

Доверие и доверенные среды

Термины, относящиеся к теме доверия в информационной безопасности. Основной источник — [ГОСТ Р 54581-2011](#) "Основы доверия к безопасности ИТ". Дополнительно: [ГОСТ "Доверенная среда исполнения"](#), [ГОСТ Р 34.14-2025 \(приложение Б\)](#), [NIST IR 7298r2](#), [RFC 9334 \(RATS\)](#), [RFC 4158 \(модели доверия PKI\)](#), [RFC 5280](#), [Matter PKI Certificate Policy](#), ПНСТ «Промышленный интернет вещей».

Доверие

В этом разделе

- [Базовые понятия доверия](#)
- [Методы и системы обеспечения доверия \(ГОСТ Р 54581-2011\)](#)
- [Оценивание и сертификация \(ГОСТ Р 54581-2011\)](#)
- [Уровни доверия идентификации и аутентификации](#)
- [Центр доверия и доверенные компоненты \(ГОСТ Р 34.14-2025\)](#)
- [Доверенная среда исполнения \(ГОСТ Р, проект\)](#)
- [Доверие в криптографии и PKI \(NIST IR 7298r2, RFC 9334\)](#)
- [Корень доверия \(GlobalPlatform RoT\)](#)
- [Модели доверия в PKI \(RFC 4158\)](#)
- [Управление доверием в инфраструктуре \(Matter PKI CP\)](#)
- [Доверие в киберфизических и IIoT-системах \(ПНСТ\)](#)

Базовые понятия доверия

Термин / Англ.	Определение
Доверенная среда исполнения; ДСИ (<i>trusted execution environment; TEE</i>)	Среда исполнения, работающая совместно с универсальной средой исполнения, но изолированная от неё в части доступа к данным и контроля потока выполнения при помощи аппаратных или программно-аппаратных возможностей компонентов устройства. [ГОСТ Р Доверенная среда исполнения, п. 3.3]
Доверенная сторона (<i>trusted entity</i>)	Сторона, у которой установлены отношения доверия с одной или несколькими сторонами информационного взаимодействия. [ГОСТ Р 34.14-2025, см. Б.2.20]
Доверенная третья сторона (<i>trusted third party</i>)	Участник процесса аутентификации, предоставляющий один или более сервисов в области защиты информации, которому доверяют другие участники процесса аутентификации как поставщику данных услуг. [ГОСТ Р 58833-2020, п. 3.15]

Термин / Англ.	Определение
Доверенное приложение; ДП (<i>trusted application; TA</i>)	Приложение, функционирующее в доверенной среде исполнения, которое обеспечивает функциональные возможности (сервисы), связанные с безопасностью информации, для клиентских приложений. [ГОСТ Р Доверенная среда исполнения, п. 3.6]
Доверенный объект (<i>trusted object</i>)	Объект, который будет действовать в полном соответствии с ожиданиями и субъекта доступа, и объекта доступа, при этом выполняя то, что он должен делать, и не выполняя то, что он не должен делать. [ГОСТ Р 58833-2020, п. 3.14]
Доверие (<i>assurance</i>)	Выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности. [ГОСТ Р 54581-2011, п. 2.4; ГОСТ Р 58833-2020, п. 3.16]
Доверие к процессу (<i>process assurance</i>)	Доверие, основанное на результатах оценки процесса. [ГОСТ Р 54581-2011, п. 2.26]
Коэффициент доверия (<i>certainty factor; confidence factor</i>)	Значение, приписанное справедливости утверждения, такого как гипотеза, правило логического вывода или результат логического вывода. [ГОСТ 33707-2016, п. 4.578]
Подлинность (<i>authenticity</i>)	Свойство, гарантирующее, что субъект или ресурс идентичен заявленному. [ГОСТ Р 70262.1-2022; ГОСТ Р ИСО/МЭК 27000-2021, п. 3.6]
Уверенность (<i>confidence</i>)	Убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком (корректно, надёжно, эффективно, в соответствии с политикой безопасности). [ГОСТ Р 54581-2011, п. 2.18; ГОСТ Р 58833-2020, п. 3.56]
Уровень доверия (<i>assurance level</i>)	Степень доверия, соответствующая специальной шкале, применяемой в методе обеспечения доверия. [ГОСТ Р 54581-2011, п. 2.10; ГОСТ Р 58833-2020, п. 3.58]
Электронное удостоверение (<i>electronic credential</i>)	Совокупность идентификационной информации и аутентификационной информации субъекта или объекта доступа, подлинность которой подтверждена доверенной третьей стороной. [ГОСТ Р 58833-2020, п. 3.62]

Методы и системы обеспечения доверия (ГОСТ Р 54581-2011)

Термин / Англ.	Определение
Аргумент доверия (<i>assurance argument</i>)	Совокупность структурированных утверждений о доверии, поддерживаемых свидетельством и обоснованием, которые наглядно демонстрируют, как были удовлетворены требования доверия. [ГОСТ Р 54581-2011, п. 2.6]
Метод обеспечения доверия (<i>assurance method</i>)	Общепризнанная спецификация получения воспроизводимых результатов обеспечения доверия. [ГОСТ Р 54581-2011, п. 2.11; ГОСТ Р 58833-2020, п. 3.28]

Термин / Англ.	Определение
Орган обеспечения доверия (<i>assurance authority</i>)	Лицо или организация, уполномоченные принимать решения, связанные с обеспечением доверия к оцениваемому объекту. [ГОСТ Р 54581-2011, п. 2.8]
Оценка доверия (<i>assurance assessment</i>)	Верификация и фиксирование всех видов и результатов обеспечения доверия, связанных с оцениваемым объектом. [ГОСТ Р 54581-2011, п. 2.7]
Подход к обеспечению доверия (<i>assurance approach</i>)	Группирование методов обеспечения доверия в соответствии с исследуемым аспектом. [ГОСТ Р 54581-2011, п. 2.5]
Результат обеспечения доверия (<i>assurance result</i>)	Документированное числовое или количественное утверждение об обеспечении доверия, относящееся к оцениваемому объекту. [ГОСТ Р 54581-2011, п. 2.13]
Свидетельство доверия (<i>assurance evidence</i>)	Документированные результаты, представленные в поддержку определения доверия. [ГОСТ Р 54581-2011, п. 2.16]
Свидетельство обеспечения доверия (<i>assurance evidence</i>)	Результаты анализа обеспечения доверия к объекту, поддерживающие утверждение о доверии. [ГОСТ Р 54581-2011, п. 2.9]
Система обеспечения доверия (<i>assurance scheme</i>)	Организационно-правовая структура, в рамках которой метод обеспечения доверия применяется органом обеспечения доверия. [ГОСТ Р 54581-2011, п. 2.14]
Система оценки (<i>scheme</i>)	Совокупность правил, определяющих условия среды, необходимые для признания результатов оценивания. [ГОСТ Р 54581-2011, п. 2.28]
Стадия обеспечения доверия (<i>assurance stage</i>)	Стадия жизненного цикла оцениваемого объекта, на которой используется заданный метод обеспечения доверия. [ГОСТ Р 54581-2011, п. 2.15]
Характеристика обеспечения доверия (<i>assurance property</i>)	Параметр метода обеспечения доверия, способствующий получению результатов доверия. [ГОСТ Р 54581-2011, п. 2.12]

Оценивание и сертификация (ГОСТ Р 54581-2011)

Термин / Англ.	Определение
Аттестация (<i>accreditation</i>)	Процедура, посредством которой официальный орган формально признаёт, утверждает и принимает остаточный риск для эксплуатации системы в определённом безопасном режиме. [ГОСТ Р 54581-2011, п. 2.1] 2 определений. Определение 2: Процесс создания доказательства (свидетельства), подтверждающего свойства системы или устройства, например, корректность их состояния или подлинность программного обеспечения. [RFC 9334]

Термин / Англ.	Определение
Безопасность (<i>security</i>)	Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, подотчётности, аутентичности и надёжности. [ГОСТ Р 54581-2011, n. 2.29]
Гарантийное обязательство (<i>warranty</i>)	Услуга безопасности, связанная с корректировками и улучшениями в части эксплуатации оцениваемого объекта. [ГОСТ Р 54581-2011, n. 2.36]
Гарантия (<i>guarantee</i>)	См. определение "гарантийное обязательство". [ГОСТ Р 54581-2011, n. 2.21]
Жизненный цикл системы (<i>system life cycle</i>)	Развитие рассматриваемой системы во времени от её зарождения до вывода из эксплуатации. [ГОСТ Р 54581-2011, n. 2.35]
Оцениваемый объект (<i>deliverable</i>)	Продукт, система, услуга, процесс безопасности ИТ или составной элемент среды функционирования, поставляемый для оценки доверия. [ГОСТ Р 54581-2011, n. 2.19]
Оценивание (<i>evaluation</i>)	Оценка оцениваемого объекта на соответствие установленным критериям. [ГОСТ Р 54581-2011, n. 2.20]
Оценка (<i>assessment</i>)	Верификация оцениваемого объекта доверия с помощью соответствующего подхода с целью установления соответствия стандарту и определения уровня доверия. [ГОСТ Р 54581-2011, n. 2.3]
Оценка безопасности (<i>security assessment</i>)	Верификация соответствия защищённого оцениваемого объекта требованиям стандарта безопасности. [ГОСТ Р 54581-2011, n. 2.30]
Подход (<i>approach</i>)	Метод или определённые действия (процедуры), используемые или предпринимаемые для достижения заявленной цели. [ГОСТ Р 54581-2011, n. 2.2]
Правообладатель (<i>stakeholder</i>)	Сторона, имеющая некоторые права, акции, а также активы, подверженные риску по отношению к оцениваемому объекту. [ГОСТ Р 54581-2011, n. 2.33]
Предыстория (<i>pedigree</i>)	Неформальное признание того, что поставщик обеспечивает соответствующую воспроизводимость оцениваемых объектов. [ГОСТ Р 54581-2011, n. 2.24]
Продукт безопасности ИТ (<i>IT security product</i>)	Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определённые функциональные возможности. [ГОСТ Р 54581-2011, n. 2.22]
Процесс (<i>process</i>)	Упорядоченная совокупность действий, использующая ресурсы для преобразования входов в выходы. [ГОСТ Р 54581-2011, n. 2.25]
Рабочая продукция (<i>work product</i>)	Все элементы (документы, отчёты, файлы, данные), производимые процессом и используемые как свидетельство. [ГОСТ Р 54581-2011, n. 2.37]
Сертификация (<i>certification</i>)	Процедура выдачи официального подтверждения о соответствии оцениваемого объекта установленным требованиям. [ГОСТ Р 54581-2011, n. 2.17]

Термин / Англ.	Определение
Стадия жизненного цикла (<i>life cycle stage</i>)	Период жизненного цикла оцениваемого объекта, выделяемый по признакам удобства управления, планирования и оценки. [ГОСТ Р 54581-2011, п. 2.23]
Услуга (<i>service</i>)	Связанные с обеспечением безопасности процесс или задача, выполняемые одной стороной для другой. [ГОСТ Р 54581-2011, п. 2.32]
Элемент безопасности (<i>security element</i>)	Неделимое требование безопасности. [ГОСТ Р 54581-2011, п. 2.31]

Уровни доверия идентификации и аутентификации

Термин / Англ.	Определение
Высокий уровень доверия	Существует значительная уверенность в соответствии субъекта доступа идентификационной информации. [ГОСТ Р 70262.1-2022; ГОСТ Р 58833-2020, п. 7.1]
Низкий уровень доверия	Имеется некоторая уверенность в соответствии субъекта доступа идентификационной информации. [ГОСТ Р 70262.1-2022; ГОСТ Р 58833-2020, п. 7.1]
Средний уровень доверия	Появляется умеренная уверенность в соответствии субъекта доступа идентификационной информации. [ГОСТ Р 70262.1-2022; ГОСТ Р 58833-2020, п. 7.1]
Уровень доверия к результатам аутентификации (<i>authentication results assurance level</i>)	Достигнутая уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом, за кого себя выдаёт. [ГОСТ Р 58833-2020, п. 7.2]
Уровень доверия к результатам идентификации (<i>identification results assurance level</i>)	Достигнутая уверенность в том, что субъект (объект) доступа действительно соответствует зарегистрированной идентификационной информации. [ГОСТ Р 70262.1-2022]

Центр доверия и доверенные компоненты (ГОСТ Р 34.14-2025)

Термин / Англ.	Определение
Аутентификация данных (<i>data authentication</i>)	Проверка целостности данных и аутентификация их источника. [ГОСТ Р 34.14-2025, см. 22]
Аутентификация источника данных (<i>data origin authentication</i>)	Проверка и подтверждение того, что набор данных (сообщение, документ) был создан именно заявленным источником. [ГОСТ Р 34.14-2025, см. Б.2.8]

Термин / Англ.	Определение
Аутентификация стороны (<i>entity authentication</i>)	Проверка одной из сторон того, что взаимодействующая с ней сторона — именно та, за которую себя выдаёт. [ГОСТ Р 34.14-2025, см. Б.2.9]
Целостность данных (<i>data integrity</i>)	Свойство, отражающее отсутствие изменений в передаваемой или хранимой информации. [ГОСТ Р 34.14-2025, см. Б.2.13]
Центр доверия (<i>trusted party</i>)	Сторона, у которой установлены отношения доверия со всеми остальными сторонами информационного взаимодействия. [ГОСТ Р 34.14-2025, см. Б.2.21]

Доверенная среда исполнения (ГОСТ Р, проект)

Термин / Англ.	Определение
Актив доверенной среды исполнения (<i>TEE asset</i>)	Физический или логический компонент доверенной среды исполнения, подлежащий защите. [ГОСТ Р Доверенная среда исполнения, п. 3.5]
Клиентское приложение; КП (<i>client application; CA</i>)	Приложение, функционирующее в универсальной среде исполнения, использующее клиентский прикладной программный интерфейс доверенной среды исполнения для доступа к сервисам, предоставляемым доверенными приложениями. [ГОСТ Р Доверенная среда исполнения, п. 3.7]
Система на кристалле; снк (<i>system on a chip; SoC</i>)	Интегральная схема, включающая в свой состав компоненты, обычно присутствующие в различных микросхемах. [ГОСТ Р Доверенная среда исполнения, п. 3.8]
Среда исполнения (<i>execution environment</i>)	Набор аппаратных и программных компонентов, обеспечивающих исполнение прикладного программного обеспечения (приложений). [ГОСТ Р Доверенная среда исполнения, п. 3.1]
Универсальная среда исполнения; УСИ (<i>rich execution environment; REE</i>)	Среда исполнения, включающая операционную систему общего назначения, специализированную или другую, либо иное системное программное обеспечение, и все компоненты устройства, которые обеспечивают её функционирование. [ГОСТ Р Доверенная среда исполнения, п. 3.2]

Доверие в криптографии и PKI (NIST IR 7298r2, RFC 9334)

Термин / Англ.	Определение
Аттестующий (<i>attester</i>)	Роль, выполняемая устройством, которое предоставляет свидетельство (evidence) о своём состоянии для проверки верификатором. [RFC 9334]
Верификатор (<i>verifier</i>)	Роль, выполняемая субъектом, который оценивает достоверность свидетельства об аттестующем и формирует результаты аттестации для использования доверяющей стороной. [RFC 9334]

Термин / Англ.	Определение
Доверенная вычислительная база (<i>trusted computing base; TCB</i>)	Совокупность механизмов защиты в компьютерной системе, включая аппаратные средства, микрокод и программное обеспечение, совместная работа которых отвечает за обеспечение политики безопасности. <i>[NIST IR 7298r2; CNSSI-4009]</i>
Доверенность (<i>trustworthiness</i>)	Атрибут лица или организации, обеспечивающий уверенность других в квалификации, возможностях и надёжности этого субъекта при выполнении конкретных задач и возложенных обязанностей. <i>[NIST IR 7298r2]</i>
Доверенный сертификат (<i>trusted certificate</i>)	Сертификат, которому доверяет доверяющая сторона на основании безопасной и достоверной процедуры. <i>[NIST IR 7298r2]</i>
Доверяющая сторона (<i>relying party</i>)	Роль, выполняемая субъектом, который зависит от достоверности информации об аттестующем для целей надёжного применения специфичных для приложения действий. <i>[RFC 9334]</i>
Поставщик эталонных значений (<i>reference value provider</i>)	Роль, выполняемая субъектом, который предоставляет эталонные значения (reference values), используемые верификатором для оценки соответствия аттестующего требованиям. <i>[RFC 9334]</i>
Результаты аттестации (<i>attestation results</i>)	Концептуальное сообщение, формируемое верификатором для доверяющей стороны, содержащее результаты оценки свидетельства об аттестующем. <i>[RFC 9334]</i>
Свидетельство аттестации (<i>evidence</i>)	Концептуальное сообщение, содержащее утверждения (claims) об аттестующем, формируемое аттестующим для верификатора. <i>[RFC 9334]</i>
Список доверия (<i>trust list</i>)	Совокупность доверенных сертификатов, используемых доверяющими сторонами для проверки сертификатов. <i>[NIST IR 7298r2]</i>
Эндорсер (<i>endorser</i>)	Роль, выполняемая субъектом (как правило, производителем), чьи подтверждения (endorsements) помогают верификатору оценить подлинность свидетельства и установить дополнительные возможности аттестующего. <i>[RFC 9334]</i>
Якорь доверия (<i>trust anchor</i>)	Открытый ключ и имя удостоверяющего центра, используемые для проверки первого сертификата в последовательности сертификатов. Безопасность процесса проверки зависит от подлинности и целостности якоря доверия. <i>[NIST IR 7298r2]</i>

Корень доверия (GlobalPlatform RoT)

Термин / Англ.	Определение
Исходный компонент корня доверия (<i>initial root of trust component</i>)	Корень доверия, целостность кода и данных которого не может быть проверена другим компонентом (он доверяется изначально). <i>[GlobalPlatform RoT v1.1]</i>

Термин / Англ.	Определение
Корень доверия; КД (<i>root of trust; RoT</i>)	Компонент, который должен всегда вести себя ожидаемым образом, поскольку его неправильное поведение не может быть обнаружено. Корень доверия — основа, на которую опираются другие доверенные функции. <i>[GlobalPlatform RoT v1.1; TCG]</i>
Начальный загрузчик корня доверия (<i>bootstrapped root of trust</i>)	Корень доверия, целостность которого устанавливается в результате процесса начальной загрузки (<i>bootstrapping</i>). <i>[GlobalPlatform RoT v1.1]</i>
Первичный корень доверия (<i>primary root of trust; pRoT</i>)	Первый основанный на платформе корень доверия, инстанцируемый на устройстве. <i>[GlobalPlatform RoT v1.1]</i>
Расширенный компонент корня доверия (<i>extended root of trust component</i>)	Блок кода и данных, целостность которого может быть проверена родительским блоком кода. <i>[GlobalPlatform RoT v1.1]</i>

Модели доверия в PKI (RFC 4158)

Термин / Англ.	Определение
Доверие к открытым ключам (<i>trust of public keys</i>)	Открытый ключ считается заслуживающим доверия, если сертификат, содержащий этот ключ, может быть проверен согласно установленным процедурам проверки пути сертификации. <i>[RFC 4158]</i>
Доверие транзитивное (<i>transitive trust</i>)	Свойство отношений между удостоверяющими центрами, при котором доверие, установленное с одним УЦ, неявно распространяется на другие УЦ через кросс-сертификацию. Создаёт риск непреднамеренных путей сертификации. <i>[RFC 4158]</i>
Кросс-сертификат (<i>cross-certificate</i>)	Сертификат, выданный одним удостоверяющим центром другому УЦ с целью установления отношений доверия между ними. <i>[RFC 4158; RFC 5280]</i>
Кросс-сертификация (<i>cross-certification</i>)	Действие по выпуску кросс-сертификатов между удостоверяющими центрами. <i>[RFC 4158]</i>
Размытие доверия (<i>dilution of trust</i>)	Потеря части уверенности с каждым последующим звеном в инфраструктуре сертификации (выпуск сертификатов УЦ и кросс-сертификация между УЦ). <i>[RFC 4158]</i>
Сертификат якоря доверия (<i>trust anchor certificate</i>)	Самоподписанный сертификат для якоря доверия, используемый при обработке пути сертификации. <i>[RFC 4158]</i>
Цепочка доверия (<i>chain of trust</i>)	Последовательность сертификатов (путь сертификации), устанавливающая доверие между якорем доверия и целевым сертификатом посредством криптографической проверки подписей. <i>[RFC 4158; RFC 5280]</i>

Управление доверием в инфраструктуре (Matter PKI CP)

Термин / Англ.	Определение
Доверенная должность (trusted position)	Должности в субъекте инфраструктуры PKI, которые должны занимать доверенные лица. [Matter PKI CP]
Доверенное лицо (trusted person)	Сотрудник, подрядчик или консультант субъекта в инфраструктуре PKI, ответственный за управление инфраструктурной надёжностью субъекта, его продуктами, сервисами, объектами и/или практиками. [Matter PKI CP]
Заслуживающая доверия система (trustworthy system)	Компьютерное аппаратное обеспечение, программное обеспечение и процедуры, обоснованно защищённые от вторжений и злоупотреблений; обеспечивающие разумный уровень доступности, надёжности и корректной работы; подходящие для выполнения предназначенных функций и принуждающие к соблюдению применимой политики безопасности. [Matter PKI CP]
Управление доверием (trust management)	Совокупность служб и процессов, обеспечивающих поддержку экосистемы в достижении её целей безопасности с использованием инфраструктуры открытых ключей. [Matter PKI CP]

Доверие в киберфизических и IIoT-системах (ПНСТ)

Термин / Англ.	Определение
Граница доверия (trust boundary)	Разделение разных приложений или доменов системы, в которых требуются разные уровни доверия. [ПНСТ «Промышленный интернет вещей», п. 3.27]
Достоверность (trustworthiness)	Степень доверия к тому, что система работает согласно ожиданиям с такими характеристиками, как функциональная безопасность, безопасность, приватность, надёжность и способность к восстановлению в условиях воздействия окружающей среды, ошибок персонала, системных сбоев и атак. [ПНСТ «Промышленный интернет вещей», п. 3.39]
Корни доверия (roots of trust)	Базис, включающий оборудование, программное обеспечение, людей и организационные процессы для установления доверия к системе. [ПНСТ «Промышленный интернет вещей», п. 3.68]

Источники

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

