ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 34.14— 2025

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Термины и определения

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным казенным научным учреждением «Академия криптографии Российской Федерации» (ФГКНУ «Академия криптографии Российской Федерации»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 17 сентября 2025 г. № 1070-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ДЕЙСТВУЕТ ВЗАМЕН ПНСТ 799—2022

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2025

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
Общие термины и определения 2
Термины и определения, относящиеся к ключевой системе 7
Термины и определения, относящиеся к системе шифрования 14
Термины и определения, относящиеся к системе цифровой подписи 17
Термины и определения, относящиеся к системе имитозащиты 22
Термины и определения, относящиеся к системе аутентификации стороны 23
Термины и определения, относящиеся к средствам криптографической защиты информации 25
Алфавитный указатель терминов на русском языке 27
Алфавитный указатель эквивалентов терминов на английском языке 33
Приложение А (справочное) Вспомогательные термины и определения в области криптографической защиты информации, не включенные в раздел 3 настоящего стандарта 38
Приложение Б (справочное) Термины и определения, применяемые в областях деятельности, смежных с криптографической защитой информации 40
Библиография 42

Введение

Установленные в настоящем стандарте термины расположены в систематизированном порядке, отражающем систему понятий в области криптографической защиты информации.

Для каждого понятия установлен один стандартизованный термин.

Не рекомендуемые к применению термины-синонимы приведены в круглых скобках после стандартизованного термина и обозначены пометой «Нрк».

Термины-синонимы без пометы «Нрк» приведены в качестве справочных данных и не являются стандартизованными.

Заключенная в круглые скобки часть термина может быть опущена при использовании термина в документах по стандартизации.

Наличие квадратных скобок в терминологической статье означает, что в нее включены два термина, имеющие общие терминоэлементы.

В алфавитном указателе эти термины приведены отдельно с указанием номера статьи.

Помета, указывающая на область применения многозначного термина, приведена в круглых скобках светлым шрифтом после термина. Помета не является частью термина.

Приведенные определения можно, при необходимости, изменять, вводя в них производные признаки, раскрывая значения используемых в них терминов, указывая объекты, входящие в объем определяемого понятия. Изменения не должны нарушать объем и содержание понятий, определенных в настоящем стандарте.

В настоящем стандарте приведены иноязычные эквиваленты стандартизованных терминов на английском (en) языке.

Термины и определения в области криптографической защиты информации, являющиеся вспомогательными по отношению к терминам, приведенным в разделе 3 настоящего стандарта, приведены в приложении А.

Термины и их определения, относящиеся к областям деятельности, смежным с криптографической защитой информации, необходимые для понимания текста стандарта, приведены в приложении Б.

Стандартизованные термины набраны полужирным шрифтом, их краткие формы, представленные аббревиатурой, сложносокращенным словом, — светлым, синонимы — курсивом.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Термины и определения

Information technology. Cryptographic data security. Terms and definitions

Дата введения — 2026—01—01

1 Область применения

Настоящий стандарт устанавливает основные термины с соответствующими определениями, применяемые при проведении работ по стандартизации в области криптографической защиты информации.

В целях унификации терминологии при разработке математического аппарата в области криптографической защиты информации, а также для исключения разночтений с терминологией смежных областей деятельности в настоящем стандарте приведены термины, введенные ГОСТ Р 7.0.8, ГОСТ Р 34.10, ГОСТ Р 34.11, ГОСТ Р 34.12, ГОСТ Р 34.13, ГОСТ Р 50922, ГОСТ Р 56205, ГОСТ Р 56498, ГОСТ Р ИСО/МЭК 27000, ГОСТ Р 57149.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 7.0.8—2025 Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения

ГОСТ Р 34.10—2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11—2012 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р 34.12—2015 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13—2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

ГОСТ Р 50922—2006 Защита информации. Основные термины и определения

ГОСТ Р 56205—2014/IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели

ГОСТ Р 56136—2014 Управление жизненным циклом продукции военного назначения. Термины и определения

ГОСТ Р 56498—2015/IEC/PAS 62443-3:2008 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления

ГОСТ Р 57149/ISO/IEC Guide 51:2014 Аспекты безопасности. Руководящие указания по включению их в стандарты

Издание официальное

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

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

Общие термины и определения

1 **криптография:** Область теоретических и прикладных исследований и практической деятельности, которая связана с разработкой и применением методов криптографической защиты информации. — cryptography

Примечание — Криптография как область теоретических и прикладных исследований подразделяется на криптографический синтез и криптографический анализ, а как область практической деятельности решает вопросы разработки и применения средств криптографической защиты информации (СКЗИ) (см. статью 177), реализующих криптосистемы.

2

криптографическая защита информации: Защита информации с помощью ее криптографического преобразования. — cryptographic protection of information

[ГОСТ Р 50922—2006, статья 2.2.3]

3 **криптографическое преобразование:** Процесс преобразования представляющих информацию данных с целью обеспечения криптографической стойкости, допускающий математическое описание. — cryptographic transformation

Примечание — Основным принципом, лежащим в основе почти всех методов криптографической защиты информации, является зависимость криптографических преобразований от сохраняемых в тайне криптографических ключей.

4 **криптографический ключ:** Изменяемый параметр криптографического алгоритма, определяющий выбор криптографического преобразования. — cryptographic key

Примечание — См. также ГОСТ Р 34.12—2015 (пункт 2.1.8); [1] (пункт 3.16), ГОСТ Р 56205—2014 (статья 3.2.35); [2] (пункты 3.1.17, 3.1.19, 3.1.25, 3.1.27, 3.1.36, 3.1.37, 3.1.41).

5 **криптографическая система;** криптосистема: Структурированная и согласованная совокупность криптографических механизмов, предназначенная для решения поставленных задач криптографической защиты информации при конкретных условиях применения. — cryptographic system; cryptosystem

Примечания

1 Криптографическая система содержит основную функциональную подсистему, обеспечивающую решение поставленных задач защиты информации, и необходимую для ее функционирования ключевую систему.

2 В качестве составных частей основной функциональной подсистемы могут выступать шифр (см. статью 98), криптографическая хеш-функция, зависящая от ключа (см. статью 162), схема цифровой подписи (см. статью 129), криптографический протокол аутентификации стороны (см. статью 165) или другие криптографические механизмы, обеспечивающие решение конкретных задач защиты информации.

3 В зависимости от типов применяемых криптографических ключей различают асимметричные (см. статью 17), симметричные (см. статью 18), и гибридные (см. статью 19) криптосистемы.

6 **задачи криптографической защиты информации:** Задачи защиты информации, для решения которых могут использоваться криптографические преобразования. — cryptographic information protection goals

Пример — Обеспечение конфиденциальности информации, аутентификации (данных, источника данных, стороны), контроля целостности данных, невозможности отрицания создания или получения информации.

7 **криптографический синтез;** криптосинтез: Область теоретических и прикладных исследований, имеющих целью создание криптографической системы или криптографического механизма. — cryptographic synthesis

Примечания

1 Составной частью разработки СКЗИ, реализующего криптосистему, является проведение тематических исследований — комплекса криптографических, инженерно-криптографических и специальных исследований для оценки соответствия СКЗИ требованиям по безопасности информации, предъявляемым к СКЗИ.

2 См. [2] (пункт 3.1.47).

8 **криптографический алгоритм:** Алгоритм, описывающий процесс криптографического преобразования информации. — cryptographic algorithm

Примечания

1 См. [3] (страница 49).

2 См. также ГОСТ Р 56205—2014 (статья 3.2.34).

3 Входом криптографического алгоритма являются изменяемые данные, которые могут включать открытый (см. статью 94) или шифрованный текст (см. статью 95), криптографический ключ или ключевой материал (см. статью 35).

9 **криптографический протокол:** Коммуникационный протокол, в рамках которого стороны информационного взаимодействия последовательно выполняют определенные действия и обмениваются сообщениями, реализованный с применением криптографических алгоритмов для решения задач защиты информации. — cryptographic protocol

Примечание — См. [3] (страница 51).

10 **криптографический механизм:** Криптографический алгоритм, криптографический протокол, или их совокупность, применяемые в криптографической системе для обеспечения решения конкретной задачи защиты информации или создания и функционирования ее ключевой системы. — cryptographic mechanism

Пример — Шифр, протокол аутентификации стороны, схема цифровой подписи, бесключевая криптографическая хеш-функция, алгоритм формирования штампа времени, протокол выработки общего секретного ключа.

11 **криптографический анализ;** криптоанализ: Область теоретических и прикладных исследований, имеющих конечной целью получение обоснованных оценок криптографической стойкости криптографической системы в целом или отдельного криптографического механизма. — cryptographic analysis; cryptanalysis

Примечания

1 Криптоанализ конкретной криптосистемы или криптографического механизма проводится путем теоретического и экспериментального анализа, в том числе путем моделирования и выполнения различных атак на криптосистему или криптографический механизм, а также путем выражения оценки стойкости криптосистемы (криптографического механизма) через известную оценку стойкости другой криптосистемы (криптографического механизма).

2 При проведении криптографических исследований СКЗИ, реализующих криптосистему, дополнительно учитываются конкретные особенности реализации, среда функционирования и условия размещения СКЗИ при их эксплуатации.

12 **метод криптографического анализа:** Совокупность приемов и способов, объединенных одной или несколькими идеями, предназначенных для исследования криптографической стойкости криптографической системы или отдельного криптографического механизма.

method of cryptanalysis

13 **(криптографическая) стойкость:** Свойство криптографической системы или отдельного криптографического механизма, характеризующее степень защищенности от атак на криптографическую систему или криптографический механизм.

(cryptographic) security

Пример — Стойкость шифра к атакам с целью восстановления ключа по известным открытому и шифрованному текстам, стойкость криптографической хеш-функции к нахождению коллизий, стойкость предварительного распределения ключей при компрометации части ключей.

Примечания

1 Различают два основных подхода к обоснованию стойкости —исследование практической стойкости (см. статью 15) и исследование теоретической стойкости (см. статью 16).

2 Стойкость криптографической системы зависит от стойкости применяемых в ней криптографических механизмов и от способа их использования в общей конструкции криптографической системы.

14 **атака на криптосистему [на криптографический механизм]:** Действие, совершаемое с целью нарушить хотя бы одно из целевых предназначений криптографической системы [криптографического механизма], использующее конкретные исходные данные о ее [его] функционировании без полного знания сохраняемых в тайне ее [его] параметров.

attack on the cryptosystem [cryptographic mechanism]

Пример — Атака на шифр с подобранным открытым текстом, подмена сообщения, подмена стороны информационного обмена на основе компрометации долговременного ключа, подбор пароля протокола аутентификации стороны по набору ранее переданных сообщений.

Примечания

1 Различают два типа атак: активная атака предполагает непосредственное воздействие на работу криптосистемы [криптографического механизма], например, путем повторной передачи, имитации или подмены передаваемых сообщений; пассивная атака осуществляется без непосредственного воздействия на функционирование криптосистемы [криптографического механизма] путем перехвата передаваемых сообщений или хранящихся зашифрованных данных и последующего их анализа с целью нахождения неизвестных параметров.

2 Здесь и далее в статьях 15 и 16 «конкретные исходные данные» могут учитывать особенности практической реализации криптосистемы (криптографического механизма) и включать, например, математическую модель возникновения ошибок (преднамеренных или непреднамеренных) или математическую модель дополнительной информации о ключе в процессе ее (его) функционирования.

15 **практическая стойкость** (для конкретной задачи криптографической защиты информации): Средняя вычислительная трудоемкость наилучшей известной атаки на криптографическую систему [криптографический механизм] для конкретных исходных данных о ее [его] функционировании и конкретной задачи криптографической защиты информации.

security strength (for a specific information protection goal)

Примечания

1 См. [1] (статья 3.25).

2 Средняя вычислительная трудоемкость атаки, проводимой до первого успеха, характеризуется отношением средней трудоемкости выполнения алгоритма, реализующего одну попытку атаки, к вероятности его успешного завершения.

3 Для удобства сравнения различных атак на криптосистему [криптографический механизм] с каждой оценкой средней вычислительной трудоемкости атаки ассоциируется число операций, соответствующее однократному выполнению соответствующего криптографического преобразования.

16 **теоретическая [доказуемая] стойкость** (для конкретной задачи защиты информации): Строго обоснованная в рамках математической модели криптографической системы или криптографического механизма неулучшаемая нижняя оценка сложности получения атакующим информации о сохраняемых в тайне параметрах системы (механизма) или о защищаемой ими информации для конкретных исходных данных и конкретной задачи криптографической защиты информации.

provable security (for a specific information protection goal)

Пример — Совершенная стойкость системы шифрования, безусловная стойкость системы имитозащиты, сведение (предположительно) вычислительно трудной задачи к рассматриваемой задаче криптографического анализа.

17 **асимметричная криптографическая система;** *криптосистема с открытым ключом:* Криптографическая система, использующая пары взаимосвязанных криптографических преобразований, одно из которых зависит от открытого ключа, а второе — от криптографического ключа, сохраняемого в тайне (личного ключа).

asymmetric cryptosystem; public key system

Примечания

1 См. [1] (пункт 3.1). См. также [4] (пункт 2.1), [5] (пункт 3.1).

2 См. определения терминов «личный ключ» и «открытый ключ» в статье 48 и статье 49 соответственно.

3 Задача нахождения сохраняемого в тайне криптографического ключа по открытому является (предполагается) вычислительно трудной.

18 **симметричная криптографическая система:** Криптографическая система, использующая пары взаимосвязанных криптографических преобразований, в которой преобразования в каждой паре зависят от одного и того же секретного ключа.

symmetric cryptosystem

Примечания

1 См. [4] (пункт 2.45).

2 См. определение термина «секретный ключ» в статье 63.

3 Симметричная криптосистема может использоваться доверяющими друг другу сторонами, где для взаимодействующих пар (групп) пользователей формируются общие секретные ключи.

19 **гибридная криптографическая система:** Криптографическая система, содержащая в качестве составных элементов как симметричную, так и асимметричную криптографические системы.

hybrid cryptosystem

20 **ключевая система:** Подсистема криптографической системы, с помощью которой обеспечивается создание криптографических ключей, необходимых для ее функционирования, и управление ими на основе инфраструктуры управления ключами. — key system

Примечание — См. определение термина «инфраструктура управления ключами» в статье 41.

21 **криптографическая система аутентификации стороны:** Криптографическая система, предназначенная для обеспечения аутентификации стороны, включающая в себя криптографический протокол аутентификации стороны и ключевую систему. — entity authentication cryptosystem

Примечание — См. определение термина «криптографический протокол аутентификации стороны» в статье 167.

22 **аутентификация данных:** Проверка целостности данных и аутентификация их источника. — data authentication

Примечание — См. определения терминов «целостность (данных)» и «аутентификация источника (данных)» в приложении Б, статьи Б.2.13 и Б.2.8 соответственно.

23 **система имитозащиты:** Симметричная криптографическая система, предназначенная для обеспечения аутентификации данных, включающая зависящую от ключа криптографическую хеш-функцию и ключевую систему. — symmetric data authentication system

Примечания

1 См. [2] (пункт 3.1.11).

2 См. определение терминов «имитозащита» и «криптографическая хеш-функция, зависящая от ключа» в статье 161 и статье 164.

24 **система цифровой подписи:** Асимметричная криптографическая система, предназначенная для обеспечения аутентификации данных и невозможности отрицания создания, включающая схему цифровой подписи и ключевую систему. — digital signature system

Примечания

1 См. [5] (пункты 3.7 и 3.40).

2 См. определение терминов «схема цифровой подписи» в статье 129 и «невозможность отрицания создания» в статье 150.

3 Ключевая система основана на инфраструктуре открытых ключей (см. статью 53).

25 **система шифрования;** шифрсистема: Криптографическая система, предназначенная для обеспечения конфиденциальности информации, включающая в себя шифр (код) и ключевую систему. — encipherment system; encryption system;

Примечания

1 См. [1] (статья 3.13).

2 См. определение термина «конфиденциальность» в приложении Б, статья Б.2.12.

3 См. определение терминов «шифр» и «код» в статье 98 и статье 108 соответственно.

26 **совершенная стойкость системы шифрования:** Вид теоретической [доказуемой] стойкости, представляющий собой свойство системы шифрования, гарантирующее, что в рамках математической модели системы шифрования по шифрованному тексту без сведений об использованном при зашифровании криптографическом ключе невозможно получить никакую информацию об открытом тексте, кроме, возможно, его длины. — perfect security of an encipherment system

Примечания

1 См. определение терминов «зашифрование», «открытый текст» и «шифрованный текст» в статье 99, статье 94 и статье 95 соответственно.

2 Пример совершенно стойкой системы шифрования — шифр гаммирования (см. статью 121) с одноразовой гаммой (см. статью 118), являющейся реализацией идеальной случайной последовательности, длина которой совпадает с длиной открытого текста.

27 **дешифрование:** Раскрытие зашифрованной информации методами криптографического анализа без предварительного полного знания применяемого криптографического ключа. — breaking an encipherment system

Примечание — Термины «дешифрование» и «расшифрование» не являются синонимами. См. определение термина «расшифрование» в статье 104.

28 **квантовая криптография:** Раздел криптографии, связанный с разработкой и применением методов криптографической защиты информации, основанных на принципах квантовой механики. — quantum cryptography

Пример — Защищенная передача ключа по квантовому каналу.

29 **постквантовая криптография:** Раздел криптографии, связанный с синтезом криптографических систем (криптографических механизмов), обеспечивающих защиту от атак с применением квантовых компьютеров. — post-quantum cryptography

30 **низкоресурсная криптография:** Раздел криптографии, связанный с криптографическим синтезом и криптографическим анализом криптографических систем, эффективно реализуемых на устройствах, имеющих существенные ограничения на используемые вычислительные ресурсы. — lightweight cryptography

Примечание — См. [6] (статья 2.6).

31 **криптографическая система на основе идентификаторов** (Нрк. *личностная криптографическая система*): Асимметричная криптографическая система, в которой открытые ключи вычисляются на основе идентификационной информации их владельцев. — identity-based cryptosystem

Примечания

1 К идентификационной информации относятся идентификатор, адрес электронной почты или произвольная строка символов.

2 См. [1] (пункт 3.16), см. также [7] (пункт 3.6).

3 Закрытые (личные) ключи вырабатываются доверенной стороной и выдаются участникам, при этом необходимость в сертификатах открытых ключей (см. статью 47) отпадает.

32 **метод полного перебора (при криптографическом анализе):** Метод криптографического анализа, основанный на рассмотрении (опробовании) всех вариантов сохраняемых в тайне криптографических ключей, паролей или других данных. — brute-force attack; exhaustive search method

Примечание — См. [8] (пункт 3.3).

Термины и определения, относящиеся к ключевой системе

33 **множество ключей:** Множество всех возможных значений криптографического ключа (для конкретного криптографического алгоритма). — key space

34 **длина [размер] ключа:** Минимальная длина записи криптографического ключа как строки символов заданного алфавита (обычно двухэлементного). — key length; key size

Примечание — Двоичное представление обычно выбирается для обеспечения возможности единообразного подхода к оценке мощности множества ключей.

35 **ключевой материал;** *исходная ключевая информация:* Данные, позволяющие сформировать секретные криптографические ключи. keying material

Примечания

1 См. [4] (пункт 2.27).

2 См. определение термина «ключевая информация» в статье 184.

36 **управление ключами:** Организация и управление процессами выработки, регистрации, сертификации, распределения, применения, хранения, архивирования, восстановления, отзыва, замены или изъятия из обращения, а также уничтожения криптографических ключей или ключевых материалов. key management

Примечание — См. [4] (пункт 2.28).

37 **инфраструктура управления ключами:** Комплекс центров доверия, аппаратно-программных и технических средств, другого оборудования и документов, обеспечивающих управление криптографическими ключами. key management infrastructure

Примечание — См. определение термина «центр доверия» в приложении Б (статья Б.2.21).

38 **жизненный цикл ключа:** Последовательность этапов работы с криптографическим ключом от момента выработки до момента уничтожения. key life cycle

39 **срок действия ключа:** Установленный временной интервал, в течение которого криптографический ключ разрешается использовать. key life time

Примечание — В случае получения сведений о компрометации ключа срок действия ключа необходимо пересмотреть.

40 **компрометация ключа:** Нарушение конфиденциальности криптографического ключа или ключевого материала. key compromise

Примечание — Различают полную компрометацию и частичную компрометацию ключа, результатом которой может быть уменьшение множества возможных значений ключа.

41 **уничтожение ключа:** Необратимое уничтожение криптографического ключа. key destruction

Примечания

1 См. [4] (пункт 2.20).

2 Уничтожению подлежат все существующие бумажные и электронные экземпляры и копии криптографического ключа, а также всех его фрагментов, в том числе на резервных копиях информационных систем.

42 **депонирование ключа:** Технология, обеспечивающая возможность восстановления криптографического ключа при участии заранее определенных одного или нескольких центров доверия. key escrow

43 **ключевая пара:** Упорядоченная пара однозначно математически связанных криптографических ключей, используемых в асимметричной криптографической системе и определяющих взаимосвязанные криптографические преобразования. key pair

Примечания

1 См. [5] (пункт 3.3).

2 Ключевая пара должна принадлежать только одной из взаимодействующих сторон.

44 **закрытый [личный] ключ:** Сохраняемый в тайне криптографический ключ из ключевой пары. private key

Примечания

1 См. [4] (пункт 2.35).

2 См. также [5] (пункт 3.32).

45 **открытый ключ:** Криптографический ключ из ключевой пары, который может быть сделан доступным другим сторонам без снижения стойкости асимметричной криптографической системы, в которой используется данная ключевая пара. public key

Примечания

1 В системе цифровой подписи открытый ключ применяется для проверки подписи. В асимметричной системе шифрования открытый ключ применяется для зашифрования. Открытый ключ может не являться общедоступным, а быть доступным только членам заранее определенной группы.

2 См. [5] (пункт 3.33). См. также [4] (пункт 2.36).

46 **информация об открытом ключе:** Структура данных, содержащая открытый ключ и идентификационные данные владельца криптографического ключа, а также, возможно, дополнительную информацию об удостоверяющем центре, области использования криптографического ключа, сроке действия, используемых криптографических алгоритмах и иные сведения, устанавливаемые удостоверяющим центром. public key information

Примечание — См. [5] (пункт 3.35).

47 **сертификат открытого ключа:** Информация об открытом ключе, подписанная цифровой подписью удостоверяющего центра. public key certificate

Примечание — См. [4] (пункты 2.37 и 2.38).

48 **центр сертификации** (открытых ключей): Компонент удостоверяющего центра, обеспечивающий создание сертификатов открытых ключей, формирование реестра (действующих) сертификатов и списка отозванных сертификатов. certification center

Примечание — См. определение термина «список отозванных сертификатов» в статье 57.

49 **центр регистрации:** Компонент удостоверяющего центра, обеспечивающий предоставление центру сертификации подтвержденных (зарегистрированных) идентификационных данных лиц, обратившихся за получением сертификата открытого ключа. registration authority

Примечания

1 См. [4] (пункт 2.40).

2 Дополнительно центр регистрации может осуществлять выработку ключевых пар, подтверждение владения заявителем закрытым ключом для имеющегося у него открытого ключа, формирование шаблонов сертификатов открытых ключей и проверку того, является ли данный сертификат действующим.

50 **удостоверяющий центр:** Центр доверия, предназначенный для создания сертификатов открытых ключей. certification authority

Примечания

1 См. [4] (пункт 2.3).

2 См. определение термина «центр доверия» в приложении Б (статья Б.2.21).

3 Удостоверяющий центр может содержать в своей структуре помимо центра сертификации несколько центров регистрации.

51 **штамп времени:** Структура, криптографически связывающая набор данных со временем ее создания и применяемая для проверки того, что данные были созданы до указанного момента времени. time-stamp token

Примечание — См. [9] (пункты 3.15, 3.18).

52 **служба штампов времени:** Доверенная сторона, формирующая штампы времени. time stamping authority

Примечания

1 См. [9] (пункт 3.17).

2 См. определение термина «доверенная сторона» в приложении Б (статья Б.2.20).

53 **инфраструктура открытых ключей;** ИОК: Инфраструктура управления ключами асимметричной криптографической системы на основе сертификатов открытых ключей. public key infrastructure; PKI

Примечание — См. определение термина «инфраструктура управления ключами» в статье 37.

54 **архитектура инфраструктуры открытых ключей;** архитектура ИОК: Система взаимодействия удостоверяющих центров и входящих в них центров сертификации и регистрации. public key infrastructure architecture; PKI architecture

55 **иерархическая архитектура инфраструктуры открытых ключей;** иерархическая архитектура ИОК: Древовидная система подчинения и взаимодействия центров сертификации и регистрации (удостоверяющих центров), при которой центры сертификации более высокого уровня формируют сертификаты открытых ключей для центров сертификации более низкого уровня. hierarchy type public key infrastructure architecture; hierarchy type PKI architecture

56 **сетевая архитектура инфраструктуры открытых ключей;** сетевая архитектура ИОК: Система взаимодействия центров сертификации и регистрации (удостоверяющих центров), при которой они формируют друг для друга сертификаты открытых ключей (кросс-сертификаты) для обеспечения возможности их проверки в прямом и обратном направлениях. network type public key infrastructure architecture; network type PKI architecture

57 **список отозванных [аннулированных] сертификатов:** Перечень досрочно прекративших действие сертификатов открытых ключей, формирование и доступ к которому обеспечивает удостоверяющий центр. certificate revocation list

Примечания

1 Для каждого отозванного сертификата указывается его уникальный номер, информация о дате прекращения действия и об основаниях аннулирования.

2 Данный список может не содержать информацию о сертификатах, действие которых прекращено по причине истечения срока их действия.

58 **секретный ключ:** Криптографический ключ симметричной криптографической системы. secret key

Примечания

1 См. [4] (пункт 2.41), [5] (пункт 3.38).

2 Секретный ключ является общим ключом для двух или большей группы пользователей криптографической системы.

59 **составной ключ:** Криптографический ключ, состоящий из нескольких компонентов, определяющих работу отдельных частей одного криптографического механизма. composite key

Пример — Компонентами ключа могут быть двоичные последовательности, перестановки или функциональные компоненты криптографического алгоритма.

60 **одноразовый ключ:** Криптографический ключ, используемый однократно. — one time key

61 **долговременный ключ:** Криптографический ключ, который используется в криптографической системе в неизменном виде длительное время. — static key; long-term key

62 **иерархия секретных ключей:** Древовидная структура, отражающая способ защиты криптографических ключей симметричной криптографической системы, соответствующих различным выполняемым ею функциям, при котором криптографические ключи промежуточных уровней используются для шифрования и имитозащиты криптографических ключей более низкого уровня, а криптографические ключи нижнего уровня являются криптографическими ключами, предназначенными для выполнения целевых функций криптографической системы. — logical key hierarchy

Примечание — См. [3], страница 112.

63 **главный секретный ключ:** Корневой (верхнеуровневый) элемент иерархии секретных ключей, предназначенный для шифрования криптографических ключей более низкого уровня. — master key

Примечание — См. [3] (страница 115).

64 **ключ шифрования данных:** Элемент иерархии секретных ключей, предназначенный для шифрования данных. — data encryption key

Примечание — Ключ шифрования данных может быть элементом составного секретного ключа.

65 **ключ шифрования ключей:** Элемент иерархии секретных ключей, предназначенный для шифрования криптографических ключей более низкого уровня. — key encryption key

66 **иерархия производных ключей:** Древовидная структура, отражающая зависимость производных ключей от исходных. — derivation key hierarchy

Примечание — См. определение термина «производный ключ» в статье 78.

67 **корневой ключ:** Криптографический ключ, соответствующий корню иерархии производных ключей. — derivation key

68 **сеансовый ключ:** Элемент иерархии производных ключей, выработанный для криптографической защиты одного сеанса связи между сторонами информационного взаимодействия, при помощи которого могут вырабатываться производные секретные ключи, используемые в данном сеансе связи. — session key

Пример криптографических ключей, производных от сеансового — криптографические ключи, предназначенные для шифрования данных, контроля целостности сообщений и аутентификации сторон.

69 **функция выработки производного ключа;** *функция диверсификации ключа:* Функция для вычисления криптографического ключа по другому криптографическому ключу и несекретным вспомогательным данным. — key derivation function

Примечание — См. [5] (пункт 3.22).

70 **производный ключ:** Криптографический ключ, полученный как значение функции выработки производного ключа. — derived key

Примечание — См. [5] (пункт 2.19).

71 **распределение секретных ключей:** Централизованное распределение секретных ключей между пользователями симметричной криптографической системы, необходимых для ее функционирования. — key distribution

Примечание — См. [4] (пункт 2.21).

72 **центр распределения ключей:** Центр доверия, обеспечивающий выработку и распределение секретных ключей. — key distribution centre

Примечание — См. [4] (пункт 2.22).

73 **центр передачи [перешифрования] ключей:** Центр доверия, осуществляющий расшифрование выработанного и зашифрованного одной стороной секретного ключа, последующее его зашифрование и передачу в зашифрованном виде другой стороне — key translation centre

Примечание — См. [4] (пункт 2.32).

74 **предварительное распределение секретных ключей:** Централизованное распределение ключевых материалов, с помощью которых пользователи симметричной криптографической системы могут независимо вычислять секретные ключи. — preliminary key distribution

Примечания

1 Применяется в сетях связи с большим числом абонентов и должно обладать устойчивостью к компрометации ключей.

2 Формирование общего ключа на основе ключевых материалов, полученных при предварительном распределении секретных ключей, не предполагает выполнение криптографического протокола.

75 **формирование общего ключа** (Нрк. *установка общего ключа*): Получение сторонами информационного взаимодействия общего секретного ключа либо с помощью протокола защищенной передачи ключа, выработанного одной из сторон, либо с помощью протокола совместной выработки общего секретного ключа, либо на основе ключевых материалов, полученных при предварительном распределении секретных ключей. — key establishment

Примечание — См. [5] (пункт 3.23). См. также [4] (пункт 2.23).

76 **защищенная передача ключа:** Процесс передачи криптографического ключа от одной стороны к другой способом, обеспечивающим конфиденциальность, подтверждение и аутентификацию пересылаемого криптографического ключа. — key transport

77 **механизм инкапсуляции ключа:** Способ выработки и защищенной передачи секретного ключа или ключевых материалов, необходимых для его формирования, использующий систему шифрования с открытым ключом. — key encapsulation mechanism

Примечание — См. [10] (пункт 8.1).

78 **(совместная) выработка общего секретного ключа:** Формирование двумя или несколькими сторонами общего секретного ключа, реализуемое криптографическим протоколом, в ходе выполнения которого ни одна из сторон не может уменьшить множество возможных значений формируемого криптографического ключа. — key agreement

Примечание — См. [5] (пункт 3.18). См. также [4] (пункт 2.13).

79 **протокол аутентификации и формирования общего ключа:** Криптографический протокол, позволяющий осуществить аутентификацию взаимодействующих сторон и формирование общего секретного ключа. — protocol for authentication and key establishment (AKE protocol)

80 **подтверждение ключа:** Получение одной стороной, участвующей в формировании общего ключа, гарантий того, что другой стороне известен сформированный общий секретный ключ. — key confirmation

Примечание — См. [4] (пункт 2.16).

81 **частичная аутентификация ключа для стороны B стороной A:** Получение стороной B гарантий того, что сформированный общий секретный ключ не известен никакой стороне, отличной от A.

implicit key authentication from entity A to entity B

Примечание — См. [5] (пункт 3.16).

82 **полная аутентификация ключа для стороны B стороной A:** Получение стороной B гарантий того, что сформированный общий секретный ключ известен стороне A и не известен никакой другой стороне.

explicit key authentication from entity A to entity B

Примечания

1 См. [5] (пункт 3.12).

2 Полная аутентификация ключа для стороны B стороной A означает одновременное выполнение частичной аутентификации ключа для стороны B стороной A и подтверждения ключа стороной A для стороны B.

83 **протокол выработки общего аутентифицированного ключа:** Криптографический протокол выработки общего секретного ключа, обеспечивающий полную аутентификацию ключа.

authenticated key agreement protocol

84 **защищенность от чтения назад по отношению к стороне A** (для протоколов выработки общего секретного ключа) (Нрк. *совершенная секретность в будущем по отношению к стороне A*): Обеспечиваемая протоколом выработки общего секретного ключа невозможность вычисления сформированных ранее общих секретных ключей в случае компрометации (в данный момент или в будущем) долговременного личного ключа стороны A.

forward secrecy with respect to entity A

Примечание — См. [5] (пункт 3.14).

85 **защищенность от чтения назад по отношению к каждой из сторон** (для протоколов выработки общего секретного ключа): Обеспечиваемая протоколом выработки общего секретного ключа невозможность вычисления сформированных ранее общих секретных ключей в случае компрометации долговременного личного ключа одной из сторон.

forward secrecy with respect to both entity A and entity B individually

Примечание — См. [5] (пункт 3.13).

86 **взаимная защищенность от чтения назад** (для протоколов выработки общего секретного ключа): Обеспечиваемая протоколом выработки общего секретного ключа невозможность вычисления сформированных ранее общих секретных ключей в случае компрометации долговременных личных ключей обеих сторон.

mutual forward secrecy

Примечание — См. [5] (пункт 3.29).

87 **устойчивость к подмене стороны при компрометации ключа** (для протоколов выработки общего секретного ключа): Обеспечиваемая протоколом выработки общего секретного ключа невозможность полностью выполнить протокол от имени одной из сторон информационного взаимодействия при компрометации долговременного личного ключа другой стороны.

key compromise impersonation resistance

88 **устойчивость к выработке общего ключа с неизвестной стороной** (для протоколов выработки общего секретного ключа): Обеспечиваемая протоколом выработки общего секретного ключа невозможность выработки общего ключа стороной A со стороной B так, чтобы при этом сторона B осталась уверенной в том, что она сформировала криптографический ключ со стороной C, отличной от A.

unknown key share attack resistance

89 **разделение секрета:** Способ формирования ключевых материалов (долей секрета) между сторонами, позволяющий одной или нескольким заранее определенным группам (правомочным коалициям) и только этим группам восстанавливать значение криптографического ключа (секрета). — secret sharing

Примечание — См. [11] (пункт 3.9).

90 **схема разделения секрета:** Совокупность, состоящая из двух криптографических протоколов, один из которых предназначен для разделения секрета между сторонами, а другой — для формирования криптографического ключа (секрета) группой участников. — secret sharing scheme

Примечание — См. [11] (пункт 3.9).

91 **пороговая схема разделения секрета:** Схема разделения секрета, в которой правомочными являются все коалиции сторон, содержащие не менее заранее оговоренного числа участников, а все коалиции с меньшим числом участников — неправомочны. — threshold secret sharing scheme

92 **совершенная схема разделения секрета:** Схема разделения секрета, в которой совокупность долей секрета любой неправомочной коалиции сторон не позволяет получить никакой информации о значении криптографического ключа (секрета). — perfect secret sharing scheme

93 **идеальная схема разделения секрета:** Совершенная схема разделения секрета, в которой мощности множеств возможных значений криптографического ключа (секрета) и долей секрета совпадают. — ideal secret sharing scheme

Термины и определения, относящиеся к системе шифрования

94 **открытый текст:** Данные, подлежащие зашифрованию или полученные в результате расшифрования. — plaintext

95 **шифрованный текст;** шифртекст: Данные, полученные в результате зашифрования открытого текста. — ciphertext

96 **симметричная система шифрования;** *система шифрования с секретным ключом:* Система шифрования, являющаяся симметричной криптографической системой, в которой для зашифрования и расшифрования применяются одинаковые секретные ключи. — symmetric encipherment system; secret key encryption system

Примечания

1 См. [1] (пункты 3.28 и 3.29).

2 «Шифрование» — термин, объединяющий термины «зашифрование» и «расшифрование».

3 Секретные ключи для зашифрования и расшифрования в конкретных средствах шифрования могут иметь различные представления.

97 **асимметричная система шифрования;** *система шифрования с открытым ключом:* Система шифрования, являющаяся асимметричной криптографической системой, в которой зашифрование осуществляется с использованием открытого ключа получателя, а расшифрование — с помощью закрытого (личного) ключа получателя. — asymmetric encipherment system; public key encryption system

Примечание — См. [4] (пункт 3.2).

98 **шифр:** Семейство преобразований, реализующих процессы зашифрования и расшифрования и зависящих от криптографического ключа и, возможно, вектора инициализации, таких, что при соответствующих криптографических ключах применение преобразования расшифрования к результату преобразования зашифрования дает исходный открытый текст. — cipher

Примечание — Шифр может рассматриваться в качестве неинтерактивного криптографического протокола, состоящего из алгоритма зашифрования и алгоритма расшифрования, и поэтому является криптографическим механизмом (см. статью 10).

99 **зашифрование:** Зависящий от криптографического ключа процесс обратимого преобразования открытого текста в шифрованный текст. — encryption; encipherment

Примечание — См. [1] (пункт 3.11). См. также [4] (пункт 2.10), [12] (пункт 3.6), [5] (пункт 3.9).

100 **расшифрование** (Нрк. *расшифровка*): Зависящий от криптографического ключа процесс преобразования шифрованного текста в соответствующий ему открытый текст. — decryption; decipherment

Примечание — См. [4] (пункт 2.6). См. также [5] (пункт 3.6), ГОСТ Р 56205—2014 (статья 3.2.39).

101 **алгоритм зашифрования:** Криптографический алгоритм, реализующий зашифрование. — encryption algorithm

Примечание — См. также ГОСТ Р 34.12—2015 (пункт 2.1.1).

102 **алгоритм расшифрования:** Криптографический алгоритм, реализующий расшифрование. — decryption algorithm

Примечание — См. также ГОСТ Р 34.12—2015 (пункт 2.1.2).

103 **шифр замены:** Шифр, в котором зашифрование осуществляется применением к последовательным фрагментам открытого текста (знакам, блокам, словам или их комбинациям) обратимых преобразований, зависящих от криптографического ключа и, возможно, от управляющей ключевой последовательности. — substitution cipher

104 **шифр простой замены**: Шифр замены, реализующий одно и то же зависящее от криптографического ключа обратимое преобразование каждого знака (блока) открытого текста. — fixed substitution cipher

105 **шифр перестановки:** Шифр, в котором зашифрование осуществляется путем зависящей от криптографического ключа перестановки знаков (блоков) открытого текста. — permutation cipher

106 **шифрование с открытым ключом:** Шифрование с использованием асимметричной системы шифрования. — public key encryption

Примечание — См. [7] (статья 3.13), [13].

107 **шифрование с секретным ключом:** Шифрование с использованием симметричной системы шифрования. — symmetric key encryption

108 **код** (в криптографии): Шифр замены, в котором фрагменты открытого текста заменяются кодовыми обозначениями в соответствии с кодовой книгой, выполняющей функцию криптографического ключа. — code

109 **кодирование** (в криптографии): Зашифрование с помощью кода. — encoding

110 **декодирование** (в криптографии): Расшифрование с помощью кода. — decoding

111 **кодовая книга:** Документ, используемый для кодирования и декодирования, содержащий кодовый словарь и слоговую таблицу. — code book

112 **кодовый словарь:** Множество фрагментов открытого текста с назначенными им кодовыми группами. — code vocabulary

113 **кодовая группа:** Буквенно-цифровая комбинация, используемая в качестве кодового обозначения фрагмента открытого текста. — code group

114 **слоговая таблица:** Список отдельных букв и комбинаций букв (или слогов) с назначенными им кодовыми группами, используемый для кодирования (декодирования) слов или собственных имен, отсутствующих в кодовом словаре. syllabary

115 **аутентифицированное шифрование:** Шифрование, позволяющее дополнительно обеспечить аутентификацию шифруемых данных. authenticated encryption

Примечания

1 См. [14] (пункт 3.2).

2 См. определение термина «аутентификация данных» в статье 22.

116 **гомоморфное шифрование:** Шифрование, при котором шифртекст для результата некоторой алгебраической операции над открытыми текстами можно построить, применив (возможно, другую) алгебраическую операцию к соответствующим им шифртекстам, без знания криптографического ключа. homomorphic encryption

Примечание — См. [15] (введение), см. также [1] (пункт 3.15).

117 **поточный шифр:** Шифр замены, в котором выбор (обратимого) преобразования каждого знака (блока) открытого (шифрованного) текста определяется соответствующим символом управляющей ключевой последовательности. stream cipher

Примечание — См. [1] (пункт 3.27).

118 **управляющая ключевая последовательность;** *гамма:* Зависящая от криптографического ключа и, возможно, от некоторого фиксированного количества предыдущих знаков шифрованного текста последовательность, однозначно определяющая порядок выбора преобразований знаков (блоков) открытого (шифрованного) текста, используемая в поточных шифрах. keystream

Примечание — Для обеспечения криптографической стойкости управляющая ключевая последовательность должна удовлетворять ряду требований, в частности, быть близкой по своим свойствам к реализациям идеальной случайной последовательности.

119 **поточный шифр с самовосстановлением:** Поточный шифр, в котором знаки управляющей ключевой последовательности являются значениями функции, зависящей от криптографического ключа и некоторого фиксированного количества предыдущих знаков шифрованного текста. self-synchronizing stream cipher

120 **синхронный поточный шифр:** Поточный шифр, в котором управляющая ключевая последовательность полностью определяется криптографическим ключом и, возможно, вектором инициализации. synchronous stream cipher

Примечание — См. определение термина «вектор инициализации» в статье 127.

121 **шифр гаммирования:** Синхронный поточный шифр, в котором алфавиты открытого текста и управляющей ключевой последовательности совпадают, а каждый знак шифрованного текста (открытого текста) является значением обратимой по каждому аргументу функции от знака открытого текста (шифрованного текста) и знака управляющей ключевой последовательности. quasigroup encryption

122 **блочный шифр:** Шифр симметричной системы шифрования, в котором алгоритм зашифрования (расшифрования) последовательно применяется к блокам открытого (шифрованного) текста для получения последовательности блоков шифрованного текста (открытого текста). block cipher

Примечание — См. ГОСТ Р 34.12—2015, (пункт 2.1.5). См. также [1], (пункт 3.6).

123

базовый блочный шифр: Блочный шифр, реализующий зашифрование и расшифрование блока текста фиксированной длины.
[Адаптировано из ГОСТ Р 34.12—2015, пункт 2.1.3]

basic block cipher

Примечание — В симметричных криптосистемах алгоритмы зашифрования и расшифрования базового блочного шифра реализуются, как правило, итерациями однотипных преобразований.

124 **итерационный ключ:** Элемент последовательности ключей, вычисляемых в процессе развертывания исходного криптографического ключа, который используется на соответствующей итерации алгоритмов зашифрования и расшифрования блочного шифра.

round key

Примечание — См. также ГОСТ Р 34.12—2015 (пункт 2.1.7).

125 **развертывание ключа:** Построение управляющей ключевой последовательности по криптографическому ключу поточного шифра или построение последовательности итерационных ключей по ключу блочного шифра.

key scheduling

Примечание — См. также ГОСТ Р 34.12—2015 (пункт 2.1.10).

126 **вектор инициализации:** Набор символов, который используется для задания начального состояния криптографического алгоритма.

initialization vector

127 **режим работы блочного шифра:** Способ использования базового блочного шифра в общей конструкции криптографического преобразования блочного шифра.

block cipher mode of operation

Примечания

1 См. [13] (стр. V), См. также ГОСТ Р 34.13—2015 (раздел 5), Изменение № 1 к ГОСТ Р 34.13—2015.

2 Выбор режима работы блочного шифра имеет целью обеспечение определенных свойств, например, ограничение распространения искажений, простота синхронизации.

3 Основными режимами работы блочного шифра являются:
- режим простой замены (ECB, англ. Electronic Codebook);
- режим простой замены с зацеплением (CBC, англ. Cipher Block Chaining);
- режим гаммирования (CTR, англ. Counter);
- режим гаммирования с обратной связью по выходу (OFB, англ. Output Feedback);
- режим гаммирования с обратной связью по шифртексту (CFB, англ. Cipher Feedback);
- режим выработки имитовставки (MAC, англ. Message Authentication Code algorithm);
- режим гаммирования с преобразованием ключа (CTR-ACPKM, англ. Counter Advanced Cryptographic Prolongation of Key Material)
- режим аутентифицированного шифрования с ассоциированными данными (AEAD, англ. Authenticated Encryption with Associated Data).

Термины и определения, относящиеся к системе цифровой подписи

128 **цифровая подпись:** Результат криптографического преобразования набора данных (сообщения), зависящего от ключа подписи и параметров схемы цифровой подписи, обеспечивающий возможность аутентификации данных и невозможность отрицания факта создания.

digital signature

Примечания

1 См. [3] (пункт 3.7). См. также [16] (пункт 3.3.26), [17] (статья 3.11).

2 См. определение терминов «ключ подписи» и «параметр схемы цифровой подписи» в статье 145 и статье 135, терминов «аутентификация источника (данных)» и «целостность (данных)» — в приложении Б (статья Б.2.8 и Б.2.13).

129 **схема цифровой подписи:** Совокупность, состоящая из двух криптографических протоколов (алгоритмов), предназначенных для формирования и проверки подписи. digital signature scheme

Примечание — Использует ключевые пары, в которых личный ключ применяется для формирования подписи, а открытый — для ее проверки.

130 **формирование подписи:** Процесс, результатом выполнения которого для заданного набора данных (сообщения), ключа подписи и параметров схемы цифровой подписи является цифровая подпись указанного набора данных (сообщения). signature process

Примечания

1 См. [16] (пункт 3.14) и ГОСТ Р 34.10—2012 (статья 3.1.9).

2 Процесс формирования подписи в зависимости от схемы цифровой подписи может описываться криптографическим алгоритмом или протоколом формирования подписи.

131 **подписанный набор данных;** *подписанное сообщение:* Цифровая подпись набора данных [сообщения], а также часть (возможно, пустая) этого набора данных [сообщения], не восстанавливаемая из цифровой подписи. signed message

Примечание — См. [18] (пункт 3.15).

132 **цифровая подпись с восстановлением сообщения:** Цифровая подпись, сформированная таким образом, что при выполнении алгоритма проверки подписи сообщение или его часть могут быть извлечены из цифровой подписи. digital signature with message recovery

Примечание — См. [18] (введение и статья 3.15).

133 **цифровая подпись с дополнением:** Цифровая подпись, сформированная таким образом, что никакая часть подписываемого сообщения не может быть извлечена из цифровой подписи, дополнением к которой служит само подписываемое сообщение. digital signature with appendix

Примечание — См. [18] (введение, статья 3.15, и примечание).

134 **проверка подписи:** Процесс, в котором в качестве исходных данных используются подписанный набор данных (подписанное сообщение), ключ проверки подписи и параметры схемы цифровой подписи, выполняемый либо независимо, либо с участием стороны, которая по предположению является подписывающей, а результатом является заключение о корректности или некорректности цифровой подписи. verification process

Примечания

1 См. [18] (пункт 3.17) и ГОСТ Р 34.10—2012 (пункт 3.1.8).

2 Процесс проверки подписи в зависимости от схемы цифровой подписи может описываться криптографическим алгоритмом или протоколом проверки подписи.

135 **параметр схемы цифровой подписи:** Элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам. domain parameter

Примечание — См. ГОСТ Р 34.10—2012 (пункт 3.1.4).

136 **схема цифровой подписи вслепую:** Схема цифровой подписи, формирование подписи в которой осуществляется двумя участниками — запрашивающей стороной (владеющей набором данных (сообщением), для которого формируется подпись) и подписывающей стороной (владеющей ключом подписи) — таким образом, что подписывающая сторона не получает никакой информации о подписанном наборе данных (сообщении). blind signature scheme

Примечания

1 См. [19] (пункт 3.3).

2 См. определение термина «подписанный набор данных [подписанное сообщение]» в статье 131.

137 **схема конфиденциальной [неоспоримой] цифровой подписи:** Схема цифровой подписи, в которой процесс проверки подписи требует участия стороны, которая по предположению является подписывающей. undeniable signature scheme

Примечания

1 При реализации данной схемы факт формирования подписи конкретной стороной остается конфиденциальным и может быть установлен только в том случае, если подписавшая сторона дает на это согласие. Второе наименование «неоспоримая подпись» объясняется тем, что если подписавшая сторона обязана участвовать в процедуре проверки подписи, то она не сможет отказаться от подписи, если подпись является подлинной, но сможет доказать, что это не ее подпись, если она не подписывала документ.

2 См. определение термина «конфиденциальность» в приложении Б (статья Б.2.12).

138 **схема анонимной цифровой подписи:** Схема цифровой подписи, обеспечивающая анонимность подписывающей стороны и несвязываемость. anonymous signature scheme

Пример — Схема групповой цифровой подписи, схема кольцевой цифровой подписи.

Примечания

1 См. [20] (пункт 2.1).

2 См. определение термина «анонимность» в приложении Б, (статья Б.2.1), определение термина «несвязываемость» в приложении А, (статья А.2.14).

139 **схема групповой цифровой подписи:** Схема анонимной цифровой подписи, в которой правом формирования подписи от имени группы, оставаясь анонимным, обладает каждый из входящих в нее членов, при этом каждый из них обладает своим личным ключом, а проверка групповой цифровой подписи осуществляется с помощью единственного открытого ключа. group signature scheme

Примечания

1 См. [20] (пункты 2.30, 2.31).

2 Подписавший набор данных (сообщение) член группы остается анонимным, и его анонимность может быть нарушена только в случае необходимости разрешения спорной ситуации.

3 Формированием группы (регистрацией и выработкой ключей участников группы) занимается один из ее членов, определенный заранее.

140 **схема кольцевой цифровой подписи:** Схема анонимной цифровой подписи, в которой сторона с целью обеспечения своей анонимности формирует подпись от имени группы, в которую помимо себя включает одного или нескольких потенциальных участников, используя свой личный ключ и открытые ключи потенциальных участников, а проверка подписи осуществляется с помощью открытых ключей всех членов сформированной группы. ring signature scheme

Примечания

1 См. [20] (пункты 2.45, 2.46).

2 Подписавший сообщение член группы остается анонимным, и его анонимность не может быть нарушена.

3 Подписавший сообщение член группы имеет возможность самостоятельно выбрать остальных членов группы, используя их открытые ключи и не оповещая их об этом.

141

электронная подпись: Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой) или иным образом связанная с такой информацией и которая используется для определения лица, подписывающего информацию.

[[21], статья 2].

electronic signature

Примечания

1 Термин применяется в документах, устанавливающих условия юридической равнозначности электронной и собственноручной подписи.

2 Для формирования электронной подписи, в зависимости от условий применения, могут быть использованы различные технологии (цифровой подписи, кода аутентификации, цифрового водяного знака, штрих-кода и др.), однако для достоверной аутентификации источника данных необходимо использовать систему цифровой подписи и инфраструктуру открытых ключей.

142 **усиленная электронная подпись:** Электронная подпись, удовлетворяющая следующим требованиям:

- получена в результате криптографического преобразования информации с использованием ключа подписи;
- с ее помощью можно подтвердить подлинность лица, подписавшего данные;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создана с использованием средств электронной подписи.

advanced electronic signature

Примечание — Из первых трех требований вытекает, что усиленная электронная подпись формируется и проверяется с помощью системы цифровой подписи.

143 **квалифицированная электронная подпись:** Электронная подпись, которая соответствует всем признакам усиленной электронной подписи, а также двум дополнительным признакам:

- ключ проверки подписи указан в квалифицированном сертификате;
- для создания и проверки подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с [21].

qualified electronic signature

Примечания

1 Уточнено для целей настоящего стандарта на основе Федерального закона [21] (статья 5, часть 4).

2 См. определение термина «квалифицированный сертификат ключа проверки электронной подписи» в статье 148.

144 **неквалифицированная электронная подпись:** Усиленная электронная подпись, которая не является квалифицированной.

unqualified electronic signature

145

ключ подписи: Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи.

[ГОСТ Р 34.10—2012, статья 3.1.2]

signature key

146

ключ проверки подписи: Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи.

[ГОСТ Р 34.10—2012, статья 3.1.3]

verification key

147

сертификат ключа проверки электронной подписи: Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

[[21], статья 2]

verification key certificate

Примечание — Содержание сертификата ключа проверки электронной подписи определяется частью 2 статьи 14 [21].

148 **квалифицированный сертификат (ключа проверки электронной подписи):** Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.

qualified verification key certificate

Примечание — См. [21] (часть 3 статьи 2).

149 **невозможность отрицания:** Свойство способа фиксации информации об имевших место действиях или событиях, исключающее возможность их последующего отрицания.

non-repudiation

150 **невозможность отрицания создания:** Свойство способа фиксации информации о факте создания сообщения (документа) конкретным лицом, исключающее возможность последующего отрицания им этого факта.

non-repudiation of creation

Примечание — См. [22] (пункт 3.23).

151 **невозможность отрицания доставки сообщения:** Свойство способа фиксации информации о доставке сообщения и ознакомления с его содержанием, исключающее возможность последующего отрицания этого факта получателем.

non-repudiation of delivery

Примечание — См. [20] пункт 3.24.

152 **невозможность отрицания ознакомления с содержанием полученного сообщения:** Свойство способа фиксации информации об ознакомлении получателя с содержанием полученного сообщения, исключающее возможность последующего отрицания этого факта.

non-repudiation of knowledge

Примечание — См. [22] (пункт 3.28).

153 **невозможность отрицания создания и отправления сообщения:** Свойство способа фиксации информации о создании и отправлении сообщения с данным содержанием конкретным лицом, исключающее возможность последующего отрицания им этого факта.

non-repudiation of origin

Примечание — См. [22] (пункт 3.29).

154 **невозможность отрицания получения:** Свойство способа фиксации информации о получении сообщения, исключающее возможность последующего отрицания этого факта.

non-repudiation of receipt

Примечание — См. [22] (пункт 3.33).

155 **невозможность отрицания отправления:** Свойство способа фиксации информации об отправке сообщения, исключающее возможность последующего отрицания этого факта.

non-repudiation of sending

Примечание — См. [22] (пункт 3.35).

156 **невозможность отрицания участия:** Свойство способа фиксации информации о принятии от отправителя сообщения доверенной стороной, осуществляющей доставку сообщения его получателю, исключающее возможность последующего отрицания ею этого факта. non-repudiation of submission

Примечание — См. [22] (пункт 3.35).

157 **невозможность отрицания передачи:** Свойство способа фиксации для отправителя информации о доставке сообщения его получателю доверенной стороной, отвечающей за доставку сообщения, исключающее возможность последующего отрицания получателем этого факта. non-repudiation of transport

Примечание — См. [22] (пункт 3.38).

158 **(бесключевая) криптографическая хеш-функция:** Функция, отображающая множество всех конечных битовых строк в множество битовых строк фиксированной длины, для которой следующие задачи являются вычислительно трудными: cryptographic hash function

- для почти каждого значения функции вычислить хотя бы одну битовую строку, отображаемую в это значение;
- для заданной битовой строки вычислить другую битовую строку, отображаемую в то же значение функции;
- вычислить какую-либо пару различных битовых строк, отображаемых в одно и то же значение.

Примечания

1 См. ГОСТ Р 34.10—2012 (пункт 3.1.14).

2 Вычислительная трудность определяется конкретными требованиями к практической стойкости данного криптографического механизма.

Термины и определения, относящиеся к системе имитозащиты

159 **имитозащита** (в криптографии): Защита от атак, имеющих целью имитацию и подмену сообщения, которая реализуется путем выработки и проверки имитовставок. imitation protection

160 **имитация (сообщения)** (в криптографии): Результат атаки на криптографическую систему, в ходе которой атакующий формирует сообщение от имени другой стороны, которое не отвергается получателем. imitation

161 **подмена сообщения** (в криптографии): Результат атаки на криптографическую систему, в ходе которой атакующий модифицирует или заменяет сообщение, переданное одной из сторон, другим сообщением от имени той же стороны, которое не отвергается получателем. substitution

162 **криптографическая хеш-функция, зависящая от ключа:** Зависящая от криптографического ключа функция, отображающая множество всех конечных битовых строк в множество битовых строк фиксированной длины и удовлетворяющая следующим условиям: keyed hash function; message authentication code algorithm (MAC algorithm)

- для любого криптографического ключа и любой входной строки функция может быть вычислена эффективно;
- для любого набора входных строк и значений функции на них, полученных при фиксированном значении криптографического ключа, вычислительно трудно, не зная этого криптографического ключа, найти значение функции на новой строке, не входящей в этот набор.

Примечания

1 См. [12] (пункт 3.10).

2 Применяется в системах имитозащиты.

3 Вычислительная трудность определяется конкретными требованиями к практической стойкости данного криптографического механизма.

163 **имитовставка;** *код аутентичности сообщения:* Битовая строка, добавляемая к сообщению с целью обеспечения возможности обнаружения подмены и/или имитации сообщения и являющаяся результатом применения к нему криптографической хеш-функции, зависящей от ключа. — message authentication code (MAC)

Примечание — См. [12] (пункт 3.9).

164 **безусловно стойкая система имитозащиты:** Система имитозащиты, обеспечивающая минимально возможные значения вероятностей успеха атак имитации и подмены сообщения. — unconditionally secure authentication system

Примечание — В данном случае в качестве математической модели системы имитозащиты, позволяющей охарактеризовать ее теоретическую стойкость, применяется теоретико-информационная модель.

Термины и определения, относящиеся к системе аутентификации стороны

165 **криптографический протокол аутентификации стороны:** Криптографический протокол с двумя участниками (проверяющей стороной и доказывающей стороной), позволяющий проверяющей стороне провести аутентификацию доказывающей стороны. — authentication protocol

Примечания

1 См. определение термина «аутентификация стороны» в приложении Б (статья Б.2.9).

2 Различают следующие виды криптографических протоколов аутентификации стороны:

- протоколы с однократной передачей сообщений, основанные на известной обеим сторонам информации (пароли, персональные идентификационные числа, криптографические ключи);
- протоколы с двукратной передачей сообщений типа «запрос—ответ»;
- протоколы с трехкратной передачей сообщений на основе техники доказательства с нулевым разглашением.

166 **доказывающая сторона** (в криптографическом протоколе аутентификации стороны): Сторона протокола, пытающаяся подтвердить другой стороне свою подлинность. — claimant; prover

Примечание — См. [17] (пункт 3.6), см. также [23] (пункт 2.7).

167 **проверяющая сторона** (в криптографическом протоколе аутентификации стороны): Сторона протокола, осуществляющая проверку подлинности другой стороны. — verifier

Примечание — См. [17] (пункт 3.40), см. также [23] (пункт 2.30).

168 **подмена стороны** (в криптографии): Результат атаки на криптографический протокол, с помощью которой атакующий выдает себя за легитимного участника этого протокола. — impersonation

169 **свидетельство** (в криптографическом протоколе аутентификации стороны): Сообщение протокола с трехкратной передачей сообщений, сформированное доказывающей стороной, зависящее от защищенного от раскрытия параметра, позволяющее проверяющей стороне убедиться, что в процессе выполнения протокола не произошла подмена доказывающей стороны. — witness

Примечания

1 См. [23] (пункт 2.31).

2 Значение защищенного от раскрытия параметра представляет собой случайное число, которое после выполнения протокола аутентификации стороны должно быть удалено доверенным образом, так как его раскрытие, как правило, влечет компрометацию ключевых параметров доказывающей стороны.

170 **запрос** (в криптографическом протоколе аутентификации стороны): Сообщение протокола с дву- или трехкратной передачей сообщений, выработанное проверяющей стороной и обрабатываемое доказывающей стороной. challenge

Примечание — См. [23] (пункт 2.6).

171 **ответ** (в криптографическом протоколе аутентификации стороны): Сообщение протокола аутентификации стороны с дву- или трехкратной передачей сообщений, выработанное доказывающей стороной в ответ на запрос и обрабатываемое проверяющей стороной. response

Примечание — См. [23] (пункт 2.25).

172 **кратность обмена** (в криптографическом протоколе аутентификации стороны): Количество сообщений, отправляемых сторонами в криптографическом протоколе аутентификации стороны. exchange multiplicity parameter

Примечание — См. [23] (пункт 2.15).

173 **взаимная аутентификация:** Обоюдная аутентификация сторон, при которой каждая из сторон убеждается в подлинности взаимодействующей с ней стороны. mutual entity authentication

Примечания

1 См. [5] (пункт 3.28).

2 См. определение термина «аутентификация стороны» в приложении Б (статья Б.2.9).

174 **доказательство с нулевым разглашением:** Криптографический протокол с двумя участниками (проверяющей стороной и доказывающей стороной), позволяющий доказывающей стороне убедить проверяющую сторону в том, что ей известен некоторый секрет, не предоставляя о нем никакой информации. zero knowledge proof

Примечания

1 Доказательство с нулевым разглашением знания личного ключа может использоваться в качестве протокола аутентификации стороны.

2 См. [23] (приложение В).

175 **обязательство (в криптографии):** Результат криптографического преобразования набора данных (сообщения) без использования криптографического ключа, которое обеспечивает невозможность получить о наборе никакой информации (свойство сокрытия) и невозможность его подмены (свойство привязки). commitment

Примечание — В отличие от свидетельства использование обязательства предполагает последующее раскрытие защищаемого набора данных (сообщения).

176 **схема обязательств:** Совокупность, состоящая из двух криптографических алгоритмов, первый из которых предназначен для формирования обязательства для некоторого набора данных (сообщения), второй — для его раскрытия. commitment scheme

Термины и определения, относящиеся к средствам криптографической защиты информации

177 **средства криптографической защиты информации;** СКЗИ: Средства, системы и комплексы, реализующие криптографическую систему или отдельные криптографические механизмы. — cryptographic module

Примечание — К средствам криптографической защиты информации относятся средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов, ключевые документы.

178 **средство шифрования;** шифрсредство: Средство криптографической защиты информации, реализующее алгоритм зашифрования или алгоритм расшифрования или шифр в целом или систему шифрования в целом. — encryption module

Примечание — См. определения терминов «система шифрования», «шифр», «алгоритм зашифрования», «алгоритм расшифрования» в статьях 26, 102, 105, 106 соответственно.

179 **средство имитозащиты:** Средство криптографической защиты информации, реализующее зависящую от ключа криптографическую хеш-функцию или систему имитозащиты в целом. — data authentication module

Примечание — См. определение термина «система имитозащиты» в статье 25.

180 **средство электронной подписи:** Средство криптографической защиты информации, реализующее хотя бы одну из следующих функций: — digital signature module

- создание электронной подписи с использованием ключа электронной подписи;
- проверка электронной подписи с использованием ключа проверки электронной подписи;
- создание ключа электронной подписи и ключа проверки электронной подписи.

Примечание — См. определение термина «электронная подпись» в статье 141.

181 **средство изготовления ключевых документов:** Средство криптографической защиты информации, реализующее в соответствии с установленными требованиями процессы изготовления и/или распределения ключевых документов для средств криптографической защиты информации независимо от вида носителя ключевой информации. — key production module

182 **средство кодирования:** Средство шифрования, реализующее зашифрование и расшифрование с помощью кода. — encoding module

183 **жизненный цикл средства криптографической защиты информации;** жизненный цикл СКЗИ: Совокупность явлений и процессов, повторяющихся с периодичностью, определяемой временем существования типовой конструкции (образца) средства криптографической защиты информации от ее замысла до утилизации, или конкретного экземпляра средства криптографической защиты информации от момента его производства до утилизации. — cryptographic module life cycle

Примечание — См. [2] (пункт 3.1.6). См. также ГОСТ Р 56136—2014 (пункт 3.16).

184 **ключевая информация:** Специальным образом организованная совокупность данных, ключевых материалов и/или криптографических ключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока. key information

Примечание — См. [2] (пункт 3.1.20).

185 **ключевой документ:** Подлежащий учету (регистрации) носитель информации, содержащий в себе ключевую информацию и/или инициализирующую последовательность, а также, при необходимости, контрольную, служебную и технологическую информацию. key document

Примечания

1 См. [2] (пункт 3.1.21).

2 См. определение термина «инициализирующая последовательность» в приложении А (статья А.2.11).

186 **ключевой носитель:** Физический носитель, предназначенный для размещения и хранения на нем ключевой информации и/или инициализирующей последовательности. key storage device

Примечание — См. [2] (пункт 3.1.22).

187 **загрузчик ключей:** Устройство, способное содержать, по крайней мере, один открытый текст, или зашифрованный криптографический ключ, или часть криптографического ключа, позволяющее осуществить их загрузку в средство криптографической защиты информации key loader

188 **устойчивость к извлечению ключа:** Свойство средства криптографической защиты информации, препятствующее несанкционированным попыткам извлечения криптографического ключа. key extraction resistance

189 **установка ключа:** Защищенный от компрометации ключа процесс ввода криптографического ключа в средство криптографической защиты информации. key installation

Примечание — См. [4] (пункт 2.26).

190 **среда функционирования средства криптографической защиты информации;** среда функционирования СКЗИ: Совокупность одного или нескольких аппаратных средств и программного обеспечения, совместно с которыми штатно функционирует средство криптографической защиты информации и которые способны повлиять на выполнение предъявляемых к нему требований. operational environment

Примечание — См. [2] (пункт 3.1.43). См. также [24] (пункт 3.83).

191 **средство предварительного шифрования:** Средство шифрования, с помощью которого процессы зашифрования и расшифрования выполняются независимо от процессов передачи и приема соответственно. off-line cryptographic module

192 **средство линейного шифрования:** Средство шифрования, с помощью которого процессы зашифрования и расшифрования выполняются совместно с процессами передачи и приема соответственно. on-line cryptographic module

193 **одноразовый блокнот:** Средство шифрования, содержащее набор криптографических ключей, используемых для однократного шифрования. one-time pad

Алфавитный указатель терминов на русском языке

алгоритм зашифрования 101
алгоритм криптографический 8
алгоритм расшифрования 102
анализ криптографический 11
архитектура инфраструктуры открытых ключей 54
архитектура инфраструктуры открытых ключей иерархическая 55
архитектура инфраструктуры открытых ключей сетевая 56
архитектура ИОК 54
архитектура ИОК иерархическая 55
архитектура ИОК сетевая 56
атака на криптографический механизм 14
атака на криптосистему 14
аутентификация взаимная 173
аутентификация данных 22
аутентификация ключа для стороны В стороной А полная 82
аутентификация ключа для стороны В стороной А частичная 81
блокнот одноразовый 193
вектор инициализации 126
выработка общего секретного ключа 78
выработка общего секретного ключа совместная 78
гамма 118
группа кодовая 113
декодирование 110
депонирование ключа 42
дешифрование 27
длина ключа 34
доказательство с нулевым разглашением 174
документ ключевой 185
загрузчик ключей 187
задачи криптографической защиты информации 6
запрос 170
зашифрование 99
защита информации криптографическая 2
защищенность от чтения назад взаимная 86
защищенность от чтения назад по отношению к каждой из сторон 85
защищенность от чтения назад по отношению к стороне А 84
иерархия секретных ключей 62
иерархия производных ключей 66
имитация 160

имитация сообщения 160
имитовставка 163
имитозащита 159
информация ключевая 184
информация ключевая исходная 35
информация об открытом ключе 46
инфраструктура открытых ключей 53
инфраструктура управления ключами 37
ИОК 53
ключ долговременный 61
ключ закрытый 44
ключ итерационный 124
ключ корневой 67
ключ криптографический 4
ключ личный 44
ключ одноразовый 60
ключ открытый 45
ключ подписи 145
ключ проверки подписи 146
ключ сеансовый 68
ключ секретный 58
ключ секретный главный 63
ключ производный 70
ключ составной 59
ключ шифрования данных 64
ключ шифрования ключей 65
книга кодовая 111
код 108
код аутентичности сообщения 163
кодирование 109
компрометация ключа 40
кратность обмена 172
криптоанализ 11
криптография 1
криптография квантовая 28
криптография постквантовая 29
криптография низкоресурсная 30
криптосинтез 7
криптосистема 5
криптосистема с открытым ключом 17

материал ключевой 35
метод криптографического анализа 12
метод полного перебора 32
метод полного перебора при криптографическом анализе 32
механизм инкапсуляции ключа 77
механизм криптографический 10
множество ключей 33
набор данных подписанный 131
невозможность отрицания 149
невозможность отрицания доставки сообщения 151
невозможность отрицания ознакомления с содержанием полученного сообщения 152
невозможность отрицания отправления 155
невозможность отрицания передачи 157
невозможность отрицания получения 154
невозможность отрицания создания 150
невозможность отрицания создания и отправления сообщения 153
невозможность отрицания участия 156
носитель ключевой 186
обязательство 175
обязательство в криптографии 175
ответ 171
пара ключевая 43
параметр схемы цифровой подписи 135
передача ключа защищенная 76
подмена сообщения 161
подмена стороны 168
подпись с восстановлением сообщения цифровая 132
подпись цифровая 128
подпись цифровая с дополнением 133
подпись электронная 141
подпись электронная квалифицированная 143
подпись электронная неквалифицированная 144
подпись электронная усиленная 142
подтверждение ключа 80
последовательность ключевая управляющая 118
преобразование криптографическое 3
проверка подписи 134
протокол аутентификации и формирования общего ключа 79
протокол аутентификации стороны криптографический 165
протокол выработки общего аутентифицированного ключа 83

протокол криптографический 9
развертывание ключа 125
разделение секрета 89
размер ключа 34
распределение секретных ключей 71
распределение секретных ключей предварительное 74
расшифрование 100
расшифровка 100
режим работы блочного шифра 127
свидетельство 169
сертификат квалифицированный 148
сертификат ключа проверки электронной подписи 147
сертификат ключа проверки электронной подписи квалифицированный 148
сертификат открытого ключа 47
синтез криптографический 7
система имитозащиты 23
система имитозащиты безусловно стойкая 164
система ключевая 20
система криптографическая 5
система криптографическая асимметричная 17
система криптографическая аутентификации стороны 21
система криптографическая гибридная 19
система криптографическая личностная 31
система криптографическая на основе идентификаторов 31
система криптографическая симметричная 18
система цифровой подписи 24
система шифрования 25
система шифрования асимметричная 97
система шифрования симметричная 96
система шифрования с открытым ключом 97
система шифрования с секретным ключом 96
СКЗИ 177
словарь кодовый 112
служба штампов времени 52
сообщение подписанное 131
список аннулированных сертификатов 57
список отозванных сертификатов 57
среда функционирования СКЗИ 190
среда функционирования средства криптографической защиты информации 190
средства криптографической защиты информации 177

средство изготовления ключевых документов 181
средство имитозащиты 179
средство кодирования 182
средство линейного шифрования 192
средство предварительного шифрования 191
средство шифрования 178
средство электронной подписи 180
срок действия ключа 39
стойкость 13
стойкость криптографическая 13
стойкость практическая 15
стойкость теоретическая 16
стойкость доказуемая 16
стойкость системы шифрования совершенная 26
сторона доказывающая 166
сторона проверяющая 167
схема анонимной цифровой подписи 138
схема групповой цифровой подписи 139
схема кольцевой цифровой подписи 140
схема конфиденциальной цифровой подписи 137
схема неоспоримой цифровой подписи 137
схема обязательств 176
схема разделения секрета 90
схема разделения секрета идеальная 93
схема разделения секрета пороговая 91
схема разделения секрета совершенная 92
схема цифровой подписи 129
схема цифровой подписи вслепую 136
таблица слоговая 114
текст открытый 94
текст шифрованный 95
уничтожение ключа 41
управление ключами 36
установка ключа 189
установка общего ключа 75
устойчивость к выработке общего ключа с неизвестной стороной 88
устойчивость к извлечению ключа 188
устойчивость к подмене стороны при компрометации ключа 87
формирование общего ключа 75
формирование подписи 130

функция выработки производного ключа 69
функция диверсификации ключа 69
хеш-функция криптогрфическая 158
хеш-функция криптографическая, зависящая от ключа 162
хеш-функция криптографическая бесключевая 158
центр передачи ключей 73
центр перешифрования ключей 73
центр распределения ключей 72
центр регистрации 49
центр сертификации 48
центр сертификации открытых ключей 48
центр удостоверяющий 50
цикл ключа жизненный 38
цикл СКЗИ жизненный 183
цикл средства криптографической защиты информации жизненный 183
шифр 98
шифр блочный 122
шифр блочный базовый 123
шифр гаммирования 121
шифр замены 103
шифр перестановки 105
шифр поточный 117
шифр простой замены 104
шифр синхронный поточный 120
шифрсредство 178
шифр с самовосстановлением поточный 119
шифрование аутентифицированное 115
шифрование гомоморфное 116
шифрование с открытым ключом 106
шифрование с секретным ключом 107
шифрсистема 25
шифртекст 95
штамп времени 51

Алфавитный указатель эквивалентов терминов на английском языке

advanced electronic signature	142
AKE protocol	79
anonymous signature scheme	138
asymmetric cryptosystem	17
asymmetric encipherment system	97
attack on the cryptographic mechanism	14
attack on the cryptosystem	14
authenticated encryption	115
authenticated key agreement protocol	83
authentication protocol	165
basic block cipher	123
blind signature scheme	136
block cipher	122
block cipher mode of operation	127
breaking an encipherment system	27
brute-force attack	32
certificate revocation list	57
certification authority	50
certification center	48
challenge	170
cipher	98
ciphersystem	25
ciphertext	95
claimant	166
code	108
code book	111
code group	113
code vocabulary	112
commitment	175
commitment scheme	176
composite key	59
cryptanalysis	11
cryptographic algorithm	8
cryptographic analysis	11
cryptographic hash function	158
cryptographic information protection goals	6
cryptographic key	4
cryptographic mechanism	10
cryptographic protocol	9
cryptographic module	177
cryptographic module life cycle	183
cryptographic synthesis	7

cryptographic protection of information 2
cryptographic transformation 3
cryptographic security 13
cryptographic system 5
cryptography 1
cryptosystem 5
data authentication 22
data authentication module 179
data encryption key 64
decipherment 100
decoding 110
decryption 100
decryption algorithm 102
derivation key 67
derivation key hierarchy 66
derived key 70
digital signature 128
digital signature module 180
digital signature scheme 129
digital signature system 24
digital signature with appendix 133
digital signature with message recovery 132
domain parameter 135
electronic signature 141
encipherment 99
encipherment system 25
encoding 109
encoding module 182
encryption 99
encryption module 178
encryption algorithm 101
encryption system 25
entity authentication cryptosystem 21
exchange multiplicity parameter 172
exhaustive search method 32
explicit key authentication from entity A to entity B 82
fixed substitution cipher 104
forward secrecy with respect to both entity A and entity B individually 85
forward secrecy with respect to entity A 84
group signature scheme 139
hierarchy type PKI architecture 55
hierarchy type public key infrastructure architecture 55
homomorphic encryption 116
hybrid cryptosystem 19

ideal secret sharing scheme 93
identity-based cryptosystem 31
imitation 160
imitation protection 159
impersonation 168
implicit key authentication from entity A to entity B 81
initialization vector 126
key agreement 78
key compromise 40
key compromise impersonation resistance 87
key confirmation 80
key derivation function 69
key destruction 41
key distribution 71
key distribution centre 72
key document 185
key encapsulation mechanism 77
key encryption key 65
key escrow 42
key establishment 75
key extraction resistance 188
keyed hash function 162
key information 184
keying material 35
key installation 189
key length 34
key life cycle 38
key life time 39
key loader 187
key management 36
key management infrastructure 37
key production module 181
key pair 43
key scheduling 125
key size 34
key space 33
key storage device 186
keystream 118
key system 20
key translation centre 73
key transport 76
lightweight cryptography 30
logical key hierarchy 62
long-term key 61

MAC 163
MAC algorithm 162
master key 63
message authentication code algorithm 162
message authentication code 163
method of cryptanalysis 12
mutual entity authentication 173
mutual forward secrecy 86
network type PKI architecture 56
network type public key infrastructure architecture 56
non-repudiation 149
non-repudiation of creation 150
non-repudiation of delivery 151
non-repudiation of knowledge 152
non-repudiation of origin 153
non-repudiation of receipt 154
non-repudiation of sending 155
non-repudiation of submission 156
non-repudiation of transport 157
off-line cryptographic module 191
one time key 60
one-time pad 193
on-line cryptographic module 192
operational environment 190
perfect secret sharing scheme 92
perfect security of an encipherment system 26
permutation cipher 105
PKI 53
PKI architecture 54
plaintext 94
post-quantum cryptography 29
preliminary key distribution 74
protocol for authentication and key establishment 79
private key 44
provable security 16
prover 166
public key 45
public key infrastructure architecture 54
public key certificate 47
public key encryption 106
public key encryption system 97
public key information 46
public key infrastructure 53
public key system 17

qualified electronic signature 143
qualified verification key certificate 148
quantum cryptography 28
quasigroup encryption 121
registration authority 49
response 171
ring signature scheme 140
round key 124
secret key 58
secret key encryption system 96
secret sharing 89
secret sharing scheme 90
security 13
security strength 15
self-synchronizing stream cipher 119
session key 68
signed message 131
signature key 145
signature process 130
static key 61
stream cipher 117
substitution 161
substitution cipher 103
syllabary 114
symmetric encipherment system 96
symmetric cryptosystem 18
symmetric data authentication system 23
symmetric key encryption 107
synchronous stream cipher 120
threshold secret sharing scheme 91
time stamping authority 52
time-stamp token 51
unconditionally secure authentication system 164
undeniable signature scheme 137
unknown key share attack resistance 88
unqualified electronic signature 144
verification key 146
verification key certificate 147
verification process 134
verifier 167
witness 169
zero knowledge proof 174

Приложение А
(справочное)

Вспомогательные термины и определения в области криптографической защиты информации, не включенные в раздел 3 настоящего стандарта

А.1 Общие положения

В настоящем приложении приведены термины с соответствующими определениями, относящиеся к области криптографической защиты информации, но являющиеся вспомогательными по отношению к терминам, включенным в раздел 3 настоящего стандарта.

А.2 Термины и определения

А.2.1

блок (block): Строка бит определенной длины. [ГОСТ Р 34.12—2015, статья 2.1.4]

См. также [1], пункт 3.5.

А.2.2 **разбиение на блоки** (partition) Разбиение открытого текста на блоки одинаковой длины, за исключением последнего блока, который может иметь меньшую длину.

А.2.3 **дополнение** (padding): Приписывание дополнительных бит к строке бит.

Примечание — См. ГОСТ Р 34.11—2012 (пункт 3.1.1). См. также [25] (пункт 3.7).

А.2.4 **однократно используемое число** (nonce): Значение, используемое в криптографических протоколах, которое никогда не повторяется с одним и тем же ключом.

А.2.5 **персональное идентификационное число;** ПИН [personal identification number (PIN)]: Последовательность цифр, используемая для аутентификации сторон и являющаяся предустановленным запоминаемым секретом.

Примечания

1 См. [4] (пункт 2.34).

2 ПИН, как и пароль, относится к так называемым слабым секретам, обладающим более низкой энтропией по сравнению с ключом и допускающим возможность подбора.

А.2.6 **криптонабор** (cipher suite): Набор данных, определяющий криптографические алгоритмы (шифрования, хеширования, электронной подписи) и их параметры, необходимые для выполнения шагов криптографического протокола.

Примечание — Криптонабору соответствует уникальный идентификатор.

А.2.7 **криптографический токен** (cryptographic token): Портативное физическое устройство, контролируемое пользователем (например, смарт-карта или PCMCIA-карта), используемое для хранения криптографического ключа и, возможно, выполнения криптографических преобразований.

А.2.8 **идеальная случайная последовательность** (ideal random sequence): Последовательность независимых случайных величин, имеющих равномерное распределение вероятностей на заданном конечном алфавите.

А.2.9 **псевдослучайная последовательность** (pseudo-random sequence): Последовательность, порожденная детерминированным устройством или программой, обладающая свойствами, близкими к свойствам типичных реализаций идеальной случайной последовательности.

Примечание — См. [26] (пункт 3.26).

А.2.10 **открытое начальное значение;** «соль» (salt): Общедоступный параметр криптографического механизма, обеспечивающий невозможность использования результатов повторного применения данного механизма к одному и тому же набору входных данных.

Примечание — См. [27] (пункт 3.2).

А.2.11 **инициализирующая последовательность** (secret seed): Совокупность данных, используемая для инициализации генератора псевдослучайных последовательностей.

Примечание — См. [2] (пункт 3.1.13).

А.2.12 **случайное число** (random number): Случайная величина, имеющая равномерное распределение вероятностей на заданном конечном алфавите.

Примечание — См. [4] (пункт 2.39).

А.2.13 **генератор случайных чисел** (random number generator): Устройство или программный модуль, вырабатывающие последовательность случайных или псевдослучайных чисел.

Примечания

1 Существуют два основных класса генераторов: детерминированные и недетерминированные. Первые основаны на детерминированных алгоритмах, которые вырабатывают последовательность бит из секретного начального заполнения (см. А.2.11). При использовании одного и того же секретного начального заполнения генератор воспроизводит одну и ту же последовательность. Недетерминированный генератор вырабатывает последовательность случайных чисел, которая зависит от некоторого непредсказуемого физического или биологического источника, и поэтому невоспроизводима.

А.2.14 **несвязываемость** (unlinkability): Невозможность установить, кто именно выполнил данное конкретное действие, а также выяснить, были ли разные действия выполнены одним и тем же участником.

Приложение Б
(справочное)

Термины и определения, применяемые в областях деятельности, смежных с криптографической защитой информации

Б.1 Общие положения

В настоящем приложении приведены термины с соответствующими определениями, относящиеся к областям деятельности, смежным с криптографической защитой информации. Перечисление данных терминов в настоящем приложении имеет целью унификацию терминологии в областях криптографической защиты информации и смежных с ней.

Б.2 Термины и определения

Б.2.1 **анонимность** (anonymity): Свойство способа информационного взаимодействия, гарантирующее отсутствие индивидуальности, отличительных признаков и узнаваемости внутри обмена сообщениями.

Примечание — См. [28] (статья 2.1).

Б.2.2 **нотаризация** (notarization): Нотариальное подтверждение характеристик сторон, участвующих во взаимодействии или событии, а также хранящихся или передаваемых данных.

Примечание — См. [22] (статья 3.41).

Б.2.3 **неотслеживаемость** (untraceability): Невозможность получения сведений о действиях данной стороны информационного взаимодействия на основании анализа трафика.

Б.2.4

анализ трафика (traffic analysis): Извлечение информации из видимых характеристик потока(ов) данных, даже если данные зашифрованы или непосредственно недоступны, причем указанные характеристики включают в себя степени идентичности и месторасположения источника(ов) и адресата(ов), наличие и объем потоков, а также частоту и длительность их передачи.

[ГОСТ Р 56205—2014/IEC/TS 62443-1-1:2009, статья 3.2.128]

Б.2.5 **защита трафика** (traffic protection): Процесс преобразования потока передаваемых данных в канале связи в целях его защиты от анализа трафика.

Б.2.6 **атака (на информационную систему)** (attack): Попытки нанести ущерб или вывести из строя информационную систему, получить, преобразовать или уничтожить защищаемую системой информацию или иным образом нарушить политику безопасности.

Примечание — См. [29] (статья 2.1).

Б.2.7

аутентификация (authentication): Обеспечение гарантии того, что заявленные характеристики субъекта или объекта являются подлинными.

[ГОСТ Р ИСО/МЭК 27000—2021, статья 3.5]

Б.2.8 **аутентификация источника (данных)** (data origin authentication): Проверка и подтверждение того, что набор данных (сообщение, документ) был создан именно заявленным источником.

Примечание — См. [28] (статья 3.3.7).

Б.2.9 **аутентификация стороны** (entity authentication): Проверка одной из сторон того, что взаимодействующая с ней сторона — именно та, за которую себя выдает.

Примечание — См. [17] (статья 3.14).

Б.2.10 **данные** (data): Информация, представленная в формализованном виде, позволяющем осуществлять ее автоматическую обработку, в том числе поиск и передачу.

Примечание — Данные могут быть представлены в аналоговой или цифровой форме. В настоящем стандарте рассматриваются только данные в цифровой форме.

Б.2.11 **сообщение** (message): Данные, предназначенные для передачи от одной из взаимодействующих сторон протокола другой стороне.

Б.2.12

конфиденциальность (confidentiality): Недоступность для неавторизованных лиц, объектов или процессов.
[ГОСТ Р ИСО/МЭК 27000—2021, статья 3.10]

Б.2.13 **целостность (данных)** (data integrity): Свойство, отражающее отсутствие изменений в передаваемой или хранимой информации.

Примечание — См. [12] (статья 3.4). См. также [16] (статья 3.3.21).

Б.2.14

целостность (информационной системы) (integrity): Свойство системы, отражающее логическую корректность и надежность операционной системы, логическую полноту аппаратного и программного обеспечений, которые реализуют защитные механизмы, а также постоянство структуры и содержания хранимых данных.
[ГОСТ Р 56205—2014/IEC/TS 62443-1-1:2009, статья 3.2.60]

Б.2.15

угроза безопасности информации (information security threat): Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
[ГОСТ Р 50922—2006, статья 2.6.1]

Б.2.16

угроза (threat): Потенциальная возможность для нарушения безопасности при наличии обстоятельства, средства, действия или события, способных нарушить безопасность и нанести ущерб.
[ГОСТ Р 56498—2015/IEC/PAS 62443-3:2008, статья 3.1.62]

Б.2.17

уязвимость (vulnerability): Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использован для реализации угроз безопасности информации.
[ГОСТ Р 56545—2015, статья 3.3]

Примечание — См. также ГОСТ Р 50922—2006 (статья 2.6.4).

Б.2.18

пользователь (user): Лицо, организационная единица или автоматический процесс, получающие доступ в систему как на санкционированной, так и несанкционированной основе.
[ГОСТ Р 56498—2015/IEC/PAS 62443-3:2008, статья 3.1.63]

Б.2.19 **отрицание** (Нрк. *отказ, отречение,* самоотказ) (repudiation): Отрицание одним из участвующих в коммуникации субъектов своего участия во всей или части коммуникации.

Примечание — См. [16] (статья 3.3.44).

Б.2.20 **доверенная сторона** (trusted entity): Сторона, у которой установлены отношения доверия с одной или несколькими сторонами информационного взаимодействия.

Б.2.21 **центр доверия** (trusted party): Сторона, у которой установлены отношения доверия со всеми остальными сторонами информационного взаимодействия.

Б.2.22

сертификация на соответствие требованиям по безопасности информации (certification for compliance with information security requirements): Форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Примечание — К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации.

[ГОСТ Р 50922—2006, статья 2.8.3]

Библиография

[1] ИСО/МЭК 18033-1:2021 Информационная технология. Технология обеспечения защиты. Алгоритмы шифрования. Часть 1. Общие положения

[2] Р 1323565.1.012—2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации

[3] Терминологический словарь по безопасности информационных технологий (АСО/МОК СТК 1 ПК 27, Рамочный документ № 6, версия 20210131) [Glossary o IT security terminology Terms and definitions (ISO/IEC JTC 15C 27 Standing document № 6; V20210131)]

[4] ИСО/МЭК 11770-1:2010 Информационная технология. Методы защиты. Управление ключами. Часть 1. Структура

[5] ИСО/МЭК 11770-3:2021 Информационная технология. Методы защиты. Управление ключами. Часть 3. Механизмы, использующие ассиметричные методы

[6] ИСО/МЭК 29192-1:2012 Информационная технология. Методы защиты. Низкоресурсная криптография. Часть 1. Общие положения

[7] ИСО/МЭК 18033-5:2015 Информационная технология. Технология обеспечения защиты. Алгоритмы кодирования. Часть 5. Шифры на основе идентификаторов

[8] ИСО/МЭК 11770-4:2017 Информационная технология. Методы защиты. Управление ключами. Часть 4. Механизмы, основанные на слабых секретах

[9] ИСО/МЭК 18014-1:2008 Информационная технология. Методы защиты. Служба штампов времени. Часть 1. Структура

[10] ИСО/МЭК 18033-2:2006 Информационная технология. Технология обеспечения защиты. Алгоритмы шифрования. Часть 2. Асимметричные шифры

[11] ИСО/МЭК 19592-1:2016 Информационная технология. Методы защиты. Разделение секретной информации. Часть 1. Общие положения

[12] ИСО/МЭК 9797-1:2011 Информационные технологии. Методы защиты. Коды аутентификации сообщений (MAC). Часть 1. Механизмы, использующие блочный шифр

[13] ИСО/МЭК 10116:2017 Информационные технологии. Методы защиты. Режимы работы для *n*-битового блочного шифра

[14] ИСО/МЭК 19772:2020 1:2020 Информационные технологии. Методы защиты. Аутентифицированное шифрование. Техническая поправка 1

[15] ИСО/МЭК 18033-6:2019 Информационная технология. Технология обеспечения защиты. Алгоритмы кодирования. Часть 6. Гомоморфное шифрование

[16] ИСО 7498-2:1989 Системы обработки информации. Взаимодействие открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты

[17] ИСО/МЭК 9798-1:2010 Информационные технологии. Методы защиты. Аутентификация объектов. Часть 1. Общие положения

[18] ИСО/МЭК 14888-1:2008 Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения

[19] ИСО/МЭК 18370-1:2016 Информационные технологии. Методы защиты. Цифровая подпись вслепую. Часть 1. Общие положения

[20] ИСО/МЭК 20008-1:2013 Информационные технологии. Методы защиты. Анонимная цифровая подпись. Часть 1. Общие положения

[21] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (в ред. Федерального закона от 27.12.2019 № 476-ФЗ).

[22] ИСО/МЭК 13888-1:2020 Информационные технологии. Методы защиты. Невозможность отказа от авторства. Часть 1. Общие положения

[23] ИСО/МЭК 9798-5:2009 Информационные технологии. Методы защиты. Аутентификация объектов. Часть 5. Механизмы с применением методов с «нулевым разглашением»

[24] ИСО/МЭК 19790:2012 Информационные технологии. Методы защиты. Требования защищенности для криптографических модулей

[25] ИСО/МЭК 10118-1:2016 Информационные технологии. Методы защиты. Хэш-функции. Часть 1. Общие положения

[26] ИСО/МЭК 18031:2011 Информационная технология. Методы обеспечения защиты. Произвольное генерирование битов

[27] Р 1323565.1.022—2018 Информационная технология. Криптографическая защита информации. Функции выработки производного ключа

[28] ISO/TR 17427-4:2015 Интеллектуальные транспортные системы Кооперативные ITS. Часть 4. Минимальные требования к системе и характеристики основных систем

[29] ИСО/МЭК 27039:2015 Информационная технология. Методы защиты. Выбор, применение и операции систем обнаружения вторжений (IDPS)

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, термины и определения, терминология, алгоритм, средства криптографической защиты информации

Редактор *Е.Ю. Митрофанова*
Технический редактор *В.Н. Прусакова*
Корректор *С.И. Фирсова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 19.09.2025. Подписано в печать 01.10.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 5,58. Уч.-изд. л. 4,85.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru