

# Криптография и СКЗИ

Термины относятся к криптографической защите информации и средствам криптографической защиты (СКЗИ). Основной источник — ГОСТ Р 34.14-2025 "Информационная технология. Криптографическая защита информации. Термины и определения".

## В этом разделе

- [Базовые понятия криптографии](#)
- [Криптоанализ и криптостойкость](#)
- [Виды криптографических систем](#)
- [Криптографические ключи](#)
- [Управление ключами](#)
- [Система шифрования](#)
- [Цифровая подпись и электронная подпись](#)
- [Хеш-функции и имитозащита](#)
- [Аутентификация стороны](#)
- [Средства криптографической защиты \(СКЗИ\)](#)
- [Дополнительные термины \(разработка СКЗИ\)](#)

# Криптография и СКЗИ

## Базовые понятия криптографии

| Термин / Англ.                                                                                      | Определение                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Задачи криптографической защиты информации<br>( <i>cryptographic information protection goals</i> ) | Задачи защиты информации, для решения которых могут использоваться криптографические преобразования (обеспечение конфиденциальности, аутентификации, контроля целостности, невозможности отрицания).<br>[ГОСТ Р 34.14-2025, ст. 6]       |
| Ключевая система ( <i>key system</i> )                                                              | Подсистема криптографической системы, с помощью которой обеспечивается создание криптографических ключей, необходимых для её функционирования, и управление ими на основе инфраструктуры управления ключами. [ГОСТ Р 34.14-2025, ст. 20] |
| Криптографическая защита информации ( <i>cryptographic protection of information</i> )              | Защита информации с помощью её криптографического преобразования.<br>[ГОСТ Р 34.14-2025, ст. 2; ГОСТ Р 50922-2006, ст. 2.2.3]                                                                                                            |

| Термин / Англ.                                                                         | Определение                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Криптографическая система; криптосистема ( <i>cryptographic system; cryptosystem</i> ) | Структурированная и согласованная совокупность криптографических механизмов, предназначенная для решения поставленных задач криптографической защиты информации при конкретных условиях применения. [ГОСТ Р 34.14-2025, ст. 5]                                                           |
| Криптографический алгоритм ( <i>cryptographic algorithm</i> )                          | Алгоритм, описывающий процесс криптографического преобразования информации. [ГОСТ Р 34.14-2025, ст. 8]                                                                                                                                                                                   |
| Криптографический ключ ( <i>cryptographic key</i> )                                    | Изменяемый параметр криптографического алгоритма, определяющий выбор криптографического преобразования. [ГОСТ Р 34.14-2025, ст. 4]                                                                                                                                                       |
| Криптографический механизм ( <i>cryptographic mechanism</i> )                          | Криптографический алгоритм, криптографический протокол или их совокупность, применяемые в криптографической системе для обеспечения решения конкретной задачи защиты информации или создания и функционирования её ключевой системы. [ГОСТ Р 34.14-2025, ст. 10]                         |
| Криптографический протокол ( <i>cryptographic protocol</i> )                           | Коммуникационный протокол, в рамках которого стороны информационного взаимодействия последовательно выполняют определённые действия и обмениваются сообщениями, реализованный с применением криптографических алгоритмов для решения задач защиты информации. [ГОСТ Р 34.14-2025, ст. 9] |
| Криптографический синтез; криптосинтез ( <i>cryptographic synthesis</i> )              | Область теоретических и прикладных исследований, имеющих целью создание криптографической системы или криптографического механизма. [ГОСТ Р 34.14-2025, ст. 7]                                                                                                                           |
| Криптографическое преобразование ( <i>cryptographic transformation</i> )               | Процесс преобразования представляющих информацию данных с целью обеспечения криптографической стойкости, допускающий математическое описание. [ГОСТ Р 34.14-2025, ст. 3]                                                                                                                 |
| Криптография ( <i>cryptography</i> )                                                   | Область теоретических и прикладных исследований и практической деятельности, которая связана с разработкой и применением методов криптографической защиты информации. [ГОСТ Р 34.14-2025, ст. 1]                                                                                         |
| Криптолог ( <i>cryptologist</i> )                                                      | Обобщающее наименование области исследований: криптография как область теоретических и прикладных исследований подразделяется на криптографический синтез и криптографический анализ. [ГОСТ Р 34.14-2025, ст. 1, примечание]                                                             |

## Криптоанализ и криптостойкость

| Термин / Англ.                                               | Определение                                                                                                                                           |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Атака на криптосистему ( <i>attack on the cryptosystem</i> ) | Действие, совершаемое с целью нарушить хотя бы одно из целевых предназначений криптографической системы, использующее конкретные исходные данные о её |

| Термин / Англ.                                                                                 | Определение                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                | функционировании без полного знания сохраняемых в тайне её параметров.<br>[ГОСТ Р 34.14-2025, см. 14]                                                                                                                                                                                                         |
| Дешифрование ( <i>breaking an encipherment system</i> )                                        | Раскрытие зашифрованной информации методами криптографического анализа без предварительного полного знания применяемого криптографического ключа.<br>[ГОСТ Р 34.14-2025, см. 27]                                                                                                                              |
| Криптографическая стойкость ( <i>cryptographic security</i> )                                  | Свойство криптографической системы или отдельного криптографического механизма, характеризующее степень защищённости от атак на криптографическую систему или криптографический механизм. [ГОСТ Р 34.14-2025, см. 13]                                                                                         |
| Криптографический анализ; криптоанализ ( <i>cryptographic analysis; cryptanalysis</i> )        | Область теоретических и прикладных исследований, имеющих конечной целью получение обоснованных оценок криптографической стойкости криптографической системы в целом или отдельного криптографического механизма.<br>[ГОСТ Р 34.14-2025, см. 11]                                                               |
| Метод криптографического анализа ( <i>method of cryptanalysis</i> )                            | Совокупность приёмов и способов, объединённых одной или несколькими идеями, предназначенных для исследования криптографической стойкости криптографической системы или отдельного криптографического механизма. [ГОСТ Р 34.14-2025, см. 12]                                                                   |
| Метод полного перебора ( <i>brute-force attack; exhaustive search method</i> )                 | Метод криптографического анализа, основанный на рассмотрении (опробовании) всех вариантов сохраняемых в тайне криптографических ключей, паролей или других данных.<br>[ГОСТ Р 34.14-2025, см. 32]                                                                                                             |
| Практическая стойкость ( <i>security strength</i> )                                            | Средняя вычислительная трудоёмкость наилучшей известной атаки на криптографическую систему для конкретных исходных данных о её функционировании и конкретной задачи криптографической защиты информации. [ГОСТ Р 34.14-2025, см. 15]                                                                          |
| Совершенная стойкость системы шифрования ( <i>perfect security of an encipherment system</i> ) | Вид теоретической стойкости, гарантирующий, что в рамках математической модели системы шифрования по зашифрованному тексту без сведений об использованном ключе невозможно получить никакую информацию об открытом тексте, кроме, возможно, его длины. [ГОСТ Р 34.14-2025, см. 26]                            |
| Теоретическая стойкость ( <i>provable security</i> )                                           | Строго обоснованная в рамках математической модели криптографической системы неулучшаемая нижняя оценка сложности получения атакующим информации о сохраняемых в тайне параметрах системы для конкретных исходных данных и конкретной задачи криптографической защиты информации. [ГОСТ Р 34.14-2025, см. 16] |

## Виды криптографических систем

| Термин / Англ.                                                                                              | Определение                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Асимметричная криптографическая система<br>( <i>asymmetric cryptosystem</i> ;<br><i>public key system</i> ) | Криптографическая система, использующая пары взаимосвязанных криптографических преобразований, одно из которых зависит от открытого ключа, а второе — от криптографического ключа, сохраняемого в тайне (личного ключа).<br>[ГОСТ Р 34.14-2025, см. 17] |
| Аутентификация данных<br>( <i>data authentication</i> )                                                     | Проверка целостности данных и аутентификация их источника.<br>[ГОСТ Р 34.14-2025, см. 22]                                                                                                                                                               |
| Гибридная криптографическая система<br>( <i>hybrid cryptosystem</i> )                                       | Криптографическая система, содержащая в качестве составных элементов как симметричную, так и асимметричную криптографические системы.<br>[ГОСТ Р 34.14-2025, см. 19]                                                                                    |
| Квантовая криптография<br>( <i>quantum cryptography</i> )                                                   | Раздел криптографии, связанный с разработкой и применением методов криптографической защиты информации, основанных на принципах квантовой механики. [ГОСТ Р 34.14-2025, см. 28]                                                                         |
| Криптографическая система аутентификации стороны<br>( <i>entity authentication cryptosystem</i> )           | Криптографическая система, предназначенная для обеспечения аутентификации стороны, включающая в себя криптографический протокол аутентификации стороны и ключевую систему. [ГОСТ Р 34.14-2025, см. 21]                                                  |
| Криптографическая система на основе идентификаторов<br>( <i>identity-based cryptosystem</i> )               | Асимметричная криптографическая система, в которой открытые ключи вычисляются на основе идентификационной информации их владельцев. [ГОСТ Р 34.14-2025, см. 31]                                                                                         |
| Низкоресурсная криптография ( <i>lightweight cryptography</i> )                                             | Раздел криптографии, связанный с криптографическим синтезом и анализом криптографических систем, эффективно реализуемых на устройствах, имеющих существенные ограничения на используемые вычислительные ресурсы.<br>[ГОСТ Р 34.14-2025, см. 30]         |
| Постквантовая криптография ( <i>post-quantum cryptography</i> )                                             | Раздел криптографии, связанный с синтезом криптографических систем, обеспечивающих защиту от атак с применением квантовых компьютеров.<br>[ГОСТ Р 34.14-2025, см. 29]                                                                                   |
| Симметричная криптографическая система<br>( <i>symmetric cryptosystem</i> )                                 | Криптографическая система, использующая пары взаимосвязанных криптографических преобразований, в которой преобразования в каждой паре зависят от одного и того же секретного ключа. [ГОСТ Р 34.14-2025, см. 18]                                         |
| Система имитозащиты<br>( <i>symmetric data authentication system</i> )                                      | Симметричная криптографическая система, предназначенная для обеспечения аутентификации данных, включающая зависящую от ключа криптографическую хеш-функцию и ключевую систему. [ГОСТ Р 34.14-2025, см. 23]                                              |
| Система цифровой подписи<br>( <i>digital signature system</i> )                                             | Асимметричная криптографическая система, предназначенная для обеспечения аутентификации данных и невозможности отрицания создания, включающая схему цифровой подписи и ключевую систему. [ГОСТ Р 34.14-2025, см. 24]                                    |
| Система шифрования; шифрсистема ( <i>encipherment</i> )                                                     | Криптографическая система, предназначенная для обеспечения конфиденциальности информации, включающая в себя шифр (код) и ключевую систему.                                                                                                              |

| Термин / Англ.                    | Определение                        |
|-----------------------------------|------------------------------------|
| <i>system; encryption system)</i> | <i>[ГОСТ Р 34.14-2025, см. 25]</i> |

## Криптографические ключи

| Термин / Англ.                                                     | Определение                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Вектор инициализации<br>( <i>initialization vector</i> )           | Набор символов, который используется для задания начального состояния криптографического алгоритма. <i>[ГОСТ Р 34.14-2025, см. 126]</i>                                                                                                                                               |
| Главный секретный ключ<br>( <i>master key</i> )                    | Корневой (верхнеуровневый) элемент иерархии секретных ключей, предназначенный для шифрования криптографических ключей более низкого уровня. <i>[ГОСТ Р 34.14-2025, см. 63]</i>                                                                                                        |
| Длина ключа ( <i>key length; key size</i> )                        | Минимальная длина записи криптографического ключа как строки символов заданного алфавита (обычно двухэлементного). <i>[ГОСТ Р 34.14-2025, см. 34]</i>                                                                                                                                 |
| Долговременный ключ<br>( <i>static key; long-term key</i> )        | Криптографический ключ, который используется в криптографической системе в неизменном виде длительное время. <i>[ГОСТ Р 34.14-2025, см. 61]</i>                                                                                                                                       |
| Закрытый ключ; личный ключ<br>( <i>private key</i> )               | Сохраняемый в тайне криптографический ключ из ключевой пары. <i>[ГОСТ Р 34.14-2025, см. 44]</i>                                                                                                                                                                                       |
| Иерархия производных ключей<br>( <i>derivation key hierarchy</i> ) | Древовидная структура, отражающая зависимость производных ключей от исходных. <i>[ГОСТ Р 34.14-2025, см. 66]</i>                                                                                                                                                                      |
| Иерархия секретных ключей<br>( <i>logical key hierarchy</i> )      | Древовидная структура, отражающая способ защиты криптографических ключей симметричной криптографической системы, при котором ключи промежуточных уровней используются для шифрования и имитозащиты ключей более низкого уровня. <i>[ГОСТ Р 34.14-2025, см. 62]</i>                    |
| Итерационный ключ ( <i>round key</i> )                             | Элемент последовательности ключей, вычисляемых в процессе развертывания исходного криптографического ключа, который используется на соответствующей итерации алгоритмов зашифрования и расшифрования блочного шифра. <i>[ГОСТ Р 34.14-2025, см. 124; ГОСТ Р 34.12-2015, п. 2.1.7]</i> |
| Ключ шифрования данных<br>( <i>data encryption key</i> )           | Элемент иерархии секретных ключей, предназначенный для шифрования данных. <i>[ГОСТ Р 34.14-2025, см. 64]</i>                                                                                                                                                                          |
| Ключ шифрования ключей<br>( <i>key encryption key</i> )            | Элемент иерархии секретных ключей, предназначенный для шифрования криптографических ключей более низкого уровня. <i>[ГОСТ Р 34.14-2025, см. 65]</i>                                                                                                                                   |
| Ключевая пара ( <i>key pair</i> )                                  | Упорядоченная пара однозначно математически связанных криптографических ключей, используемых в асимметричной криптографической системе. <i>[ГОСТ Р 34.14-2025, см. 43]</i>                                                                                                            |

| Термин / Англ.                                                                                                     | Определение                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ключевой материал;<br>исходная ключевая<br>информация ( <i>keying<br/>material</i> )                               | Данные, позволяющие сформировать секретные криптографические ключи.<br>[ГОСТ Р 34.14-2025, см. 35]                                                                                                                                       |
| Корневой ключ ( <i>derivation<br/>key</i> )                                                                        | Криптографический ключ, соответствующий корню иерархии производных ключей.<br>[ГОСТ Р 34.14-2025, см. 67]                                                                                                                                |
| Множество ключей ( <i>key<br/>space</i> )                                                                          | Множество всех возможных значений криптографического ключа (для конкретного криптографического алгоритма). [ГОСТ Р 34.14-2025, см. 33]                                                                                                   |
| Одноразовый ключ ( <i>one<br/>time key</i> )                                                                       | Криптографический ключ, используемый однократно. [ГОСТ Р 34.14-2025, см. 60]                                                                                                                                                             |
| Открытый ключ ( <i>public key</i> )                                                                                | Криптографический ключ из ключевой пары, который может быть сделан доступным другим сторонам без снижения стойкости асимметричной криптографической системы.<br>[ГОСТ Р 34.14-2025, см. 45]                                              |
| Пароль ( <i>password</i> )                                                                                         | Криптографический ключ, принимающий значения из множества малой мощности, элементами которого являются осмысленные слова или последовательности символов, которые могут быть запомнены пользователем. [П 1323565.1.012-2017, п. 3.1.37]  |
| Производный ключ ( <i>derived<br/>key</i> )                                                                        | Криптографический ключ, полученный как значение функции выработки производного ключа. [ГОСТ Р 34.14-2025, см. 70]                                                                                                                        |
| Развертывание ключа ( <i>key<br/>scheduling</i> )                                                                  | Построение управляющей ключевой последовательности по криптографическому ключу поточного шифра или построение последовательности итерационных ключей по ключу блочного шифра. [ГОСТ Р 34.14-2025, см. 125; ГОСТ Р 34.12-2015, п. 2.1.10] |
| Сеансовый ключ ( <i>session<br/>key</i> )                                                                          | Элемент иерархии производных ключей, выработанный для криптографической защиты одного сеанса связи между сторонами информационного взаимодействия.<br>[ГОСТ Р 34.14-2025, см. 68]                                                        |
| Секретный ключ ( <i>secret key</i> )                                                                               | Криптографический ключ симметричной криптографической системы.<br>[ГОСТ Р 34.14-2025, см. 58]                                                                                                                                            |
| Составной ключ ( <i>composite<br/>key</i> )                                                                        | Криптографический ключ, состоящий из нескольких компонентов, определяющих работу отдельных частей одного криптографического механизма.<br>[ГОСТ Р 34.14-2025, см. 59]                                                                    |
| Функция выработки<br>производного ключа;<br>функция диверсификации<br>ключа ( <i>key derivation<br/>function</i> ) | Функция для вычисления криптографического ключа по другому криптографическому ключу и несекретным вспомогательным данным. [ГОСТ Р 34.14-2025, см. 69]                                                                                    |

# Управление ключами

| Термин / Англ.                                                                         | Определение                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Жизненный цикл ключа ( <i>key life cycle</i> )                                         | Последовательность этапов работы с криптографическим ключом от момента выработки до момента уничтожения. [ГОСТ Р 34.14-2025, см. 38]                                                                                                                                            |
| Защищенная передача ключа ( <i>key transport</i> )                                     | Процесс передачи криптографического ключа от одной стороны к другой способом, обеспечивающим конфиденциальность, подтверждение и аутентификацию пересылаемого криптографического ключа. [ГОСТ Р 34.14-2025, см. 76]                                                             |
| Инфраструктура управления ключами ( <i>key management infrastructure</i> )             | Комплекс центров доверия, аппаратно-программных и технических средств, другого оборудования и документов, обеспечивающих управление криптографическими ключами. [ГОСТ Р 34.14-2025, см. 37]                                                                                     |
| Компрометация ключа ( <i>key compromise</i> )                                          | Нарушение конфиденциальности криптографического ключа или ключевого материала. [ГОСТ Р 34.14-2025, см. 40]                                                                                                                                                                      |
| Механизм инкапсуляции ключа ( <i>key encapsulation mechanism</i> )                     | Способ выработки и защищенной передачи секретного ключа или ключевых материалов, необходимых для его формирования, использующий систему шифрования с открытым ключом. [ГОСТ Р 34.14-2025, см. 77]                                                                               |
| Пороговая схема разделения секрета ( <i>threshold secret sharing scheme</i> )          | Схема разделения секрета, в которой правомочными являются все коалиции сторон, содержащие не менее заранее оговорённого числа участников. [ГОСТ Р 34.14-2025, см. 91]                                                                                                           |
| Предварительное распределение секретных ключей ( <i>preliminary key distribution</i> ) | Централизованное распределение ключевых материалов, с помощью которых пользователи симметричной криптографической системы могут независимо вычислять секретные ключи. [ГОСТ Р 34.14-2025, см. 74]                                                                               |
| Разделение секрета ( <i>secret sharing</i> )                                           | Способ формирования ключевых материалов (долей секрета) между сторонами, позволяющий одной или нескольким заранее определённым группам восстанавливать значение криптографического ключа (секрета). [ГОСТ Р 34.14-2025, см. 89]                                                 |
| Распределение секретных ключей ( <i>key distribution</i> )                             | Централизованное распределение секретных ключей между пользователями симметричной криптографической системы, необходимых для её функционирования. [ГОСТ Р 34.14-2025, см. 71]                                                                                                   |
| Совместная выработка общего секретного ключа ( <i>key agreement</i> )                  | 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. [ГОСТ Р 34.14-2025, см. 78] |
| Срок действия ключа ( <i>key life time</i> )                                           | Установленный временной интервал, в течение которого криптографический ключ разрешается использовать. [ГОСТ Р 34.14-2025, см. 39]                                                                                                                                               |

| Термин / Англ.                                                                       | Определение                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Схема разделения секрета ( <i>secret sharing scheme</i> )                            | Совокупность, состоящая из двух криптографических протоколов, один из которых предназначен для разделения секрета между сторонами, а другой — для формирования криптографического ключа (секрета) группой участников. [ГОСТ Р 34.14-2025, см. 90]                                                    |
| Уничтожение ключа ( <i>key destruction</i> )                                         | Необратимое уничтожение криптографического ключа. [ГОСТ Р 34.14-2025, см. 41]                                                                                                                                                                                                                        |
| Управление ключами ( <i>key management</i> )                                         | 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. [ГОСТ Р 34.14-2025, см. 36]             |
| Формирование общего ключа ( <i>key establishment</i> )                               | Получение сторонами информационного взаимодействия общего секретного ключа либо с помощью протокола защищенной передачи ключа, либо с помощью протокола совместной выработки общего секретного ключа, либо на основе ключевых материалов предварительного распределения. [ГОСТ Р 34.14-2025, см. 75] |
| Центр передачи ключей; центр перешифрования ключей ( <i>key translation centre</i> ) | Центр доверия, осуществляющий расшифрование выработанного и зашифрованного одной стороной секретного ключа, последующее его зашифрование и передачу в зашифрованном виде другой стороне. [ГОСТ Р 34.14-2025, см. 73]                                                                                 |
| Центр распределения ключей ( <i>key distribution centre</i> )                        | Центр доверия, обеспечивающий выработку и распределение секретных ключей. [ГОСТ Р 34.14-2025, см. 72]                                                                                                                                                                                                |

## Система шифрования

| Термин / Англ.                                                                                                   | Определение                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Алгоритм зашифрования ( <i>encryption algorithm</i> )                                                            | Криптографический алгоритм, реализующий зашифрование. [ГОСТ Р 34.14-2025, см. 101; ГОСТ Р 34.12-2015, п. 2.1.1]                                                                                                                                           |
| Алгоритм расшифрования ( <i>decryption algorithm</i> )                                                           | Криптографический алгоритм, реализующий расшифрование. [ГОСТ Р 34.14-2025, см. 102; ГОСТ Р 34.12-2015, п. 2.1.2]                                                                                                                                          |
| Асимметричная система шифрования; система шифрования с открытым ключом ( <i>asymmetric encipherment system</i> ) | Система шифрования, являющаяся асимметричной криптографической системой, в которой зашифрование осуществляется с использованием открытого ключа получателя, а расшифрование — с помощью закрытого (личного) ключа получателя. [ГОСТ Р 34.14-2025, см. 97] |
| Аутентифицированное шифрование ( <i>authenticated encryption</i> )                                               | Шифрование, позволяющее дополнительно обеспечить аутентификацию шифруемых данных. [ГОСТ Р 34.14-2025, см. 115]                                                                                                                                            |

| Термин / Англ.                                                                            | Определение                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Базовый блочный шифр<br>( <i>basic block cipher</i> )                                     | Блочный шифр, реализующий зашифрование и расшифрование блока текста фиксированной длины. [ГОСТ Р 34.14-2025, ст. 123; ГОСТ Р 34.12-2015, п. 2.1.3]                                                                                                                     |
| Блочный шифр ( <i>block cipher</i> )                                                      | Шифр симметричной системы шифрования, в котором алгоритм зашифрования (расшифрования) последовательно применяется к блокам открытого (шифрованного) текста. [ГОСТ Р 34.14-2025, ст. 122; ГОСТ Р 34.12-2015, п. 2.1.5]                                                  |
| Гомоморфное шифрование<br>( <i>homomorphic encryption</i> )                               | Шифрование, при котором шифртекст для результата некоторой алгебраической операции над открытыми текстами можно построить, применив другую алгебраическую операцию к соответствующим им шифртекстам, без знания криптографического ключа. [ГОСТ Р 34.14-2025, ст. 116] |
| Зашифрование ( <i>encryption; encipherment</i> )                                          | Зависящий от криптографического ключа процесс обратимого преобразования открытого текста в шифрованный текст. [ГОСТ Р 34.14-2025, ст. 99]                                                                                                                              |
| Код ( <i>code</i> )                                                                       | Шифр замены, в котором фрагменты открытого текста заменяются кодовыми обозначениями в соответствии с кодовой книгой, выполняющей функцию криптографического ключа. [ГОСТ Р 34.14-2025, ст. 108]                                                                        |
| Кодирование ( <i>encoding</i> )                                                           | Зашифрование с помощью кода. [ГОСТ Р 34.14-2025, ст. 109]                                                                                                                                                                                                              |
| Кодовая книга ( <i>code book</i> )                                                        | Документ, используемый для кодирования и декодирования, содержащий кодовый словарь и слоговую таблицу. [ГОСТ Р 34.14-2025, ст. 111]                                                                                                                                    |
| Открытый текст ( <i>plaintext</i> )                                                       | Данные, подлежащие зашифрованию или полученные в результате расшифрования. [ГОСТ Р 34.14-2025, ст. 94]                                                                                                                                                                 |
| Поточный шифр ( <i>stream cipher</i> )                                                    | Шифр замены, в котором выбор обратимого преобразования каждого знака (блока) открытого (шифрованного) текста определяется соответствующим символом управляющей ключевой последовательности. [ГОСТ Р 34.14-2025, ст. 117]                                               |
| Поточный шифр с самовосстановлением ( <i>self-synchronizing stream cipher</i> )           | Поточный шифр, в котором знаки управляющей ключевой последовательности являются значениями функции, зависящей от криптографического ключа и некоторого фиксированного количества предыдущих знаков шифрованного текста. [ГОСТ Р 34.14-2025, ст. 119]                   |
| Расшифрование ( <i>decryption; decipherment</i> )                                         | Зависящий от криптографического ключа процесс преобразования шифрованного текста в соответствующий ему открытый текст. [ГОСТ Р 34.14-2025, ст. 100]                                                                                                                    |
| Режим работы блочного шифра ( <i>block cipher mode of operation</i> )                     | Способ использования базового блочного шифра в общей конструкции криптографического преобразования блочного шифра. [ГОСТ Р 34.14-2025, ст. 127; ГОСТ Р 34.13-2015]                                                                                                     |
| Симметричная система шифрования; система шифрования с секретным ключом ( <i>symmetric</i> | Система шифрования, являющаяся симметричной криптографической системой, в которой для зашифрования и расшифрования применяются одинаковые секретные ключи. [ГОСТ Р 34.14-2025, ст. 96]                                                                                 |

| Термин / Англ.                                                      | Определение                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>encipherment system; secret key encryption system</i>            |                                                                                                                                                                                                                                                 |
| Синхронный поточный шифр ( <i>synchronous stream cipher</i> )       | Поточный шифр, в котором управляющая ключевая последовательность полностью определяется криптографическим ключом и, возможно, вектором инициализации.<br>[ГОСТ Р 34.14-2025, ст. 120]                                                           |
| Управляющая ключевая последовательность; гамма ( <i>keystream</i> ) | Зависящая от криптографического ключа последовательность, однозначно определяющая порядок выбора преобразований знаков (блоков) открытого (шифрованного) текста, используемая в поточных шифрах.<br>[ГОСТ Р 34.14-2025, ст. 118]                |
| Шифр ( <i>cipher</i> )                                              | Семейство преобразований, реализующих процессы зашифрования и расшифрования и зависящих от криптографического ключа и, возможно, вектора инициализации.<br>[ГОСТ Р 34.14-2025, ст. 98]                                                          |
| Шифр гаммирования ( <i>quasigroup encryption</i> )                  | Синхронный поточный шифр, в котором алфавиты открытого текста и управляющей ключевой последовательности совпадают, а каждый знак шифрованного текста является значением обратимой по каждому аргументу функции.<br>[ГОСТ Р 34.14-2025, ст. 121] |
| Шифр замены ( <i>substitution cipher</i> )                          | Шифр, в котором зашифрование осуществляется применением к последовательным фрагментам открытого текста обратимых преобразований, зависящих от криптографического ключа.<br>[ГОСТ Р 34.14-2025, ст. 103]                                         |
| Шифр перестановки ( <i>permutation cipher</i> )                     | Шифр, в котором зашифрование осуществляется путём зависящей от криптографического ключа перестановки знаков (блоков) открытого текста.<br>[ГОСТ Р 34.14-2025, ст. 105]                                                                          |
| Шифр простой замены ( <i>fixed substitution cipher</i> )            | Шифр замены, реализующий одно и то же зависящее от криптографического ключа обратимое преобразование каждого знака (блока) открытого текста.<br>[ГОСТ Р 34.14-2025, ст. 104]                                                                    |
| Шифрование с открытым ключом ( <i>public key encryption</i> )       | Шифрование с использованием асимметричной системы шифрования.<br>[ГОСТ Р 34.14-2025, ст. 106]                                                                                                                                                   |
| Шифрование с секретным ключом ( <i>symmetric key encryption</i> )   | Шифрование с использованием симметричной системы шифрования.<br>[ГОСТ Р 34.14-2025, ст. 107]                                                                                                                                                    |
| Шифрованный текст; шифртекст ( <i>ciphertext</i> )                  | Данные, полученные в результате зашифрования открытого текста.<br>[ГОСТ Р 34.14-2025, ст. 95]                                                                                                                                                   |

## Цифровая подпись и электронная подпись

| Термин / Англ.                                                                         | Определение                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Квалифицированная электронная подпись<br>( <i>qualified electronic signature</i> )     | 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.<br>[ГОСТ Р 34.14-2025, <i>см. 143</i> ] |
| Ключ подписи ( <i>signature key</i> )                                                  | Элемент секретных данных, специфичный для субъекта и используемый только данным субъектом в процессе формирования цифровой подписи.<br>[ГОСТ Р 34.14-2025, <i>см. 145</i> ; ГОСТ Р 34.10-2012, <i>см. 3.1.2</i> ]                                                                                                                                       |
| Ключ проверки подписи<br>( <i>verification key</i> )                                   | Элемент данных, математически связанный с ключом подписи и используемый проверяющей стороной в процессе проверки цифровой подписи.<br>[ГОСТ Р 34.14-2025, <i>см. 146</i> ; ГОСТ Р 34.10-2012, <i>см. 3.1.3</i> ]                                                                                                                                        |
| Невозможность отрицания<br>( <i>non-repudiation</i> )                                  | Свойство способа фиксации информации об имевших место действиях или событиях, исключающее возможность их последующего отрицания. [ГОСТ Р 34.14-2025, <i>см. 149</i> ]                                                                                                                                                                                   |
| Невозможность отрицания создания<br>( <i>non-repudiation of creation</i> )             | Свойство способа фиксации информации о факте создания сообщения (документа) конкретным лицом, исключающее возможность последующего отрицания им этого факта. [ГОСТ Р 34.14-2025, <i>см. 150</i> ]                                                                                                                                                       |
| Неквалифицированная электронная подпись<br>( <i>unqualified electronic signature</i> ) | Усиленная электронная подпись, которая не является квалифицированной.<br>[ГОСТ Р 34.14-2025, <i>см. 144</i> ]                                                                                                                                                                                                                                           |
| Параметр схемы цифровой подписи<br>( <i>domain parameter</i> )                         | Элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам. [ГОСТ Р 34.14-2025, <i>см. 135</i> ; ГОСТ Р 34.10-2012, <i>см. 3.1.4</i> ]                                                                                                                                                                |
| Подписанный набор данных; подписанное сообщение<br>( <i>signed message</i> )           | Цифровая подпись набора данных [сообщения], а также часть (возможно, пустая) этого набора данных, не восстанавливаемая из цифровой подписи.<br>[ГОСТ Р 34.14-2025, <i>см. 131</i> ]                                                                                                                                                                     |
| Проверка подписи<br>( <i>verification process</i> )                                    | Процесс, в котором в качестве исходных данных используются подписанный набор данных, ключ проверки подписи и параметры схемы цифровой подписи, результатом которого является заключение о корректности или некорректности цифровой подписи.<br>[ГОСТ Р 34.14-2025, <i>см. 134</i> ; ГОСТ Р 34.10-2012, <i>п. 3.1.8</i> ]                                |
| Схема анонимной цифровой подписи<br>( <i>anonymous signature scheme</i> )              | Схема цифровой подписи, обеспечивающая анонимность подписывающей стороны и несвязываемость. [ГОСТ Р 34.14-2025, <i>см. 138</i> ]                                                                                                                                                                                                                        |
| Схема групповой цифровой подписи<br>( <i>group signature scheme</i> )                  | Схема анонимной цифровой подписи, в которой правом формирования подписи от имени группы, оставаясь анонимным, обладает каждый из входящих в неё членов.<br>[ГОСТ Р 34.14-2025, <i>см. 139</i> ]                                                                                                                                                         |

| Термин / Англ.                                                                                      | Определение                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Схема кольцевой цифровой подписи ( <i>ring signature scheme</i> )                                   | 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. [ГОСТ Р 34.14-2025, ст. 140]                                                                            |
| Схема конфиденциальной цифровой подписи; неоспоримая подпись ( <i>undeniable signature scheme</i> ) | Схема цифровой подписи, в которой процесс проверки подписи требует участия стороны, которая по предположению является подписывающей. [ГОСТ Р 34.14-2025, ст. 137]                                                                                                                                                   |
| Схема цифровой подписи ( <i>digital signature scheme</i> )                                          | Совокупность, состоящая из двух криптографических протоколов (алгоритмов), предназначенных для формирования и проверки подписи. [ГОСТ Р 34.14-2025, ст. 129]                                                                                                                                                        |
| Схема цифровой подписи вслепую ( <i>blind signature scheme</i> )                                    | Схема цифровой подписи, формирование подписи в которой осуществляется двумя участниками таким образом, что подписывающая сторона не получает никакой информации о подписанном наборе данных. [ГОСТ Р 34.14-2025, ст. 136]                                                                                           |
| Усиленная электронная подпись ( <i>advanced electronic signature</i> )                              | Электронная подпись, полученная в результате криптографического преобразования информации с использованием ключа подписи, позволяющая обнаружить факт внесения изменений в электронный документ после момента его подписания и созданная с использованием средств электронной подписи. [ГОСТ Р 34.14-2025, ст. 142] |
| Формирование подписи ( <i>signature process</i> )                                                   | Процесс, результатом выполнения которого для заданного набора данных (сообщения), ключа подписи и параметров схемы цифровой подписи является цифровая подпись указанного набора данных. [ГОСТ Р 34.14-2025, ст. 130; ГОСТ Р 34.10-2012, ст. 3.1.9]                                                                  |
| Цифровая подпись ( <i>digital signature</i> )                                                       | Результат криптографического преобразования набора данных (сообщения), зависящего от ключа подписи и параметров схемы цифровой подписи, обеспечивающий возможность аутентификации данных и невозможность отрицания факта создания. [ГОСТ Р 34.14-2025, ст. 128]                                                     |
| Цифровая подпись с восстановлением сообщения ( <i>digital signature with message recovery</i> )     | Цифровая подпись, сформированная таким образом, что при выполнении алгоритма проверки подписи сообщение или его часть могут быть извлечены из цифровой подписи. [ГОСТ Р 34.14-2025, ст. 132]                                                                                                                        |
| Цифровая подпись с дополнением ( <i>digital signature with appendix</i> )                           | Цифровая подпись, сформированная таким образом, что никакая часть подписываемого сообщения не может быть извлечена из цифровой подписи, дополнением к которой служит само подписываемое сообщение. [ГОСТ Р 34.14-2025, ст. 133]                                                                                     |
| Электронная подпись ( <i>electronic signature</i> )                                                 | 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. [ГОСТ Р 34.14-2025, ст. 141; ФЗ № 63-ФЗ]                                        |

## Хеш-функции и имитозащита

| Термин / Англ.                                                                                    | Определение                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Безусловно стойкая система имитозащиты<br>( <i>unconditionally secure authentication system</i> ) | Система имитозащиты, обеспечивающая минимально возможные значения вероятностей успеха атак имитации и подмены сообщения. [ГОСТ Р 34.14-2025, см. 164]                                                                                                                   |
| Имитация сообщения<br>( <i>imitation</i> )                                                        | Результат атаки на криптографическую систему, в ходе которой атакующий формирует сообщение от имени другой стороны, которое не отвергается получателем. [ГОСТ Р 34.14-2025, см. 160]                                                                                    |
| Имитовставка; код аутентичности сообщения<br>( <i>message authentication code; MAC</i> )          | 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. [ГОСТ Р 34.14-2025, см. 163]                         |
| Имитозащита ( <i>imitation protection</i> )                                                       | Защита от атак, имеющих целью имитацию и подмену сообщения, которая реализуется путём выработки и проверки имитовставок. [ГОСТ Р 34.14-2025, см. 159]                                                                                                                   |
| Криптографическая хеш-функция ( <i>cryptographic hash function</i> )                              | Функция, отображающая множество всех конечных битовых строк в множество битовых строк фиксированной длины, для которой вычислительно трудны задачи нахождения прообраза, второго прообраза и коллизии. [ГОСТ Р 34.14-2025, см. 158; ГОСТ Р 34.10-2012, п. 3.1.14]       |
| Криптографическая хеш-функция, зависящая от ключа ( <i>keyed hash function; MAC algorithm</i> )   | Зависящая от криптографического ключа функция, отображающая множество всех конечных битовых строк в множество битовых строк фиксированной длины, для которой без знания ключа вычислительно трудно найти значение функции на новой строке. [ГОСТ Р 34.14-2025, см. 162] |
| Подмена сообщения<br>( <i>substitution</i> )                                                      | Результат атаки на криптографическую систему, в ходе которой атакующий модифицирует или заменяет сообщение, переданное одной из сторон, другим сообщением от имени той же стороны. [ГОСТ Р 34.14-2025, см. 161]                                                         |
| Хеш-код ( <i>hash-code</i> )                                                                      | Строка бит, являющаяся выходным результатом хеш-функции. [ГОСТ Р 34.11-2012, см. 3.1.5; ГОСТ Р 34.10-2012, см. 3.1.13]                                                                                                                                                  |
| Хеш-функция ( <i>collision-resistant hash-function</i> )                                          | Функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая свойствам стойкости к нахождению прообраза, второго прообраза и коллизии. [ГОСТ Р 34.11-2012, см. 3.1.6; ГОСТ Р 34.10-2012, см. 3.1.14]                                             |

## Аутентификация стороны

| Термин / Англ.                                                     | Определение                                                                                                                                         |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Взаимная аутентификация<br>( <i>mutual entity authentication</i> ) | Обоюдная аутентификация сторон, при которой каждая из сторон убеждается в подлинности взаимодействующей с ней стороны. [ГОСТ Р 34.14-2025, см. 173] |

| Термин / Англ.                                                                       | Определение                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Доказательство с нулевым разглашением ( <i>zero knowledge proof</i> )                | 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 нём никакой информации. [ГОСТ Р 34.14-2025, см. 174]                          |
| Доказывающая сторона ( <i>claimant; prover</i> )                                     | Сторона протокола, пытающаяся подтвердить другой стороне свою подлинность. [ГОСТ Р 34.14-2025, см. 166]                                                                                                                                                                                              |
| Запрос ( <i>challenge</i> )                                                          | Сообщение протокола с дву- или трёхкратной передачей сообщений, выработанное проверяющей стороной и обрабатываемое доказывающей стороной. [ГОСТ Р 34.14-2025, см. 170]                                                                                                                               |
| Кратность обмена ( <i>exchange multiplicity parameter</i> )                          | Количество сообщений, отправляемых сторонами в криптографическом протоколе аутентификации стороны. [ГОСТ Р 34.14-2025, см. 172]                                                                                                                                                                      |
| Криптографический протокол аутентификации стороны ( <i>authentication protocol</i> ) | Криптографический протокол с двумя участниками (проверяющей стороной и доказывающей стороной), позволяющий проверяющей стороне провести аутентификацию доказывающей стороны. [ГОСТ Р 34.14-2025, см. 165]                                                                                            |
| Обязательство ( <i>commitment</i> )                                                  | Результат криптографического преобразования набора данных (сообщения) без использования криптографического ключа, которое обеспечивает невозможность получить о наборе никакой информации (сокрытие) и невозможность его подмены (привязка). [ГОСТ Р 34.14-2025, см. 175]                            |
| Ответ ( <i>response</i> )                                                            | Сообщение протокола аутентификации стороны с дву- или трёхкратной передачей сообщений, выработанное доказывающей стороной в ответ на запрос и обрабатываемое проверяющей стороной. [ГОСТ Р 34.14-2025, см. 171]                                                                                      |
| Подмена стороны ( <i>impersonation</i> )                                             | Результат атаки на криптографический протокол, с помощью которой атакующий выдаёт себя за легитимного участника этого протокола. [ГОСТ Р 34.14-2025, см. 168]                                                                                                                                        |
| Проверяющая сторона ( <i>verifier</i> )                                              | Сторона протокола, осуществляющая проверку подлинности другой стороны. [ГОСТ Р 34.14-2025, см. 167]                                                                                                                                                                                                  |
| Свидетельство ( <i>witness</i> )                                                     | Сообщение протокола с трёхкратной передачей сообщений, сформированное доказывающей стороной, зависящее от защищённого от раскрытия параметра, позволяющее проверяющей стороне убедиться, что в процессе выполнения протокола не произошла подмена доказывающей стороны. [ГОСТ Р 34.14-2025, см. 169] |
| Схема обязательств ( <i>commitment scheme</i> )                                      | Совокупность, состоящая из двух криптографических алгоритмов, первый из которых предназначен для формирования обязательства для некоторого набора данных, второй — для его раскрытия. [ГОСТ Р 34.14-2025, см. 176]                                                                                   |

## Средства криптографической защиты (СКЗИ)

| Термин / Англ.                                                                                                              | Определение                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Жизненный цикл средства криптографической защиты информации; жизненный цикл СКЗИ ( <i>cryptographic module life cycle</i> ) | Совокупность явлений и процессов, повторяющихся с периодичностью, определяемой временем существования типовой конструкции (образца) СКЗИ от её замысла до утилизации, или конкретного экземпляра СКЗИ от момента его производства до утилизации. [ГОСТ Р 34.14-2025, см. 183]                                                                       |
| Ключевая информация ( <i>key information</i> )                                                                              | Специальным образом организованная совокупность данных, ключевых материалов и/или криптографических ключей, предназначенная для осуществления криптографической защиты информации в течение определённого срока. [ГОСТ Р 34.14-2025, см. 184; Р 1323565.1.012-2017, п. 3.1.20]                                                                      |
| Ключевой документ ( <i>key document</i> )                                                                                   | Подлежащий учёту (регистрации) носитель информации, содержащий в себе ключевую информацию и/или инициализирующую последовательность, а также при необходимости контрольную, служебную и технологическую информацию. [ГОСТ Р 34.14-2025, см. 185; Р 1323565.1.012-2017, п. 3.1.21]                                                                   |
| Ключевой носитель ( <i>key storage device</i> )                                                                             | Физический носитель, предназначенный для размещения и хранения на нём ключевой информации и/или инициализирующей последовательности. [ГОСТ Р 34.14-2025, см. 186; Р 1323565.1.012-2017, п. 3.1.22]                                                                                                                                                  |
| Средства криптографической защиты информации; СКЗИ ( <i>cryptographic module</i> )                                          | Средства, системы и комплексы, реализующие криптографическую систему или отдельные криптографические механизмы. [ГОСТ Р 34.14-2025, см. 177; Р 1323565.1.012-2017, п. 3.1.44]                                                                                                                                                                       |
| Средство изготовления ключевых документов ( <i>key production module</i> )                                                  | Средство криптографической защиты информации, реализующее процессы изготовления и/или распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации. [ГОСТ Р 34.14-2025, см. 181]                                                                                                                                      |
| Средство имитозащиты ( <i>data authentication module</i> )                                                                  | Средство криптографической защиты информации, реализующее зависящую от ключа криптографическую хеш-функцию или систему имитозащиты в целом. [ГОСТ Р 34.14-2025, см. 179]                                                                                                                                                                            |
| Средство кодирования ( <i>encoding module</i> )                                                                             | Средство шифрования, реализующее зашифрование и расшифрование с помощью кода. [ГОСТ Р 34.14-2025, см. 182]                                                                                                                                                                                                                                          |
| Средство шифрования; шифрсредство ( <i>encryption module</i> )                                                              | Средство криптографической защиты информации, реализующее алгоритм зашифрования или алгоритм расшифрования, или шифр в целом, или систему шифрования в целом. [ГОСТ Р 34.14-2025, см. 178]                                                                                                                                                          |
| Средство электронной подписи ( <i>digital signature module</i> )                                                            | Средство криптографической защиты информации, реализующее хотя бы одну из функций: 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. [ГОСТ Р 34.14-2025, см. 180] |

## Дополнительные термины (разработка СКЗИ)

| Термин / Англ.                                                                                       | Определение                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Биологический датчик случайных чисел; БДСЧ ( <i>biological random number generator</i> )             | Датчик, вырабатывающий случайную последовательность путём детерминированного преобразования инициализирующей последовательности, источником которой являются физические (биологические) процессы. [P 1323565.1.012-2017, п. 3.1.4]                   |
| Инженерно-криптографический механизм ( <i>engineering cryptographic mechanism</i> )                  | Алгоритмическая или техническая мера, реализуемая аппаратным средством, программным обеспечением или средой функционирования СКЗИ и направленная на обеспечение защиты информации от несанкционированного доступа. [P 1323565.1.012-2017, п. 3.1.12] |
| Инициализирующая последовательность; исходная ключевая информация ( <i>initialization sequence</i> ) | Совокупность данных, используемых для начальной установки (инициализации) состояния криптографического алгоритма или генератора ключей. [P 1323565.1.012-2017, п. 3.1.13]                                                                            |
| Информативный сигнал ( <i>informative signal</i> )                                                   | Сигнал, по значениям и/или параметрам которого может быть определена защищаемая информация. [P 1323565.1.012-2017, п. 3.1.14]                                                                                                                        |
| Криптографическая функция ( <i>cryptographic function</i> )                                          | Параметрическая функция, реализуемая СКЗИ и предназначенная для криптографического преобразования информации. [P 1323565.1.012-2017, п. 3.1.25]                                                                                                      |
| Криптографически опасная информация ( <i>cryptographically dangerous information</i> )               | Любая информация, хранимая и/или вырабатываемая СКЗИ, средой функционирования или штатными средствами, которая может быть использована для криптографического анализа. [P 1323565.1.012-2017, п. 3.1.26]                                             |
| Криптонабор ( <i>cipher suite</i> )                                                                  | Набор криптографических алгоритмов и их параметров, определяющий порядок использования криптографической защиты в протоколе защищённого взаимодействия. [P 1323565.1.020-2018, п. 3.1.1]                                                             |
| Место эксплуатации СКЗИ ( <i>cryptographic module operation site</i> )                               | Место расположения штатных средств, на котором происходит штатное функционирование СКЗИ. [P 1323565.1.012-2017, п. 3.1.32]                                                                                                                           |
| Навязывание ( <i>imposition</i> )                                                                    | Атака, осуществляемая путём доведения до пользователя имитации истинного сообщения. [P 1323565.1.012-2017, п. 3.1.29]                                                                                                                                |
| Программный датчик случайных чисел; ПДСЧ ( <i>software random number generator</i> )                 | Датчик, вырабатывающий псевдослучайную последовательность путём детерминированного преобразования инициализирующей последовательности, реализованный программно. [P 1323565.1.012-2017, п. 3.1.39]                                                   |

| Термин / Англ.                                                                        | Определение                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Среда функционирования СКЗИ; СФ ( <i>cryptographic module operating environment</i> ) | Совокупность одного или нескольких аппаратных средств и/или программного обеспечения, на которых реализована ключевая система СКЗИ и/или обеспечивается её функционирование. [P 1323565.1.012-2017, н. 3.1.43]                  |
| Тематические исследования СКЗИ ( <i>cryptographic module thematic research</i> )      | Комплекс криптографических, инженерно-криптографических и специальных исследований для оценки соответствия СКЗИ требованиям по безопасности информации. [ГОСТ Р 34.14-2025, ст. 7, примечание; P 1323565.1.012-2017, н. 3.1.47] |
| Уязвимость ( <i>vulnerability</i> )                                                   | Свойство аппаратного средства и/или программного обеспечения, вытекающее, в частности, из ошибок реализации или проектирования, использование которого нарушает защищённость информации. [P 1323565.1.012-2017, н. 3.1.51]      |
| Физический датчик случайных чисел; ФДСЧ ( <i>physical random number generator</i> )   | Датчик, вырабатывающий случайную последовательность путём преобразования сигналов от физических источников случайности. [P 1323565.1.012-2017, н. 3.1.52]                                                                       |
| Штатные средства ( <i>regular means</i> )                                             | Совокупность аппаратных средств и программного обеспечения, на которых реализованы информационная система, среда функционирования и СКЗИ. [P 1323565.1.012-2017, н. 3.1.53]                                                     |
| Экспортируемая функция ( <i>exported function</i> )                                   | Реализованная в программном обеспечении СКЗИ и описанная в документации функция, к которой могут получать доступ внешние компоненты. [P 1323565.1.012-2017, н. 3.1.54]                                                          |

## Источники

Полный перечень источников с переходами от шифров — в разделе ["Источники и литература"](#).