ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ГОСТ Р 54581— 2011/ ISO/IEC/TR 15443-1:2005**

## Информационная технология

# МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

## Основы доверия к безопасности ИТ

### Часть 1

## Обзор и основы

**(ISO/IEC TR 15443-1:2005, IDT)**

**Издание официальное**

Москва
Стандартинформ
2018

gost.e-ecolog.ru

## Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»), Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ») на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации «Защита информации» ТК 362

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 689-ст

4 Настоящий стандарт идентичен международному документу ISO/IEC TR 15443-1:2005 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы» (ISO/IEC TR 15443-1:2005 «Information technology — Security techniques — A framework for IT security assurance — Part 1: Overview and framework», IDT)

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Октябрь 2018 г.

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

© ISO, 2005 — Все права сохраняются
© Стандартинформ, оформление, 2012, 2018

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

## Содержание

1 Область применения . . . . . 1
1.1 Назначение . . . . . 1
1.2 Подход . . . . . 1
1.3 Применение . . . . . 1
1.4 Сфера применения . . . . . 1
1.5 Ограничения . . . . . 1
2 Термины и определения . . . . . 1
3 Обозначения и сокращения . . . . . 5
4 Общие понятия . . . . . 5
4.1 Необходимость доверия . . . . . 5
4.2 Отличие доверия от уверенности . . . . . 6
4.3 Что такое «оцениваемый объект» . . . . . 6
4.4 Правообладатели . . . . . 7
4.5 Требования доверия . . . . . 7
4.6 Применимость методов обеспечения доверия к безопасности информационных технологий . . 8
4.7 Системы обеспечения доверия . . . . . 8
4.8 Количественное определение риска доверия и устойчивости механизма обеспечения безопасности . . . . . 9
4.9 Доверие снижает риск безопасности . . . . . 9
4.10 Количественное определение доверия . . . . . 9
4.11 Орган обеспечения доверия . . . . . 9
5 Выбор доверия к безопасности . . . . . 10
5.1 Спецификация требований доверия . . . . . 11
5.2 Экономические вопросы . . . . . 12
5.3 Организационные вопросы . . . . . 12
5.4 Тип доверия . . . . . 12
5.5 Технические вопросы . . . . . 13
5.6 Рассмотрение вопросов оптимизации . . . . . 13
6 Базовая структура доверия . . . . . 14
6.1 Подход к обеспечению доверия . . . . . 14
6.2 Методы обеспечения доверия . . . . . 14
6.3 Аспекты жизненного цикла . . . . . 15
6.4 Сопоставление доверия к эффективности с доверием к корректности . . . . . 16
6.5 Классификация методов обеспечения доверия . . . . . 17
6.6 Составное доверие . . . . . 18
6.7 Классификация доверия . . . . . 19
Библиография . . . . . 20

## Введение

На пленарном заседании ИСО/МЭК СТК 1/ПК 27 в ноябре 1994 года была создана исследовательская группа для рассмотрения вопросов тестирования методов обеспечения доверия и оценки соответствия продуктов и систем информационных технологий (ИТ) стандартам безопасности ПК 27 и других организаций (например, стандартам ПК 21 и Европейского института стандартов по телекоммуникациям, а также некоторым Интернет-стандартам, содержащим аспекты, связанные с безопасностью). Параллельно в начале 1996 года для проекта «Общие критерии» была создана рабочая группа, занимающаяся методами обеспечения доверия. ISO/IEC TR 15443 является результатом деятельности этих двух групп.

Назначением ISO/IEC TR 15443 является представление различных методов обеспечения доверия и содействие специалистам в области ИТ в выборе соответствующего метода обеспечения доверия (или комбинации методов) с целью получения уверенности в том, что оцениваемый объект удовлетворяет установленным требованиям доверия к безопасности ИТ. В ISO/IEC TR 15443 изучаются подходы и методы обеспечения доверия, предложенные организациями различного типа, независимо от того, включают ли в себя эти методы и подходы утвержденные стандарты или стандарты «де-факто».

ISO/IEC TR 15443 рассматривает:

a) структурную модель взаимосвязи существующих методов обеспечения доверия;

b) совокупность методов обеспечения доверия, их описание и ссылки на них;

c) представление общих и уникальных свойств, присущих методам обеспечения доверия;

d) качественное и (по возможности) количественное сравнение существующих методов обеспечения доверия;

e) идентификацию систем оценки доверия, связанных с методами обеспечения доверия;

f) описание взаимосвязей между различными методами обеспечения доверия;

g) руководство по созданию, применению и идентификации методов обеспечения доверия.

ISO/IEC TR 15443 состоит из трех частей:

- часть 1. Обзор и основы; представляет собой обзор фундаментальных концепций и общее описание методов обеспечения доверия. Данный материал способствует пониманию частей 2 и 3 ISO/IEC TR 15443. Часть 1 предназначена для руководителей в области безопасности, ответственных за разработку программы обеспечения доверия к безопасности, определение степени доверия к безопасности своих объектов, осуществление проверки оценки степени доверия (например, ИСО 9000, SSE-CMM (ИСО/МЭК 21827), ИСО/МЭК 15408-3) или других видов деятельности по обеспечению доверия;

- часть 2. Методы доверия; приводится описание различных методов обеспечения доверия и подходов, их связи со структурной моделью обеспечения доверия к безопасности из части 1. Акцент делается на идентификацию качественных характеристик методов обеспечения доверия. Данный документ способствует пониманию специалистом в области безопасности ИТ процедуры получения доверия на различных этапах жизненного цикла объекта;

- часть 3. Анализ методов доверия; приводится анализ обеспечения доверия относительно их различных характеристик. Анализ способствует принятию органом обеспечения доверия решения по относительной значимости каждого подхода к обеспечению доверия и выбору подхода(ов), который(е) обеспечит(ат) результаты, наиболее соответствующие требованиям этого органа. Анализ также способствует органу обеспечения доверия в использовании результатов доверия для получения требуемой уверенности в объекте. Данный документ предназначен для специалистов в области безопасности ИТ, которые должны осуществить выбор методов обеспечения доверия и подходов к ним.

В ISO/IEC TR 15443 анализируются методы обеспечения доверия, которые могут предназначаться не только для безопасности ИТ; однако руководство, приведенное в ISO/IEC TR 15443, ограничивается требованиями к безопасности ИТ. В ISO/IEC TR 15443 включены дополнительные термины и понятия, регламентированные в других инициативах международной стандартизации (CASCO) и международных руководствах (например, в Руководстве 2 ИСО/МЭК), однако представленное в ISO/IEC TR 15443 руководство предназначено только для области обеспечения безопасности ИТ и не предназначено для общего менеджмента и оценки качества или обеспечения соответствия ИТ требованиям безопасности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Информационная технология**

**МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ**

**Основы доверия к безопасности ИТ**

**Часть 1**

**Обзор и основы**

Information technology. Security techniques. A framework for IT security assurance. Part 1. Overview and framework

**Дата введения — 2012—07—01**

## 1 Область применения

### 1.1 Назначение

Настоящий стандарт предназначен для описания методов обеспечения доверия к безопасности, соотнесения их с базовой моделью жизненного цикла объекта и классификации методов обеспечения доверия для получения высокой степени уверенности в функциональных возможностях обеспечения безопасности объекта.

### 1.2 Подход

В настоящем стандарте представлен краткий обзор основных понятий обеспечения доверия и терминов, необходимых для понимания и применения методов обеспечения доверия, посредством идентификации различных подходов и стадий обеспечения доверия.

### 1.3 Применение

Классификация методов обеспечения доверия с учетом требований ISO/IEC TR 15443 позволяет пользователю осуществлять выбор и возможное сочетание методов обеспечения доверия, которые целесообразно применить к конкретному объекту.

### 1.4 Сфера применения

Настоящий стандарт содержит руководство по классификации методов обеспечения доверия, включая методы, не специфичные для обеспечения безопасности ИТ. Настоящее руководство может применяться даже в областях, не связанных с безопасностью ИТ, но критичных к обеспечению доверия.

### 1.5 Ограничения

Требования настоящего стандарта применяют только к объектам, указанным в 4.3, и связанным с ними организационным вопросам обеспечения безопасности.

## 2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

Примечание — Термины и определения представлены в общем виде для поддержки общей модели доверия, представленной в настоящем стандарте, в целях обеспечения ее применимости к широкому ряду подходов обеспечения доверия.

**Издание официальное**

В ISO/IEC TR 15443 применены термины и определения, обеспечивающие нейтральность структуры обеспечения доверия и ее применимость для широкого ряда методов обеспечения доверия. Для этого применялись термины из международных стандартов, в частности для поддержки совместимости настоящего стандарта с частями 1—3 ИСО/МЭК 15408 и серией стандартов ИСО 9000.

При наличии нескольких определений для одного и того же термина вначале представлено основное определение, соответствующее целям ISO/IEC TR 15443. Альтернативные определения, выделенные курсивом, считают применимыми только в контексте их источника.

2.1 **аттестация** (accreditation): Процедура, посредством которой официальный орган формально признает, утверждает и принимает остаточный риск:

*a) для эксплуатации автоматизированной системы в определенном безопасном режиме с использованием заданного набора мер безопасности*

*[адаптировано из AGCA];*

*b) того, что орган или лицо, обеспечивающие безопасность, достаточно компетентны для выполнения конкретных задач*

*[адаптировано из Руководства 2 ИСО/МЭК] и*

*c) того, что услуга по обеспечению безопасности соответствует предопределенной среде применения.*

2.2 **подход** (approach): Метод или определенные действия (процедуры), используемые или предпринимаемые для выполнения задания или решения задачи.

2.3 **оценка** (assessment): Верификация оцениваемого объекта доверия с помощью соответствующего подхода с целью установления соответствия стандарту и определения степени (уровня) доверия.

2.4 **доверие** (assurance): Выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям безопасности.

*a) основание для уверенности в том, что сущность отвечает своим целям безопасности.*

*[ИСО/МЭК 15408-1]*

2.5 **подход к обеспечению доверия** (assurance approach): Группирование методов обеспечения доверия в соответствии с исследуемым аспектом.

2.6 **аргумент доверия** (assurance argument): Совокупность структурированных утверждений о доверии, поддерживаемых свидетельством и обоснованием, которые наглядно демонстрируют то, как были удовлетворены требования доверия.

2.7 **оценка доверия** (assurance assessment): Верификация и фиксирование всех видов и результатов обеспечения доверия, связанных с оцениваемым объектом (приобщенных к аргументу доверия).

2.8 **орган обеспечения доверия** (assurance authority): Лицо или организация, уполномоченные принимать решения (например, по выбору, спецификации, принятию, контролю за исполнением), связанные с обеспечением доверия к оцениваемому объекту, что однозначно приводит к формированию уверенности в безопасности данного объекта.

Примечание — В конкретных системах и организациях понятие «орган обеспечения доверия» может иметь другое значение, например «орган оценки».

2.9 **свидетельство обеспечения доверия** (assurance evidence): Результаты анализа обеспечения доверия к объекту (включая итоговые отчеты или другие обоснования), поддерживающие утверждение о доверии.

2.10 **уровень доверия** (assurance level): Степень доверия, соответствующая специальной шкале, применяемой в методе обеспечения доверия.

Примечания

1 Уровень доверия не измеряется количественными показателями.

2 Степень доверия обычно определяется усилиями, затраченными на выполнение определенных действий.

2.11 **метод обеспечения доверия** (assurance method): Общепризнанная спецификация получения воспроизводимых результатов обеспечения доверия.

2.12 **характеристика обеспечения доверия** (assurance property): Параметр метода обеспечения доверия, способствующий получению результатов доверия.

2.13 **результат обеспечения доверия** (assurance result): Документированное числовое или количественное утверждение об обеспечении доверия, относящееся к какому-либо оцениваемому объекту.

2.14 **система обеспечения доверия** (assurance scheme): Организационно-правовая структура, в рамках которой метод обеспечения доверия применяется органом обеспечения доверия в пределах определенного сообщества или организации.

*а) организационно-правовая структура, в рамках которой в определенном сообществе органы оценки применяют требования ИСО/МЭК 15408.*

*[ИСО/МЭК 15408-1]*

2.15 **стадия обеспечения доверия** (assurance stage): Стадия жизненного цикла оцениваемого объекта, на которой используется заданный метод обеспечения доверия. При обеспечении общего доверия к оцениваемому объекту учитываются результаты реализации методов обеспечения доверия, применяемых на всех стадиях его жизненного цикла.

2.16 **свидетельство доверия** (assurance evidence): Документированные результаты, представленные данными, полученными при анализе доверия к оцениваемому объекту, включая отчеты (обоснования) в поддержку утверждения о доверии.

2.17 **сертификация** (certification): Процедура выдачи официального подтверждения о соответствии оцениваемого объекта установленным требованиям. Сертификация может проводиться третьей стороной.

[адаптировано из Руководства 2 ИСО/МЭК]

*а) выдача официального подтверждения результатов оценки и правильности применения критериев оценки.*

*[Стандарт ITSEC]*

*b) процесс сертификации является независимой проверкой результатов оценивания, приводящей к получению окончательного сертификата или утверждения.*

*[ИСО/МЭК 15408-1]*

*c) всесторонняя оценка технических и нетехнических характеристик безопасности системы информационных технологий, осуществленная в поддержку сертификации, которая устанавливает степень соответствия системы установленной политике безопасности.*

*[AGCA]*

2.18 **уверенность** (confidence): Убежденность в том, что оцениваемый объект будет функционировать в соответствии с заданным или установленным порядком (то есть корректно, надежно, эффективно в соответствии с политикой безопасности).

2.19 **оцениваемый объект** (deliverable): Продукт, система, услуга, процесс безопасности ИТ или составной элемент среды функционирования (связанный, например, с персоналом, организацией) или другой объект, поставляемый для оценки доверия. Таким объектом может быть профиль защиты или задание по безопасности, определенные в ИСО/МЭК 15408-1.

Примечание — В ИСО 9000:2000 услуга (сервис) считается одним из типов продукта, и в серии стандартов ИСО 9000 используется сочетание «продукт и/или услуга».

2.20 **оценивание** (evaluation): Оценка оцениваемого объекта на соответствие установленным критериям (адаптировано из ИСО/МЭК 15408-1).

*а) систематическое оценивание (оценивание качества) степени, в которой логический объект способен выполнять установленные требования.*

*[ИСО/МЭК 14598-1]*

2.21 **гарантия** (guarantee): См. определение «гарантийное обязательство» в 2.36.

2.22 **продукт безопасности ИТ** (IT security product): Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы.

[ИСО/МЭК 15408-1]

2.23 **стадия жизненного цикла** (life cycle stage): Период жизненного цикла оцениваемого объекта, связанный с его определенным состоянием.

*а) период в пределах жизненного цикла системы, относящийся к состоянию системного описания или непосредственно к самой системе.*

*[ИСО/МЭК 15288]*

2.24 **предыстория** (pedigree): Неформальное признание того, что поставщик обеспечивает соответствующую воспроизводимость оцениваемых объектов, которые удовлетворяют требованиям их политики безопасности или функционируют в соответствии с заявлением поставщика (предыстория является фактором среды, связанным с поставщиком или оцениваемым объектом).

2.25 **процесс** (process): Упорядоченная совокупность действий, использующая ресурсы для преобразования входных данных в выходные.

2.26 **доверие к процессу** (process assurance): Доверие, основанное на результатах оценки процесса.

2.27 **продукт** (product) — См. определение термина «оцениваемый объект».

2.28 **система оценки** (sheme): Совокупность правил, определяющих условия среды, необходимые для проведения оценки, включая критерии и методологию.

[Адаптировано из ИСО/МЭК 18045 (Общая методология оценки)].

2.29 **безопасность** (security): Все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, подотчетности, аутентичности и достоверности.

Примечание — Считаются защищенными до тех пор, пока их пользователи могут быть уверенными в их должном функционировании. Защищенность продукта, системы или услуги обычно рассматриваются в контексте оценки фактических или ожидаемых угроз.

*а) способность программного продукта защитить информацию и данные так, чтобы неуполномоченные лица или системы не могли их считать или модифицировать, а уполномоченные — не получали бы отказ в доступе к ним.*

*[ИСО/МЭК 9126-1]*

2.30 **оценка безопасности** (security assessment): Верификация соответствия защищенного оцениваемого объекта требованиям стандарта безопасности, используя соответствующий метод обеспечения безопасности и определения доверия к безопасности.

*а) последний этап процесса оценки продукта.*

*[ИСО/МЭК 14598-1]*

2.31 **элемент безопасности** (security element): Неделимое требование безопасности.

2.32 **услуга** (service): Связанные с обеспечением безопасности процесс или задача, выполняемый или решаемая оцениваемым объектом, организацией или конкретным лицом.

2.33 **правообладатель** (stakeholder): Сторона, имеющая некоторые права, акции, а также активы, подверженные риску по отношению к оцениваемому объекту или их характеристикам, отвечающим потребностям и ожиданиям этой стороны.

*а) сторона, владеющая правом, долей или активом в системе с характеристиками, отвечающими потребностям и ожиданиям этой стороны.*

*[ИСО/МЭК 15288]*

2.34 **система** (system): Специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

[ИСО/МЭК 15408-1]

*а) комбинация взаимодействующих компонентов, организованных для достижения одной или нескольких поставленных целей.*

*[ИСО/МЭК 15288]*

Примечания

1 Система может рассматриваться как продукт или совокупность услуг, которые она обеспечивает.

[ИСО/МЭК 15288]

2 На практике интерпретация данного зачастую уточняется с помощью ассоциативного существительного, например «система самолета». В некоторых случаях слово «система» допускается заменять, например, контекстным синонимом «самолет», хотя это может впоследствии затруднить восприятие системных принципов.

[ИСО/МЭК 15288]

2.35 **жизненный цикл системы** (system life cycle): Развитие рассматриваемой системы во времени от замысла до списания.

[ИСО/МЭК 15288]

2.36 **гарантийное обязательство** (warranty): Услуга (сервис) безопасности, связанная(ый) с корректировками и улучшениями в части эксплуатации (развертывания, функционирования или доставки) оцениваемого объекта, если они не соответствуют его политике безопасности.

2.37 **рабочая продукция** (work product): Все элементы (то есть документы, отчеты, файлы, данные и т. д.), полученные в ходе выполнения любого процесса по разработке и поставке оцениваемого объекта.

[SSE-CMM (ИСО/МЭК 21827)]

*а) результат выполнения совокупности действий, использующих ресурсы для преобразования входных данных в выходные.*

*[ИСО 9001]*

## 3 Обозначения и сокращения

BSI — немецкое агентство информационной безопасности;

CASCO — комитет ИСО по оценке соответствия;

CEM — общая методология оценки;

CMM — модель зрелости возможностей;

CSE — Институт безопасности коммуникаций (канадская Организация по безопасности ИТ);

CTCPEC — канадские критерии оценки надежного программного продукта (издаваемые CSE);

ITSEC — европейский стандарт оценки безопасности компьютерных систем;

ITSEM — методология оценки безопасности информационных технологий;

HCD — проектирование, основанное на участии человека;

NSA — Агентство национальной безопасности (США);

SE-CMM — модель зрелости системного проектирования (модель технологической зрелости является торговым знаком университета Карнеги Мелона);

SSAM® — методология оценки в соответствии с SSE-CMM;

SSE-CMM® — Проектирование систем безопасности — Модель зрелости процесса ИСО/МЭК 21827;

TCSEC — критерии оценки доверенных компьютерных систем;

TREP — доверенная программа оценивания продукта (стандарты TCSEC и CTCPEC);

АЗБ (AST) — абстрактное задание по безопасности;

ИСО (ISO) — Международная организация по стандартизации;

ИТ (IT) — информационная технология;

ЗБ (ST) — задание по безопасности (определено в ИСО/МЭК 15408-1);

МЭК (IEC) — Международная электротехническая комиссия;

ОО (TOE) — объект оценки (термин, специфичный для ИСО/МЭК 15408 и определенный в ИСО/МЭК 15408-1);

ПЗ (PP) — профиль защиты (определено в ИСО/МЭК 15408-1);

СТС (SCT) — строгое тестирование на соответствие (требованиям безопасности).

## 4 Общие понятия

Настоящий раздел содержит общие понятия обеспечения доверия и предназначен для определения применимости этих понятий к обеспечению доверия к безопасности ИТ в целом. Приведенные в настоящем разделе понятия используются в широком смысле, а не относятся непосредственно к обеспечению безопасности ИТ или оценке соответствия.

### 4.1 Необходимость доверия

Системы ИТ вследствие ошибок и уязвимостей подвержены сбоям и нарушениям в обеспечении безопасности. Эти ошибки и уязвимости могут быть следствием частого изменения технологий, ошибок оператора, неудовлетворительных технических требований и организации процессов разработки или результатом недооценки угроз. Кроме того, проводятся модификации систем, появляются новые дефекты и атаки на системы, способствующие увеличению числа уязвимостей, сбоев и нарушений обеспечения безопасности в течение всего жизненного цикла системы ИТ.

Обычно безошибочное и устойчивое функционирование системы ИТ в рамках приемлемых ограничений по стоимости и времени невозможно осуществить в течение всего ее жизненного цикла вследствие ошибок или недосмотра оператора, отказа какого-либо компонента оборудования или несовершенства механизмов обеспечения безопасности. В данной ситуации почти невозможно гарантировать безошибочность, устойчивость и безопасность функционирования системы ИТ.

В соответствии с вышеизложенным очевидно, что ошибки, уязвимости и риски, по-видимому, будут всегда существовать и изменяться на всех стадиях жизненного цикла оцениваемого объекта. Следовательно, ошибками, уязвимостями и рисками надо управлять в пределах допустимых параметров в

течение жизненного цикла оцениваемого объекта, иначе доверие к нему будет изменяться. Задачей при проектировании и управлении безопасностью ИТ является обеспечение менеджмента рисков безопасности посредством ослабления уязвимостей и угроз, используя технические и организационные меры безопасности с целью обеспечения достаточно приемлемого уровня доверия к безопасности оцениваемого объекта. Дополнительной задачей управления безопасностью ИТ является установление приемлемого уровня доверия обеспечения менеджмента риска. Таким образом, правообладатели, связанные с системой ИТ, получат обоснованную уверенность в том, что оцениваемый объект будет функционировать в соответствии с намеченным и утвержденным планом, с приемлемым риском и в рамках бюджета. С точки зрения безопасности это означает уверенность в осуществлении оцениваемым объектом принятой политики безопасности.

### 4.2 Отличие доверия от уверенности

Следует отметить, что «доверие» и «уверенность» не являются идентичными и взаимозаменяемыми. Очень часто из-за их тесной взаимосвязи понятия используются неправильно. Важно, чтобы пользователь понимал различие между этими понятиями. Уверенность, с точки зрения отдельного лица, связана с убеждением, что он обладает доверием к оцениваемому объекту, тогда как доверие связано с доказанной способностью данного объекта обеспечивать выполнение цели безопасности. Таким образом, уверенность не является несомненным фактом, а выражением убежденности, полученной через оценку доверия.

Доверие определяется свидетельством, полученным в результате оценки объекта. Свидетельство, обычно включающее в себя аргумент доверия, документацию и другие соответствующие рабочие материалы, служит основанием для утверждения доверия, которое основано на результатах действий, связанных с проектированием и оценкой безопасности.

Уверенность является предметом восприятия отдельным лицом специфических требований безопасности и информации, полученной в результате оценки, о том, что оцениваемый объект будет функционировать в соответствии с установленными требованиями. Уверенность подразумевает знание критериев, метода, системы обеспечения доверия и используемых процедур оценки. Более того, репутация оценщиков и операторов является важным фактором формирования уверенности в оцениваемом объекте, поскольку их квалификация и опыт могут быть востребованы. В результате индивидуального восприятия у правообладателей могут возникнуть различные степени уверенности в результате использования соответствующего метода обеспечения доверия как отдельным лицом, так и организацией в целом.

### 4.3 Что такое «оцениваемый объект»

Традиционно термин «доверие» ассоциировался только с продуктами и системами ИТ, состоящими из аппаратных средств и программного обеспечения (ПО), и рассматривался как доверие к продукту или системе. Теперь общепризнано, что для рассмотрения более широкого диапазона рисков существует потребность в доверии к другим объектам, таким как услуга обеспечения безопасности, процесс, персонал, организация и другие факторы внешней среды, влияющие на безопасность. С учетом этого нового фактора и используется термин «оцениваемый объект» для ссылки на объект оценки безопасности.

Понятие «оцениваемый объект» (далее — объект) в широком смысле охватывает элементы безопасности, перечисленные в договоре и обязательные для выполнения или предоставления клиенту (например, услуги) в зависимости от обстоятельств и условий. В пункты договора могут включаться продукты безопасности ИТ, услуги и любые другие материальные и нематериальные элементы безопасности, продаваемые (произведенные поштучно или в массовом порядке), сдаваемые в аренду или используемые для обучения. Более того, указанные составляющие договора подразумевают любой объект, представленный услугой, условно-бесплатным ПО, свободно распространяемым ПО, образцами или другими средствами и поставляемый прямо или опосредованно (гарантийное обязательство, поручительство, предыстория и т. д.) или предлагаемый поставщиком для поставки (предыстория, гарантийное обязательство и т. д.). Объекты имеют измеряемые атрибуты безопасности, которые можно верифицировать на предмет их соответствия политике безопасности. Например, объект может ссылаться на услугу по оценке рисков и угроз, осуществляемую какой-либо организацией, или на сертификацию персонала, компетентного в выполнении оценок с помощью критериев ИСО/МЭК 15408. Персонал, предоставляющий услугу или выполняющий задачу по обеспечению безопасности, также считается объектом. Например, лица, обучаемые по специальности оценщика, заключают контракт с

обучающей организацией и оцениваются по их способности воспринимать знания и выполнять конкретные действия. Консультанты в области безопасности, предоставляющие услугу или выполняющие задачу, также работают по контракту.

Некоторые объекты не всегда являются отдельными элементами, хотя обеспечивают различные степени доверия к органам обеспечения доверия и, следовательно, должны подвергаться оценке безопасности по частям. Например, гарантийные обязательства и поручительства являются специфичными услугами, предоставляемыми поставщиком отдельно или в качестве дополнительной функции, или поставляемой в комплекте с объектом. Услуги по предоставлению гарантийного обязательства способствуют корректированию или снижению требований к функционированию объекта (ввод в действие, функционирование или доставка), если он не соответствует требованиям его политики безопасности. Предыстория является фактором влияния внешней среды, связанным с поставщиком или объектом. Этот фактор, несмотря на его некоторую расплывчатость, нельзя игнорировать из-за предыстории специфического функционирования объекта, например непрерывного или циклического, с тем чтобы соответствовать политике безопасности или утверждениям поставщика.

Примечание — Данное определение объекта подобно определению понятия «объект оценки», приведенному в ИСО/МЭК 15408-1, за исключением того, что объект имеет более широкое применение.

### 4.4 Правообладатели

В состав оцениваемого объекта могут входить подверженные риску активы, принадлежащие различным правообладателям. Следовательно, для правообладателей может потребоваться определение приемлемого метода обеспечения доверия и уровня доверия. Некоторые из этих сторон указаны ниже:

a) органы по стандартизации;

b) национальные, международные законы и положения;

c) специальные организации (такие, как правительство или банковские организации);

d) полномочные подразделения внутри организации;

e) владельцы политик (политик безопасности, политик в отношении персонала, закупок, маркетинга, сертификации и т. д.);

f) владельцы системы;

g) органы аттестации системы;

h) конечные пользователи;

i) общественность.

### 4.5 Требования доверия

Исходя из безопасности ИТ, приемлемое (адекватное) доверие означает удовлетворение специальных заранее определенных требований посредством выполнения соответствующих процедур и действий по обеспечению доверия, то есть в соответствии с выбранным методом обеспечения доверия. Требования доверия определяются исходя из требований безопасности и других факторов.

Требования доверия к безопасности определяются анализом требований безопасности для объекта, факторов влияния, требований безопасности (политик), развития бизнеса и целевой среды объекта. Факторами влияния являются любые соображения, подлежащие изучению, поскольку они могут оказать воздействие на формирование требования доверия к объекту. Влияние может включать в себя любую предысторию и даже быть представлено нематериально, например политикой, культурой, местными законами и обязательными (предписанными) требованиями. Оценка риска проводится с целью тщательного изучения конфиденциальности актива, уязвимостей и угроз, а также для определения остаточного риска и рекомендаций по использованию существующих и предполагаемых мер безопасности. Реализованные рекомендации включаются в первичные требования безопасности для пересмотра требований доверия к безопасности.

Общие рекомендации по управлению безопасностью и проведению анализа риска можно найти в ISO/IEC TR 13335 и ИСО/МЭК 17799. ИСО/МЭК 15408 содержит информацию о функциональных требованиях безопасности и требованиях доверия к безопасности продуктов и систем ИТ, характерных для традиционных оценок безопасности ИТ. Требования доверия уникальны для каждой среды вследствие наличия множества требований, предъявляемых к бизнесу и безопасности каждой среды. Следовательно, один и тот же объект может не соответствовать другим средам без его модификации, поскольку в этом случае обычно требуется удовлетворение других требований доверия.

### 4.6 Применимость методов обеспечения доверия к безопасности информационных технологий

В настоящем подразделе более подробно раскрывается определение термина «доверие», приведенное в статье 2.4. В настоящем подразделе рассматриваются различные аспекты доверия с целью демонстрации возможных путей применения этих аспектов применительно к обеспечению безопасности ИТ.

Из определения термина «доверие» очевидно, что именно выполнение соответствующих действий по обеспечению доверия обеспечивает уверенность заинтересованного лица в том, что объект соответствует требованиям безопасности. Уверенность приобретается при анализе свидетельства доверия, полученного при помощи процедур оценки в процессе разработки, ввода в действие и функционирования объекта, а также опыта, полученного при фактическом его использовании. При определении доверия к безопасности полезна любая деятельность, которая может снизить неопределенность посредством представления свидетельства, подтверждающего правильность, эффективность и качество компонентов объекта. Признавая, что некоторые виды свидетельств более четко, чем другие, формулируют утверждения, основной задачей является формирование многостороннего аргумента доверия, который формулирует вид и степень доверия, полученные с помощью определенных методов обеспечения доверия. Существует много методов обеспечения доверия, но лишь небольшое их число связано с безопасностью ИТ. Однако не связанные с безопасностью ИТ методы также могут содержать определенные характеристики, связанные с обеспечением доверия к безопасности ИТ. Вследствие наличия небольшого числа методов обеспечения доверия, относящихся к безопасности, важно уметь определить их значимость, поскольку в области ИТ используют многие не связанные с безопасностью ИТ методы. Свидетельства доверия часто представлены документацией, разработанной в ходе обычной деятельности по проектированию ИТ. Большое значение имеет все, что может использоваться для создания аргумента доверия и, таким образом, снижать неопределенность (риск), связанную(ый) с определенным объектом.

В данном случае основной идеей являются выявление методов обеспечения доверия, не связанных с безопасностью ИТ, и недопустимость недооценки значимости методов, связанных с безопасностью ИТ. Несомненно, более предпочтительны методы, связанные с безопасностью ИТ, однако некоторую степень доверия к безопасности можно получить из многих источников, и ее не следует игнорировать, поскольку она не является результатом применения признанного метода обеспечения доверия к безопасности. Исходя из вышесказанного, очень важно определить источник получения свидетельства и учитывать его при разработке аргумента доверия. Более того, необходимо знать требования безопасности и требования доверия и понимать важность свидетельства и его источника для удовлетворения ими необходимых потребностей обеспечения безопасности.

Например, ИСО 9000 является документом по обеспечению доверия к качеству продукции, изначально разработанным для организации производства, однако он также содержит характеристики доверия к процессу, приемлемые для ПО и, таким образом, для программных продуктов и систем обеспечения безопасности ИТ. Напротив, SSE-CMM (ИСО/МЭК 21827) является методом обеспечения доверия к безопасности, хотя и не традиционным. Данный метод обеспечивает свидетельство доверия посредством оценки процессов проектирования безопасности в организации, а не оценки непосредственно самих объектов.

Некоторые методы обеспечения доверия специально сфокусированы на определении согласованного и полного набора характеристик безопасности, которые часто связаны со стандартными сценариями угроз или с хорошими практиками обеспечения безопасности. Различные методы обеспечения доверия могут иметь общие компоненты или аспекты доверия.

Все эти факторы влияют на общую структуру обеспечения доверия и, в частности, на определение метрик. Данные факторы должны учитываться при соотнесении различных методов обеспечения доверия.

### 4.7 Системы обеспечения доверия

Специфический метод обеспечения доверия, который можно реализовать так, чтобы придать особое значение контексту, и в рамках которого осуществляется данный метод, называется «системой оценки доверия». Общепризнанные системы оценки доверия и оценщики могут обеспечить более высокую степень доверия, чем полученную посредством использования соответствующего метода обеспечения доверия. Подобная система оценки доверия может также предоставлять основу для при-

знания результатов или суждений, полученных применением метода обеспечения доверия для более широкой аудитории.

### 4.8 Количественное определение риска доверия и устойчивости механизма обеспечения безопасности

Доверие не обеспечивает предоставление объекту каких-либо дополнительных мер безопасности или услуг. Поэтому иногда персоналу, не связанному с безопасностью, трудно осознать преимущества, которые он получает от вложения ресурсов в обеспечение доверия. Например, в отношении какого-либо продукта безопасности ИТ утверждалось, что доверие способствует устойчивости механизма обеспечения безопасности, однако фактически доверие способствует приобретению уверенности в устойчивости этого механизма путем снижения неопределенности (или риска) в отношении возникновения угрозы, приводящей к нарушению безопасности. Например, ошибочно считается, что двухфакторная аутентификация вызывает больше доверия, чем простой механизм применения пароля, хотя в реальности это просто механизм более строгой аутентификации. Двухфакторная аутентификация является механизмом более строгой аутентификации, так как она верифицирует два атрибута пользователя по сравнению с одним атрибутом в случае применения механизма с применением пароля. Сама по себе такая аутентификация не обеспечивает доверия, поскольку при разработке механизма обеспечения безопасности именно действия по обеспечению доверия способствуют созданию доверия к этому механизму.

Следует понимать, что доверие автоматически не подразумевает достаточную безопасность, а только соответствие ее целям (политике безопасности). Другими словами, доверие обеспечивает уверенность в выполнении объектом заданных целей безопасности без проверки того, учитывают ли эти цели конкретные риски и угрозы. Например, хотя продукту ИТ можно доверять в части его соответствия целям безопасности, но от характера этих целей зависит безопасное поведение продукта. Напротив, продукт с низкой степенью доверия, но с более соответствующими целями безопасности, может быть фактически более безопасным.

### 4.9 Доверие снижает риск безопасности

Доверие способствует снижению риска, поскольку уменьшает неопределенность, связанную с уязвимостями объекта, таким образом уменьшая его потенциальную уязвимость и приводя к снижению общего риска, связанного с объектом. В предыдущем подразделе указано, что доверие не обеспечивает каких-либо дополнительных мер безопасности для противостояния рискам, связанным с безопасностью. Скорее, деятельностью по созданию доверия делается попытка доказать соответствие объекта его целям безопасности. Соответствие объекта его целям безопасности подразумевает предъявление свидетельства об обеспечении соответствующего доверия и обоснования для обеспечения уверенности в том, что внедренные меры безопасности снизят ожидаемый риск.

### 4.10 Количественное определение доверия

Прямое определение или оценку вклада обеспечения доверия или его повышения в процесс деятельности организации осуществить непросто. Тем не менее повышение доверия к какой-либо мере безопасности снижает неопределенность, связанную с конкретным риском, в частности с элементами риска, относящимися к уязвимостям, по отношению к которым внедрена данная мера безопасности. Таким образом, в этом случае значимость доверия можно вывести из степени снижения неопределенности, связанной с риском. Установление связи доверия с неопределенностью риска или его составляющими элементами упрощает измерение степени доверия, поскольку неопределенность возникновения риска количественно определить легче, чем само доверие. Измерение степени доверия можно провести косвенно, измерением вероятности возникновения риска и последующей его корректировки, так как эта вероятность обратно пропорциональна доверию.

### 4.11 Орган обеспечения доверия

Органом обеспечения доверия является лицо (или организация), ответственное за принятие решений, имеющих отношение к объекту на конкретной стадии его жизненного цикла. При наличии нескольких стадий жизненного цикла и нескольких правообладателей существуют различные органы обеспечения доверия, каждый со своими правами и обязанностями. Например, на стадии разработки органом обеспечения доверия может быть разработчик, ответственный за обеспечение доверия к объекту организации-поставщика. Одновременно у организации-клиента может быть собственный орган

обеспечения доверия, ответственный за рассмотрение требований доверия, предъявляемых к организации-поставщику. Кроме того, еще один орган обеспечения доверия может существовать в организации, проводящей оценку, который является ответственным за соответствие объекта системе оценки доверия. Каждый из упомянутых органов обеспечения доверия несет ответственность за определенную стадию жизненного цикла объекта. Более того, орган обеспечения доверия может нести ответственность за несколько стадий. Примером может служить орган обеспечения доверия клиента, который также отвечает за принятие отчета о сертификации, представленного органом по сертификации.

Органы обеспечения доверия существуют для всех видов защищенных объектов, независимо от того, являются ли они продуктом, системой, услугой, процессом, персоналом и т. д. Орган обеспечения доверия несет ответственность за принятие решений в отношении объекта с учетом его целей безопасности.

В зависимости от организации и ее вида орган обеспечения доверия может иметь множество обязанностей. Некоторые из его задач могут включать в себя выбор соответствующего метода обеспечения доверия и определение необходимой степени и вида доверия, требуемых для соответствия определенным требованиям. Орган обеспечения доверия также отвечает за установление связи с другими организациями обеспечения доверия, такими как организация по оценке доверия, связанная с системой оценки безопасности ИТ, например, в случае применения требований ИСО/МЭК 15408 и использования его системы оценки.

В рамках некоторых организаций, в особенности государственных и военных, степень доверия можно регулировать, ограничивая возможность выбора органа обеспечения доверия и одновременно ограничивая риск для него. Организации могут играть различные роли в качестве органа обеспечения доверия, и его обязанности могут быть различными в зависимости от их уникальных эксплуатационных моделей; тем не менее орган обеспечения доверия несет ответственность за выполнение установленных обязанностей. В небольших организациях работник обычно выполняет дополнительные обязанности в качестве органа обеспечения доверия, тогда как крупные организации могут иметь специального работника с обязанностями, возложенными только на орган обеспечения доверия. Более крупные организации обычно назначают одного из руководителей выполнять функции органа обеспечения доверия и отвечать за внедрение метода обеспечения доверия и принятие результатов оценки доверия.

В зависимости от организации лицо, ответственное за окончательное принятие результатов доверия, может также отвечать и за функционирование объекта (то есть за ввод системы в эксплуатацию или за принятие предоставленной услуги). Следовательно, органу обеспечения доверия часто приходится выполнять действия, направленные на особенности равновесия между степенью, глубиной реализации доверия и стоимостью, а также продолжительностью оценочной деятельности, связанной с этой реализацией.

## 5 Выбор доверия к безопасности

Выбор метода обеспечения доверия к безопасности и соответствующей степени доверия является решением, которое основывается на изучении политики доверия к безопасности организации, бизнес-требований и вида объекта (продукта, процесса, окружающей среды, системы, услуги или персонала). Например, некоторые методы обеспечения доверия применимы только к процессам [например, SSE-CMM (см. ИСО/МЭК 21827)], в то время как другие — к продуктам (см. ИСО/МЭК 15408).

Выбранный метод обеспечения доверия должен быть совместим с окружающей средой организации и обладать способностью проверять требуемые характеристики на стадиях жизненного цикла объекта. При выборе метода обеспечения доверия необходимо учитывать имеющиеся ресурсы (временные) кадровые, финансовые и т. д.) для обеспечения соответствия использованных ресурсов виду и степени полученного доверия. Например, обеспечение объекта с низкой степенью доверия мерами безопасности стоимостью пятьдесят тысяч долларов было бы нецелесообразно. Аналогично нет необходимости выбирать оценочный метод обеспечения доверия (то есть TCSEC, ITSEC, CTCPEC, см. ИСО/МЭК 15408), когда вполне приемлем более короткий метод (при условии необязательности применения метода обеспечения доверия к оценке), позволяющий сэкономить месяцы рабочего графика[1)]. Для некоторых организаций (например, государственных учреждений) требуется выбор поставщиков, разработавших оцененные продукты безопасности, а также использование этих продуктов для получения

[1)] Упрощенные методы демонстрации сути без указания фактических сумм и периодов времени в отношении определенного метода обеспечения доверия.

доверия. Требований по принятию решения в отношении выбора поставщиков может быть немного, что позволяет сэкономить бóльшую часть ресурсов при рассмотрении вариантов поставщиков.

Например, частная организация может использовать метод SSE-CMM (ИСО/МЭК 21827) для создания доверия к ее корпоративному веб-сайту с целью предотвращения несанкционированного доступа к его частной локальной сети. Для этого требуется оценка процессов, связанных с разработкой, вводом в действие и функционированием веб-сайта, включая процессы эксплуатации и реализации политик безопасности. На основе полученных данных формируется аргумент доверия вместе с уровнем зрелости возможностей организации [SSE-CMM (ИСО/МЭК 21827)]. Для этого достаточно использовать метод обеспечения доверия, поскольку органу обеспечения доверия требуется рассмотреть только внутреннюю политику доверия организации к безопасности. Вторым примером является государственное учреждение, которое использовало метод обеспечения доверия по ИСО/МЭК 15408 для формирования высокой степени доверия, так как от него требовалось использование именно этого подхода для выполнения специальных требований государства по обеспечению безопасности. Данный пример демонстрирует степень зависимости органа обеспечения доверия от типа организации и ее политик безопасности. Не делается никаких утверждений относительно того, какой метод лучше или обеспечивает бóльшую степень доверия. В случае, если существующая политика или регламент не предписывают использование определенного метода и не задают уровень доверия, их выбор приходится осуществлять в процессе выполнения требований доверия, которые соответствуют заданным требованиям и являются функцией целей безопасности. Однако существует вероятность выявления ситуации при менеджменте рисков безопасности, когда требуется обеспечивать бóльшую степень доверия. Если менеджменту рисков безопасности приходится иметь дело с высокими уровнями неопределенности, то повышенное доверие может способствовать снижению общей неопределенности и, таким образом, общему снижению риска безопасности.

Следует отметить, что даже в случае обязательного применения метода обеспечения доверия могут быть полезны некоторые вопросы, например:

a) чему доверять;

b) какова степень доверия;

c) какую лабораторию оценки использовать;

d) какие услуги по сертификации и аттестации использовать?

Существует много различных подходов и методов обеспечения доверия, и лишь некоторые из них регламентированы и приняты повсеместно. Следовательно, для выбора и применения какого-либо метода обеспечения доверия правообладателям потребуются рекомендации.

### 5.1 Спецификация требований доверия

Перед выбором и/или применением методов обеспечения доверия следует специфицировать требования доверия. Под эти спецификации подпадают различные методы. Процедуре выбора метода обеспечения доверия предшествует анализ требований доверия к безопасности организации, а также требований, предъявляемых к оценке рисков и угроз. Требования могут также включать в себя анализ региональных аспектов и некоторых аспектов бизнеса, например если потребителю требуется такой специфический подход к обеспечению доверия, как использование требований ИСО/МЭК 15408 в целях удовлетворения внутренних требований организации или требований к поставкам на рынок.

Для изучения требований организации или рынка спецификация требований доверия может включать в себя варианты, такие как признание или принятие метода обеспечения доверия или системы оценки доверия, взаимное признание метода или системы оценки и минимальный уровень доверия.

Например, требования могут включать в себя ограничения по строгости выполнения процесса разработки и/или требования к поиску потенциальных уязвимостей безопасности и анализу их воздействия.

Когда объект имеет такие механизмы безопасности, как пароль или хэш-функция, требования доверия могут специфицировать минимальный уровень стойкости, соответствующий заявленным целям безопасности.

Спецификации требований доверия должны учитывать все требования организации и содержать все взаимно поддерживающие компоненты доверия, такие как доверие к корректности и доверие к эффективности. Более того, следует детализировать соответствующие подходы и методы обеспечения доверия, а также учитывать органы обеспечения доверия, их обязанности и используемые каналы связи.

### 5.2 Экономические вопросы

Обычно доверие является затратным ресурсом, ведущим к издержкам. Более того, доверие связано скорее с потерями, чем с доходами или какой-либо выгодой. Следовательно, рентабельность инвестирования в него является не измеряемой, а гипотетической величиной и ее можно сравнить со страховыми потерями. Даже если поставщик амортизирует издержки на обеспечение доверия к некоторым продуктам безопасности ИТ, то может потребоваться несколько лет для возмещения стоимости инвестиций в зависимости от выбранного метода обеспечения и требуемого уровня доверия. Преимущество, получаемое организацией от вложения ресурсов в обеспечение доверия, не является очевидным для людей, незнакомых с вопросами безопасности, и, следовательно, может потребоваться исчерпывающее обоснование, которое должно быть представлено в надлежащем виде для получения одобрения руководством организации.

Для разных аудиторий используются различные типы доверия. Например, доверие, обеспечиваемое гарантийным обязательством, является незначительным для пользователя системы при ее остановке, но имеет значение для руководителя, оплачивающего стоимость простоя системы. Аналогично доверие, обеспечиваемое гарантией технической поддержки системы в случае ее выхода из строя, является незначительным при нормальном ее функционировании, но будет иметь существенное значение для производственного процесса в случае нарушения ее функционирования.

Все типы доверия обеспечивают различные преимущества разным подразделениям организации. Отсутствие оценки этих различных преимуществ обесценивает результаты получаемого доверия.

Фактически доверие уменьшает неопределенность, по крайней мере, в отношении уязвимостей продуктов или услуг, связанных с обеспечением безопасности ИТ. Неопределенность имеет отношение ко всем факторам, используемым в оценке риска безопасности. Таким образом, снижение неопределенности облегчает сосредоточение на аспектах, представляющих наибольший риск для организации, что дает существенное преимущество организации и обеспечивает выгодное вложение ее ресурсов.

### 5.3 Организационные вопросы

Важно уметь распознавать среду безопасности и, в частности, понимать, что требования доверия отражают культуру и бизнес-требования организации. Понимание требований организации необходимо для принятия решения о приемлемости определенного метода обеспечения доверия и/или достаточности доверия. Политика организации должна регламентировать:

a) способ определять требования безопасности;

b) обстоятельства, при которых объект должен быть сертифицирован на соответствие требованиям конкретного стандарта;

c) стандарты, на соответствие требованиям которых должны сертифицироваться объекты;

d) степень доверия, необходимую для процедур сертификации при заданных условиях;

e) обязанности органа обеспечения доверия;

f) обстоятельства, при которых необходима аттестация объектов.

Например, государственная организация может принять решение о спецификации и контроле процесса сертификации в конкретных условиях. Она может разработать все аспекты этого процесса, такие, например, как методы обеспечения доверия, критерии (стандарт), руководство по использованию стандарта и даже уровень требуемого доверия. Однако органу обеспечения доверия к аккредитации тем не менее придется принимать окончательное решение по приемлемому доверию и нести ответственность за ресурсы и график выполнения работ. По сравнению с государственной организацией для проведения разработок частная организация в рамках своей организации может предпочесть неформальный метод обеспечения доверия, если от ее органа обеспечения доверия не требуется выполнение соответствия внешним требованиям безопасности. Политики организации важны для определения того, что потребуется организации при верификации приемлемости для нее мер безопасности.

### 5.4 Тип доверия

При рассмотрении комбинации нескольких методов обеспечения доверия для конкретного объекта лучше всего построить модель доверия к безопасности для демонстрации того, как различные типы доверия будут взаимодействовать для обеспечения общего доверия, связанного с объектом. Затем модель доверия к безопасности можно построить из различных составных элементов модели доверия, каждая из которых соответствует конкретному подходу к обеспечению доверия (то есть доверие к оценке, доверие к процессу, доверие к разработке). Таким образом, в модели доверия к объекту, пред-

ставленной комбинацией нескольких отдельных моделей доверия, рассматривают то, как составлены эти модели, независимо от стадии обеспечения доверия, к которой они применялись. Далее может случиться так, что какой-либо тип доверия к безопасности, связанный с объектом, не предназначен напрямую следующему получателю объекта, а используется фактически для конечного получателя. Модель может четко установить это и помочь обеспечить формирование точной картины доверия к безопасности для конечного получателя.

Затем для упрощения сравнения моделей доверия каждая из моделей может специфицировать тип и степень доверия для конкретной стадии жизненного цикла объекта. Модель доверия к объекту объединяет отдельные модели посредством изложения альтернатив и предоставления логического обоснования для описания полученного доверия к объекту.

### 5.5 Технические вопросы

Существует большой выбор методов обеспечения доверия, которые предлагают возможность оптимизации заданных интервалов времени и использования ресурсов. Метод обеспечения доверия, подходящий для объекта или его атрибутов и предназначенный для оценки, следует выбирать из:

a) методов обеспечения доверия, применимых исключительно для конкретных объектов ИТ, таких как безопасные аппаратные средства или программные продукты ИТ, системы, сети, персонал, услуги и т. д.;

b) методов обеспечения доверия, предназначенных специально для процесса жизненного цикла;

c) методов обеспечения доверия, основанных на практическом опыте и фактическом применении.

Применение метода обеспечения доверия для оценки объекта может привести к получению разных типов или степеней (уровней) доверия вследствие воздействия следующих факторов, которые необходимо учитывать:

a) имеющиеся недостатки объекта или его характеристики;

b) размеры и сложность объекта;

c) различия в применяемых методах обеспечения доверия;

d) связь применения метода обеспечения доверия с ограничениями по строгости или объему работ;

e) цели безопасности;

f) конкретные условия;

g) конкретные стадии жизненного цикла ИТ;

h) возможность комбинации с другими методами.

Дополнительное доверие к объекту можно получить путем:

a) углубленных знаний о предыдущих функциональных возможностях ИТ;

b) изучения информации об улучшенных функциональных возможностях механизмов обеспечения безопасности ИТ.

Каждый метод обеспечения доверия применяется в зависимости от имеющихся преимуществ и недостатков, а также от учета индивидуальных требований безопасности. Необходимо понять, как метод обеспечения доверия устанавливает доверие с целью принятия решения, соответствует ли тот или иной метод обеспечения доверия требованиям доверия к безопасности.

Например, при использовании системы, состоящей из набора продуктов (уровень доверия к которому может быть известен или не известен, или принят из-за используемого метода обеспечения доверия), идентифицируемый уровень доверия обычно определяется посредством сертификации этой системы перед эксплуатацией.

На принятие решения влияют также технические аспекты, поскольку некоторые методы обеспечения доверия более подходят для простых, чем сложных объектов. Например, обычно легче верифицировать объект с минимальными функциональными возможностями (то есть тысячи кодовых строк) и получить результат с высокой степенью доверия, чем верифицировать объект доверия с множественными функциональными возможностями, представленный миллионами кодовых строк.

Тип и уровень доверия, полученные определенным методом, определяются характеристиками последнего, то есть конкретно тем, какие стадии жизненного цикла и элементы безопасности оценивались.

### 5.6 Рассмотрение вопросов оптимизации

Решение по выбору необходимых методов обеспечения доверия и степени доверия не принимается полностью на научной основе, поэтому органу обеспечения доверия для определения рацио-

нальной комбинации методов обеспечения доверия и степени доверия требуется решать вопрос об их достаточности для соответствия требованиям организации. В этом случае необходимо учитывать атрибуты систем ИТ и методов обеспечения доверия.

При применении нескольких методов обеспечения доверия большее значение имеют результаты, полученные при использовании последнего метода обеспечения доверия, примененного непосредственно перед окончательной приемкой объекта. Следовательно, орган обеспечения доверия должен оценивать текущие результаты применения последнего метода обеспечения доверия, и ему может потребоваться запрос по обоснованию применения, если результаты применения предыдущего метода обеспечения доверия оказались неудовлетворительными. Более того, в качестве основания для последнего действия по обеспечению доверия эти результаты будут полностью определяться характеристиками функционирования объекта.

Доверие допускается обеспечивать поэтапно, например через поставщика продукта безопасности ИТ, интегратора систем или провайдера услуг в виде какой-либо гарантии или гарантийного обязательства по функционированию продукта или услуги.

В отношении отдельных объектов с соответствующим уровнем доверия следует отметить, что их интеграция в их окончательную целевую среду, как правило, отрицательно воздействует на итоговый уровень доверия к безопасности. Следовательно, могут потребоваться дополнительные действия для обеспечение доверия.

## 6 Базовая структура доверия

### 6.1 Подход к обеспечению доверия

Методы обеспечения доверия можно классифицировать по трем следующим высокоуровневым подходам к обеспечению доверия:

a) оценка объекта доверия посредством оценивания и тестирования;

b) оценка процессов, используемых для разработки и создания объекта;

c) оценка среды, такой, например, как персонал и оборудование.

Оценка объекта (продукт, система, услуга) включает в себя процедуру его проверки. В данном случае этими методами обеспечения доверия проверяются объект и связанная с ним проектная документация по безопасности, независимо от процессов разработки.

Оценка технологического процесса включает в себя проверку организационных процессов, используемых для производства и эксплуатации объекта в течение его жизненного цикла (разработка, ввод в действие (развертывание), доставка, тестирование, обслуживание, ликвидация и т. д.). Доверие достигается посредством допущения, что организуемые людьми процессы влияют на качество разработки и внедрения объекта и, следовательно, в результате обеспечения доверия к безопасности реализуются в объектах безопасности ИТ и его приложениях.

Оценка внешних факторов включает в себя проверку влияния условий окружающей среды, вносящих вклад в качество процессов производства объектов (непосредственной проверки объекта или процесса не происходит). К этим факторам относятся персонал и физическое оборудование (для разработки, производства, доставки, эксплуатации и т. д.).

Примечание — По сравнению с вышеизложенным такие подходы к обеспечению доверия, как доверие через оценку, полученное при применении критериев по ИСО/МЭК 15408, предусматривают непосредственную оценку конкретного объекта защиты применительно к его жизненному циклу и предлагают уникальную комбинацию типов доверия.

***Пример — ИСО/МЭК 15408 предусматривает непосредственное исследование объекта оценки и обеспечивает в результате доверие через оценку, которое является согласованным набором типов доверия к разработке, оценке и тестированию, тогда как ИСО 9001 ориентирован на исследование производственных процессов.***

### 6.2 Методы обеспечения доверия

ISO/IEC TR 15443 рассматривает широкий диапазон существующих методов обеспечения доверия. Методы обеспечения доверия включают в себя официальные национальные и международные стандарты, стандарты «де-факто» и другие общепринятые методы, имеющие или использующие определенный и систематический метод.

Примером стандарта «де-факто» является метод оценки SSE-CMM (SSAM), который является детально документированным методом обеспечения доверия; однако он не является национальным или международным стандартом. Примером другого стандарта де-факто является метод обеспечения доверия ТРЕР (надежный процесс оценивания продукта). Несмотря на то, что ТРЕР является распространенным стандартом, успешно используемым некоторыми государственными учреждениями для оценивания продуктов безопасности ИТ, он также является недокументированным специализированным методом оценивания.

Результатом применения методов обеспечения доверия является выбор конкретных типов доверия в зависимости от направленности этих методов на технические требования и аспекты жизненного цикла, что облегчает их классифицирование по подходам к обеспечению доверия. Примеры некоторых из наиболее широко известных методов обеспечения доверия в соответствии с их направленностью и подходом представлены в таблице 1. Более полный перечень методов обеспечения доверия будет представлен в последующих частях ISO/IEC TR 15443, в которых будут рассматриваться технические подробности и их сравнение.

Таблица 1 — Примеры методов обеспечения доверия

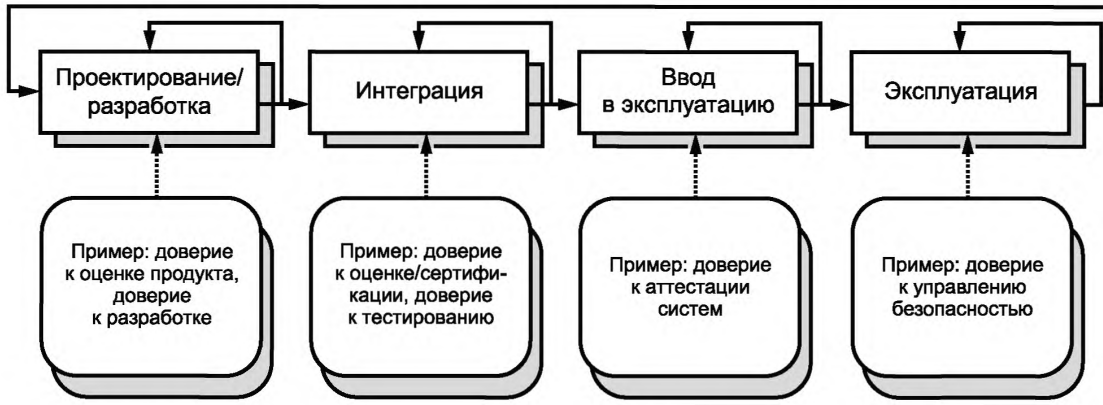
| Подход к обеспечению доверия | Направленность доверия | Примеры методов обеспечения доверия (соответствующие критерии или модель) |
|---|---|---|
| Процесс | Процесс «качество и разработка» | ИСО 9000.<br>ИСО/МЭК 15504.<br>HCD.<br>SSAM [SSE-CMM(ИСО/МЭК 21827)] |
| Объект, процесс, внешние условия | Брендинг — признание фирмы, производящей качественные объекты (на основе исторических взаимосвязей или данных) | Предыстория разработчика |
| Объект | Страхование (поддержанное обязательством изготовителя исправлять дефекты объекта) | Гарантийное обязательство |
| Объект | Собственная декларация | Декларация поставщика |
| Внешние условия | Квалификация и знания персонала | Профессиональная сертификация и лицензирование.<br>Средства безопасности |
| Объект | Непосредственная оценка объекта | CEM (ИСО/МЭК 18045).<br>ITSEM (ITSEC).<br>ТРЕР (TCSEC).<br>ТРЕР (CTCPEC).<br>Номинальное обслуживание [RAMP (TCSEC)].<br>Номинальное обслуживание [RM (CTCPEC)].<br>Доверие к сертификации и аккредитации.<br>ИСО/МЭК 14598-1 Оценивание программного продукта |
| Объект, процесс, внешние условия | Управление безопасностью | Системы менеджмента информационной безопасности — спецификация и руководство по применению (BS 7799.2).<br>GISA/BSA Руководство по защите базовой линии.<br>ИСО/МЭК 13335.<br>ИСО/МЭК 17799 |

### 6.3 Аспекты жизненного цикла

Поскольку ошибки оператора, отказы оборудования, новые уязвимости и угрозы могут возникнуть на любой стадии жизненного цикла объекта, для каждой из стадий жизненного цикла объекта [то есть идея, разработка, интеграция, ввод в действие, эксплуатация и удаление (ликвидация)] требуется обеспечение соответствующего доверия. Следовательно, методы обеспечения доверия должны соответствовать конкретным стадиям жизненного цикла объекта.

Функциональные дефекты, изменения в требованиях и новые уязвимости влияют на доверие и требуют воспроизведения их на более ранних стадиях жизненного цикла объекта. Следовательно, в модели жизненного цикла объекта следует вводить поправку на наложение повторяющихся стадий или итеративную взаимосвязь между ними.

Для демонстрации связи методов обеспечения доверия с той или иной стадией жизненного цикла объекта используют типовую модель жизненного цикла, представленную на рисунке 1. Эта модель состоит из четырех основных стадий, достаточно общих для сопоставления с любой конкретной моделью жизненного цикла. Хотя графические представления каждой стадии, представленной на рисунке 1, схожи, виды деятельности и обратная связь будут изменяться вследствие уникальности применяемого метода обеспечения доверия. Например, некоторые методы обеспечения доверия используют фазу обслуживания (то есть номинальное обслуживание ТРЕР) на стадии эксплуатации для обнаружения отказов и изменения требований, которые влияют только на доверие к этой стадии. Данный подход демонстрирует возможность поддержки моделью жизненного цикла конкретного метода обеспечения доверия, который будет определять, должна ли обратная связь осуществляться с его собственной стадией или с началом стадии проектирования/разработки объекта.




Примечание — Модель жизненного цикла, представленная на рисунке 1, является примером модели, демонстрирующей совместимость с другими моделями жизненного цикла и структурами для облегчения анализа методов обеспечения доверия в рамках стандартов серии ISO/IEC TR 15443. Предписание или рекомендации использования определенной модели жизненного цикла не предусмотрены.

Рисунок 1 — Методы обеспечения доверия типовой модели стадий жизненного цикла

Методы обеспечения доверия могут быть специфичными для конкретной стадии (например, для аттестации системы) или применяться для нескольких стадий жизненного цикла объекта доверия в соответствии со стандартами серии ИСО 9000, ИСО/МЭК 15408 и стандартом SSE-CMM (ИСО/МЭК 21827).

Для получения интегрального результата доверие, полученное на каждой стадии, должно переноситься на следующую стадию, где оно дополняет доверие этой стадии. Метод дополнения доверия применяют до последней стадии модели жизненного цикла, которой является стадия эксплуатации, представленная в типовой модели стадий жизненного цикла, приведенной на рисунке 1.

### 6.4 Сопоставление доверия к эффективности с доверием к корректности

При обеспечении доверия к корректности дается ссылка на оценку объекта с целью верификации корректности его внедрения в соответствии с проектом. Напротив, доверие к эффективности относится к способности функций безопасности объекта противостоять осознанным или идентифицированным угрозам. В следующем подразделе показано, что как доверие к корректности, так и доверие к эффективности являются важными характеристиками, и ни одна из них не обладает преимуществом, поскольку оба типа доверия оперируют значимыми аспектами объекта.

Если функциональные возможности обеспечения безопасности объекта учитывают потенциальные угрозы и эти возможности не были проанализированы относительно установления корректности и реализации проекта, то нельзя быть уверенным в успехе противостояния объекта атаке. Из этого примера видно, что доверие к эффективности было обеспечено, но доверие к корректности вследствие от-

сутствия верификации функциональных возможностей безопасности обеспечено не было. Аналогично если анализ установил корректность проекта и правильность реализации функциональных возможностей обеспечения безопасности объекта, а в проекте не предусмотрены соответствующие функции безопасности для противостояния вероятным угрозам, то нельзя быть уверенным, что объект устоит перед этими угрозами. В данном примере при наличии доверия к корректности отсутствует доверие к эффективности вследствие реализации неэффективных функциональных возможностей противостояния вероятным угрозам. С целью получения общего доверия объект должен быть оценен на предмет корректности проекта, внедрения и эксплуатации (элемент корректности) и должен обладать соответствующими функциональными возможностями обеспечения безопасности для противостояния идентифицированным угрозам (элемент эффективности).

**6.5 Классификация методов обеспечения доверия**

Методы обеспечения доверия можно классифицировать по трем высокоуровневым подходам к обеспечению доверия в соответствии с 6.1. В рамках каждого подхода к обеспечению доверия метод обеспечения доверия может предназначаться для конкретной стадии или нескольких стадий жизненного цикла в зависимости от характеристик конкретного метода.

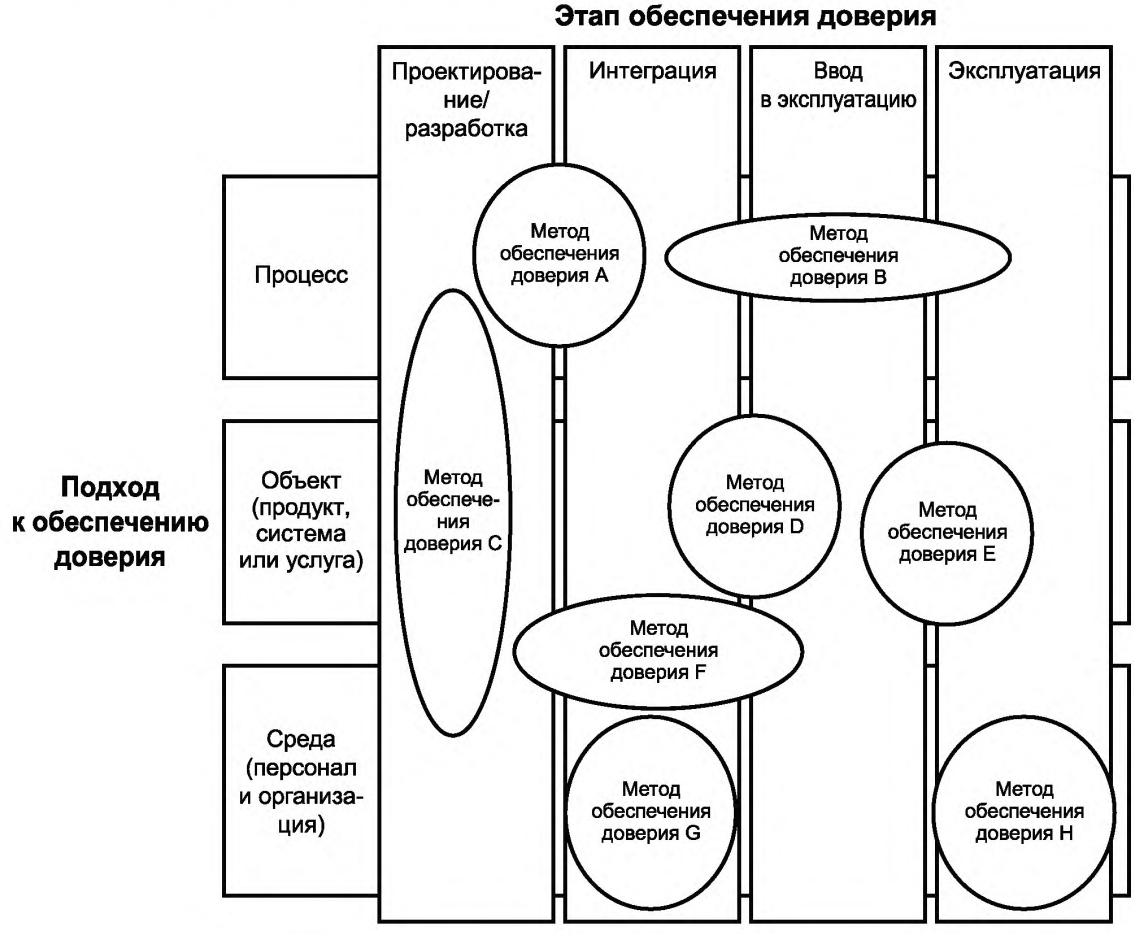



Рисунок 2 — Классификация существующих методов обеспечения доверия

В зависимости от типа метода обеспечения доверия полученное доверие основывается на оцененном аспекте и стадии жизненного цикла. Например, методы обеспечения доверия через оценку формируют доверие, связанное со стадиями проектирования, разработки и функционирования; методы обеспечения доверия к разработке создают доверие, связанное конкретно со стадией разработки;

методы обеспечения доверия к тестированию формируют доверие, связанное конкретно с аспектами тестирования на различных стадиях в зависимости от метода обеспечения доверия.

Классификация существующих методов обеспечения доверия, а также возможность применения подходов к обеспечению доверия на нескольких стадиях показаны на рисунке 2. Подходы к обеспечению доверия уточняются в частях 2 и 3 ISO/IEC TR 15443, а в части 2 также приведены конкретные примеры методов обеспечения доверия.

Методы обеспечения доверия из различных высокоуровневых подходов к обеспечению доверия создают различные типы доверия вследствие их разной направленности. Однако даже в рамках приведенных высокоуровневых подходов к обеспечению доверия методы обеспечения доверия будут формировать различные типы доверия вследствие различий между проверяемыми аспектами объекта (компонентами ИТ или услугами).

Подходы к обеспечению доверия будут формировать различные типы доверия вследствие различий между проверяемыми аспектами объекта (компонентами ИТ или услугами). Некоторые подходы исследуют различные стадии жизненного цикла объекта, тогда как другие — процессы производства объекта (косвенное исследование объекта). Подходы к обеспечению доверия включают в себя разработку, анализ, тестирование, исправление дефектов, функционирование, гарантийные обязательства, персонал и оборудование и т. д. Эти высокоуровневые подходы к обеспечению доверия можно далее детализировать; например, подход обеспечения доверия к тестированию может включать в себя общее тестирование и методы обеспечения доверия к строгому тестированию на совместимость.

Используя подобные структуры, можно проверять специфические методы обеспечения доверия одного и того же высокоуровневого подхода на наличие избыточных или синергетических характеристик. Методы обеспечения доверия разных классов можно различать по их дополнительным характеристикам. Некоторые методы могут охватывать несколько классов полностью или частично, тогда как другие — только частично.

### 6.6 Составное доверие

Результатом объединения или комбинации различных методов обеспечения доверия, применяемых на различных стадиях жизненного цикла объекта, обычно является составное доверие, полученное для объекта. Доверие может быть представлено в виде важности, типа или другого соответствующего доверию показателя.

Получение составного доверия трудно осуществимо по причине упорядочения малого числа методов обеспечения доверия и отсутствия метрических шкал и возможности измерения доверия методами обеспечения доверия. В настоящий момент составление доверия возможно только путем формирования аргумента доверия и субъективного суждения квалифицированного специалиста в области безопасности ИТ. Более того, в конечном счете приемлемость доверия определяется органом обеспечения доверия.

В настоящее время составное доверие является результатом постадийного формирования доверия в течение жизненного цикла с применением различных методов обеспечения доверия. Возможные сценарии обеспечения доверия и проблемы, которые они поднимают, продемонстрированы на следующих примерах:

1) среди методов обеспечения доверия существуют метод проверки процессов производства объекта и метод проверки непосредственно объекта в различных точках одной и той же стадии жизненного цикла;

2) два метода из одного и того же подхода, применяемые к обеспечению доверия на различных стадиях жизненного цикла объекта;

3) сложная система ИТ (для конкретной эксплуатационной среды), составленная из многочисленных продуктов ИТ и услуг, с разными степенями доверия, установленными методом обеспечения доверия к оцениванию, гарантийному обязательству, сертификации и аккредитации (оценочными, гарантийными, сертификационными и аттестационными методами).

На примере 1 представлена простейшая проблема, где составное доверие определяется объединением различных типов доверия из соответствующих методов.

Пример 2, несмотря на его кажущуюся простоту, поскольку методы обеспечения доверия принадлежат к одинаковому подходу, является сложным, так как идентичность методов обеспечения доверия осложняет рассмотрение вопроса о значимости подхода к обеспечению доверия, что происходит на более поздней стадии жизненного цикла объекта.

Пример 3 является еще более сложным, так как различные методы обеспечения доверия применяются на разных стадиях жизненного цикла, и метод обеспечения доверия к аттестации является основой для решения вопроса о принятии системы. Даже несмотря на то, что при сертификации системы учитывается раннее свидетельство доверия, может отсутствовать потребность в определенном подходе к доверию. Это предполагает придание большего значения методам обеспечения доверия, применяемым на более поздних стадиях жизненного цикла.

Следует отметить, что в настоящее время существует тенденция к использованию типовой базовой модели непрерывного улучшения процессов, изложенных в подходах к обеспечению доверия к процессам и основанных на стандартах. Примером является модель PDCA (планирование, осуществление, проверка, действие), используемая как в ИСО 9001 к качеству продукции, так и в BS 7799 по управлению безопасностью информации. В ISO/IEC TR 15443-2 и ISO/IEC TR 15443-3 будет рассмотрен вопрос, касающийся подхода к обеспечению доверия с точки зрения повышения его значимости или доверия на более поздней стадии жизненного цикла объекта.

### 6.7 Классификация доверия

Анализ методов обеспечения доверия в ISO/IEC TR 15443-3 основан на системе показателей доверия как способа классифицирования методов обеспечения доверия и измерения степени доверия, получаемого при применении того или иного метода (то есть уровней доверия к разработке). Регламентация системы показателей доверия также облегчает описание взаимосвязей между методами.

Ниже приведены некоторые положения, связанные с анализом и классифицированием методов обеспечения доверия, которые будут рассмотрены в ISO/IEC TR 15443-3:

a) сравнение различных методов обеспечения доверия;

b) определение методов обеспечения доверия в количественном отношении;

c) выбор подходящих методов обеспечения доверия;

d) взаимосвязи между различными методами обеспечения доверия;

e) определение возможности объединения некоторых методов обеспечения доверия;

f) определение времени и способов объединения методов обеспечения доверия;

g) определение способности воздействия последовательности применения методов обеспечения доверия на общее доверие и то, каким образом осуществляется это воздействие;

h) определение технических проблем для обеспечения результатов доверия (и условий) и выполнения валидации во время жизненного цикла объекта (эксплуатации и обслуживания) в случае применения нескольких подходов к обеспечению доверия.

## Библиография


| | | |
|---|---|---|
| [1] | ISO/IEC Guide 2<br>(ИСО/МЭК Руководство 2) | Standardization and related activities — General vocabulary<br>(Стандартизация и смежные виды деятельности. Общий словарь)[1)] |
| [2] | ISO 9000<br>(ИСО 9000) | Quality management systems — Fundamentals and vocabulary<br>(Системы менеджмента качества. Основные положения и словарь)[1)] |
| [3] | ISO 9001<br>(ИСО 9001) | Quality management systems — Requirements<br>(Системы менеджмента качества. Требования)[1)] |
| [4] | ISO/IEC 9126-1<br>(ИСО/МЭК 9126-1) | Software engineering — Product quality — Part 1: Quality model<br>(Программирование. Качество продукта. Часть 1. Модель качества)[1)] |
| [5] | ISO/IEC TR 13335 (all parts)<br>[(ISO/IEC TR 13335 (все части)] | Information technology — Guidelines for the management of IT Security<br>(Информационная технология. Руководства по менеджменту безопасности информационных технологий)[1)] |
| [6] | ISO/IEC 14598 (all parts)<br>[(ИСО/МЭК 14598 (все части)] | Software engineering — Product evaluation<br>(Программирование. Оценка продукта)[1)] |
| [7] | SO/IEC 15288<br>(ИСО/МЭК 15288) | Systems engineering — System life cycle processes<br>(Системотехника. Процессы жизненного цикла системы)[1)] |
| [8] | ISO/IEC 15504 (all parts)<br>[(ИСО/МЭК 15504) (все части)] | Information technology — Process assessment<br>(Информационная технология. Оценка процессов)[1)] |
| [9] | ISO/IEC 15408 (all parts)<br>[(ИСО/МЭК 15408 (все части)] | Information technology — Security techniques — Evaluation criteria for IT security<br>(Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ)[1)] |
| [10] | ISO/IEC 17799<br>(ИСО/МЭК 17799) | Information technology — Security techniques — Code of practice for information security management<br>(Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по менеджменту информационной безопасности)[1)] |
| [11] | ISO/IEC 18045<br>(ИСО/МЭК 18045) | Information technology — Security techniques — Methodology for IT security evaluation (also known as Common Evaluation Methodology (CEM)[2)]<br>(Информационная технология. Методы и средства обеспечения безопасности. Методология[3)] оценки безопасности ИТ)[1)] |
| [12] | ISO/IEC 21827<br>(ИСО/МЭК 21827) | Information technology — Security techniques — System security Engineering — Capability Maturity Model (SSE-CMM®)<br>(Информационная технология. Методы и средства обеспечения безопасности. Проектирование безопасности систем. Модель зрелости процесса (SSE-CMM®) |
| [13] | Aaron Cohen, Review of ISO Assurance Approaches, The First Annual International Systems Security Conference, San Antonio, Texas, February 3-4, 2000 | |
| [14] | AAWG Task 1 Report, Draft Version 0,9 Common Criteria Project: Assurance Approaches Working Group (AAWG) (report: AAWG-97/037, annex A: AAWG-97/038), August 1997 | |
| [15] | AGCA: A Guide to Certification and Accreditation for Information Technology Systems, Communications Security Establishment, Government of Canada, Ottawa, 1996 | |
| [16] | Abadi, Burrows, Lampson, Plotkin: A calculus for access control in distributed systems, Digital Equipment Corporation, Palo Alto, 1991 | |
| [17] | British Standard BS 7799-2, Information Security management systems — specification and guidance for use, British Standards Institution, 2002 | |
| [18] | CMM® (model): Capability Maturity Model for Software, Version 1.1, February 1993 | |
| [19] | CMM® (method): Key Practices of the Capability Maturity Model, Version 1.1, February 1993 | |
| [20] | Gasser, Goldstein, Kaufmann, Lampson: The Digital distributed security architecture, Proc. of National Computer Security Conference, USA, 1989 | |


---

[1)] Официальный перевод этого стандарта находится в Федеральном информационном фонде.

[2)] Готовится к утверждению.

[3)] Также известная как Общая Методология Оценки (ОМО).

[21] Information technology Security Evaluation Criteria (ITSEC), Version 1.2 (Provisional), Office for Official Publications of the European Communities, June

[22] Korea Information Security Evaluation Criteria, Ministry of Information and Communication, Republic of Korea, February 1998

[23] Korea Information Security Product Evaluation Program, Ministry of Information and Communication, Republic of Korea, February 1998

[24] The application of quality assurance procedures to security evaluation, NPL Report DITC 236/95, UK, July 1995

[25] SCT, Strict Conformance Testing, UK, March 1997

[26] SE-CMM® (model). A System Engineering Capability Maturity Model, Version 1.1, Carnegie Mellon University (CMU/SEI-95-MM-003), November 1995

[27] SE-CMM® (method). A Description of the Systems Engineering Capability Maturity Model Appraisal Method, Version 1.1. Carnegie Mellon University

[28] Strack/Lam: Context-dependent access control in distributed systems, Proc. of IFIP/SEC'93, Toronto 1993 (IFIP transactions a-37, North Holland, 1993)

[29] SSAM® (method) the System Security Engineering Capability Maturity Model Appraisal Methodology, Version 1.1. June 1997. Available for Internet: <http: //gost.e-ecolog.ru

[30] The Canadian trusted computer product evaluation criteria: version 3.0e/Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993. Available from: National Library of Canada [ xxv, 208p.: ill.;28 cm], LC Call no.: QA 76.9.A25 C36 199.1

[31] Trusted Capability Maturity Model, Version 2.0. National Security Agency (NSA), June 20, 1996

[32] Trusted Computer System Evaluation Criteria (TCSEC), DoD Standard 5200.28-STD, U.S. Department of Defense, December 1985

[33] Trusted Product Evaluation Program (TPEP) Overview, National Computer Security Center (NCSC)

[34] UK Certificate Maintenance Scheme, Part II Impact Analysis And Evaluation Methodology, UKSP 16, Issue 1.0, UK IT Security Evaluation & Certification Scheme Certification Body, 31 July 1996

[35] X/Open CAE Specification Baseline Security Services (XBSS), Document Number C529, UK: X/Open Company, Ltd., December 1995

УДК 681.324:006.354 ОКС 35.040

Ключевые слова: информационная технология, безопасность информационных технологий, доверие, оцениваемый объект доверия, риск доверия

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 29.10.2018. Подписано в печать 28.11.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,95.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru