к критериям оценки безопасности ИТ.

В настоящее время в Программу национальной стандартизации по ТК 362 на 2025 год, а также в план работы ТК 362 на 2025 год включены работы по разработке национальных стандартов в области безопасного программного обеспечения, идентификации и аутентификации.

ЗАКЛЮЧЕНИЕ

С января по март 2025 года проведен анализ требований утвержденных стандартов, а также результатов деятельности ПК 27 СТК 1 ИСО/МЭК в части совершенствования международных стандартов в области ЗИ.

По результатам выполнения работы установлено следующее.

1 С января по март 2025 года Росстандартом утверждены два национальных стандарта:

ГОСТ Р 59453.3-2025 «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке»;

ГОСТ Р 59453.4-2025 «Защита информации. Формальная модель управления доступом. Часть 4. Рекомендации по верификации средства защиты информации, реализующего политики управления доступом, на основе формализованных описаний модели управления доступом».

Международной организацией по стандартизации и Международной электротехнической комиссией международные стандарты не утверждались.

2 В области ЗИ и обеспечения безопасности информационных технологий в сфере деятельности ПК 27 СТК 1 ИСО/МЭК состояние разработки международных стандартов характеризуется следующим:

действуют 110 международных стандартов и документов (23 из которых пересматриваются);

разрабатываются 12 международных стандартов и документов;

5 международных стандартов и документов отменены, но в Российской Федерации действуют соответствующие им национальные стандарты.

В Российской Федерации действуют 59 национальных и 5 межгосударственных стандартов, разработанных (гармонизированных) на основе международных стандартов и документов, из которых 37 национальных и 5 межгосударственных стандартов разработаны на основе актуальных версий международных стандартов.

Вместе с тем, в целях обеспечения технологического суверенитета Российской Федерации за счет импортозамещения по приоритетным направлениям, закрепленным в Указе Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года», в настоящее время основные работы по стандартизации в области ЗИ должны базироваться преимущественно на национальных нормативных правовых актах и методических документах в данной области. Однако в интересах учета при разработке национальных документов по стандартизации перспективных практик в области информационной безопасности, закрепленных в международных документах по стандартизации, необходимо своевременное отслеживание проводимых на международном уровне работ по стандартизации в области ЗИ и обеспечения безопасности ИТ и проведение на постоянной основе работ по переводу на русский язык международных стандартов, для которых отсутствуют национальные аналоги.

Наиболее актуальным при проведении работ по подготовке переводов международных стандартов из вышеуказанного числа стандартов является перевод на русский язык международных стандартов, устанавливающих требования к обеспечению безопасности приложений, к процессам идентификации и аутентификации, к критериям оценки безопасности ИТ.

В настоящее время в Программу национальной стандартизации по ТК 362 на 2025 год, а также в план работы ТК 362 на 2025 год включены работы по разработке национальных стандартов в области безопасного программного обеспечения, а также идентификации и аутентификации.

З Полученные результаты анализа состояния стандартизации в области ЗИ целесообразно использовать при планировании работ по стандартизации, в том числе в части проведения работ по подготовке переводов на русский язык международных стандартов, не имеющих российских аналогов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Официальный сайт Федерального агентства по техническому регулированию и метрологии [Электронный ресурс]. – Режим доступа – http:// www.rst.gov.ru.

2 Федеральная государственная информационная система Росстандарта ФГИС «Береста» [Электронный ресурс]. – Режим доступа – www.fgis.gost.ru.

3 Официальный сайт Группы ИТ-Стандарт (ТК 22/МТК 22) [Электронный ресурс]. – Режим доступа – http://www.itstandard.ru.

4 Официальный сайт Международной организации по стандартизации ISO [Электронный ресурс]. – Режим доступа – http://www.iso.org.

5 Официальный сайт Международной электротехнической комиссии IEC [Электронный ресурс]. – Режим доступа – http://www.iec.ch.