ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 54583— 2011/ ISO/IEC/TR 15443-3:2007

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы доверия к безопасности информационных технологий

Часть 3

Анализ методов доверия

ISO/IEC TR 15443-3:2007
Information technology — Security techniques — A framework for IT security assurance — Part 3: Analysis of assurance methods (IDT)

Издание официальное

Москва
Стандартинформ
2013

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

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» (ООО «ЦБИ») на основе собственного аутентичного перевода на русский язык стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 691-ст

4 Настоящий стандарт идентичен международному документу ISO/IEC TR 15443-3:2007 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 3. Анализ методов доверия» (ISO/IEC TR 15443-3:2007 («Information technology — Security techniques — A framework for IT security assurance — Part 3: Analysis of assurance methods»)

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом 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

© Стандартинформ, 2013

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 Применение . . . 1
1.3 Область применения . . . 1
1.4 Недостатки . . . 1
2 Термины и определения . . . 1
3 Сокращения . . . 3
4 Понятие «доверие» . . . 3
4.1 Определение цели доверия . . . 3
4.2 Применение методов обеспечения доверия . . . 6
4.3 Оценка результатов доверия . . . 10
4.4 Пример . . . 11
5 Сравнение, выбор и формирование доверия . . . 11
5.1 Выбор подхода к обеспечению доверия . . . 12
5.2 Формирование методов обеспечения доверия . . . 13
5.3 Сравнение методов обеспечения доверия . . . 14
5.4 Сосредоточенность на характеристиках доверия . . . 15
6 Руководство . . . 19
6.1 Доверие к разработке (ДР) . . . 20
6.2 Доверие к интеграции (ДИ) . . . 20
6.3 Доверие к эксплуатации (ДЭ) . . . 23
Приложение А (справочное) Сравнения данных таблицы . . . 27
Приложение В (справочное) Характеристики доверия выбранных методов . . . 29
Приложение С (справочное) Формирование методов обеспечения доверия . . . 41
Приложение D (справочное) Изучение конкретных случаев . . . 43
Приложение Е (справочное) Определение цели обеспечения доверия . . . 45
Библиография . . . 49

Введение

Назначением ИСО/МЭК ТО 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 для него требованиям доверия к безопасности ИТ. В ИСО/МЭК ТО 15443 изучаются подходы и методы обеспечения доверия, предложенные организациями различного типа, независимо от того, являются ли эти методы и подходы частью утвержденных или неофициальных стандартов.

ИСО/МЭК ТО 15443 рассматривает:

- структурную модель взаимосвязи существующих методов обеспечения доверия;
- совокупность методов обеспечения доверия, их описание и ссылки на них;
- представление общих и уникальных свойств, присущих методам обеспечения доверия;
- качественное и по возможности количественное сравнение существующих методов обеспечения доверия;
- идентификацию систем оценки доверия, связанных с методами обеспечения доверия;
- описание взаимосвязей между различными методами обеспечения доверия;
- руководство по созданию, применению и идентификации методов обеспечения доверия.

ИСО/МЭК ТО 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 ИСО/МЭК ТО 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 ИСО/МЭК ТО 15443 анализируются методы обеспечения доверия, которые могут предназначаться не только для безопасности ИТ; однако руководство, приведенное в ИСО/МЭК ТО 15443, ограничивается требованиями к безопасности ИТ. В ИСО/МЭК ТО 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 ИСО/МЭК ТО 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 информационных технологий

Часть 3

Анализ методов доверия

Information technology. Security techniques.
A framework for IT security assurance. Part 3. Analysis of assurance methods

Дата введения — 2012—12—01

1 Область применения

1.1 Назначение

Назначением настоящего стандарта является предоставление органу по обеспечению доверия общего руководства по выбору подходящего метода обеспечения доверия к информационным и коммуникационным технологиям и формированию структуры анализа конкретных методов обеспечения доверия в конкретных условиях.

1.2 Применение

Настоящий стандарт позволяет пользователю согласовывать конкретные требования доверия и/или типичные ситуации с доверием с общими характеристиками имеющихся методов обеспечения доверия.

1.3 Область применения

Руководство, представленное в настоящем стандарте, применимо для разработки, внедрения и эксплуатации продуктов и систем информационных и коммуникационных технологий с требованиями безопасности.

1.4 Недостатки

Требования безопасности могут быть слишком сложными, методы обеспечения доверия — очень разнородными, а ресурсы и корпоративные культуры организаций могут в значительной степени отличаться друг от друга.

По этим причинам руководство, приведенное в настоящем стандарте, является кратким и относится к качественным характеристикам, и пользователю следует самому принимать решение о том, какие методы в соответствии с ИСО/МЭК ТО 15443-2 лучше всего соответствуют его конкретным объектам и соответствуют требованиям безопасности организации.

2 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК ТО 15443-1 и ИСО/МЭК ТО 15443-2, а также следующие термины с соответствующими определениями.

2.1 **активы** (assets): Все, имеющее ценность для организации.

2.2 **оценка** (assessment): Систематическая проверка степени, в которой субъект способен выполнить определенные требования; является синонимом термина «оценивание» при применении к объекту.

[ISO/IEC 14598-1].

Издание официальное

2.3 **метод оценки** (assessment method): Действие по применению конкретных документированных критериев оценки к объекту с целью определения приемлемости или разрешения на выпуск этого объекта.

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

Примечание — В конкретных системах и организациях термин «орган обеспечения доверия» может иметь вид «орган оценки».

2.5 **администратор доверия** (assurance administrator): Лицо, ответственное (подотчетное) за выбор, внедрение или приемку объекта.

2.6 **цель обеспечения доверия** (assurance goal): Общие ожидаемые результаты в области безопасности, получаемые посредством применения действий по формальной и неформальной оценке.

2.7 **предмет обеспечения доверия** (assurance concern): Общий тип цели доверия, выполняемой главной группой органов доверия.

Примечание — В настоящем стандарте предмет доверия используется в целях обоснования анализов и выводов для руководства по обеспечению доверия, данного группе пользователей.

2.8 **объект** (deliverable): Продукт безопасности информационной технологии, система, услуга, процесс или в особенности фактор среды (то есть персонал, организация) как объект оценки доверия.

Примечания

1 Как определено ИСО/МЭК 15408-1, объектом может быть профиль защиты (ПЗ) или задание по безопасности (ЗБ).

2 В ИСО 9000 утверждается, что при использовании стандартов ИСО 9000 услугой является тип продукта или «продукта и/или услуги».

3 В настоящем стандарте и аналогично применению в ИСО 9000 термин «продукт» будет применяться вместо термина «объект» во всех частях ИСО/МЭК ТО 15443.

2.9 **среда** (environment): Условия, в которых выполняются процессы жизненного цикла (то есть люди, оборудование и другие ресурсы), и связанные с этими условиями характеристики доверия (например, репутация, сертификация).

Примечание — В настоящем стандарте «доверие к среде» означает то же, что «доверие к продукту» и «доверие к процессу».

2.10 **система менеджмента информационной безопасности** (information security management system; ISMS); **СМИБ:** Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

[ИСО/МЭК 27001:2005]

2.11 **метод** (method): Способ выполнения определенных действий в соответствии с планом получения воспроизводимых результатов систематическим и отслеживаемым образом.

2.12 **показатель** (metric): Количественная шкала и метод, которые могут применяться для измерений.

2.13 **возможность процесса** (process capability): Способность процесса к достижению требуемой цели.

2.14 **продукт** (product): Продукт, система, услуга безопасности информационных технологий.

Примечания

1 В ИСО/МЭК ТО 15443 и аналогично применению в ИСО 9000 во всех частях ИСО/МЭК ТО 15443 будет применяться термин «продукт» вместо термина «объект».

2 Термин «продукт» является синонимом термина «объект».

2.15 **остаточный риск** (residual risk): Риск, остающийся после обработки риска.

2.16 **оценка риска** (risk assessment): Общий процесс анализа и оценивания риска.

[определение 3.3.1, Руководство 73: 2002 ИСО/МЭК]

Примечания

1 Оценивание риска является процессом сравнения оцененного риска с заданными критериями риска для определения значимости риска.

2 В настоящем стандарте «оценка риска», «анализ риска» и «анализ риска угрозы» обобщенно называются «оценкой риска».

2.17 **обработка риска** (risk treatment): Процесс выбора и осуществления мер по модификации риска.

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

2.19 **цель безопасности** (security objective): Изложенное намерение противостоять установленным угрозам и/или соответствовать установленной политике безопасности организации и предположениям.

[ИСО/МЭК 15408-1:2005, определение 2.42]

2.20 **политика безопасности** (security policy): Свод правил, являющийся внутренним сводом для подразделений организации и регламентирующий управление этими подразделениями защитой своих активов, с тем чтобы соответствовать заданным целям организации в рамках ее правового и культурного контекстов.

2.21 **этап** (stage): Период в рамках жизненного цикла объекта, включающего в себя процессы и виды деятельности.

Примечание — Заимствовано из ИСО/МЭК 15288.

3 Сокращения

В настоящем стандарте применяются сокращения по ИСО/МЭК ТО 15443-1, ИСО/МЭК ТО 15443-2, а также следующие сокращения:

COBIT — цели управления информацией и связанной с ней технологией, метод ISACA;

ISACA — Ассоциация аудита и контроля информационных систем;

ISSEA — Международная ассоциация проектирования безопасности систем;

ДИ (IA) — доверие к интеграции;

ДР (DA) — доверие к разработке;

ДЭ (OA) — доверие к эксплуатации;

ЗБ (ST) — задание безопасности.

4 Понятие «доверие»

Целью обеспечения доверия является создание уверенности в надежном функционировании продукта в заданных условиях. В настоящем разделе рассматриваются некоторые общие вопросы, тогда как детальный анализ и руководство представлены далее.

Исходя из концепций, разработанных в ИСО/МЭК ТО 15443-1, ИСО/МЭК ТО 15443-2, надежное функционирование продукта отвечает заданной цели доверия. Цель доверия следует устанавливать более или менее формальным образом, и пользователь должен быть осведомлен об остаточном риске.

Уверенность достигается посредством использования и интерпретации результатов доверия, которые уже могут быть в наличии или которые можно получить применением методов обеспечения доверия. Эти методы следует выбирать и применять должным образом.

Существует большое число методов, и многие из них представлены в ИСО/МЭК ТО 15443-2. Некоторые основные аспекты их применения разъясняются в 4.2.

Пользователь результата доверия может потребовать использование методов разных уровней сложности. Эта сложность может обуславливать связанный с ней уровень строгости методов обеспечения доверия (см. 4.2.1), диапазон применения (см. 4.2.2) и стадии жизненного цикла (см. 4.2.3).

Особое внимание следует уделять оценке результатов доверия. Для достижения более высоких степеней уверенности может потребоваться формальная оценка или сертификация (см. 4.3).

4.1 Определение цели доверия

Цели доверия зависят от следующих заданных требований доверия:

- поставщик продуктов может иметь обобщенные требования доверия, предназначенные для удовлетворения конкретных требований более чем одного пользователя, то есть требованиям коллектива пользователей его продукта, системы или услуги;

- у пользователя продукта существуют очень специфические требования, обычно зависящие от конкретной политики безопасности организации пользователя.

Ниже дается разъяснение заданных требований доверия и показана их связь с соответствующими предложениями доверия и их использованием.

Примечания

1 В А.1 приложения А приводятся различия между поставщиком аппаратных средств, поставщиком программного обеспечения, провайдером сети, оператором сервера, поставщиком он-лайновой информации и предприятием в качестве пользователя. В этом примере поставщики, очевидно, принадлежат к первой группе провайдеров доверия, а организация пользователя — к группе пользователей доверия. Однако остальные являются как поставщиками (провайдерами), так и пользователями доверия.

2 Организации может потребоваться объединение результатов доверия вследствие наличия двух или более источников доверия в совместимый общий результат. Это является важным аспектом, который будет рассматриваться в 5.2 и 6.2.3.1. Подобная ситуация возникает при наличии многочисленных результатов доверия для пользователя или при планировании провайдером доверия использования двух или более методов обеспечения доверия.

4.1.1 и 4.1.2 относятся к доверию к продукту во время его разработки и интеграции. Различие между предметами доверия обсуждается в разделе 6.

3 Следует учитывать, что организация пользователя обычно полностью отвечает за эксплуатацию продукта, даже если услуги по безопасности обусловлены субдоговором с провайдером услуг. Таким образом, требования пунктов 4.1.1 и 4.1.2 неприменимы напрямую к доверию к эксплуатации продукта.

4.1.1 Предложение доверия

С точки зрения организации, предлагающей продукты, системы или услуги в промышленных масштабах (или внутренним потребителям), применение соответствующего(их) метода(ов) обеспечения доверия будет определяться перспективным пользователем или коллективом пользователей, их опытом и размером их организации. Вследствие этих различий доверие придется модифицировать в соответствии с требованиями потребителя. В частности, доверие должно быть достаточно обобщенным, если получателем является коллектив пользователей.

Обычно, исходя из дополнительного периода от начала разработки изделия до выхода его на рынок и/или стоимости изделия, обеспечение доверия становится значимым фактором. Организации, обеспечивающей доверие, следует сравнить выгоды от обеспечения доверия со своими издержками на это обеспечение.

При условии вышеуказанного первыми двумя этапами процесса принятия решения является идентификация:

- причины возможной готовности пользователя заплатить за доверие;
- цели использования доверия пользователем.

Разрабатывая далее эти этапы, мы можем определить требования доверия потребителя и в итоге — приемлемые методы обеспечения доверия.



Рисунок 1 — Предложение доверия

Предлагаемые виды доверия можно представить, как это показано в таблице 1.

Требования доверия потребителя идентифицируются в виде утверждения о доверии, обусловленного методом обеспечения доверия.

Необходимо также учитывать вспомогательные аргументы доверия и в особенности «строгость доверия» (см. таблицу 3). Большинство методов обеспечения доверия предъявляют более одного вида

требований доверия, а строгость доверия изменяется в зависимости от метода обеспечения доверия. Следовательно, выбранные методы обеспечения доверия должны тщательно комбинироваться с целью безусловного удовлетворения требований пользователей и достижения их целей доверия.

Таблица 1 — Предлагаемые виды доверия

Вид предлагаемого доверия	Целевой потребитель	Требования доверия потребителя	Требуемая строгость оценки
Сквозное доверие	Конечный пользователь	Маркировка содержимого: понятная и различимая для конечного пользователя	Малая
Доверие маркетинга	Общий коллектив пользователей	Маркер, метка, печать: - маркировка со ссылкой на общие требования доверия; - представлены в очень краткой форме или защищены от внешних воздействий; - понятная и различимая для конечного пользователя, то есть признанный «знак качества»	Низкая
Внутреннее доверие	Внутренний потребитель	Пользовательская форма утверждения о доверии; предоставляется внутри организации и основана на доверии	Любая
Внешнее доверие	Конкретный коллектив пользователей	Маркировка, включающая в себя исчерпывающие вспомогательные аргументы и материалы; может иметь ограниченное обращение	Высокая
Доверие к небольшой организации	Небольшие организации	Маркер или печать; предназначены для создания доверия посредством убежденности; понятные и различимые для конечного пользователя, то есть признанный «знак качества». Примечание — Обычно у небольших организаций из-за их размера для верификации представленных претензий к доверию недостаточно квалификации	Средняя
Доверие к крупным организациям	Крупные организации	Детальное утверждение о доверии. Примечание — Квалификации для верификации претензий к доверию достаточно	Высокая
Санкционированное доверие	Конкретная современная организация	Сертификат или утверждение о пригодности. Форма доверия и даже используемый метод разрешается организацией, например, посредством договорных или регистрационных требований	Высокая

4.1.2 Использование доверия

Пользователь предложения вида доверия имеет альтернативу. Будучи последней инстанцией доверия этого пользователя, целью пользователя является получение уверенности в том, что конкретный продукт соответствует его цели доверия, что и ожидается от продукта в плане безопасности в контексте организации, в рамках которой продукт должен внедряться, вводиться в действие и эксплуатироваться.

В идеале цель доверия определяется оценкой риска или политикой организации (см. приложение Е).

Уверенность в доверии может быть достигнута посредством выбора и применения формальных и неформальных действий по оценке, которые могут предлагаться поставщиками, системными интеграторами или осуществляться пользователями.

Доверие может использоваться так, как показано в таблице 2. В таблице 2 также представлены виды деятельности по оценке доверия, при помощи которых можно создать уверенность пользователя в продукте.

Таблица 2 — Применяемые предложения доверия

Профиль пользователя	Искомый вид доверия	Виды деятельности по оценке доверия пользователя	Строгость оценки
Конкретный пользователь	Маркировка содержания	Проверка понятности, распознаваемости маркировки, содержания и ее применимости для воспринимаемой цели доверия	Низкая
Общий пользователь	Маркер, метка, печать	Проверка понятности, распознаваемости маркировки, содержания и ее применимости для воспринимаемой цели доверия	Низкая
Внутренний потребитель	Пользовательская форма заявления о доверии	Валидация внутреннего доверия, например, через соответствующий опрос	Любая
Член конкретного коллектива пользователей	Маркировка	Валидация доверия к метке, например, через опрос других членов коллектива или организаций	Высокая
Небольшая организация	Маркер или печать	Проверка понятности, распознаваемости маркировки содержания и ее применимости для воспринимаемой цели доверия. Предпочтительной является метка «знак качества»	Средняя
Крупная организация	Детальное заявление о доверии	Верификация и проверка достоверности заявлений о доверии специалистами организации	Высокая
Конкретная современная организация	Сертификат или утверждение о пригодности	Доверие может обеспечиваться оцениванием третьей стороной и/или сертификацией, по меньшей мере, посредством репутации провайдера, обеспечивающего доверие	Высокая

4.1.3 Остаточный риск

На базовом уровне доверие обеспечивает пользователю уверенность в функционировании продукта так, как утверждается поставщиком, без каких-либо непредусмотренных отклонений. Однако в отличие от других гарантий безопасности доверие само по себе не обеспечивает каких-либо дополнительных функциональных возможностей (механизмов защиты) и, следовательно, не противодействует какой-либо дополнительной угрозе или уязвимости.

Все элементы безопасности, в частности менеджмент риска, независимо от применяемого метода, включают в себя неопределенность. Неопределенность исходит от многих источников, таких как недостаточное знание всех факторов, допусков при измерениях, экстраполяции факторов и т. д. Эта неопределенность может иногда быть настолько велика, что становится основным фактором остаточного риска. Другими факторами являются уязвимости целевой эксплуатационной среды и несовершенство механизмов безопасности. При увеличении строгости доверия и усилении характеристик и механизмов безопасности связанная с этими факторами неопределенность снижается, таким образом снижая общий риск.

В определенных ситуациях доверие может быть единственным способом снижения неопределенности. Доверие может снизить риск до приемлемого уровня без добавления новых механизмов безопасности. В этом случае стоимость обеспечения доверия оправдывается получением преимуществ от безопасности. Из всего вышеизложенного можно сделать вывод о том, что обеспечение доверия направлено на снижение риска.

4.2 Применение методов обеспечения доверия

Методы обеспечения доверия обладают различимыми характеристиками, представленными в виде компонентов или аспектов. Для выбора из одного или нескольких методов необходимо определить те компоненты и аспекты, которые можно найти в различных методах обеспечения доверия в аналогичной форме. Тот или иной метод обеспечения доверия может включать в себя общие характеристики доверия или основываться на конкретных характеристиках.

В соответствии с ИСО/МЭК ТО 15443-1 и ИСО/МЭК ТО 15443-2 методы обеспечения могут формировать доверие к продукту путем оценки:

- продукта во время или после его изготовления;
- процессов, используемых при изготовлении продукта;
- среды, в которой реализуется продукт, то есть персонала и организации.

4.2.1 Строгость доверия

Строгость метода обеспечения доверия обычно определяет его применение (см. таблицу 3).

Таблица 3 — Строгость доверия и его использование

Уровень строгости	Использование доверия
1	Простая «печать утверждения доверия»
2	Заявления о доверии позитивного уровня
3	Конкретные факты, поддерживающие заявленное доверие
4	Конкретные факты, поддерживающие заявленное доверие, которое можно верифицировать
5	Представление доверия общей аудитории, например, совету директоров, и признание этой аудиторией
6	Представление доверия аудитории из специалистов по безопасности и признание этой аудиторией

Примечания

1 Кроме того, необходимо принимать во внимание состав представительства и поддерживающих его аргументов. В особых ситуациях допускается применять ограничения.

2 При объединении оцененных компонентов доверия в развертываемую систему может произойти наложение систем показателей и/или могут задаваться вопросы по поводу брешей в системе безопасности.

3 В ИСО/МЭК ТО 15443-2 не приводится классификация строгости оценки.

4.2.2 Область применения

Полученное доверие также может изменяться в зависимости от области применения подхода к обеспечению доверия (см. таблицу 4).

Таблица 4 — Область применения подхода к обеспечению доверия

Подход к обеспечению доверия	Сосредоточенность метода обеспечения доверия	Область применения
Продукт	Характеристики (завершенного конкретного) продукта, системы или услуги для определения доверия, которые можно вывести для этого продукта или системы	Некоторые аспекты продукта или системы
		Все аспекты продукта или системы
Процесс	Процесс разработки, используемый организацией для конкретного продукта или системы с целью определения доверия, которое можно получить для этого продукта или системы	Некоторые аспекты разработки
		Все аспекты разработки
	Процесс разработки, используемый организацией для всех продуктов и систем	Некоторые аспекты разработки
		Все аспекты разработки
Среда	Лицо(лица), занятое(ые) в выполнении задач	Квалификация лица(лиц)
		Репутация
	Организация	Меры, наглядно принимаемые организацией в отношении любых обнаруженных позднее проблем, и время реализации этих мер
		Репутация

4.2.3 Применение и жизненный цикл

В ИСО/МЭК ТО 15443-1 была принята поэтапная модель на основе ИСО/МЭК ТО 15288. Каждый этап жизненного цикла системы соответствует процессам, применяемым к продукту в определенной среде. Каждый из процессов включает в себя совокупность видов деятельности и использует ресурсы своей среды.

Продукт, система или предоставляемая услуга обрабатываются в течение их жизненного цикла с применением процессов каждого этапа и их видов деятельности.

В ИСО/МЭК ТО 15443-1 представлена структура, позволяющая характеризовать тип продукта, подход к обеспечению доверия и этап обеспечения доверия, предназначенный для оценки.

По-прежнему существует много вопросов, касающихся обеспечения доверия, подлежащих рассмотрению. В данном разделе настоящего стандарта приводится расширение концептуальной структуры, представленной в ИСО/МЭК ТО 15443-1, в целях проведения дальнейшего анализа.

В настоящем стандарте поэтапная модель жизненного цикла усовершенствуется прибавлением этапа «Концепция/специализация» (см. таблицу 5).

Наличие процессов, соответствующих этапу концепции/специализации, обусловливается многими стандартами. Однако конкретный этап жизненного цикла этих процессов обычно не определяется. Некоторые методы обеспечения доверия предлагают определенные процессы и виды деятельности.

Поводом для этого расширения в настоящем стандарте является то, что безопасность ИКТ требует особого внимания и дополнительных усилий для получения согласованной и непротиворечивой спецификации характеристик безопасности продукта. Существует много методов обеспечения доверия, предлагающих определенные процессы и виды деятельности для этого этапа жизненного цикла системы, применимые для области безопасности ИКТ.

В расширенной модели доверия различные этапы жизненного цикла представлены в таблице пятью столбцами. В соответствии с концепциями ИСО/МЭК 15288 и ИСО 9000 технологические процессы жизненного цикла группируются в пять этапов (по одному на каждый столбец), обозначенных одной (1) буквой:

C (Conception) — концепция формирования требований к проектированию безопасности, которая может включать в себя общую архитектуру;

D (Design) — проектирование, включая процессы определения требований заинтересованных сторон, анализа требований, архитектурного проектирования и реализации;

I (Integration) — интеграция, включая процессы интеграции и верификации;

T (Transition) — переход, включая процессы дублирования, перемещения, ввода в действие и приемочные испытания;

O (Operation) — эксплуатация, включая процессы эксплуатации, обслуживания и ликвидации.

Таблица 5 — Модель доверия жизненного цикла

Доверие-этап → доверие-подход ↓	Концепция/ спецификация	Проектирование/ реализация	Интеграция/ верификация	Ввод в действие/переход	Эксплуатация
Продукт	→C→	→D→	→I→	→T→	→O→
Процесс	C	D	I	T	O
Среда	C	D	I	T	O

В ИСО/МЭК ТО 15443-1 разработана следующая концепция:

- доверие может быть сосредоточено на результате процесса, являющегося продуктом, в итоге появляется доверие к продукту;

- применяемые процессы обычно являются предметом внимания организации и ее заказчиков, поскольку они более или менее формально специфицируются и относительно улучшаются. Доверие может фокусироваться на процессах, примененных к продукту, а не на самом продукте, приводя к формированию доверия к процессу;

- для осуществления процессов требуется среда, а именно: люди, оборудование и другие ресурсы. Доверие может фокусироваться на среде, в которой обрабатывается продукт, а не на продукте или процессах, приводя к формированию доверия к среде.

Примечание — В настоящем стандарте не детализируется метод применения жизненных циклов, а также его процессы и виды деятельности; однако могут потребоваться подробности при уточнении сравнения методов обеспечения доверия.

4.2.4 Управление процессами жизненного цикла

Этапы жизненного цикла C-D-I-T-O включают в себя процессы, которые можно применять к конкретному объекту ИКТ и его компонентам, то есть к аппаратным средствам, программному обеспечению, услугам.

В интересах повышения качества и усовершенствования эти процессы и их виды деятельности можно сделать объектом управления.

Управление процессом само по себе является процессом. Следовательно, оно осуществляется не на уровне проекта, а на уровне организации.

Однако управление процессом имеет смысл только при повторном выполнении процесса (например, администраторами эксплуатации ИТ или разработчиками продуктов проектов ИКТ).

Модель процесса жизненного цикла по ИСО/МЭК ТО 15443-1 совершенствуется в настоящем стандарте за счет добавления управления процессом в качестве еще одного измерения.

В области безопасности ИКТ это измерение имеет особое значение для методов управления безопасностью, применяемых к системам ИКТ на производственном этапе, как в случае с ИСО/МЭК 27002 и связанным с ним ИСО/МЭК 27001.

Управление процессом касается разработки, использования и улучшения процессов жизненного цикла. По существу, управление включает в себя следующие этапы:

- определение процесса, включая разработку и документацию;
- повторное использование процесса;
- оценку и измерение процесса;
- улучшение процесса.

Процессы могут сертифицироваться третьими сторонами. Числа, связанные с этими этапами, соответствуют зависимости:

- нет повторного использования без разработанных и документированных процессов;
- нет оценки и измерения процесса без повторного использования процесса;
- нет улучшения процесса без оценки и/или измерения процесса;
- нет сертификации без оценки и/или измерения процесса.

Поскольку улучшение модели жизненного цикла приводит к появлению изменений в процессах и их документации, управление процессом может считаться круговой моделью непрерывного улучшения, как показано на рисунке 2.

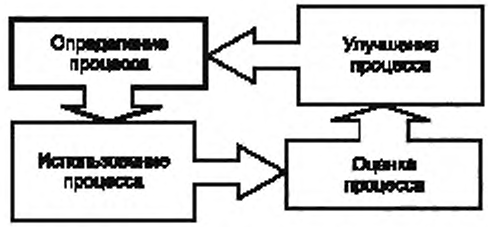


Рисунок 2 — Управление процессами жизненного цикла

Примечание — Для обеспечения измеримости процессов последние должны документироваться.

Управление процессом является вторым измерением, которое является независимым процессом от измерения этапа C-D-I-T-O. Если метод обеспечения доверия обеспечивает доверие к процессу, это означает наличие управления процессами (применимыми к продукту).

Если этап доверия к методу показан серым цветом (см. таблицу 6, уровни 2, 4, 6 и 7), метод обеспечивает управление процессами.

Примечание — Термины «разработка продукта» и «разработка процесса» кажутся похожими и, следовательно, создают путаницу. Термины должны быть различимыми и применяться раздельно.

4.2.5 Объединение характеристик жизненного цикла

Методы могут быть более и менее полными в отношении характеристик их жизненного цикла. Эти характеристики можно объединить, что характеризует не только совершенство, но и сложность метода.

В ИСО/МЭК ТО 15443-1 специфицируются соответствующие подходы к обеспечению доверия, которые могут характеризовать метод обеспечения доверия. Символически подходы представлены следующим образом (см. рисунок 2):

- доверие к продукту: показано буквой этапа жизненного цикла между стрелками на светлом фоне, например, →**D**→;
- доверие к процессу: показано белой буквой этапа жизненного цикла на затененном фоне, например, **D**;
- доверие к среде: показано ячейкой этапа жизненного цикла с полосками слева и справа, например, **D**

Очевидно, что исходя из числа компонентов уровень 7 является наиболее полным и имеет, по меньшей мере, преимущества полноты и последовательности с точки зрения лексики, процессов и результатов. Все это оказывает положительное воздействие на обучение методу и его стоимость.

Примечание — Однако полнота не подразумевает того, что самый полный метод является наилучшим для конкретной ситуации с доверием. Следует учитывать другие аспекты метода, такие как «строгость», «уровень детализации» и связанные с ними затраты.

Таблица 6 — Подход к обеспечению доверия

Уровень	Доверие к продукту	Доверие к процессу	Доверие к среде	Графическое представление этапа X жизненного цикла
1	✓			→X→
2		✓		X
3			✓	X
4	✓	✓		→X→
5	✓		✓	→X→
6		✓	✓	X
7	✓	✓	✓	→X→

4.3 Оценка результатов доверия

Относящиеся к безопасности характеристики продукта, процесса или среды, обеспечивающие доверие, являются утверждениями в наиболее примитивной форме, сделанными инициирующей стороной, обычно изготовителем объекта, услуги или среды. Для верификации доверия к этим утверждениям может потребоваться оценка и сертификация результата доверия.

Можно создать модель оценки доверия. В ней будет определена серия обобщенных этапов, применимых к любому из методов обеспечения доверия из настоящего стандарта.

Для модели доверия к качеству требуются:

- лицо, оценщик или организация для верификации применения критериев;
- правила, критерии и/или методология оценки в качестве ее основы;
- сертификация наличия достаточной квалификации у аудитора и выполнения процедуры оценки в соответствии с правилами;
- заключение о результатах оценки.

Полная модель этого типа обычно называется «структурой доверия».

4.3.1 Оценщик

Оценка характеристик доверия к безопасности продукта может проводиться пользователем продукта при наличии у него специальных знаний. Для экономии времени и расходов целесообразно обратиться к квалифицированной третьей стороне.

Оценка третьей стороной может обеспечить дальнейшее повышение доверия вследствие только лишь факта ее независимости.

Примечание — Доверие персонала подтверждает приемлемость квалификации оценщика.

4.3.2 Методология и критерии оценки

Для гарантии воспроизводимости правила оценки следует документировать и сопровождать соответствующей методологией.

Примечание — При оценке персонала оцениваемым объектом является отдельное лицо.

4.3.3 Свидетельство доверия

Общим для всех методов оценки является то, что результаты оценки основаны на свидетельстве. Свидетельство представляется утверждениями, которые обычно имеют форму документации.

Свидетельство подтверждает эффективное предполагаемое выполнение действий в рамках соответствующих процессов, планов и процедур согласно политикам и концепциям безопасности. Эти политики и концепции должны регулярно пересматриваться и при необходимости обновляться.

Наиболее значимыми требованиями к документации являются:

- стабильность (документация должна отражать фактическую ситуацию);
- полнота (все значимые проблемы должны быть документированы);
- достаточная степень детализации;
- контроль конфигурации и целостности (отсутствие несанкционированных изменений в документации).

Следовательно, при детальном анализе методов обеспечения доверия можно дополнительно исследовать требования и сопоставимость этой документации.

4.3.4 Заключение об оценке

Результаты количественной или качественной оценки должны быть специфицированы. В простейшей форме это может быть приемка/браковка, тогда как более точный результат принимает форму ранжирования, например, нескольких уровней (степеней), например, уровня, соответствующего браковке.

Целям безопасности, в противоположность техническим областям, характерна постоянная эволюция. Из-за сложности объектов могут появляться новые дефекты безопасности, и вследствие наличия среды угроз может возникнуть необходимость противодействия новым угрозам.

4.3.5 Поддержка оценки

После завершения оценки она должна повторяться периодически или в случаях возникновения каких-либо событий.

Поддержкой оценки является поддержание достоверности заданного результата доверия к безопасности или ранжирования в течение длительного времени.

Примечание — В отношении доверия к персоналу это может означать постоянное обучение и периодическую переоценку или переаттестацию конкретного лица.

4.4 Пример

Орган обеспечения доверия — поставщик создает доверенную систему для удовлетворения общих требований безопасности в соответствии с ИСО/МЭК 15408 (критерии оценки). Оценщики (эксперты органа оценки) оценивают систему на предмет выполнения этой системой требований ИСО/МЭК 15408.

В целях обеспечения доверия орган оценки применяет ИСО/МЭК 18045 (методологию оценки) и выдает соответствующий статус подтверждения (ознакомление, согласование, утверждение).

Оценщики и орган оценки уполномочиваются национальным органом по сертификации в соответствии с соглашением о взаимном признании общих критериев.

Национальный орган сертификации выдает сертификат с результатами оценивания и полученным статусом подтверждения.

Для этого сертификата может потребоваться периодическое оценивание для гарантии того, что модификация продуктов не меняет результаты оценивания.

5 Сравнение, выбор и формирование доверия

Назначением настоящего стандарта является обеспечение органа обеспечения доверия руководством по выбору соответствующих методов обеспечения доверия к информационным и телекоммуникационным технологиям для выполнения поставленной цели доверия, то есть выполнения политики безопасности организации. Это руководство содействует органу обеспечения доверия в определении:

- подхода к обеспечению доверия, который обеспечит требуемые результаты доверия, наиболее соответствующие требованиям органа оценки;

- относительной ценности каждого подхода к обеспечению доверия, наиболее соответствующего конкретным условиям органа обеспечения доверия;

- способа обращения с доверием сложного объекта (то есть с несколькими компонентами аппаратных средств, программного обеспечения, услуг по безопасности, аспектами среды или их комбинациями).

5.1 Выбор подхода к обеспечению доверия

Разных степеней доверия можно достигнуть различными методами. В настоящем подразделе рассматривается сравнение каждого из последующих подходов к обеспечению доверия (не методов) по принципу «один к одному»:

- доверие к продукту в сравнении с доверием к процессу;

- доверие к процессу в сравнении с доверием к среде;

- доверие к продукту в сравнении с доверием к среде.

Эти подходы соответствуют первым трем уровням в таблице 6. Целью данного сравнения является понимание того, какой вид подхода к обеспечению доверия следует выбрать.

Примечание — Совокупность подходов соответствующих уровней в таблице 6, от 4 до 7, обсуждается в 5.2.

5.1.1 Сопоставление доверия к продукту с доверием к процессу

По определению доверие к продукту сосредоточено на продукте, тогда как доверие к процессу сосредоточено на процессах, применяемых к продуктам на определенных этапах жизненного цикла.

В случае с доверием к продукту утверждается, что характеристики продукта и его функционирование интенсивно оценивались, тестировались и подтверждались в отношении их корректности, пока не была получена требуемая степень доверия к продукту. Степень доверия к продукту является функцией используемых критериев (что оценивается) и методологии обеспечения доверия (как верифицируется соответствие критериям).

В случае с доверием к процессу предпосылкой доверия является наличие у организаций процессов, использованных для проектирования, разработки, производства и эксплуатации продукта прогнозируемых и воспроизводимых результатов. Эти процессы производят продукт с заданной степенью доверия к нему.

Однако даже самая высокая степень доверия пользователя к процессам, используемым производителем, не может гарантировать правильного и эффективного применения этих процессов к данному продукту. Другими словами, при высоких степенях доверия к продукту необходимо оценивание продукта.

В случае с доверием к продукту каждый продукт должен оцениваться в отдельности так, чтобы общая стоимость оценивания возрастала с увеличением числа разработанных продуктов. Однако с точки зрения производителя этого повторного оценивания аналогичной или идентичной продукции можно избежать, если пользователь удовлетворен доверием к процессу производителя, то есть используемые процессы соответствуют стандартам качества процесса. Преимущество метода обеспечения доверия к процессу заключается в том, что организация может производить различную продукцию без дополнительных оценок (за исключением периодических оценок для поддержки ее сертификата).

Очевидно, что это сравнение справедливо только для сопоставимой эффективности, детализации и корректности методов обеспечения доверия и по возможности дополняется доверием, обеспечиваемым третьими сторонами, к которым обращались для большей объективности обеспечения доверия.

При применении комбинации из двух подходов следует также использовать информацию из области синэнергетики. Например, производитель с доверием к своим процессам затратит меньше ресурсов на оценивание продукта, который он производит посредством процессов, обеспечивающих доверие.

5.1.2 Сопоставление доверия к процессу с доверием к среде

Доверие к процессу сосредоточено на процессах, применяемых к продукту на конкретных этапах жизненного цикла, тогда как доверие к среде сосредоточено на ресурсах и среде, в которой использовались эти ресурсы.

Уверенность в продукте, обеспечиваемая доверием к среде, обуславливается уверенностью в организации и ее персонале, а также в других ресурсах, применяемых к продукту. Эта уверенность может быть обеспечена аттестацией персонала и/или организации с применением соответствующих стандартов или хорошей профессиональной практики, где самым низким уровнем является репутация персонала или организации, ответственной за продукт.

Очевидно, что при условии применения сопоставимой степени детализации доверие к среде обычно менее эффективно, чем доверие к процессу. Фактически любая организация или конкретное лицо могут обладать общими знаниями о возможностях процессов, предназначенных для применения к продукту. Однако доказательство того, что процессы были документированы, оценены или сертифицированы, отсутствует.

Доверие к среде является самой низкой формой доверия, которую обеспечить легче всего. Существуют ситуации, когда доверие к среде является единственной осуществимой и доступной по цене формой доверия. Доверие может иметь место:

- в небольших организациях, которые не могут позволить себе расходы на обеспечение доверия к процессу или продукту;
- в отношении коммерческих серийных продуктов, когда поставщик не обеспечивает доверия к продукту или процессу.

5.1.3 Сопоставление доверия к продукту с доверием к среде

Исходя из вышеизложенного становится очевидным наличие области обеспечения доверия определенного прогресса. Если доверие к продукту недоступно, доверие к процессу является «почти не уступающим по качеству». Если недоступно доверие к процессу, оставшейся возможностью является доверие к среде.

5.1.4 Заключение

В заключение, при условии отказа от сопоставимости данных подходов к обеспечению доверия можно утверждать следующее:

- при самых высоких требованиях доверия следует выбирать доверие к продукту;
- доверие к процессу обеспечивает приемлемое и, по большей части, допустимое доверие посредством обеспечения доверия к качеству соответствующих процессов;
- доверие к среде должно выбираться в небольших организациях или в случаях, если продукт и/или его производитель не доступны для оценивания процесса и/или продукта.

В общем можно утверждать, что:

- доверие повышенной строгости к продукту ограничивается доверием к разработке относительно менее сложных продуктов, тогда как
- доверие к среде применимо в основном к доверию к эксплуатации, если системы являются относительно сложными и доверие менее строгим.

Возможность использования методов обеспечения доверия показана на рисунке 3.



Рисунок 3 — Возможность использования методов обеспечения доверия

5.2 Формирование методов обеспечения доверия

Несомненно, многие пользователи будут применять несколько методов обеспечения доверия как по ИСО/МЭК 15408 и ИСО 9000, так и по ИСО/МЭК 15408 и ИСО/МЭК 21827.

В настоящем стандарте представлена структура, которую можно использовать для записи свидетельства/опыта лиц, применявших более одного метода обеспечения доверия. В нем также представлены понятия и универсальный язык, которым можно изложить взаимодействие между методами и подходами и таким образом способствовать изучению возможных комбинаций методов и подходов.

Способность объединять характеристики доверия различных подходов к обеспечению доверия облегчает достижение доверия к продуктам и системам путем принятия компонентов доверия из других подходов к обеспечению доверия в дополнение к используемому в данный момент подходу.

Например, если организация была сертифицирована по уровню 3 ИСО/МЭК 21827, ей может быть обеспечено доверие в рамках структуры оценивания ИСО/МЭК 15408 без необходимости для организации повторно предоставлять свидетельство, которое она уже представила для другого подхода к обеспечению доверия. Более того, это облегчит работу сертифицирующей организации, поскольку у нее имеется дополнительное свидетельство, которое теперь будет приемлемо при определении общего доверия к системе.

Сравнение методов обеспечения доверия может способствовать пониманию потенциальных ограничений подхода формирования доверия. Сравнение методов обеспечения доверия связано с возможностью устранения характеристик доверия, если существует вероятность их базирования на других атрибутах.

При применении методов обеспечения доверия безопасность рассматривается с разных сторон и в различном объеме, и эти методы предназначаются для разных пользователей и подразделений организации для выполнения разных целей. Ни один метод, рассматриваемый в настоящем стандарте, не может гарантировать «всеобщей» безопасности, которая должным образом обеспечит защиту имеющейся системы ИТ от всех значимых угроз. Следовательно, в большинстве случаев необходимо использовать комбинацию методов обеспечения доверия синергетическим способом.

Оптимального уровня безопасности можно достичь при условии сотрудничества поставщиков и пользователей ИТ.

Примеры, демонстрирующие аспекты формирования методов обеспечения доверия, приведены в приложении С.

5.3 Сравнение методов обеспечения доверия

Для сравнения относительного значения методов обеспечения доверия, указанных в ИСО/МЭК ТО 15443-2, могут использоваться два основных подхода:

- матрица характеристик;
- образование пар (сравнение матриц по принципу «один к одному»).

Если требуется сравнение многих, то есть более трех элементов друг с другом, как показано на рисунке 4, становится очевидной необходимость сравнения элементов по их общим характеристикам. С увеличением числа элементов становится очевидным неоспоримость этого подхода. Безусловно, предпосылкой неоспоримости является значительное число аналогий в рамках этих методов.

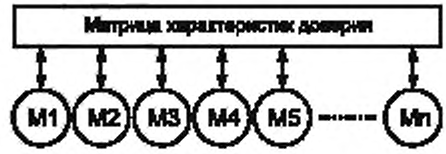


Рисунок 4 — Принцип сравнения матриц

Для сравнения матриц надо разработать перечень характеристик доверия. Основной трудностью этого подхода является формирования оптимального перечня характеристик, приемлемых для изложения в общих чертах основных различий между этими методами.

Сравнение матриц характеристик доверия методов обеспечения доверия состоит из их описания и ранжирования отдельных методов по перечню. Представление результатов упрощается применением количественных мер измерения или степеней. Подходящим способом представления руководству результатов оценивания является представление графических контрольных списков.

Для принятия информированного решения по выбору методов обеспечения доверия для дальнейшего применения и значению (ценности) результата применения конкретного метода при анализе сравнения матриц исследуют совокупность специфических методов обеспечения доверия.

Подобные сравнения матриц можно адаптировать для конкретных проблемных областей в соответствии с требованиями заинтересованных сторон, например, для производителя продукта, крупной организации.

В разделе 6 настоящего стандарта определены три проблемы, связанные с доверием, которые выбраны в качестве руководства.

Краткое изложение метода сравнения матриц специфических общих характеристик выбранных методов приведено в приложении А.

5.3.1 Сравнение по принципу «один к одному»

Для более подробного сравнения элементов матриц может использоваться пользовательский (заказной) перечень: элементы добавляются или удаляются, с тем чтобы соответствовать паре выбранных элементов. Однако по мере увеличения числа сравниваемых методов число сравнений «один к одному» будет увеличиваться с двоичным коэффициентом «n» и 2, где n — число методов (например, для 6 элементов потребуются 15 отдельных сравнений). По этой причине данный тип сравнения в настоящем стандарте не применяется.

Сравнение по принципу «один к одному» приемлемо для пользователя, способного проводить такое сравнение на основе описаний, содержащихся в ИСО/МЭК ТО 15443-2, и используемого ссылочного материала в настоящем стандарте. Пользователь может также подготовить резюме, с тем чтобы сделать выводы из конкретного числа сравнений «один к одному».

5.3.2 Матрица характеристик доверия

Характеристики доверия являются фактическим источником доверия и могут иметь соответствующую систему показателей. Характеристики доверия включают в себя ценность (значимость) и различные качественные аспекты, такие, например, как строгость, надежность, воспроизводимость, эффективность и т. д.

Какой метод обеспечения доверия подходит для рассматриваемой проблемы доверия и как его применять? Для ответа на эти вопросы надо понять преимущества методов обеспечения доверия исходя из достигнутого с их помощью доверия и с учетом связанных с ним издержек. Другими словами, для облегчения сравнения методов обеспечения доверия свойства (признаки) доверия, определяющие значимость метода, должны получить характеристики.

5.4 Сосредоточенность на характеристиках доверия

Для сравнения принятых методов обеспечения доверия было разработано несколько типичных характеристик доверия. Назначением настоящего стандарта является оказание помощи пользователю при принятии решения о применении одного метода или комбинации из двух или более методов для конкретного случая.

Характеристики доверия (см. таблицу 7) имеют общий характер, а определенные методы обеспечения доверия анализируются на общей основе в приложении В.

Общая ориентация методов, представленная в резюме, приведена в приложении А. Из таблицы 7 можно сделать выводы о применимости или неприменимости конкретного метода в конкретном контексте.

Примечание — Исходную и последующую информацию о методах обеспечения доверия см. в ИСО/МЭК ТО 15443-2.

Таблица 7 — Ключевые аспекты сравнения

	Аспект	Описание
1	Цель доверия	Предусматривает ли метод определение цели обеспечения доверия? Каким методом была определена эта цель? Как эта цель достигается?
2	Целевая аудитория	Какую проблему обеспечения доверия решает метод? Для каких компаний и каких ролей в рамках предприятия предназначен метод?
3	Характеристики	Каково назначение рассматриваемого метода? Какие методологические элементы он содержит? Насколько метод применим для общепринятых структур предприятий? Насколько метод применим для конкретного случая?
4	Разносторонность	Какова взаимосвязь между объемом работ по применению метода и его стоимостью? Какой величиной и сложностью исследуемого объекта можно оперировать? Можно ли это контролировать путем применения разных степеней детализации?
5	Своевременность	Отражает ли настоящая версия метода новейшие технологии? Как обеспечивается в случае необходимости регулярное обновление метода?

Окончание таблицы 7

	Аспект	Описание
6	Завершенность	Образуют ли критерии закрытый исчерпывающий каталог элементов или охватывают только выбранные аспекты? Для какого уровня безопасности адаптирован релевантный каталог соответствующих критериев?
7	Издержки при внедрении/объем работ по внедрению	Чего надо ждать в отношении объема работ и издержек при применении данной системы критериев безопасности ИТ к типичным сценариям?
8	Поддержка инструментальными средствами	Существуют ли какие-либо инструменты поддержки пользователя при применении рассматриваемого метода?
9	Сфера действия криптографии	Содержит ли рассматриваемая система критериев безопасности ИТ какие-либо положения или руководство по криптографическим процедурам или алгоритмам?
10	Оценка и сертификация	Существует ли для метода квалификационная и/или сертификационная система? Применим ли метод для продуктов или итоговых решений?
11	Убедительность и признание	Является ли воздействие успешного оценивания и сертификации потенциально удовлетворяющим заказчика или администрацию или, по меньшей мере, основой для дополнительных тестов? Какова зрелость (развитость) структуры? Каково рыночное признание и его движущие силы?

5.4.1 Цель обеспечения доверия

Задачей органа по обеспечению доверия является утверждение адекватности доверия, а также числа и качества свидетельств доверия, которые надо получить для достижения приемлемого уровня риска. Это означает, что остаточный риск для предполагаемой среды не превысит уровень, приемлемый для заинтересованных сторон и принятый ими.

Для уверенности в результате обеспечения доверия орган по обеспечению доверия обязан обосновать этот результат рациональным способом, продемонстрировав требуемое функционирование продукта с обеспечением требуемых функциональных возможностей и одновременным выполнением политики безопасности. Степень уверенности является прямым результатом процесса обеспечения доверия и степени удобства для конкретного заинтересованного лица.

Следовательно, процессы и стандарты, используемые для формирования доверия, должны быть понятны и включать в себя определение, сбор и проверку свидетельств доверия. Свидетельства допускается собирать методами, применяемыми для разработки, составления и поддержания результата доверия.

Цель обеспечения доверия может основываться на оценке риска, политике безопасности или профиле защиты (см. также приложение Е).

Для характеристики доверия «цель обеспечения доверия» сравнение дает ответы на следующие вопросы:

- предусматривает ли метод определение цели обеспечения доверия;
- каким методом была определена эта цель;
- как эта цель достигается?

Если метод не определяет цель обеспечения доверия или если эта цель не соответствует требованиям органа по обеспечению доверия, то для определения цели рекомендуется оценка риска или верификация обоснованности. При необходимости рекомендованная цель обеспечения доверия может быть расширена для отражения практической деятельности в промышленности и управлении.

Примечания

1 Сама по себе оценка риска может быть гарантирована, например, оценкой персонала, проводящего оценку риска на основе своего опыта, его уровня подготовки и/или других факторов, например, места, где персонал проходил подготовку.

Цель обеспечения доверия может определять характеристики, которыми должен обладать предполагаемый метод обеспечения доверия, и/или способ представления доверия, таким образом уменьшая число методов, которыми можно получить доверие.

2 Соответствующие концепции и процессы выражены в существующих стандартах и технических отчетах по безопасности ИТ, таких, например, как ИСО/МЭК 13335, ИСО/МЭК 27002, ИСО/МЭК 21827 и ИСО/МЭК 15408.

5.4.2 Целевая аудитория

Настоящий стандарт адаптирован для предоставления руководства по трем типичным ситуациям в соответствии с разделом 6. Эта характеристика доверия имеет следующие категории:

- доверие к разработке: разработка продуктов ИКТ, например, в области безопасности;
- доверие к интеграции: закупка продуктов и их компоновка в систему ИКТ, например, в соответствии с определенной политикой безопасности;
- доверие к функционированию системы информационных и коммуникационных технологий, например, в соответствии с политикой безопасности данной организации.

Кроме того, сравнение может дать ответ на следующие вопросы:

- для каких компаний предназначен метод;
- для каких ролей в рамках организации предназначено содержимое;
- насколько метод применим к общепринятым структурам предприятий?

5.4.3 Характеристики

Подход к обеспечению доверия, определение которому приведено в ИСО/МЭК ТО 15443-1 и ИСО/МЭК ТО 15443-2, рассматривается и разъясняется в 6.1 настоящего стандарта.

Кроме того, сравнение может дать ответы на следующие вопросы:

- насколько метод применим к общепринятым структурам предприятий;
- каково назначение рассматриваемого метода;
- какие методологические элементы он содержит?

Примечание — Общее руководство по выбору приемлемого подхода к обеспечению доверия для достижения конкретной цели по обеспечению доверия см. в 5.1.

5.4.4 Разносторонность

Возможность повторного использования частей процедуры оценки позволяет амортизировать стоимость работ, выполненных в отношении какого-либо продукта, например, будущего оценивания. В особых случаях стоимость работ следует амортизировать с помощью, например, специальной версии продукта в отличие от семейства существующих или будущих объектов.

Кроме того, сравнение может дать ответ на следующие вопросы:

- какова взаимосвязь между объемом работ и стоимостью применения;
- какой величиной и сложностью исследуемого объекта можно оперировать;
- можно ли это контролировать путем применения разных степеней детализации?

5.4.5 Своевременность

Кроме того, сравнение может дать ответ на следующие вопросы:

- отражает ли настоящая версия метода новейшие технологии;
- как обеспечивается в случае необходимости регулярное обновление метода;
- что такое рыночное признание и каковы его движущие силы?

5.4.6 Завершенность

Кроме того, сравнение может дать ответ на следующие вопросы:

- образуют ли критерии по основному вопросу закрытый исчерпывающий каталог элементов или охватывают только выбранные аспекты;
- для какого уровня безопасности адаптирован релевантный каталог соответствующих критериев;
- рассматривает ли метод цели безопасности только с помощью полного исчерпывающего каталога элементов или охвачены только выбранные аспекты;
- для какого уровня безопасности адаптирован метод?

5.4.7 Издержки при внедрении/объем работ по внедрению

Кроме того, сравнение может дать ответ на следующие вопросы:

- чего надо ждать в отношении объема работ и издержек при применении данной системы критериев безопасности ИТ к типичным сценариям?

Характеристики доверия являются фактическим источником доверия и могут иметь соответствующую систему показателей. Характеристики доверия включают в себя стоимость и различные качественные аспекты, такие, например, как строгость, надежность, воспроизводимость, эффективность и т. д.;

- какой метод обеспечения доверия является правильным для имеющейся проблемы доверия и как его применять? Для ответа на этот вопрос надо понять преимущества методов обеспечения доверия, исходя из доверия, приобретенного этими методами наряду со связанными с ними издержками. Другими словами, свойства доверия, содействующие определению его значимости, должны измеряться и сравниваться после идентификации альтернатив.

Оценка является дополнением доверия, для получения которого требуются дополнительное время, персонал и значительные расходы.

Таким образом, органу по обеспечению доверия следует логически обосновать целесообразность использования такой оценки.

Доверие служит причиной издержек, и поэтому их величина может быть оспорена.

При определении стоимости конкретного подхода к обеспечению доверия важно учитывать конкретное окружение, в котором действует орган обеспечения доверия. Стоимость определяется конкретными требованиями органа обеспечения доверия, для которого она определяется, и должна соответствовать потребностям доверия, уделяя особое внимание конечному пользователю доверия.

При наличии альтернатив доверия надо определить относительную стоимость методов обеспечения доверия.

Политика безопасности или культура организации может определять форму доверия. Форма доверия может быть продиктована суммой, которую организация готова заплатить, или какими-то другими значимыми критериями, например, политическим указом или законодательством. Критерии предназначены для получения данных о том, почему пользователь готов заплатить за доверие и применительно к чему организация намерена оказать доверие, которое она оплачивает.

Примечание — При рассмотрении методов обеспечения доверия первым шагом может стать определение причины готовности пользователя заплатить за доверие и то, для какой цели он намеревается применить это доверие. Определение причины готовности пользователя заплатить за доверие может послужить причиной отказа от других методов обеспечения доверия, а также в значительной степени воздействовать на достижение целей обеспечения доверия.

5.4.8 Поддержка инструментальными средствами

Сравнение может дать ответ на вопрос:

существуют ли какие-либо инструменты поддержки пользователя при применении рассматриваемого метода?

5.4.9 Сфера действия криптографии

Сравнение может дать ответ на вопрос:

содержит ли рассматриваемая система критериев безопасности ИТ какие-либо положения или руководство по криптографическим процедурам или алгоритмам?

5.4.10 Оценка и сертификация

Еще большее увеличение доверия достигается при определении и/или сертификации оценки результата доверия по какой-либо признанной схеме сертификации.

Сравнение этой характеристики доверия может дать ответ на следующие вопросы:

- существует ли для метода квалификационная и/или сертификационная система;
- подходит ли метод для продуктов или итоговых решений;
- полагаются ли на независимых оценщиков при выдаче сертификатов, или сертификация обеспечивается специализированным органом или организацией;
- подлежит ли сам орган по сертификации оценке и аттестации? Каковы правила аттестации;
- имеются ли соглашения о взаимном признании сертификатов;
- каково воздействие успешного оценивания сертификации, то есть какова потенциальная возможность удовлетворения требованиям заказчика или администрации;
- какова зрелость схемы?

Примечание — Методы обеспечения доверия со связанными с ними схемами сертификации представлены в приложении А.

5.4.11 Надежность и признание

Надежность метода обеспечения доверия и, возможно, связанная с ним схема сертификации оказывают сильное влияние на принятие результата его применения пользователем.

Надежность метода обеспечения доверия определяется его известностью на рынке, поддержкой заслуживающей доверия организацией, принятием правительством или поддержкой с его стороны.

Для глобальных пользователей признание должно быть получено на международном уровне.

6 Руководство

Для любого эффективного руководства требуются обобщение, упрощение и сосредоточенность. Для уменьшения числа методов, сравниваемых со значимыми и приемлемыми методами, анализируются три типичные ситуации. Эти ситуации называются «проблемы обеспечения доверия» и определяются следующим образом:

- доверие к разработке — разработка продуктов ИКТ обычно с учетом целей безопасности;
- доверие к интеграции — закупка и компоновка продуктов в систему информационных и коммуникационных технологий обычно для достижения целей или политики безопасности;
- доверие к функционированию системы ИКТ в соответствии с политикой безопасности данной организации.

Каждая проблема имеет свои особенности и отличия.

Концепцию проблемы обеспечения доверия можно легко представить наглядно, используя концепции жизненного цикла и подхода к обеспечению доверия, разработанные в ИСО/МЭК ТО 15443-1, наполненные содержанием в ИСО/МЭК ТО 15443-2 и дополненные этапом концепция/спецификация в соответствии с 4.2.3 настоящего стандарта.

Знание различных методов обеспечения доверия и подходов к ним позволяет органу обеспечения доверия определять методы, соответствующие бизнес-требованиям и проблеме обеспечения доверия. Важным аспектом, который следует иметь в виду, является конечная цель обеспечения доверия: получение уверенности заинтересованных сторон независимо от применяемого(ых) метода(ов).

Ввиду сложности требований безопасности, разнообразия методов обеспечения доверия и различия между ресурсами и культурами организаций рекомендация, приведенная в настоящем стандарте, будет носить качественный и обобщенный характер.

В настоящем стандарте руководство сосредоточено на нескольких методах, испытанных и повсеместно принятых для этих трех ситуаций с обеспечением доверия.

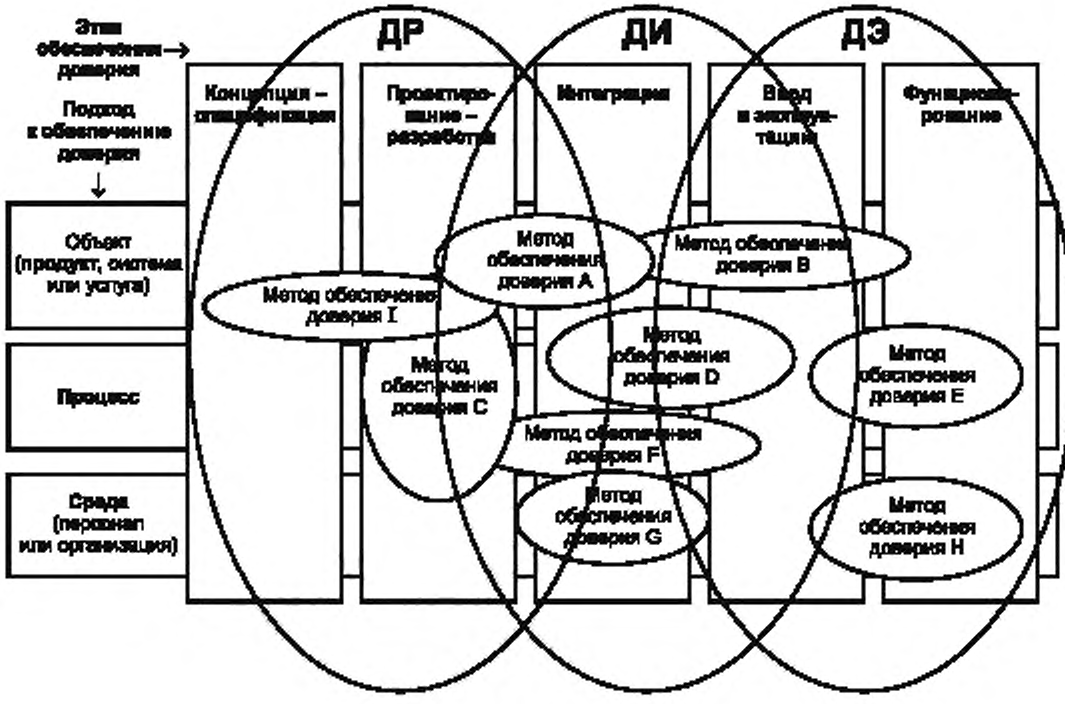


Рисунок 5 — Обеспечение доверия

6.1 Доверие к разработке (ДР)

ДР может применяться во время разработки продукта, системы или услуги. Теоретически разработка:

- начинается с концепции;
- развивает концепцию в спецификацию, которая затем материализуется в процесс разработки;
- завершается получением продукта с заданными требованиям, успешной демонстрацией заданных характеристик продукта или валидацией его свойств в целевой среде.

Требования доверия могут специфицироваться, а методы обеспечения доверия — выбираться и применяться в соответствии с требованиями ДР.

6.1.1 Цель обеспечения доверия

Цель обеспечения доверия надо определять так, как показано на примере в приложении Е. В качестве альтернативы методы обеспечения доверия можно выбирать — комбинировать для обеспечения этапа концепции с учетом определения целей безопасности с необходимым уточнением.

Для ДР целями безопасности могут быть:

a) для отдельного продукта — политика безопасности;

b) для серийного продукта — общие цели безопасности, принятые в целевом коллективе пользователей.

6.1.2 Существующие методы

Некоторые существующие методы обеспечения доверия для ДР в общих чертах приведены в приложении А.2. Другие методы обеспечения доверия можно выбрать в соответствии с ИСО/МЭК ТО 15443-2.

Методы, приведенные в приложении А.2 настоящего стандарта, приведены в соответствии с ИСО/МЭК 15408, ИСО/МЭК 19790, ИСО/МЭК 21827, ИСО/МЭК 27001 и ИСО 9000. Основные аспекты этих методов приведены в приложении В настоящего стандарта.

6.1.3 Основные аспекты

При высоких требованиях доверия к безопасности необходимо оценивать стойкость и корректность функций безопасности. В этом случае выбранный метод обеспечения доверия должен содержать (ссылаться на них или дополняться ими) процедуры оценки, обеспечивающие стойкость и корректность функций безопасности.

6.1.3.1 Верификация стойкости

Верификация стойкости является обеспечением противостояния таких критических механизмов, как шифрование, хэширование, алгоритмы паролей противодействия атакам, в особенности грубым атакам.

6.1.3.2 Верификация корректности

Целью верификации корректности является обеспечение правильности выполнения этапов процесса разработки от функциональных требований до эксплуатации системы. Следовательно, верификация корректности относится к оценке согласования нижнего уровня проектирования (включая внедрение) с более высокими уровнями. Эти действия не связаны с угрозами или целями безопасности, а только с должным проведением разработки. Они тесно связаны с верификацией качества или функцией обеспечения доверия к качеству.

Верификация корректности является процессом подтверждения соответствия системы спецификации и проекта нижнего уровня, и соответствия спецификации более высоким уровням проекта. Эта верификация подразумевает проверку соответствия требований к системе спецификации, поскольку требования сформулированы способом, позволяющим проводить прямую проверку соответствия спецификации. Верификация корректности также включает в себя методику испытаний наряду с неформальным или формальным конструкторским анализом и средствами верификации. Строгость верификации корректности зависит от точного и однозначного представления различных уровней проектирования. Для формальных методов анализа и верификации при представлении проекта требуются более высокие уровни точности, что ограничивает число методов, которые могут использоваться для описания проекта. Проект не должен быть неопределенным, в особенности при высоких степенях (уровнях) уверенности в правильности системы.

6.2 Доверие к интеграции (ДИ)

ДИ может применяться при интеграции нескольких продуктов, обычно многих продуктов различного происхождения и с разными результатами доверия, в систему.

Многие продукты представляют собой готовую и проверенную коммерческую продукцию с результатами доверия, но часто эти результаты не доступны по запросу пользователя. Следовательно, в большинстве случаев пользователю как последней инстанции обеспечения доверия к разворачиваемой системе приходится иметь дело со сложной ситуацией в отношении обеспечением доверия.

Интегратор коммерческой системы, разрабатывающий какую-либо систему, обычно поставляет и, следовательно, учитывает только часть развернутой системы, и следовательно, перед ним стоит менее сложная задача, если только он не отвечает за систему в целом.

Обычно для сложных ситуаций, связанных с интеграцией, требуются дополнительные продукты или меры безопасности, что может создать дефицит доверия. Дефицит доверия необходимо заполнить для того, чтобы достигнуть установленных целей безопасности.

Для получения необходимой уверенности может потребоваться валидация абстрактного или сложного (комплексного) результата доверия в действии.

Примечание — В ИСО/МЭК ТО 15443 не охвачены аспекты способности системы к компоновке и доверия к ней — даже если каждая подсистема в отдельности соответствует своим функциональным требованиям и требованиям безопасности, общая составная система может не функционировать должным образом и не быть безопасной. Аспект доверия к способности системы к компоновке может подвергаться дополнительному системному тесту и валидации.

6.2.1 Цель обеспечения доверия

Цель ДИ должна определяться в соответствии с приложением Е. Целями ДИ являются:

- для отдельной системы — политика безопасности системы или профиль защиты;
- для серийных систем — общие цели безопасности, принятые в целевом коллективе пользователей;
- для очень сложной пользовательской системы — ранее существовавшая политика безопасности организации.

В качестве альтернативы имеющиеся методы могут выбираться/комбинироваться в интересах определения целей безопасности ДИ с необходимым уточнением.

6.2.2 Существующие методы

Некоторые существующие методы обеспечения ДИ в общих чертах изложены в приложении А. Другие методы допускается выбрать в соответствии с ИСО/МЭК ТО 15443-2.

Методы, представленные в приложении А, взяты из ИСО/МЭК 21827 и ИСО 9000.

Примечание — К перечню существующих методов обеспечения ДИ можно добавить ИСО/МЭК 19791, в котором соответствующее руководство не представлено.

6.2.3 Основные вопросы

6.2.3.1 Применение комбинации терминов

Для получения результата, соответствующего цели обеспечения доверия, исходя из соображений полноты (завершенности) продукта интегратору коммерческих комплексных продуктов могут потребоваться несколько методов обеспечения доверия.

Обычно интегратор свободен в выборе конкретных методов обеспечения доверия. Текущие и будущие расходы на создание продукта влияют на этот выбор наряду с ожиданиями заказчика и рыночными факторами.

Выбор методов может основываться на анализе свойств методов обеспечения доверия в том виде, в каком они представлены в ИСО/МЭК ТО 15443-2. Целью настоящего стандарта является сравнение основных признаков метода (аргументы «за» и «против») для выполнения требований интегратора.

Стратегия формирования комбинированного метода обеспечения доверия представлена на примере изучения конкретного случая, приведенного в приложении D.1.

6.2.3.2 Использование разных результатов доверия

ДИ всегда подразумевает интеграцию нескольких (обычно многих) продуктов в качестве компонентов в завершенную работоспособную и/или разворачиваемую систему вместе с пакетом требований доверия для этой системы.

Для создания такого пакета интегратору следует:

- скомпилировать ранее существовавшее доверие идентичных или аналогичных методов обеспечения из различных источников;
- преобразовать и гармонизировать доверие, полученное различными методами;
- интерпретировать неопределенные результаты доверия;

- добавить несуществующее доверие;

- объединить все вышеуказанное.

Результаты доверия необходимо пересматривать в контексте ситуации, для которой были установлены цели безопасности и было проведено последующее оценивание доверия.

Может потребоваться формирование ограничений для избежания непреднамеренного использования доверия для непредусмотренных целей.

Конечным результатом доверия должна быть уверенность в том, что «система безопасна» для применения в рассматриваемой ситуации.

6.2.3.3 Сравнение и интеграция доверия

Высокая степень уверенности как результат интегрированного доверия к системе тесно связана с хорошим знанием основного процесса обеспечения доверия, каждого отдельного компонента доверия исходя из:

- входных данных, приводящих к обеспечению доверия;

- логического обоснования и концепции соответствующего метода обеспечения доверия;

- объединенного результата доверия.

Меньшая степень уверенности получается при сравнении результатов доверия путем оценивания только входных данных и последующих выходных данных, считая каждый метод «черным ящиком».

Наименьшая степень уверенности может быть получена с учетом только результатов доверия. Однако такая степень уверенности может быть единственным выбором, доступным для небольших организаций или применяемым в системах с незначительными активами с низкой степенью риска.

6.2.3.4 Сравнение результатов доверия

Поскольку большинство результатов доверия не могут быть сравнимы непосредственно, они должны быть упорядочены.

Методы обеспечения доверия, а также связанные с ними результаты доверия могут быть более или менее строгими:

- строгие (точные) методы обеспечения доверия основаны на конкретной методологии, что приводит к измеряемым и воспроизводимым результатам, даже если они являются эмпиричными и уникальными для самого метода обеспечения доверия;

- для менее строгих методов обеспечения доверия обычно конкретная методология отсутствует, и их вряд ли можно воспроизвести с идентичными результатами. Такие результаты, как, например, оцененная репутация организации, могут считаться «неопределенными» и субъективными.

В случае с результатами применения только строгих методов обеспечения доверия сравнение результатов сводится к согласованию шкал. Большинство подобных методов имеют определенную форму «шкалы доверия», даже если эта шкала содержит только одно порядковое число, то есть результат отбраковки. Должна быть возможность идентификации путем анализа точки пересечения или относительности между шкалами строгих методов обеспечения доверия и сравнения результатов после соответствующего согласования шкал.

В случае с результатами применения менее строгих методов обеспечения доверия в сочетании с результатами применения строгих методов обеспечения доверия объединение результатов может быть более сложным, безусловно, более интуитивным, субъективным и, как следствие, может стать предметом оспаривания или обсуждения.

6.2.3.5 Формирование результатов доверия

При наличии затруднений с объединением результатов доверия, в особенности результатов применения менее строгих методов обеспечения доверия, эти методы можно рациональным способом скомбинировать.

Принцип комбинирования заключается в гарантировании того, что:

- собраны поддерживающие результаты доверия;

- все собранные результаты доверия в совокупности способствуют получению и повышению надежности требуемого составного результата;

- доверие серьезно не умаляет вклад, внесенный другими результатами доверия (иначе цель комбинирования становится недействительной).

Процесс оценивания и тестирования систем показан на рисунке 6.

В случаях с противоречивыми результатами доверия следует принимать рациональные решения об использовании источника доверия. Принятие такого решения может быть трудно осуществимым, если наряду с результатом в него не включено обоснование использования источника доверия.

Комбинирование следует ограничивать точным использованием результатов доверия по назначению. Такое ограничение должно быть сформулировано для избежания непреднамеренного использования пакета требований доверия по нецелевому назначению.

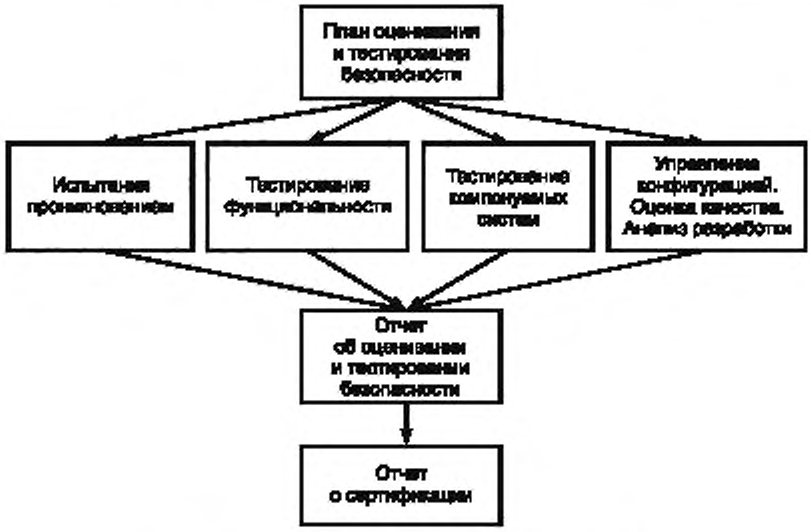


Рисунок 6 — Оценивание и тестирование систем

6.2.3.6 Проверка достоверности доверия

ДИ может включать в себя доверие к перемещению продукта информационных и коммуникационных технологий от поставщика к пользователю, то есть от стадии разработки/интеграции к эксплуатации.

Целью деятельности по валидации доверия является выявление критических проблем с безопасностью, которые могут оставаться после демонстрации соответствия системы ее спецификации.

Требования безопасности можно характеризовать как высокоуровневые цели, не всегда преобразуемые непосредственно в точные технические требования, следовательно, соответствие нельзя продемонстрировать действиями визуальной верификации правильности.

Валидация доверия может быть единственным средством доказательства эффективности функций обеспечения безопасности и охвата побочных эффектов системы, неохваченных или несоответствующих аспектов.

Валидация доверия включает в себя оценку уязвимостей, испытание проникновением, анализ скрытых каналов, надежность анализа функций обеспечения безопасности, анализ злоупотреблений, валидацию допущений дефектов и испытание на прочность.

6.3 Доверие к эксплуатации (ДЭ)

ДЭ имеет место при эксплуатации системы ИКТ или совокупности систем ИКТ и активного управления безопасностью в определенной общей безопасной среде, включающей в себя людей и оборудование.

Обычно орган по обеспечению доверия имеет дело с действующей системой, работающей для поддержания деловой деятельности организации. Большинство продуктов обеспечения доверия являются готовыми, и органу по обеспечению доверия приходится в большинстве случаев иметь дело со сложной ситуацией с доверием. Следовательно, в любом руководстве необходимо учитывать множество ранее существующих или, возможно, несуществующих или неопределенных характеристик доверия, присущих каждому отдельному компоненту продукта. В этой ситуации обычно требуются дополнительные продукты или меры безопасности для компенсации недостающего уровня доверия, соответствующего необходимой цели обеспечения доверия.

6.3.1 Цель обеспечения доверия

Цель обеспечения ДЭ определяют, например, в соответствии с приложением Е. В качестве альтернативы допускается выбрать и объединить имеющиеся методы обеспечения доверия, чтобы получить этап концепции, позволяющий определить цели безопасности с требуемым уточнением.

При обеспечении ДЭ целями безопасности могут быть:

- в больших организациях — политика безопасности;
- в небольших организациях — цели безопасности, принятые в целевых коллективах пользователей в качестве основных;
- в любых других конкретных случаях — цели безопасности, определенные посредством оценивания риска.

В целях соответствия требованиям реального окружения (то есть нескольких компонентов аппаратных средств и программного обеспечения, услуг по обеспечению безопасности, аспектов среды или комбинации этих элементов) руководство по обеспечению доверия для этапа эксплуатации должно быть приемлемым для сложных систем, составленных из многих элементов.

6.3.2 Имеющиеся методы

Некоторые методы обеспечения ДЭ в общих чертах приведены в приложении А. Другие можно выбрать по ИСО/МЭК ТО 15443-2.

Методы, приведенные в приложении А настоящего стандарта, представлены в ИСО/МЭК 27001, COBIT, Руководстве по основам ИТ и ИСО 9000. Главные аспекты этих методов приведены в приложении В настоящего стандарта.

6.3.3 Основные вопросы

6.3.3.1 Области безопасности

Существует много областей безопасности, некоторые из них считаются устаревшими, но все еще довольно часто используются (см. таблицу 8). Эти области могут иметь цели безопасности и каталоги мер измерения. Необходимо убедиться в охвате этих областей в соответствии с современной оценкой риска.

Таблица 8 — Области безопасности

Область безопасности
Административная и организационная безопасность
Безопасность персонала
Физическая безопасность и безопасность среды
Безопасность аппаратных средств
Безопасность программного обеспечения
Безопасность функционирования
Коммуникационная безопасность
Безопасность передачи
Криптографическая безопасность
Безопасность работы радиоэлектронных устройств
Сетевая безопасность

6.3.3.2 Области управления безопасностью

В таблице 9 представлен пример развернутого перечня доменов (областей управления безопасностью). Имеющиеся методы обеспечения доверия можно сопоставить с этим перечнем для проверки того, достаточно ли подробно освещены соответствующие области.

Таблица 9 — Области управления безопасностью

Домен	Домен COBIT	Процесс
Планирование и организация	PO1	Определяет стратегический план ИТ
	PO2	Обеспечивает соответствие внешним требованиям
	PO3	Управляет людскими ресурсами
	PO4	Передает цели управления и направление
	PO5	Управляет инвестициями в ИТ
	PO6	Определяет техническое направление
	PO7	Дает определение организации и взаимосвязям ИТ
Приобретение и внедрение	PO8	Дает определение информационной структуре
	PO9	Оценивает риски
	PO10	Управляет проектами
	PO11	Управляет качеством
	AI1	Управляет изменениями
	AI2	Устанавливает и аккредитует системы
	AI3	Приобретает и поддерживает инфраструктуру технологий
	AI4	Разрабатывает и поддерживает процедуры
	AI5	Приобретает и поддерживает прикладное программное обеспечение
	AI6	Идентифицирует автоматизированные решения
Доставка и поддержка	DS1	Управляет работой
	DS2	Управляет оборудованием
	DS3	Управляет данными
	DS4	Управляет проблемами и инцидентами
	DS5	Управляет конфигурацией
	DS6	Оказывает помощь и выдает рекомендации заказчикам
	DS7	Обучает и подготавливает пользователей
	DS8	Определяет и распределяет расходы
	DS9	Обеспечивает безопасность работы систем
	DS10	Обеспечивает непрерывное обслуживание
	DS11	Управляет функционированием и производственными мощностями
	DS12	Управляет услугами третьей стороны
	DS13	Дает определение уровням обслуживания и управляет ими
Мониторинг	M1	Предусматривает независимый аудит
	M2	Получает независимое доверие
	M3	Оценивает адекватность внутреннего контроля
	M4	Проводит мониторинг процессов

6.3.3.3 Зрелость (развитость) доверия к эксплуатации

Реализацию политики безопасности в организации можно исследовать на предмет зрелости. В таблице 10 приведено описание зрелости ДЭ. Сертификация (подтверждение) зрелости ДЭ может стать ценным дополнением к доверию.

Таблица 10 — Описание уровней зрелости доверия к эксплуатации

Уровень зрелости ДЭ	Описание
1	Все имеющиеся специфические или общие политики
2	Управляемый и принятый конкретный или общий риски
3	Определенные, внедренные и управляемые меры
4	Оцененные, исправленные и поддержанные меры
5	Сертифицированные меры и их поддержание

Приложение А
(справочное)

Сравнения данных таблицы

Содержание настоящего приложения было сформировано из общедоступного материала.

А.1 Методы и целевые группы пользователей

Для идентификации альтернатив сформирована сводная таблица. Она характеризует различные методы обеспечения доверия в отношении того:

- ориентированы ли они на организационные или технические аспекты;
- ориентировано ли их использование на продукты или общие системы;
- предназначены ли они для поставщика или пользователя?

Таблица А.1 — Методы и целевые группы пользователей

Ключ: P: основная целевая группа; S: вторичная целевая группа; X: любая организация		ИСО/МЭК 15408	ИСО/МЭК 19790	ИСО/МЭК 21827	ИСО/МЭК 13335	ИСО/МЭК 27001, ИСО/МЭК 27002	Руководство по защите основы ИТ	COBIT	ИСО 9000
Тип предприятия	Поставщик аппаратных средств	S	P	P	S		S		X
	Поставщик программного обеспечения	P	P	P	S	S	S		X
	Оператор сервера		S	P	S	S		S	X
	Сетевой провайдер		S	P	S	P	P	S	X
	Поставщик онлайновой информации			P	S	P	P		X
	Предприятие в качестве пользователя		S	S	P	P	P	P	X
Роль в рамках предприятия	Управление				P	P	S	P	P
	Управление проектом	P	P	P	P	P	P	P	P
	Ответственный за безопасность ИТ	P	P	P	P	P	P	S	S
	Управление ИТ	S	S	P	P	P	P	P	S
	Администратор		S			S	P	S	S
	Аудитор				S	S	S	P	S

Основные схемы сертификации

Некоторые методы обеспечения доверия имеют ассоциированные схемы сертификации для оценки результата доверия (см. таблицу А.2).

Таблица А.2 — Основные схемы сертификации

Подход к обеспечению доверия	Критерий оценки	Методология оценки	Аттестация персонала и/или оборудования	Схема оценки
Продукт	ИСО/МЭК 15408	ИСО/МЭК 18045	Аттестация?	Национальные органы по сертификации с международным взаимным признанием

Окончание таблицы А.2

Подход к обеспечению доверия	Критерий оценки	Методология оценки	Аттестация персонала и/или оборудования	Схема оценки
Процесс	ИСО/МЭК 21827	SSAM	SSO	Национальные/международные органы по сертификации, например, ISSEA
Среда (эксплуатация ИТ)	ИСО/МЭК 27001		ИСО/МЭК 27006	
Среда (организация)	ИСО 9000		Национальные/международные органы по сертификации	Национальные/международные органы по сертификации

А.2 Существующие методы обеспечения доверия

Методы, представленные в приложении В, и выводы в отношении проблем пользователя, приведенные в 5.1.4, представлены в таблице А.3.

Таблица А.3 — Существующие методы обеспечения доверия

	Доверие к разработке	Доверие к интеграции	Доверие к эксплуатации
Доверие к продукту	По ИСО/МЭК 15408, По ИСО/МЭК 19790		
Доверие к процессу	По ИСО/МЭК 21827	По ИСО/МЭК 21827	По ИСО/МЭК 27001, COBIT, Основа ИТ
Доверие к среде	По ИСО/МЭК 27001, ИСО 9000	По ИСО/МЭК 27001, ИСО 9000	По ИСО/МЭК 27001, ИСО 9000

Приложение В
(справочное)

Характеристики доверия выбранных методов

Содержание настоящего приложения было сформировано из общедоступного материала.

В.1 ИСО/МЭК 15408

В основу ИСО/МЭК 15408 положены общие критерии оценки безопасности ИТ. Основные положения методологии по ИСО/МЭК 15408 подробно изложены в ИСО/МЭК ТО 15443-1.

В ИСО/МЭК 15408 границы оцениваемого определены в разделе «Объект оценки».

Объект оценки имеет четкое определение и представляет заданные функциональные возможности продукта, связанные с безопасностью.

Объект оценки не обязательно представлен готовым продуктом. Тем не менее в целях упрощения в настоящем разделе объект оценки называется «продуктом».

В.1.1 Цель обеспечения доверия

ИСО/МЭК 15408 допускает сравнимость результатов независимых оценок безопасности. Данный стандарт делает сравнимость возможной путем предоставления общепринятого набора требований к функциональным возможностям продуктов, связанным с обеспечением безопасности, и к мерам измерения доверия, примененным к продуктам при оценивании безопасности. Процедура оценивания определяет степень уверенности в том, что функциональные возможности продуктов, связанные с обеспечением безопасности, и меры измерения, примененные к доверию к этим продуктам ИТ, соответствуют общепринятому набору требований. Результаты оценивания могут помочь пользователям в определении того, соответствуют ли эти продукты ИТ требованиям безопасности.

ИСО/МЭК 15408 полезен также в качестве руководства по разработке, оцениванию и/или закупке продуктов с функциями обеспечения безопасности.

ИСО/МЭК 15408 предусматривает защиту от трех типов сбоев в системе безопасности: несанкционированное раскрытие, модификация или невозможность использования. Категории защиты, связанные с этими тремя типами сбоев в системе безопасности, обычно называются «конфиденциальность», «целостность» и «доступность» соответственно. Стандарт можно также применять к риску, являющемуся результатом человеческой деятельности (вредоносной или любой другой), или к риску, являющемуся результатом деятельности, не связанной с человеком. ИСО/МЭК 15408 может также применяться к другим областям ИТ, но не претендует на компетентность в этих областях ИТ.

ИСО/МЭК 15408 может использоваться также применительно к функциям безопасности, внедренным в аппаратные, программно-аппаратные средства или программное обеспечение.

В.1.2 Целевая аудитория

Существуют три группы, заинтересованные в оценивании характеристик безопасности объекта оценки: пользователи, разработчики и оценщики. Все они считаются главными пользователями

В.1.2.1 Пользователи

Пользователи могут использовать результаты оценивания для принятия решения о соответствии продукта предъявляемым требованиям безопасности. Обычно эти требования идентифицируются в результате как в отношении оценки риска, так и направления политики. ИСО/МЭК 15408 представляет пользователям, в особенности группам и коллективам пользователей, независимую от реализации структуру под названием «профиль защиты» («ПЗ»), в которой изложены их конкретные требования безопасности.

В.1.2.2 Разработчики

ИСО/МЭК 15408 предназначен для содействия разработчикам в подготовке оценивания их продуктов и определении требований безопасности, которым эти продукты должны соответствовать. Требования безопасности содержатся в зависимой от реализации конструкции, называемой «задание безопасности» («ЗБ»). ЗБ может иметь в основе один или несколько профилей защиты (с требованиями безопасности, как было определено ранее).

Затем ИСО/МЭК 15408 может применяться для определения обязанностей и мер по поддержке свидетельства, необходимого для поддержки оценивания продукта в отношении этих требований. Он также дает определение содержанию и представлению этого свидетельства.

В.1.2.3 Оценщики

ИСО/МЭК 15408 содержит критерии, предназначенные для применения оценщиками при формировании заключений о соответствии продуктов требованиям их безопасности. В ИСО/МЭК 15408 описывается совокупность основных действий, которые оценщик должен выполнять, и функциональных требований безопасности (ФТБ), в соответствии с которыми должны выполняться эти действия. Следует отметить, что ИСО/МЭК 15408 не специфицирует процедуры выполнения этих действий.

В.1.2.4 Другие заинтересованные стороны

ИСО/МЭК 15408 может также использоваться в качестве ссылочного материала для всех сторон, заинтересованных в безопасности ИТ или несущих ответственность за нее. Некоторые дополнительные заинтересованные группы, которые могут извлечь из него пользу, включают в себя:

- лиц, ответственных за систему и ее безопасность;

- внутренних и внешних аудиторов;
- архитекторов и проектировщиков безопасности, ответственных за спецификацию характеристик безопасности продуктов,
- аттестующих лиц, ответственных за принятие решения по использованию ИТ в определенной среде;
- спонсоров оценивания, ответственных за запрос и поддержку оценивания;
- органы оценки, ответственные за управление программами оценивания безопасности ИТ и контроль за их выполнением.

В.1.3 Характеристики доверия

Уверенность в безопасности ИТ можно обеспечить мерами, принимаемыми в ходе процессов разработки, оценивания и эксплуатации. Продукт специфицируется заданием по безопасности. Проектно-конструкторская информация предоставляется неформально, полуформально или формально.

Подробные инструкции по испытанию доверия представлены в ИСО/МЭК 18045 — аналоге «Общей методологии оценки» и предназначены для обеспечения последовательного проведения оценивания и предоставления воспроизводимых результатов.

Формальные структуры созданы за пределами области действия ИСО/МЭК 15408 для управления действиями по оцениванию, осуществляемыми независимыми тестирующими организациями, и наблюдения за ними.

В.1.4 Разносторонность

ИСО/МЭК 15408 предлагает наборы как функциональных требований, так и требований доверия, выбираемых пользователем в соответствии со своими потребностями. ИСО/МЭК 15408 также содержит семь предопределенных пакетов требований доверия EAL1-7 для облегчения выбора пользователем и признания на рынке.

В.1.5 Своевременность

Группы методов обеспечения доверия являются относительно стабильными и редко модифицируются. Предыдущие системы критериев безопасности (TCSEC, ITSEC и т. д.) были заменены в ИСО/МЭК 15408, первая редакция которого была опубликована в 1999 г. с последующей редакцией в 2005 г.

В.1.6 Завершенность

Данная характеристика специфицирована в ЗБ.

В.1.7 Стоимость реализации/объем работ по реализации

Объем работ по оцениванию одного из наборов критериев и расходы на них возрастают при специфицировании большей степени доверия.

Промежуток времени, требуемый для оценивания, может зависеть от нескольких факторов, включая:
- способность повторного использования предыдущей работы,
- зрелость технологического процесса организации-разработчика;
- зрелость продукта, опыт лаборатории;
- принятую стратегию оценивания (например, выполнение оценивания параллельно разработке);
- ресурсы, доступные для органа по валидации (схема).

Стоимость формального оценивания включает в себя следующие элементы:
- оплата схем (изменяется от схемы к схеме);
- оплата лаборатории (изменяется от лаборатории к лаборатории);
- внутренняя работа по контрактам и незначительные модификации, требуемые для оценщика;
- разработка задания по безопасности.

Кроме того:
- некоторые документы, такие как модель политики безопасности и анализ уязвимостей, редко предоставляются разработчиком;
- процедура оценивания часто выявляет уязвимости продукта, требующие устранения. Эти уязвимости могут ранжироваться от незначительных до серьезных.

В.1.8 Поддержка инструментальными средствами

На коммерческом рынке имеются лишь несколько инструментальных средств. Имеются вспомогательные документы, например, ИСО/МЭК ТО 15446 «Руководство по разработке профилей защиты и заданий по безопасности».

В.1.9 Сфера применения криптографии

Формальное оценивание не включает в себя оценку качества выбранных криптографических алгоритмов. Однако правильность внедрения выбранного алгоритма можно оценить.

В.1.10 Оценка и сертификация

Оценивание с использованием методологий, соответствующих требованиям ИСО/МЭК 15408, может проводиться испытательными лабораториями. На примере системы оценки, определенной Советом по разработке Общих критериев, лаборатории должны сертифицироваться в соответствии с ИСО/МЭК 17025, а результаты испытаний могут документироваться путем опубликования отчета о сертификации и выдачи сертификата. Сертификаты выдаются аккредитованными органами по сертификации (национальные схемы) и публикуются на международном уровне.

В.1.11 Убедительность и признание

ИСО/МЭК 15408 является международным стандартом, который соответствует стандартам Общих критериев, опубликованным Советом по разработке Общих критериев.

ИСО/МЭК 15408 и Общие критерии имеют широкое признание и в достаточной степени убедительны.

В.2 ИСО/МЭК 19790

В.2.1 Цель обеспечения доверия

Документ «Требования безопасности для криптографических модулей» был изначально опубликован как федеральный стандарт по обработке информации (FIPS) 140-2 Национальный институт стандартов и технологий (НИСТ) США и применялся для спецификации криптографических модулей. НИСТ и Институт безопасности коммуникаций (CSE) Канады разработали в июле 1995 г. совместную программу верификации криптографических модулей (CMVP), которая использует испытательную схему и дополняет FIPS 140-2 документацией, включающей в себя «Руководство по реализации FIPS 140-2» и «Производные требования к испытаниям FIPS 140-2», предназначенные для поддержки и разъяснения FIPS, а также процесса испытаний и валидации.

Проверка соответствия FIPS проводится лабораториями, аккредитованными национальной программой добровольной аккредитации лабораторий (NVLAP), и по стандартам Канады. CMVP анализирует результаты проверок на соответствие и при успешном завершении анализа проверяет достоверность и выдает аттестационные сертификаты проверенным криптографическим модулям. На сегодняшний день было выдано более 650 сертификатов более чем для 1000 проверенных модулей.

Подгруппа требований FIPS 140-2 была опубликована в 2006 г. как ИСО/МЭК 19790.

В.2.2 Целевая аудитория

ИСО/МЭК 19790 применяется для криптографических модулей и является без исключения обязательным для правительства США, как и FIPS 140-2. Другие организации и правительственные учреждения подтвердили их использование.

В.2.3 Характеристики доверия

Метод обеспечения доверия использует подход проверки на соответствие и применяется главным образом в следующих областях:

- спецификация криптографических модулей;
- порты и интерфейсы;
- роли, услуги (сервисы) и аутентификация;
- машинная модель конечного состояния;
- физическая защита;
- эксплуатационная среда;
- распределение криптографического ключа;
- самопроверки;
- доверие к проекту;
- ослабление атак.

В.2.4 Разносторонность

Различные области испытаний структурированы по четырем уровням 1—4, расположенным один на другом. Испытание по ИСО/МЭК 19790 проводилось со ссылкой на специфическую версию криптографического модуля. В случае любых модификаций испытание должно проводиться повторно. CMVP предоставляет собой программное руководство по различным методам поддержания валидации (в зависимости от характера изменения) для обеспечения своевременного и экономически эффективного поддержания валидации.

Эволюция требований к испытаниям представлена на рисунке В.1.

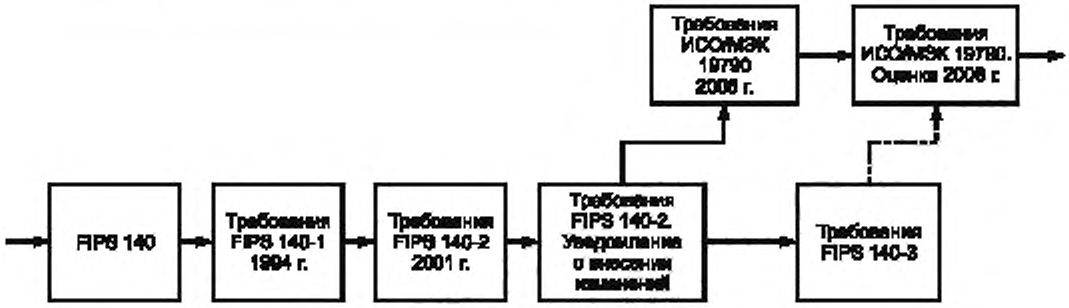


Рисунок В.1 — Эволюция требований к испытаниям

В.2.5 Своевременность

В.2.6 Полнота

В качестве соответствующей проверки — доверие к соответствию криптографического модуля требованиям спецификации (ИСО/МЭК 19790) является высоким.

Производные требования к испытаниям и руководство по реализации предназначены для обеспечения полноты и воспроизводимости испытаний.

В.2.7 Стоимость реализации/объем работ по реализации

Расходы на проверку достоверности могут включать в себя следующие элементы:

- расходы на организацию, проводящую проверку (например, стоимость CMVP НИСТ),
- расходы на испытательную лабораторию;
- стоимость внутренних работ по проведению валидации, проведению незначительных модификаций, требуемых для испытателя, и написанию специальной документации.

Проверка по ИСО/МЭК 19790 по времени всегда короче оценивания по ИСО/МЭК 15408, поскольку область ее действия уже. Продолжительность проверки по ИСО/МЭК 19790 меняется в зависимости от.

- зрелости организации-разработчика;
- квалификации лаборатории;
- ограничений по органу по валидации;
- зрелости продукта;
- соответствия в сравнении с оцениванием.

В.2.8 Поддержка инструментальными средствами

Коммерчески доступны лишь несколько инструментов. Вспомогательная документация и инструментарий предоставляются НИСТ на сайте http://csrc/nist.gov/criptval.

В.2.9 Сфера действия криптографии

Метод обеспечения доверия определяет, что для криптографических модулей утвержденные функции обеспечения безопасности должны проходить валидацию и сертифицироваться для правильной реализации по программе валидации криптографического алгоритма (CAVP), разработанной НИСТ, который обеспечивает алгоритмические инструменты проверки для испытательных лабораторий, аккредитованных NVLAP.

В.2.10 Оценка и сертификация

Североамериканская схема аккредитации CMVP существует и поддерживается совместно с НИСТ и CSE.

В.2.11 Убедительность и признание

ИСО/МЭК 19790 является производным от FIPS 140-2, признанной спецификации США, опубликованной НИСТ. Соответствие спецификации требуется администрацией США для продуктов безопасности, содержащих криптографическое устройство для защиты уязвимых несекретных данных. Сертификаты выдаются для криптографических модулей, прошедших проверку на соответствие и соответствующих другим программным требованиям.

В.3 ИСО/МЭК 21827

В.3.1 Цель обеспечения безопасности

Назначением ИСО/МЭК 21827 является обеспечение доверия, относящегося к процессам проектирования безопасности системы организации пользователя.

В.3.2 Целевая аудитория

Данный метод обеспечения доверия включает в себя, в первую очередь, доверие к разработке и доверие к интеграции и, таким образом, предназначен как для разработчиков, так и для интеграторов системы.

В.3.3 Характеристики

Метод обеспечения доверия использует подход доверия к процессу.

В.3.4 Разносторонность

В ИСО/МЭК 21827 рассматриваются требования на пяти уровнях возможностей, связанных со зрелостью процесса, определенных организацией на основе ее доминирующих целей.

В.3.5 Своевременность

В основу ИСО/МЭК 21827 была положена более ранняя работа, проведенная ISSEA в период с 1994 по 2001 г. Данный стандарт был опубликован ИСО/МЭК в 2001 г. и основан на представлении общедоступной спецификации от ISSEA. Пересмотр ИСО/МЭК 21827 был начат в 2005 г. и завершен в 2007 г.

В.3.6 Завершенность

В ИСО/МЭК 21827 подробно рассматриваются пять уровней требований к функциональным возможностям, включающим в себя все аспекты дисциплины проектирования безопасности. Организация базовых практик, участвующих в процессе, обеспечивает организации потребителя гибкость для комбинирования процессов способом, соответствующим ее организационной структуре.

В.3.7 Стоимость реализации/объем работ по реализации

Основная часть стоимости оценивания по ИСО/МЭК 21827 приходится на первый проект. Стоимость дополнительных проектов, использующих аналогичную методологию, представляет собой только малую часть этой начальной стоимости. Начальная стоимость уменьшается посредством привлечения внутренних оценщиков. Обычно никакая специальная документация не прилагается.

При наличии необходимого персонала процесс оценивания может быть недолгим и длиться от двух до трех недель.

В.3.8 Поддержка инструментальными средствами

Существуют несколько общедоступных основанных на электронных таблицах инструментальных средств, поддерживающих прослеживание результатов оценки, суммирующих и представляющих эти результаты.

В.3.9 Сфера действия криптографии

Специфические требования отсутствуют.

В.3.10 Оценка и сертификация

В отношении данного метода существуют система подготовки и квалификационная система.

В.3.11 Убедительность и признание

Схема, представленная в ИСО/МЭК 21827, обеспечивает оценивание группой оценки.

Организация поддержки SSE-CMM (SSO) предоставляет опытных методистов и группы по оценке по ИСО/МЭК 21827 для оказания помощи организациям при оценке их возможностей проектирования безопасности. Ниже приведены следующие предоставляемые услуги:

a) содействие в оценке по ИСО/МЭК 21827;

b) оценка по ИСО/МЭК 21827;

c) последующий аудит по ИСО/МЭК 21827;

d) составление плана улучшения процесса проектирования безопасности.

В отличие от ИСО/МЭК 15408 или ИСО/МЭК 19790 любое официальное или федеральное агентство, представляющее какую-нибудь систему сертификации по ИСО/МЭК 21827, отсутствует.

В.4 ИСО/МЭК 13335

В 4.1 Цель обеспечения безопасности

Комплект, в настоящее время содержащий ИСО/МЭК 13335-1, был опубликован как технический отчет (часть 1 — в 1996 г., часть 2 — в 1997 г., часть 3 — в 1998 г., часть 4 — в 2000 г. и часть 5 — в 2001 г.). В части 1 «Концепции и модели безопасности ИТ» даны определения основных терминов, относящихся к безопасности ИТ, элементарным аспектам (угрозы, риск, уязвимости и т. д.) и процессам (например, планирование непредвиденных обстоятельств, оценка риска, повышение осведомленности). Данная часть предназначена для ответственных руководителей и работников службы безопасности в организациях. В части 2 «Управление безопасностью ИТ и ее планирование» представлена информация по проектированию процесса обеспечения безопасности ИТ и его интеграции в существующие технологические процессы предприятия и предлагается организация безопасности ИТ. В части 3 «Способы управления безопасностью ИТ» уточняются этапы процесса обеспечения безопасности ИТ и предоставляется информация о методах и способах, которые могут использоваться для достижения этой цели. Наконец, в части 4 «Выбор мер безопасности» представлена информация о том, какие меры безопасности соответствуют каким угрозам и как можно определить приемлемый уровень базовой защиты для организации. В части 5 «Руководство по управлению сетевой безопасностью» представлены рекомендации по управлению безопасностью ИТ без регламентирования каких-либо определенных решений.

Вторая редакция ИСО/МЭК 13335 была опубликована как международный стандарт, состоящий из двух частей, ИСО/МЭК 13335-1 был издан в 2004 г.; он отменяет и заменяет ИСО/МЭК ТО 13335-1-1996 г. и ИСО/МЭК ТО 13335-2-1997 г. ИСО/МЭК 13335-2 заменяет ИСО/МЭК ТО 13335-3 и ИСО/МЭК ТО 13335-4. ИСО/МЭК ТО 13335-5 (управление сетями) объединен с ИСО/МЭК 18028-1.

Существует намерение изменить обозначение стандарта ИСО/МЭК 13335-2 на ИСО/МЭК 27005.

В.4.2 Целевая аудитория

Данный метод обеспечения доверия касается доверия к эксплуатации.

Основной целевой группой являются руководители предприятий или организаций, непосредственно участвующие в планировании и реализации процесса обеспечения безопасности ИТ.

Часть 1 предназначена для руководителей на уровне правления, особенно тех, кто несет ответственность за программу обеспечения безопасности ИТ в масштабе предприятия.

Часть 2 предназначена для руководителей, ответственных за системы ИТ предприятия, или для тех, чья сфера ответственности в значительной степени зависит от использования ИТ.

Части 3 и 4 предназначены для тех, кому приходится иметь дело с безопасностью ИТ на различных этапах жизненного цикла проектов.

Отчеты могут использоваться учреждениями независимо от их начальной структуры. Однако они предназначены для изучения и (при необходимости) модификации структуры необходимых процессов обеспечения безопасности ИТ. Предоставляемая для этого информация не зависит от сложности имеющихся структур и целевого уровня безопасности.

В.4.3 Характеристики

Метод обеспечения доверия включает в себя подход к доверию к среде. В отдельных частях ИСО/МЭК 13335 не излагаются какие-либо конкретные процедуры и решения, а содержатся рекомендации по разработке этих процедур и решений и их адаптации для конкретного предприятия, а также существующие для этих целей методы и модели. Документация не предназначена для измерения уровня безопасности ИТ или любой демонстрации соответствия стандарту.

В.4.4 Разносторонность

В основном стандарты следует адаптировать к конкретным особенностям учреждений и инфраструктуре их ИТ или проектам. Различные части стандарта содержат рекомендации для разных уровней — от уровня правления до уровня проекта. В реальности процессы и процедуры могут реализоваться полностью только в учреждениях

среднего масштаба или крупных учреждениях. Однако повсеместно стандарты используются в качестве руководства.

В.4.5 Своевременность

ИСО/МЭК 13335 был опубликован недавно и находился в процессе публикации на момент разработки ИСО/МЭК 15443. Однако общий характер положений ИСО/МЭК 13335 не предполагает необходимости в повторном их пересмотре в обозримом будущем.

В.4.6 Завершенность

Данные стандарты являются завершенными относительно описания организации и компонентов процесса обеспечения безопасности ИТ. Они дают только направление определения этих процессов и структур внутри организации; уровень безопасности не обозначается, так как определение этого уровня происходит только в рамках сформированных с их использованием организации и процессов.

В.4.7 Стоимость реализации/объем работ по реализации

Расходы на внедрение и поддержание процесса обеспечения безопасности ИТ на предприятии зависят от имеющейся организационной структуры и не могут утверждаться для всех аспектов. Аналогичные соображения применимы к ИСО/МЭК 27002.

В.4.8 Поддержка инструментальными средствами

Поддержка инструментальными средствами не кажется целесообразной. Решения по управлению, которые должны приниматься с учетом формы управления безопасностью ИТ на предприятии, не зависят от системы показателей.

В.4.9 Сфера действия криптографии

Криптография рассматривается на уровне мер (единиц измерения). Требования не обозначены, а вместо них дается ссылка на ИСО/МЭК 11770-1, особенно в отношении управления ключами.

В.4.10 Оценка и сертификация

Сертификация не предусматривается и не считается необходимой.

В.4.11 Убедительность и признание

Признан в качестве международного метастандарта.

В.5 ИСО/МЭК 27001 и ИСО/МЭК 27002

В.5.1 Цель обеспечения безопасности

Назначением ИСО/МЭК 27001 и ИСО/МЭК 27002 является представление требований к подходу «передовой опыт» в управлении информационной безопасностью. В ИСО/МЭК 27002 даются рекомендации по методам обеспечения информационной безопасности, тогда как в ИСО/МЭК 27001 определены требования к системам менеджмента информационной безопасности.

Основные рассматриваемые темы включают в себя планирование, внедрение (реализацию), эксплуатацию и улучшение системы менеджмента информационной безопасности. Связанные с основными темы касаются идентификации и оценки риска, а также выбора соответствующих целей средств управления.

В.5.2 Целевая аудитория

ИСО/МЭК 27001 и ИСО/МЭК 27002 предназначены для предприятий и учреждений всех размеров, но не для частных пользователей. Кроме того, стандарты могут применяться сервисными фирмами в областях аудита и сертификации.

Целевой аудиторией стандартов являются:

- руководители, ответственные за обеспечение адекватной защиты информации, соответствующей их обязанностям;
- лица, ответственные за выбор и внедрение мер безопасности ИТ, такие, например, как работники службы безопасности ИТ, лица, ответственные за ИТ;
- персонал с обязанностями по мониторингу, например, внутренние и внешние аудиторы;
- внешние заинтересованные стороны, такие, например, как заказчики и поставщики, полагающиеся на меры безопасности ИТ;
- органы по сертификации систем менеджмента информационной безопасности.

Применимость стандартов в целом не зависит от организационной структуры. Ориентированный на руководство подход не ограничивает применимость стандартов к определенным технологическим системам и типам систем.

В.5.3 Характеристики

Данный метод обеспечения доверия использует подход к доверию к процессу и охватывает следующие этапы:

- формирование системы менеджмента информационной безопасности;
- внедрение и эксплуатация системы менеджмента информационной безопасности;
- мониторинг и проверка системы менеджмента информационной безопасности,
- поддержание и улучшение системы менеджмента информационной безопасности.

Будучи связан с этими этапами, ИСО/МЭК 27001 содержит требования к документации, обязанностям руководства, внутренним аудитам системы менеджмента информационной безопасности, ее проверкам со стороны руководства и улучшению системы менеджмента информационной безопасности.

ИСО/МЭК 27001 содержит требования к выбору мер управления обработкой риска информационной безопасности, основанным на ИСО/МЭК 27002.

Данные стандарты можно применять различными путями. Во-первых, ИСО/МЭК 27002 можно использовать как ссылку для конкретного руководства в отношении спецификации и применения отдельных мер управления. Во-вторых, ИСО/МЭК 27001 может использоваться для внедрения современной системы менеджмента информационной безопасности. В-третьих, для внедрения системы менеджмента информационной безопасности, которая может сертифицироваться независимым органом по сертификации, может применяться комбинация требований ИСО/МЭК 27001 и ИСО/МЭК 27002.

В.5.4 Разносторонность

ИСО/МЭК 27001 и ИСО/МЭК 27002 предназначены для организаций любого размера, а также для отдельно идентифицируемых подразделений организаций. При наличии у организации нескольких систем менеджмента информационной безопасности, включающих в себя различные сферы применения (например, различных подразделений организации), отсутствует какой-либо автоматизированный способ, помогающий сделать вывод о безопасности информации вообще. Однако на основе документации, имеющейся по каждой системе менеджмента информационной безопасности, можно провести экспертную оценку и определить согласованность подходов к информационной безопасности с общими целями.

В.5.5 Своевременность

ИСО/МЭК 27001 и ИСО/МЭК 27002 апробированы и полностью совместимы. Запланированы регулярные обновления в соответствии с общим подходом к модификации стандартов ИСО/МЭК и сохранение при таких обновлениях совместимости стандартов.

В.5.6 Завершенность

ИСО/МЭК 27001 и ИСО/МЭК 27002 в значительной степени ориентированы на нисходящий подход и содержат общие требования и руководство по безопасности. Эти требования охватывают все области, имеющие значение в настоящее время. Стандарты не содержат каких-либо ориентированных на продукт требований, а ориентированные на технологии требования обобщены и содержат лишь незначительное число подробностей.

ИСО/МЭК 27001 и ИСО/МЭК 27002 не ограничиваются одним конкретным уровнем безопасности, а рекомендуемые ими меры управления ориентированы на основной подход к обеспечению безопасности и пригодны только для уровней безопасности от высокого до максимального после модификации. Однако ориентированный на руководство подход обеспечивает поддержку всем уровням безопасности.

ИСО/МЭК 27001 позволяет исключить меры управления, изложенные в ИСО/МЭК 27002, на основании, например, их несоответствия деятельности в рамках сферы действия или отсутствия необходимости обработки связанных с этой деятельностью рисков безопасности. Для адаптации к небольшим предприятиям возможна модификация мер управления.

В.5.7 Стоимость реализации/объем работ по реализации

Придание особого значения деятельности руководства делает усилия, необходимые для внедрения систем менеджмента информационной безопасности, в большой степени зависимыми от общего качества организованности учреждения. Для недостаточно хорошо организованных учреждений требуются значительно бóльшие усилия, чем для учреждений с вполне определенными организационными структурами.

Метод использования правил для обеспечения рекомендаций по внедрению мер управления в основном делает возможным применение имеющихся мер управления для выполнения относящихся к ним требований без дополнительных затрат.

Объем работ по внедрению системы менеджмента информационной безопасности на основе требований ИСО/МЭК 27001 в значительной мере определяется областью действия системы. Выбор метода оценки риска оказывает большое влияние на необходимый объем работы.

Стоимость сертификации по ИСО/МЭК 27001 аналогична стоимости сертификации по ИСО/МЭК 9000.

Следует отметить, что стоимость сертификации надо рассматривать отдельно от стоимости внедрения соответствующей системы менеджмента информационной безопасности. Подобные затраты зависят от масштаба организации, характера принятых мер и имеющихся угроз. Обобщенное определение таких затрат невозможно.

Для оценивания обычно требуется определенный период времени с перерывами на внедрение различных аспектов СМИБ или решение возникающих проблем. Обычно фактическая продолжительность оценивания составляет от трех до 12 месяцев.

В.5.8 Поддержка инструментальными средствами

ИСО/МЭК 27001 и ИСО/МЭК 27002 можно поддерживать различными инструментальными средствами. Для оценки риска, поддержки разработки и сохранения необходимых документов и записей и сравнения внедренных мер управления с поставленными целями существуют специфические инструментальные средства в соответствии с ИСО/МЭК 27001.

В.5.9 Сфера действия криптографии

Криптография рассматривается в ИСО/МЭК 27002, в котором представлен практический опыт, касающийся политики применения криптографических мер контроля и управления ключами. Учитывая общий характер данного стандарта, какие-либо специфические для продукта рекомендации отсутствуют.

В.5.10 Оценка и сертификация

ИСО/МЭК 27001 был разработан для того, чтобы сделать возможной сертификацию реализаций независимыми органами по сертификациям. Независимая сертификация СМИБ действительна несколько лет (обычно три года). Надзорные аудиты проводятся через каждые 6—12 месяцев в течение этого периода. Сертификация аннулируется при наличии серьезных несоответствий и/или если они своевременно не устранены. Находящийся в настоящее время на стадии разработки ИСО/МЭК 27006 специфицирует требования по аккредитации органов по сертификации.

В.5.11 Убедительность и признание

Различные федеральные и региональные службы по аккредитации обеспечивают независимое доверие к тому, что органы по сертификации по ИСО/МЭК 27001 выполняют стабильные процедуры, задействуют компетентный персонал и выдают непротиворечивые результаты. Примерами этих органов по аккредитации являются UKAS в Великобритании и JANSANZ в Австралии и Новой Зеландии.

Федеральные и региональные службы по аккредитации сотрудничают в международном масштабе посредством форума международного аккредитования (IAF) и Европейской организации сотрудничества по аккредитации. Эти региональные и международные ассоциации обеспечивают согласованность действий по международной аккредитации.

В.6 Руководство по базовой защите ИТ

В.6.1 Цель обеспечения доверия

В руководстве по базовой защите ИТ представлены стандартные меры безопасности, направленные на формирование предопределенного уровня безопасности для систем ИТ. Этот уровень может также служить отправной точкой для областей с более строгими требованиями безопасности. Руководство по базовой защите ИТ содержит перечни стандартных мер безопасности в каждой из областей: Инфраструктура, Персонал, Аппаратные средства и программное обеспечение, Коммуникация и планирование непредвиденных обстоятельств. Подход включает в себя следующие действия: анализ структур ИТ, оценка требований к защите, моделирование, основные проверки безопасности, дополнительный анализ безопасности и внедрение мер безопасности ИТ.

В.6.2 Целевая аудитория

Данный метод обеспечения доверия включает в себя доверие к эксплуатации, а также доверие к разработке и интеграции в условиях эксплуатации ИТ.

Руководство по базовой защите ИТ предназначено для учреждений и предприятий всех масштабов, а не для частных пользователей. Для облегчения адресации стандартных мер безопасности ответственным работникам текстовая информация по каждой мере начинается с информации о том, кто несет ответственность за инициирование и внедрение рассматриваемой меры. В каждом случае для этого в рамках учреждения или предприятия обозначены одна или более ролей. Примерами таких ролей являются начальник отделения ИТ, работник службы безопасности ИТ, персонал, инспектор пожарной охраны, администратор и пользователь ИТ.

Основываясь на типичных компонентах, которые преимущественно рассматриваются в руководстве по базовой защите ИТ, данное руководство очень полезно для провайдеров услуг, создающих или предоставляющих содержание в Интернете, но менее полезно для операторов сети. По причине расширенного набора требований по безопасности ИТ, содержащихся в руководстве по базовой защите ИТ, документ также применим для поставщиков аппаратных изделий или программных продуктов. Однако о разработке программного обеспечения упоминается лишь мимоходом. Администраторы найдут в руководстве по базовой защите ИТ всеобъемлющую и подробную техническую информацию.

Поскольку руководство по базовой защите ИТ следует общему принципу рассмотрения типичных компонентов (ИТ), оно в основном не зависит от структуры предприятия. Руководство применимо для всех областей, в которых используются стандартные системы и приложения ИТ и в которых (в общем) требования безопасности являются обычными. Меры безопасности ИТ с более высокими требованиями безопасности сохраняются лишь в ограниченном объеме.

В.6.3 Характеристики

Метод обеспечения доверия использует подход к доверию к процессу, но включает в себя также элемент доверия к продукту в случае его модификации во время эксплуатации. В зависимости от компонентов рассматриваемой среды ИТ пользователь выбирает подходящие разделы (или «модули») в руководстве по базовой защите ИТ и использует их для «моделирования» среды ИТ. Подход делится на пять уровней: аспекты высшего порядка, инфраструктура, системы ИТ, сети и приложения.

Уровень 1. Аспекты высшего порядка охватывают аспекты безопасности ИТ, которые нельзя зафиксировать для отдельной ИТ или компонентами инфраструктуры, но которые оказывают влияние на большие области или даже всю среду ИТ.

В.6.4 Разносторонность

Поскольку руководство по базовой защите ИТ предназначено для компонентов рассматриваемой среды ИТ, объем работ и расходы, затраченные на применение этого метода, в значительной степени зависят от однородности рассматриваемой среды. В руководстве по базовой защите ИТ содержится механизм группирования идентичных

компонентов, чтобы избежать необходимости обрабатывать каждый компонент в отдельности. Однако, если среда ИТ неоднородна в целом, объем работ и расходы возрастают пропорционально числу компонентов (систем ИТ, приложений ИТ, и т. д.).

В.6.5 Своевременность

Руководство по базовой защите ИТ пересматривают и расширяют дважды в год. Это особенно необходимо для адаптации технического содержания к новейшим разработкам. Дополнительный материал основан на требованиях, определенных зарегистрированными пользователями руководства по базовой защите ИТ.

В.6.6 Завершенность

Руководство по базовой защите ИТ содержит как общие, так и специфические для продукта и технологий стандартные меры безопасности. Общие меры охватывают все важные аспекты безопасности ИТ, например, планирование организационной структуры или непредвиденных обстоятельств. С учетом огромного разнообразия продуктов и решений в области ИТ неизбежен охват специфическими для продукта и технологий мерами безопасности только наиболее широко применяемых компонентов.

Руководство по базовой защите ИТ ориентировано, в первую очередь, на защиту информации, приложения ИТ и системы ИТ, к которым предъявляются так называемые «нормальные» требования безопасности. При более высоких требованиях к стандартным мерам безопасности, приведенным в руководстве по базовой защите ИТ, необходимо привлекать дополнительные меры.

В.6.7 Стоимость реализации/объем работ по реализации

Поскольку стандартные меры безопасности ориентированы на нормальные требования безопасности, обычно дорогостоящие услуги или компоненты безопасности или инфраструктуры не требуются. Следовательно, основными издержками внедрения мер безопасности являются организационные усилия и затраты на оплату труда. Следует также учитывать работу по проведению анализа. Это в значительной степени зависит от однородности рассматриваемой среды. Для анализа базовой защиты ИТ предприятия среднего масштаба необходимо планировать по крайней мере три месяца.

В.6.8 Поддержка инструментальными средствами

Руководство по базовой защите ИТ поддерживается инструментальными средствами в отношении как подхода (программа базовой защиты ИТ BSI), так и содержания (администрация UNIX программы USEIT-BSI).

Дальнейшая разработка инструментальных средств ориентирована на продление действия руководства по базовой защите ИТ. Другие инструментальные средства обеспечения безопасности, ориентированные на подход или содержание руководства по базовой защите ИТ или к его содержанию, также имеются в продаже.

В.6.9 Сфера действия криптографии

Подобно другим рекомендациям рекомендации по применению криптографических процедур также ориентированы на стандартные требования безопасности. Руководство включает введение в основное понятие о криптографии, общие рекомендации по применению криптографических механизмов и специфические рекомендации по продуктам.

В.6.10 Оценка и сертификация

Недавно разработана классификационная схема, предлагающая администрации и предприятиям возможность документировать факт успешного внедрения ими базовой защиты ИТ в интересах внешнего мира. Были предусмотрены три уровня: самопровозглашенный «начальный уровень», самопровозглашенный «повышенный уровень» и действительный сертификат базовой защиты ИТ. Такой сертификат выдают только независимые сертификационные организации.

В рамках отдельных глав руководства по базовой защите ИТ дается разъяснение о том, какие меры требуются для каждого квалификационного уровня. Завершение разработки классификационной схемы планировалось к концу 2001 г.

В.6.11 Убедительность и признание

Руководство по базовой защите ИТ является национальным стандартом, доступным на немецком и английском языках.

В.7 COBIT

В.7.1 Цель обеспечения доверия

Интенсивное использование ИТ для поддержки и обработки значимых для бизнеса операций делает крайне важным создание соответствующей среды контроля. COBIT (цели контроля информационных и связанными с ними технологий) были разработаны ISACA как метод тестирования полноты и эффективности такой среды контроля при ограничении риска.

В.7.2 Целевая аудитория

Этот метод обеспечения доверия включает в себя доверие к эксплуатации.

COBIT применяется следующими целевыми группами:

- руководством — для оказания поддержки при взвешивании риска в сопоставлении с капиталовложениями, сопряженными с применением мер контроля;
- пользователями — для улучшения оценки надежности и мониторинга услуг ИТ, предоставляемых в рамках организации или третьими сторонами;
- испытателями — для объективного обоснования фактов испытаний и выдачи консультаций в связи с созданием и эксплуатацией внутрифирменных средств контроля;
- владельцами процесса или лицами, ответственными за ИТ — для поддержки своей работы.

COBIT может применяться в качестве ориентированного на процесс метода независимо от внутренней структуры или правовой формы предприятия.

В.7.3 Характеристики

Этот метод обеспечения доверия применяет подход к доверию к среде.

При использовании COBIT пользователь вначале определяет процессы ИТ, значимые для конкретной ситуации. Затем для каждой цели контроля выбранных процессов ИТ ему необходимо взвесить и решить, в какой степени существующие меры контроля соответствуют его требованиям.

COBIT различает семь разных бизнес-требований и группирует их по трем категориям — качества, безопасности и регулярности:

- качество ИТ, определяемое эффективностью и экономичностью выполняемых процессов, выражается критериями эффективности и результативности;
- требования безопасности по конфиденциальности, целостности и доступности — отражены в COBIT;
- критерий надежности — применяется в COBIT для обеспечения надежности финансовой отчетности (требования по финансовой отчетности) наряду с критерием соблюдения правовых требований внутренних и внешних стандартов.

В соответствии с COBIT поддерживаемые ИТ бизнес-процессы основываются на следующих ресурсах:

- данные: элементы данных от внутренних и внешних источников в самом широком смысле;
- совокупность ручных и запрограммированных процедур, называемая «приложениями»;
- технологии, включающие в себя аппаратные средства, операционные системы, системы администрирования базами данных, сети, коммуникационные приложения и т. д.;
- активы: все ресурсы, используемые для обеспечения и поддержки информационных систем;
- персонал: знания, осведомленность и продуктивность, связанные с планированием, организацией, закупкой, обеспечением соответствия, поддержкой и мониторингом информационных систем и услуг.

Ресурсы ИТ следует планировать, разрабатывать, внедрять, эксплуатировать и подвергать мониторингу контролируемым способом. В COBIT дано определение 34 критическим процессам, играющим важную роль в определении успешности управления ИТ. Эти процессы, использующие ресурсы ИТ, можно сгруппировать в четыре основные области, которые образуют следующий замкнутый жизненный цикл:

- планирование и организация;
- закупка и внедрение;
- эксплуатация и поддержка;
- наблюдение.

Для 34 критических процессов ИТ указано общее число из 300 основных задач (заданий). Для каждого задания распределены необходимые ресурсы и определены цели контроля, основанные на требованиях категорий качества, безопасности и регулярности.

В.7.4 Разносторонность

Благодаря матричной структуре COBIT пользователь может рассматривать только отдельные области или процессы и/или выбирать подгруппу из семи бизнес-требований (например, только требования безопасности к конфиденциальности, целостности и доступности).

В.7.5 Своевременность

COBIT были разработаны в 1996 г. Ассоциацией аудита и контроля информационных систем. В 1998 г. они были расширены и полностью переработаны. Во второй редакции были предложены материалы и программное обеспечение для работы с COBIT. Третья редакция (опубликованная в 2000 г.) была издана как «открытый стандарт».

В.7.6 Завершенность

COBIT предлагает метод фиксирования ориентированных на ИТ и сопутствующих им процессов. Связанные с ними цели контроля определяются независимо от технологий и могут использоваться для различных системных окружений. Однако для создания концепций безопасности необходимо добавить дополнительные меры контроля, специфические для той или иной системы.

COBIT ориентированы на интересы типичного предприятия, связанные с безопасностью. Рассматриваются сохранение основных интересов компаний (целостность и конфиденциальность внутренней информации и процессов) и соблюдение обязательных положений (защита секретности данных, финансовая отчетность).

Фиксированный уровень безопасности отсутствует, а ориентация делается на цели предприятия.

В.7.7 Стоимость реализации/работа по реализации

Полный анализ всех целей контроля в рамках предприятия среднего масштаба с COBIT длится не более одного рабочего месяца.

В.7.8 Поддержка инструментальными средствами

Применение COBIT поддерживается различными инструментальными средствами, среди которых:

- «Консультант по COBIT» — Methodware Limited, г. Веллингтон, Новая Зеландия;
- «Самооценка по COBIT» — Институт по обучению в области сертификации, США.

Вторая редакция COBIT содержит также полезную дополнительную информацию, заявочные материалы и материалы по представлению.

В самом COBIT упоминаются примеры проведения проверок (специфические меры безопасности). С помощью этих примеров можно оценить степень удовлетворения целей контроля. Однако, как правило, пользователи COBIT (например, аудиторские организации) применяют собственные схемы оценки.

В.7.9 Сфера действия криптографии

Криптографические процедуры рассматриваются как меры, применимые для защиты информации и верификации аутентичности. В этой связи учитываются как соблюдение обязательных требований, так и проблемы легального сохранения зашифрованных данных.

В.7.10 Оценка и сертификация

Сертификат COBIT в полном смысле этого слова не существует. Однако метод используется аудиторскими организациями в условиях ежегодного аудита счетов для тестирования среды контроля ИТ. Результаты тестирования ИТ помещаются в ревизионный отчет о годовой отчетности.

В.7.11 Убедительность и признание

COBIT является стандартом, поддерживаемым крупнейшими международными бухгалтерскими фирмами.

В.8 ИСО 9000

В.8.1 Цель обеспечения доверия

Назначением серии ИСО 9000 является определение метода испытаний, в котором обозначена необходимость документирования требований к системе менеджмента качества как доказательство ее способности соответствовать требованиям заказчика и возможности оценивать эту способность внутренними и внешними контролерами. Проводятся также проверки в отношении выполнения средой ИТ организации требований заказчика и ее соответствия бизнес-целям заказчика.

Данный стандарт не подразумевает однородность систем менеджмента качества. На проектирование и внедрение системы менеджмента качества в организации оказывают влияние цели организации, требования заказчика, продукция или предлагаемые услуги и процессы.

В.8.2 Целевая аудитория

К данному методу обеспечения доверия относится доверие к среде в рамках любой организации на относительно высоком уровне. Содержащиеся в ИСО 9000 требования являются высокоуровневыми и независимыми от какого-либо промышленного или экономического сектора. Они относятся к организациям любого типа и масштаба.

В данном случае документация по процессам помогает организации достичь единообразия, определить области взаимодействия и разъяснить установившуюся практику каждому работнику.

Благодаря интеграции в процессы менеджмента структура стандарта стопроцентно применима к предприятию. Стандарты применимы ко всем областям, в которых структура ИТ применяется для поддержки внутренних процессов и/или требований заказчика. Более того, по причине их доминирования данные стандарты можно применять ко всем категориям продуктов или услуг и в любом промышленном или экономическом секторе. Они также независимы от типа и масштаба организации.

В.8.3 Характеристики

Этот метод обеспечения доверия использует доверие к среде.

Содержащиеся в данном стандарте требования не заставляют предприятия изменять структуры своих систем менеджмента качества или подгонять свою документацию под структуру стандарта.

Более того, документация по процессам в системе менеджмента качества организации должна быть создана в виде, наиболее соответствующем деятельности этой организации.

Документация по сопровождению ИТ на предприятии интегрирована в среду процесса системы менеджмента качества и в качестве такового может восприниматься только в контексте других процессов управления.

В данном случае ИТ служит для поддержки внутренних процессов и требований заказчика и должна всегда рассматриваться как средство сопряжения. Функциональный аспект существует только как функция других документированных процессов управления организации.

В.8.4 Разносторонность

Поскольку ИТ в серии стандартов ИСО 9000 зависит от других процессов управления, объем работ, затраченных на тестирование, зависит от согласованности документации и функциональности других процессов. Если доля ИТ в производственном процессе, процессе предоставления услуг или из-за требований заказчика очень велика, метод испытаний будет более детальным. Однако, поскольку ИТ-процесс никогда нельзя рассматривать отдельно от других процессов управления, объем тестирования остается пропорционально постоянным.

В.8.5 Своевременность

Содержащиеся в ИСО 9001 требования относительно стабильны и модифицируются редко.

Однако они часто пересматриваются на предмет их современности и полезности. Например, технический комитет ИСО опубликовал переработанное издание данного стандарта под обозначением ИСО 9000:2000. В названии, а также в пересмотренной области применения данного издания стандарта исключен термин «доверие к качеству». Это означает, что основное значение имеет способность выполнять требования заказчика и осуществлять постоянное улучшение качества продукта. Более того, результат лучше соответствует требованиям серии стандартов ИСО 14000 и системе управления средой.

В.8.6 Завершенность

Требования в отношении системы менеджмента качества, в первую очередь, служат цели достижения удовлетворения заказчика через выполнение его требований, как минимум, путем приложения этих требований и постоянного их совершенствования и предотвращения ошибок. Таким образом, в данном случае обеспечивается только функциональность среды ИТ в рамках документированных процессов. Следовательно, требование о пересмотре самой технологии отсутствует, а существует только пересмотр функциональности в рамках организации, например, концепция непредвиденных обстоятельств, назначение лица, ответственного за защиту секретности данных.

В.8.7 Стоимость реализации/объем работ по реализации

Объем работ и издержки, связанные с интеграцией среды ИТ в процесс, относительно невелики. При условии сосредоточения на внутренних процессах и требованиях заказчика обычно отсутствует какая-либо потребность в дорогостоящих услугах или компонентах обеспечения безопасности. Большинство издержек в данном случае отражают трудовые и организационные усилия, затраченные на интегрирование процессов в процессную среду и выдачу определений средств сопряжения.

Так как этот процесс ИТ нельзя отделить от общего рассмотрения документации серии ИСО 9000, оценка усилия, требуемого для этой подобласти, вряд ли возможна.

В.8.8 Поддержка инструментальными средствами

В данном случае вопрос о том, какие инструментальные средства следует использовать, в значительной степени зависит от предприятия.

Допускается рассматривать все имеющиеся в продаже инструментальные средства.

В.8.9 Сфера действия криптографии

Как и во всех других процессах среды ИТ, серия стандартов ИСО 9000 ориентирована на деловые операции организации и требования заказчика, применимые для этой организации. Следовательно, возможны серьезные противоречия между ними.

В.8.10 Оценка и сертификация

Тестирование и сертификация по серии стандартов ИСО 9000:2000 проводятся независимыми аккредитованными органами, и результаты тестов документируются посредством выдачи сертификата. Эти сертификаты выдаются и публикуются во многих странах многими организациями.

В.8.11 Убедительность и признание

Существует возможность наиболее широкого признания в качестве международного стандарта.

Приложение С
(справочное)

Формирование методов обеспечения доверия

Содержание настоящего приложения было сформировано из общедоступного материала.

Производители аппаратных средств и программного обеспечения должны обеспечивать свою продукцию функциями обеспечения безопасности, соответствующими заданной цели и предполагаемой эксплуатационной среде. С учетом систематического подхода для этого следует применять установленный метод обеспечения доверия, такой как в ИСО/МЭК 15408 и ИСО/МЭК 19790.

Со стороны пользователей должны предприниматься шаги по обеспечению внедрения сопутствующих мер, необходимых для безопасного функционирования всего решения, что подразумевает эффективное управление безопасностью ИТ, а также организационные и технические меры обеспечения безопасности и меры обеспечения безопасности персонала. В этих целях должны применяться такие методы, как представленные в ИСО/МЭК 13335, ИСО/МЭК 27002 и Руководстве по базовой защите ИТ.

Профили защиты из ИСО/МЭК 15408 могут служить мостом между производителями и пользователями. Профили защиты могут помочь пользователям сформулировать точные требования к характеристикам и функциям безопасности продукции. Со своей стороны производители могут конкретизировать, какие профили защиты соответствуют конкретному продукту, и сопровождать такие заявления сертификатом.

Часто используют комбинацию, представленную в настоящем приложении.

С.1 ИСО/МЭК 15408 + Руководство по базовой защите ИТ

Стандарт серии ИСО/МЭК 15408 и Руководство по базовой защите ИТ могут использоваться в комбинации. Применение стандартных мер безопасности, указанных в руководстве по базовой защите ИТ, приводит к защите всей системы, охватывая как управление безопасностью ИТ, так и технические меры безопасности на уровне компонентов. Однако обычно во время оценки требований защиты или сравнительного анализа безопасности становится очевидно, что в подразделениях учреждения, которые невозможно защитить с помощью одного лишь руководства по базовой защите ИТ, имеются специфические потребности или требования. В этом случае для формулирования требований безопасности и выбора подходящей по возможности должным образом сертифицированной продукции могут применяться профили защиты, обеспечивающие необходимые функции обеспечения безопасности. Таким образом, соответствующего уровня безопасности ИТ можно достичь посредством комбинированного использования руководства по базовой защите ИТ и ИСО/МЭК 15408.

С.2 ИСО/МЭК 27002 + Руководство по базовой защите ИТ

ИСО/МЭК 27002 связан с управлением информационной безопасностью и предлагает применение ориентированного на процесс доступа. Основным содержанием данного стандарта является каталог общих мер, полученных на основе передового опыта. Для защиты общего решения от прогнозируемой угрозы эти общие меры должны реализовываться при помощи специальных и технических инструкций по действиям по их реализации и мер по обеспечению безопасности. В данном случае руководство по базовой защите ИТ может оказать существенное содействие. Руководство содержит каталоги с подробными рекомендациями, построенными на информации по областям «Организация», «Персонал», «Инфраструктура» и «Технология». Следовательно, комбинация руководства по базовой защите ИТ и ИСО/МЭК 27002 может обеспечить подход, который четко отделяет контроль безопасности ИТ от практического внедрения. По этому сценарию в случае с подобластями со специфическими требованиями безопасности можно обратиться к ИСО/МЭК 15408 и/или профилям защиты.

С.3 ИСО/МЭК 27001 и ИСО/МЭК 27002

ИСО/МЭК 27001 специфицирует требования к системам менеджмента информационной безопасности. Существуют стандарты на сертификацию, основанные на Руководстве 62 ИСО и ИСО/МЭК 17021. Данный подход можно применить к совершенно разным предприятиям и организациям, что позволяет интегрировать деятельность по менеджменту информационной безопасности в системы менеджмента, основанные на других стандартах ИСО.

На всех этапах жизненного цикла определены подлежащие оценке требования по менеджменту информационной безопасности. Документированные процессы могут быть оценены в контексте целей организации. Для определения правильности следования процессам и достижения нужных результатов можно оценивать ассоциативные записи. В случае возникновения обстоятельств, когда система менеджмента не может достичь требуемых результатов, требования к системам менеджмента включают в себя требования к корректирующим и превентивным мерам. Соблюдение ИСО/МЭК 27001 требует от руководства проявления ответственного отношения к менеджменту информационной безопасности, играя в нем главную роль и обеспечивая адекватные ресурсы и подготовку персонала.

ИСО/МЭК 27001 требует использования мер управления по ИСО/МЭК 27002 как основы для обработки неприемлемого риска.

С.4 ИСО/МЭК 27002 + ИСО 9000

В ИСО 9000 определены требования к системам менеджмента качества и дано определение соответствующего метода испытаний. Метод может применяться на совершенно разных предприятиях и в разных организациях; однако конкретные соображения об информационной безопасности отсутствуют. Специфицирован только тест на соответствие среды ИТ организации требованиям заказчика и бизнес-целям. Для увеличения области информационной безопасности ИСО/МЭК 27002 может использоваться как приложение, конкретно связанное с управлением информационной безопасностью.

В частности, ИСО/МЭК 27002 также содержит меры, охватывающие процессы разработки так, чтобы два стандарта дополняли друг друга. Требования необходимо обосновать и выполнить, так как выполнение требований и ИСО 9000, и ИСО/МЭК 27002 предписаны на уровне руководства.

С.5 COBIT + базовая защита ИТ

В то время как базовая защита ИТ ориентирована на технические системы, COBIT сосредоточен на главных целях контроля. Поскольку внутренняя организация предприятия структурирована, в основном, с ориентацией на выполнение заданий, а не на технологии, с помощью COBIT часто легче определять действия и распределять обязанности отдельным организационным единицам. С другой стороны, COBIT предъявляет требования только к необходимым механизмам безопасности ИТ без конкретизации каких-либо специфических технических мер. Комбинирование двух методов может привести к получению эффективного подхода к формированию конкретных для предприятия концепций обеспечения безопасности ИТ. Для этой цели с помощью COBIT выбирают бизнес-процессы и определяют их требования безопасности. Формируется технологический профиль (технологии) (распределение систем ИТ по бизнес-процессам), следуя которому метод базовой защиты ИТ становится приемлемым путем получения специфических мер по выполнению релевантных требований безопасности.

Изложенные выше сценарии следует рассматривать просто как примеры способов успешного комбинирования наборов критериев безопасности. В особых случаях допускается применение других подходов. Например, применение COBIT рекомендуется, если проведение аудита является основной целью, а применение ИСО/МЭК 19790 — если предметом интереса являются криптографические процедуры.

Приложение D
(справочное)

Изучение конкретных случаев

D.1 Стратегия формирования комбинированного метода обеспечения доверия производителя микропроцессорных карточек

Производитель микропроцессорных карточек выбрал комбинацию ИСО/МЭК 15408 + ИСО/МЭК 19790 + + ИСО/МЭК 21827. Стратегия обеспечения доверия основывалась на прошлом опыте и снижении себестоимости в будущем.

Компания провела успешную расширенную оценку по оценочному уровню доверия (ОУД) 4 и расширенную оценку по ОУД 1. Это означает, что несколько групп имеют опыт работы с ИСО/МЭК 15408.

Дополнительно компания провела три успешные оценки уровня 3 по ИСО/МЭК 19790.

Компанию привлекла идея сертификации процессов, но, к сожалению, она не имела опыта работы с ИСО/МЭК 21827.

Причиной создания этой комбинации является потребность производителя в оптимальном сочетании видов доверия.

Обоснованием комбинации стал сравнительный анализ производительности. Выбор был сделан на основе следующих положений.

- ИСО/МЭК 19790 рассматривает:
соответствие функций безопасности продукта требованиям,
стойкость продукта;
- ИСО/МЭК 15408 рассматривает:
соответствие функций безопасности продукта требованиям,
стойкость продукта,
методологию и среду разработки;
- ИСО/МЭК 21827:
рассматривает процесс разработки безопасных услуг и продуктов,
очень хорошо согласуется с ИСО/МЭК 15408.

Общий подход заключается в использовании соответствующих процессов ИСО/МЭК 21827 для обеспечения разработки продуктов, а ИСО/МЭК 19790 или ИСО/МЭК 15408 — для их оценки. Преимуществом является то, что:

- документы, требуемые для ОУД4 по ИСО/МЭК 15408 или ИСО/МЭК 19790, могут быть в виде обычных выходных данных процессов, соответствующих всем техническим требованиям;

- для менее критичных продуктов доверие получается в соответствии с ИСО/МЭК 21827 без необходимости оплаты оценки готового продукта и задержки на эту оценку. Как сертифицированный процесс, так и ссылка на оцененные продукты дают уверенность, достаточную для заказчиков;

- для критичных продуктов и в зависимости от финансовых требований и требований заказчика проводят оценку и сертификацию по ОУД 4 ИСО/МЭК 15408 и ИСО/МЭК 19790 соответственно.

D.2 Провайдер услуг обеспечивает модернизацию бизнес-процессов

Предоставляющей услуги компании потребовалось модернизировать свои бизнес-процессы для:

- поставки товаров и услуг в режиме «он-лайн» в дополнение к использованию традиционных каналов;

- снижения расходов, связанных с торговыми операциями по цепочке поставок;

- предоставления персоналу возможности работать дистанционно.

Информационная безопасность и конфиденциальность были признаны критичными для успешного изменения бизнес-процессов и систем ИТ. Специальные требования были сформулированы на основе отчетов внутреннего и внешнего аудитов и обратной связи от заказчиков, партнеров по бизнесу и поставщиков.

Компания выбрала ИСО/МЭК 27001 и ИСО/МЭК 27002 из-за международного признания передового опыта их применения и пригодности для всех видов управления информационной безопасностью.

Было признано, что программа управления информационной безопасностью должна охватывать всю информацию независимо от ее носителей и технологию, используемую для ее обработки. Методы и средства менеджмента рисков и документация основывались на требованиях ИСО/МЭК 27001. В ИСО/МЭК 27002 были внесены изменения по инициативе пользователей с дополнительными подробностями, относящимися к требованиям контроля безопасности, отвечающим специфическим потребностям компании.

Внедрение было предпринято в виде проекта с использованием обычных внутренних процедур управления проектом, когда внедрение обусловливалось профилем риска каждой задействованной области. Для внедрения выбранного подхода потребовалось много усилий, открытого и честного информирования заинтересованных сторон и получения необходимой поддержки. Поддержка, полученная при этих начальных усилиях, в результате значительно облегчила процесс внедрения.

Проведя после внедрения анализ, компания пришла к выводу, что критичными факторами успеха были:

- поддержка руководства на раннем этапе;
- использование методов менеджмента рисков для обоснования выбора подхода и назначения приоритетов видам деятельности;
- вовлечение возможно большего числа людей в процессы планирования и внедрения,
- информирование работников о происходящем и его причинах в процессе внедрения;
- признание необходимости непрерывности управления информационной безопасностью.

Полученными уроками стали.

- сосредоточение усилий на наиболее раннем обслуживании системы менеджмента информационной безопасности;
- стремление к максимальному упрощению процессов (было обнаружено, что некоторые процессы вначале были слишком усложнены);
- обеспечение концентрации документирования систем управления на вопросах управления, а не на технических вопросах.

В результате внедрения своей системы менеджмента информационной безопасности компания удовлетворена наличием обоснованной системы информационной безопасности, соответствующей ее потребностям. Компания также имеет возможность изложить свою программу обеспечения информационной безопасности заказчикам и другим внешним заинтересованным сторонам, применяющим критерии, признанные на международном уровне.

Приложение Е
(справочное)

Определение цели обеспечения доверия

Е.1 Оценка риска

В идеале цель обеспечения доверия является результатом оценки и обработки риска. Остаточный риск является риском, остающимся после его обработки. Остаточный риск должен быть приемлемым и быть принятым заинтересованными сторонами. Если он неприемлем, то следует его обработка, например, запрашивают дополнительные меры безопасности.

Примечание — Остаточный риск может использоваться как показатель значимости, обеспечиваемой доверием.

Е.2 Менеджмент рисков

При внедрении любой меры безопасности и ее шкалы руководствуются менеджментом риска. Менеджмент риска является процессом идентификации, управления и устранения или минимизации последствий неблагоприятных событий, способных воздействовать на активы, имеющие приемлемую себестоимость.

Примечание — Применяемая в настоящем документе терминология основана на Руководстве 73 ИСО/МЭК. Возможно применение ИСО/МЭК 27005.

Возможными видами обработки рисков являются:
- избежание риска,
- снижение риска;
- смягчение риска,
- перенос риска.

Остающийся после обработки риск является остаточным. Хорошей практикой является эксплуатация продукта только при приемлемом и принятом остаточном риске. Предназначенная для внедрения политика безопасности системы соответствует этапу «смягчение» обработки риска и является результатом оценки риска.

Сам менеджмент риска и полученная в результате политика безопасности системы могут пройти процесс обеспечения доверия.

Е.3 Модель безопасности

В отношении приведенного ниже рисунка Д.1 можно сформулировать следующие положения:

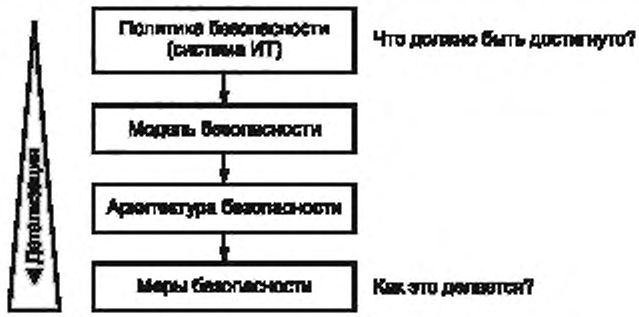


Рисунок Д.1 — Модель безопасности

- модель безопасности является схематическим описанием группы объектов и взаимосвязей, посредством которых заданный набор услуг по обеспечению безопасности предоставляется системой или в рамках системы;
- архитектура безопасности представлена планом и совокупностью принципов, которые считаются частью проектирования безопасности системы:

услуги по обеспечению безопасности, требуемые от системы для выполнения требований пользователей,

элементы системы, требуемые для выполнения услуг,

уровни производительности, необходимые в элементах системы для работы в условиях угроз;

- мера обеспечения безопасности является процессом (или устройством, осуществляющим подобный процесс), который может применяться для выполнения услуги по обеспечению безопасности, предоставляемой системой или в рамках системы, например механизмом предупреждения событий, мерой по обнаружению атак, мерой по восстановлению после события.

На основе результатов оценки риска меры по обработке риска могут быть определены в рамках процесса разработки концепции безопасности.

В рамках концепции безопасности дается определение мер безопасности, которые определялись в контексте оценки риска как необходимые.

Объектом доверия, связанным с моделью безопасности, может быть анализ или проверка доступности и связности модели безопасности.

Методы обеспечения доверия, основанные на оценке риска, предлагают поэтапный подход с возрастающей детализацией от политики до определения выполненных мер безопасности.

Е.4 Политика безопасности организации

Системы ИТ следуют определенной политике безопасности системы ИТ, которая может следовать политике безопасности организации. Политика безопасности организации в основном базируется на оценке риска с учетом целей организации (например, бизнес-целей). Она применима ко всем проблемам безопасности организации и обязательна для руководства всеми усилиями по обеспечению безопасности.

В этих случаях политика безопасности организации модифицируется и адаптируется в иерархическом виде для всех подразделений организации и систем.

Любая политика безопасности должна периодически инспектироваться для учета всех изменений угроз, рисков и активов.

Политика безопасности может включать в себя следующие темы для обсуждения:

- область применения политики безопасности,
- подотчетность руководства,
- подчеркивание важности безопасности,
- определение общих и конкретных ролей и обязанностей; распределение должностей;
- определение целей обеспечения безопасности;
- классификация информации;
- вопросы коммуникации, осведомленности, обучения и подготовки.

В крупных организациях для конкретного отдела, подразделения или филиала, а также при наличии разнообразных отдельных систем может потребоваться разработка более специфических политик безопасности. На уровне конкретной системы, услуги или продукта разработка принимает форму целевой политики безопасности ИТ, которая соответствует иерархии политик.

Возможная иерархия политик предоставлена на рисунке Е.2.

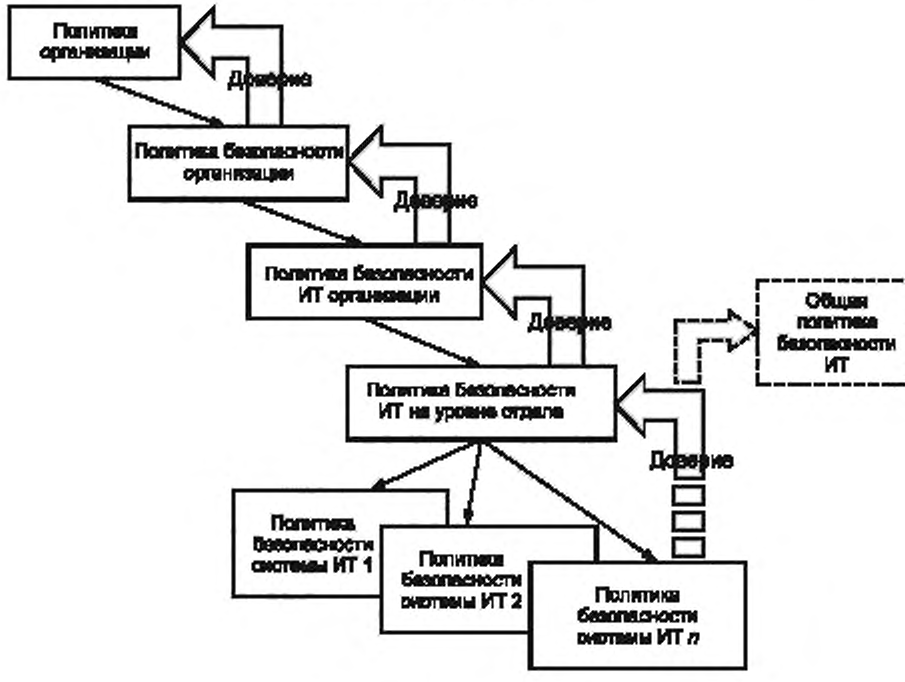


Рисунок Е.2 — Иерархия политик и доверия

Для обеспечения зависимостей иерархии политик должны предприниматься соответствующие меры по обеспечению доверия. Дополнительным объектом обеспечения доверия может быть анализ или проверка доступности и согласованности политик безопасности.

Е.5 Применимая цель обеспечения доверия

Целью обеспечения любого доверия к безопасности является обеспечение уверенности в соответствии системы ИТ объекта руководящей политике на следующем более высоком уровне для гарантии соответствия объекта политике организации.

Таким образом, в данном случае доверие может быть производной оценки риска и/или политики безопасности организации.

Для многих операций с ИТ, в особенности ИТ средних или небольших организаций, определенная политика безопасности не предписывается. В этом случае можно использовать имеющуюся в наличии общую политику безопасности.

Данное положение также относится к случаю, когда пользователь внедряет стандартную систему безопасности, например, из справочников по базовой безопасности. Здесь доверие обеспечивается для общих потребностей среды, которые должны быть разъяснены в прилагаемых справочниках по базовой безопасности.

Другим подходом является применение имеющегося задания по безопасности или профиля защиты, который был подготовлен для данной целевой среды в соответствии с ИСО/МЭК 15408.

Примечание — Проведение оценки риска является процессом, который сам по себе может быть предметом обеспечения доверия к процессу. При данном подходе к обеспечению доверия оценивается применение процессов и их результатов, включая их обратную связь, которая обеспечивает выполнение процесса, получение результатов и их обработку заданным способом связанным с безопасностью персоналом.

Е.6 Меры безопасности

Меры безопасности, определения которым даны в процессе менеджмента рисков, добавляют к функциональным требованиям объекта с целью производства технической спецификации или спецификации по поставке.

В случаях применения обобщенной политики политика безопасности, модель и архитектура предопределены и не изменяются. Однако в большинстве случаев предлагается сделать выбор или предлагается каталог, из которого выбирают меры безопасности, наиболее подходящие для конкретной ситуации с угрозами.

В данном случае очень важно проверить описание имеющихся целей безопасности, если весь применимый риск смягчается. Требование не относится к случаю, когда активы обладают особой ценностью и/или подвергаются особым угрозам. В этом случае и при наличии каких-либо сомнений следует провести специальную оценку риска, которая приведет к применению специальных мер. Эта гибридная технология показана на рисунке Е.3.

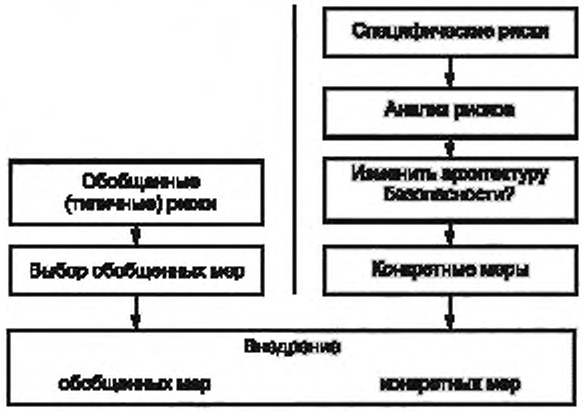


Рисунок Е.3 — Гибридная модель безопасности

Объектом доверия, связанным с определением мер безопасности, может быть анализ или проверка доступности или связности модели безопасности.

Примечание — В зависимости от методов обеспечения безопасности применяются меры, принимающие вид, например, мер защиты (см. ИСО/МЭК 13335), мер контроля (см. ИСО/МЭК 27002) или задания по безопасности (см. ИСО/МЭК 15408).

Е.7 Пример: ИСО/МЭК 15408

В ИСО/МЭК 15408 используется следующая терминология:

- объект оценки (ОО) — продукт или система ИТ и связанная с ними руководящая документация, подлежащие оценке;
- политика безопасности объекта оценки (ПБО) — совокупность правил, регулирующих управление активами, их защиту и распределение в пределах ОО;
- задание по безопасности (ЗБ) — совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки продукта;
- функция безопасности (ФБ) — функциональные возможности части или частей продукта, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО;
- политика функции безопасности (ПФБ) — политика безопасности, осуществляемая ФБ.

Библиография

[1] ISO/IEC Guide 61[1], *General requirements for assessment and accreditation of certification/registration bodies*

[2] ISO/IEC Guide 65, *General requirements for bodies operating product certification systems*

[3] ISO/IEC Guide 67, *Conformity Assessment — Fundamentals of product certification*

[4] ISO/IEC Guide 73, *Risk Management — Vocabulary — Guidelines for use in standards*

[5] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[6] ISO 9001, *Quality management systems — Requirements*

[7] ISO/IEC 13335-1, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[8] ISO/IEC 15288, *Systems and software engineering — System life cycle processes*

[9] ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[10] ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*

[11] ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*

[12] ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

[13] ISO/IEC 17024, *Conformity Assessment — General requirements for bodies operating certification of persons*

[14] ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*

[15] ISO/IEC 19791, *Information technology — Security techniques — Security assessment of operational systems*

[16] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

[17] ISO/IEC 21827, *Information technology — Security techniques — Systems Security Engineering — Capability maturity model® (SSE-CMM®)*

[18] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[19] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

[20] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[21] CEN/CENELEC EN 45013: General criteria for certification bodies operating certification of personnel

[22] FIPS 140-1: Federal Information Processing Standard: Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST),gost.e-ecolog.ru

[23] IT Grundschutz (Baseline Protection) Manual, Bundesamt für Sicherheit in der IT (BSI), 2004, gost.e-ecolog.ru

[24] A Comparative Study of IT Security Criteria, Initiative D21, Initiative D21 e. V., Siemensdamm 50, 13629 Berlin, Germany

[25] A Guide to Certification and Accreditation for Information Technology Systems (MG-4), January 1996, CSE, The ITS Publications Section, (613) 991-7514/7468 *or http://*gost.e-ecolog.ru

[26] A Guide To Risk Assessment and Safeguard Selection for Information Technology Systems, January 1996, CSE, The ITS Publications Section, (613) 991-7514/7468 or gost.e-ecolog.ru

[27] COBIT MAPPING — Overview of International IT Guidance, IT Governance Institute, January 2004, IT Governance Institute, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA, (847) 590 7491 or gost.e-ecolog.ru

[28] Fiona Pattinson, Comparing ISO 17799:2000 with SSE CMM V2, 2002, gost.e-ecolog.ru *SSE CMM comparison.pdf*

[29] Susanne Rohrig, Using Process Models To Analyse IT Security Requirements, Thesis, Faculty of Economics, University of Zurich, Switzerland, March 2003

[1] Отменено и заменено на ISO/IEC 17011.

УДК 681.324:006.354 ОКС 35.040

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

Редактор *В.Н. Копысов*
Технический редактор *В.Н. Прусакова*
Корректор *В.Е. Нестерова*
Компьютерная верстка *В.И. Грищенко*

Сдано в набор 27.12.2012. Подписано в печать 07.02.2013. Формат 60x84 1/8. Гарнитура Ариал. Усл. печ. л. 6,05. Уч.-изд. л. 5,45. Тираж 96 экз. Зак. 131.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru