ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 54582—2011/ ISO/IEC/TR 15443-2:2005

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы доверия к безопасности информационных технологий

Часть 2

Методы доверия

ISO/IEC TR 15443-2:2005
Information technology — Security techniques — A framework for IT security assurance — Part 2: 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 международного стандарта, указанного в пункте 4

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 690-ст

3 Настоящий стандарт идентичен международному документу ISO/IEC TR 15443-2:2005 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 2. Методы доверия» (ISO/IEC TR 15443-2:2005 «Information technology — Security techniques — A framework for IT security assurance — Part 2: Assurance methods»)

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

4 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, уведомления 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 Область применения . . . 1
1.3 Ограничения . . . 2
2 Нормативные ссылки . . . 2
3 Термины, определения и сокращения . . . 4
4 Краткий обзор и представление методов обеспечения доверия . . . 4
5 Фаза жизненного цикла доверия и условные обозначения . . . 4
5.1 Подход к обеспечению доверия и условные обозначения . . . 4
5.2 Актуальность и условные обозначения . . . 5
5.3 Значимость безопасности и условные обозначения . . . 5
5.4 Обзор методов обеспечения доверия . . . 5
5.5 Методология представления . . . 7
6 Методы обеспечения доверия . . . 7
6.1 ИСО/МЭК 15408 — критерии оценки безопасности информационных технологий . . . 7
6.2 TCSEC — критерии оценки безопасности доверенных компьютерных систем . . . 8
6.3 ITSEC/ITSEM — методология и критерии оценивания безопасности информационных технологий . . . 10
6.4 CTCPEC — канадские критерии оценивания доверенного продукта . . . 11
6.5 KISEC/KISEM — корейские критерии и методология оценивания информационной безопасности . . . 12
6.6 RAMP — фаза поддержания классификации . . . 13
6.7 ERM — поддержание классификации при оценивании (в общем) . . . 13
6.8 TTAP — программа оценки доверенных технологий . . . 14
6.9 TPEP — программа оценивания доверенного продукта . . . 15
6.10 Рациональный универсальный процесс® (RUP®) . . . 15
6.11 ИСО/МЭК 15288 — процессы жизненного цикла системы . . . 16
6.12 ИСО/МЭК 12207 — процессы жизненного цикла программного обеспечения . . . 17
6.13 V-модель . . . 18
6.14 ИСО/МЭК 14598 — оценивание программного продукта . . . 19
6.15 Основные услуги по безопасности базовой структуры X/Open . . . 20
6.16 SCT — строгое тестирование соответствия . . . 21
6.17 ИСО/МЭК 21827 — Проектирование безопасности систем — Модель зрелости процесса (SSE-CMM®) . . . 22
6.18 TCMM — доверенная модель зрелости процесса . . . 23
6.19 CMMI — интеграция модели зрелости процесса® . . . 24
6.20 ИСО/МЭК 15504 — оценка программного процесса . . . 25
6.21 CMM — модель CMM® (для программного обеспечения) . . . 25
6.22 SE-CMM® — модель зрелости процесса системного проектирования® . . . 26
6.23 TSDM — методология разработки доверенного программного обеспечения . . . 27

6.24 SdoC — декларация поставщика о соответствии . . . 28
6.25 SA-CMM® — модель зрелости возможностей приобретения программного обеспечения® . . 28
6.26 Серия ИСО 9000 — менеджмент качества . . . 29
6.27 ИСО 13407 — ориентированное на человека проектирование (HCD) . . . 30
6.28 Характеристика разработчика (в общем) . . . 31
6.29 ИСО/МЭК 17025 — доверие к аттестации . . . 32
6.30 ИСО/МЭК 13335 — менеджмент безопасности информационных и телекоммуникационных технологий . . . 33
6.31 BS 7799-2 — системы менеджмента информационной безопасности. Спецификация с руководством по применению . . . 34
6.32 ИСО/МЭК 17799 — практические правила менеджмента информационной безопасности . . . 34
6.33 FR — исправление дефектов (в общем) . . . 35
6.34 Руководство по базовой защите информационных технологий . . . 36
6.35 Испытание проникновением . . . 37
6.36 Аттестация персонала (в общем) . . . 38
6.37 Аттестация персонала (в части безопасности) . . . 39
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 41
Библиография . . . 43

Введение

В настоящем стандарте представлено описание методов обеспечения доверия и подходов, которые можно применить к безопасности информационных и коммуникационных технологий (ИКТ), предложенных или используемых различными типами организаций, независимо от того, утверждены ли они, одобрены неофициально или стандартизированы, а также их привязка к модели доверия по ГОСТ Р 54581—2011/ISO/IEC/TR 15443-1:2005. Акцент делается на идентификацию качественных характеристик методов, способствующих обеспечению доверия, и на их ранжирование. Настоящий стандарт предназначен для разъяснения специалистам в области безопасности ИКТ способов получения доверия на любом этапе жизненного цикла продукта или услуги.

В настоящем стандарте также приводятся цель и описание методов обеспечения доверия, а также указывается их место в структуре, определенной в ГОСТ Р 54581—2011/ISO/IEC/TR 15443-1:2005.

Считается, что методы обеспечения доверия, указанные в настоящем стандарте, содержат общеизвестные элементы. Могут появляться новые методы обеспечения доверия, а также модифицироваться и совершенствоваться уже существующие.

Из настоящего стандарта разработчики, оценщики, менеджеры по качеству и покупатели могут выбирать методы обеспечения доверия к программному обеспечению и системам безопасности ИКТ, определяя требования доверия, оценивая продукты, измеряя аспекты безопасности и т. д. Кроме того, они могут использовать методы обеспечения доверия, не включенные в настоящий стандарт, которые применимы к методам обеспечения доверия в отношении аспектов безопасности, хотя многие из этих методов могут также применяться в интересах обеспечения доверия к другим критическим аспектам программного обеспечения и систем.

Настоящий стандарт предназначен для совместного использования с ГОСТ Р 54581—2011/ISO/IEC/TR 15443-1:2005.

В настоящем стандарте также проведен анализ методов обеспечения доверия, не уникальных для безопасности ИКТ; однако руководство, приведенное в настоящем стандарте, ограничено требованиями безопасности ИКТ. В него включены также термины и понятия, получившие определение в других инициативах международной стандартизации (например, CASCO) и международных справочниках (ИСО/МЭК Руководство 2); однако руководство, приведенное в настоящем стандарте, будет связано исключительно с областью безопасности ИКТ и не предназначено для общего менеджмента и оценки качества, а также согласованности ИКТ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы доверия к безопасности информационных технологий

Часть 2

Методы доверия

Information technology. Security techniques. A framework for IT security assurance. Part 2. Assurance methods

Дата введения — 2012—12—01

1 Область применения

1.1 Назначение

В настоящем стандарте представлена совокупность методов обеспечения доверия, включая методы, не являющиеся уникальными для безопасности информационных и коммуникационных технологий (ИКТ), поскольку они способствуют обеспечению общей безопасности ИКТ. В настоящем стандарте приведен краткий обзор их назначения, описание, ссылки на документы и аспекты стандартизации.

В принципе результирующее доверие к безопасности ИКТ является доверием к продукту, системе или предоставленной услуге. Следовательно, результирующее доверие является суммой приращений доверия, полученных каждым из методов обеспечения доверия, примененным к продукту, системе или услуге на стадиях их жизненных циклов. Большое количество методов делает необходимым создание руководства в отношении того, какой метод применять к данной области ИКТ для обеспечения общепризнанного доверия.

Каждый элемент совокупности методов обеспечения доверия, представленной в настоящем стандарте, классифицируется в виде краткого обзора с помощью основных терминов и понятий о доверии, разработанных в ИСО/МЭК ТО 15443-1.

Посредством такого распределения по категориям настоящий стандарт оказывает содействие специалисту по ИКТ при выборе и возможном комбинировании методов обеспечения доверия, соответствующих данному продукту безопасности ИКТ, системе или услуге и их специфичным средам.

1.2 Область применения

Настоящий стандарт представляет собой руководство в сокращенном обзорном варианте. Его достаточно для формирования из представленной совокупности методов обеспечения доверия сокращенного набора методов, применимых продукту, системе или услуге.

Краткое изложение применимых методов обеспечения доверия является информативным, представляющим основы для облегчения его понимания без обращения к первоисточникам.

Предполагаемыми пользователями настоящего стандарта являются:

1) покупатель (конкретное лицо или организация, приобретающая или покупающая систему, программный продукт или услугу у поставщика);

2) оценщик (конкретное лицо или организация, проводящая оценку; оценщиком может быть испытательная лаборатория, отдел технического контроля организации, разрабатывающей программное обеспечение (ПО), государственная организация или пользователь);

3) разработчик (конкретное лицо или организация, осуществляющая деятельность по разработке, включая анализ требований, проектирование и тестирование посредством приемки во время процесса жизненного цикла ПО);

Издание официальное

4) обслуживающее лицо (конкретное лицо или организация, осуществляющая деятельность по обслуживанию);

5) поставщик (конкретное лицо или организация, заключающая договор с покупателем о поставке системы, программного продукта или услуги по программированию на условиях договора);

6) пользователь (конкретное лицо или организация, применяющая программный продукт для выполнения специфичной функции) при оценке качества какого-либо программного продукта во время приемо-сдаточных испытаний;

7) работник или отдел службы безопасности (конкретное лицо или организация, проводящая системную проверку программного продукта или услуг по программированию) при оценке качества ПО во время квалификационных испытаний.

1.3 Ограничения

Настоящий стандарт представляет собой руководство в виде краткого обзора. ИСО/МЭК ТО 15443-3 определяет направления совершенствования этого выбора методов обеспечения безопасности в целях лучшей реализации требований доверия, делая возможным анализ их сравнительных и синергетических характеристик.

Требования к инфраструктуре поддержки верификации подхода к обеспечению доверия и требования к персоналу проведения верификации в настоящем стандарте не рассматриваются.

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные документальные источники. Для недатированных ссылок применяют последнее издание упомянутого ниже документа (включая опубликованные изменения).

ИСО 9000 Системы менеджмента качества. Основные положения и словарь (ISO 9000, Quality management systems — Fundamentals and vocabulary)

ИСО 9001 Системы менеджмента качества. Требования (ISO 9001, Quality management systems — Requirements)

ИСО/МЭК 9126-1[1)] Программотехника. Качество продукта. Часть 1. Модель качества (ISO/IEC 9126-1, Software engineering — Product quality — Part 1: Quality model)

ИСО/МЭК 12207[2)] Информационная технология. Процессы жизненного цикла программного обеспечения (ISO/IEC 12207, Information technology — Software life cycle processes)

ИСО/МЭК 13335-1[3)] Информационная технология. Методы и средства обеспечения безопасности. Менеджмент безопасности информационных и телекоммуникационных технологий. Часть 1. Концепция и модели управления безопасностью информационных и коммуникационных технологий (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)

ИСО/МЭК ТО 13335-2[4)] Информационная технология. Руководство по менеджменту безопасности информационных технологий. Часть 2. Планирование и менеджмент безопасности информационных технологий (ISO/IEC TR 13335-2, Information technology — Guidelines for the management of IT Security — Part 2: Managing and planning IT Security)

ИСО/МЭК ТО 13335-3[5)] Информационная технология. Руководство по менеджменту безопасности информационных технологий. Часть 3. Методы менеджмента безопасности информационных технологий (ISO/IEC TR 13335-3, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT Security)

[1)] Заменен на ИСО/МЭК 25010—2011 «Проектирование систем и разработка программного обеспечения. Требования к качеству систем и программного обеспечения и их оценка (SQuaRE). Модели качества систем и программного обеспечения (ISO/IEC 25010 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models)».

[2)] Заменен на ИСО/МЭК 12207 «Информационные технологии. Процессы жизненного цикла программного обеспечения» (ISO/IEC 12207, Systems and software engineering — Software life cycle processes).

[3)] Отменен.

[4)] Отменен.

[5)] Заменен на ИСО/МЭК 27005 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (ISO/IEC 27005 Information technology — Security techniques — Information security risk management).

ИСО/МЭК ТО 13335-4[1)] Информационная технология. Руководство по менеджменту безопасности информационных технологий. Часть 4. Выбор защитных мер (ISO/IEC TR 13335-4, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards)

ИСО/МЭК ТО 13335-5[2)] Информационная технология. Руководство по менеджменту безопасности информационных технологий. Часть 5. Руководство по менеджменту безопасности сети (ISO/IEC TR 13335-5, Information technobgy — Guidelines for the management of IT Security — Part 5: Management guidance on network security)

ИСО/МЭК ТО 14598-1 Информационная технология. Оценка программного продукта. Часть 1. Общий обзор (ISO/IEC 14598-1, Information technology — Software product evaluation — Part 1: General overview)

ИСО/МЭК 15939 Технология программного обеспечения. Процесс измерения (ISO/IEC 15939, Software engineering — Software measurement process)

ИСО/МЭК 15288 Системное проектирование. Процессы жизненного цикла систем (ISO/IEC 15288, Systems engineering — System life cycle processes)

ИСО/МЭК 15408-1 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель (ISO/EC 15408-1, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model)

ИСО/МЭК 15408-2[3)] Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (ISO/EC 15408-2, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements)

ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности (ISO/EC 15408-3, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements)

ИСО/МЭК 15504-1 Информационная технология. Оценка процессов. Часть 1. Концепции и словарь (ISO/EC 15504-1, Information technology — Process assessment — Part 1: Concepts and vocabulary)

ИСО/МЭК 15504-2 Информационная технология. Оценка процессов. Часть 2. Проведение оценки (ISO/EC 15504-2, Information technology — Process assessment — Part 2: Performing and assessment)

ИСО/МЭК 15504-3 Информационная технология. Оценка процессов. Часть 3. Руководство по проведению оценки (ISO/EC 15504-3, Information technology — Process assessment — Part 3: Guidance on performing an assessment)

ИСО/МЭК 15504-4 Информационная технология. Оценка процессов. Часть 4. Руководство по использованию для усовершенствования и определения возможностей процесса (ISO/EC 15504-4, Information technology — Process assessment — Part 4: Guidance on use for process improvement and process capability determination)

ИСО/МЭК 15504-5 Информационная технология. Оценка процессов программного обеспечения. Часть 5. Пример модели оценки и руководство по указателям (ISO/IEC TR 15504-5, Information technology — Software Process Assessment — Part 5: An assessment model and indicator guidance)

ИСО/МЭК 17799[4)] Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью (ISO/EC 17799, Information technology — Security techniques — Code of practice for information security management)

ИСО/МЭК 21827 Информационная технология. Проектирование безопасности работы систем. Модель технологической зрелости (SSE-CMM®) (ISO/EC 21827, Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®))

ИСО/МЭК 90003 Техника программного обеспечения. Рекомендации по применению ИСО 9001:2000 к компьютерному программному обеспечению (ISO/EC 90003, Software engineering — Guidelines for the application of ISO 9001:2000 to computer software)

[1)] Заменен на ИСО/МЭК 27005 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (ISO/IEC 27005 Information technology — Security techniques — Information security risk management).

[2)] Отменен.

[3)] Заменен на ИСО/МЭК 15504-2 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (ISO/IEC 27005 Information technology — Security techniques — Information security risk management).

[4)] Заменен на ИСО/МЭК 27002 Информационные технологии. Свод правил по управлению защитой информации. ((ISO/IEC Information technology — Security techniques — Code of practice for information security management).

3 Термины, определения и сокращения

В настоящем стандарте применены термины, определения и сокращения по ИСО/МЭК ТО 15443-1.

4 Краткий обзор и представление методов обеспечения доверия

В ИСО/МЭК ТО 15443-1 представлена схема распределения по категориям существующих методов обеспечения доверия, перечислены и представлены существующие методы обеспечения доверия, представляющие интерес и непосредственно связанные с областью безопасности ИКТ. В настоящем разделе эти методы классифицируются по следующей схеме:

- в соответствии с различными фазами доверия — описание аспектов жизненного цикла: проектирование, реализация, интеграция, верификация, ввод в действие, перемещение или эксплуатация;
- в соответствии с различным подходом к обеспечению доверия: продукт, процесс или среда.

В ИСО/МЭК ТО 15443-1 указано, что метод обеспечения доверия может включать в себя комбинацию подхода к доверию и фазы доверия.

В качестве дополнительного руководства для пользователя в таблице 2 подраздела 5.4 настоящего стандарта представлено распределение по категориям:

- со значимостью отдельных методов для безопасности ИКТ;
- с актуальностью отдельных методов.

5 Фаза жизненного цикла доверия и условные обозначения

В таблице 2 подраздела 5.4 настоящего стандарта перечислены представленные ниже методы, классифицированные в соответствии с фазой жизненного цикла. В названии каждого отдельного перечисления повторяется его классификация.

Представляющие наибольший интерес фазы жизненного цикла представлены графически четырьмя столбцами таблицы. В соответствии с требованиями ИСО/МЭК 15288 и ИСО 9000 технологические процессы жизненного цикла сгруппированы в четыре стадии, по одной на каждый столбец, и сокращенно обозначены:

- 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.

Примечания

1 Конкретный метод обеспечения доверия может охватывать какую-то фазу жизненного цикла только приблизительно. В этом случае эта фаза отсутствует в графическом представлении.

2 Процессы жизненного цикла D-I-T-O применимы к любой конкретной системе ИКТ и ее компонентам, т. е. к аппаратным средствам и ПО. Разработка и улучшение процессов жизненного цикла являются вторым измерением, которое можно представить графически, но в настоящее время это измерение не представлено. В области безопасности ИКТ это измерение имеет особое значение из-за методов управления безопасностью, примененных к системам ИКТ на фазе функционирования в соответствии с ИСО/МЭК 17799 и BS 7799-2. По существу разработка и улучшение процессов жизненного цикла включает в себя оценку и документирование, разработку, измерение, улучшение и сертификацию процессов. Это второе измерение является прямоугольным (ортогональным) по отношению к измерению D-I-T-O.

5.1 Подход к обеспечению доверия и условные обозначения

В таблице 2 подраздела 5.4 настоящего стандарта перечислены представленные ниже методы, распределенные по категориям в соответствии с их подходом к обеспечению доверия. В названии каждого отдельного метода отражается его соответствие по категории.

Категории методов обеспечения доверия наглядно представлены в таблице 1:

- доверие к продукту: обозначено заглавной буквой названия фазы жизненного цикла между стрелками, например, →D→;
- доверие к процессу: обозначено заглавной буквой названия фазы жизненного цикла на темном фоне, например, D;
- доверие к среде: обозначено заглавной буквой названия фазы жизненного цикла с полосками слева и справа, например, ▌D ▐.

Таблица 1 — Структура методов обеспечения доверия — условные обозначения

Раздел	Доверие — фаза→ — подход ↓	Проект/ реализация	Интеграция/ верификация	Ввод в действие/ переход	Эксплуатация
	Продукт [/Система/Услуга][🔒] Процесс [🔒]	→D→	→|→	→T→	→O→
		D	I	T	O
	Среда [/Организация/ Персонал] [🔒]	D	I	T	O

Примечания

1 Поскольку методы обеспечения доверия могут характеризовать комбинацию подходов, символы можно объединить, например, метод, обеспечивающий как доверие к процессу, так и доверие к среде, может быть представлен буквой на темном фоне с полосками слева и справа.

2 Конкретный метод может охватывать более или менее полно один подход. Презентация в виде визуального обзора не годится для представления степени охвата различных подходов к обеспечению доверия данным методом.

3 Конкретный метод обеспечения доверия может охватывать какой-то подход только приблизительно. В этом случае в графическом представлении данный подход отсутствует.

5.2 Актуальность и условные обозначения

Вследствие большого числа методов пользователю настоящего стандарта дается указание в отношении их состояния. В таблице 2 эти состояния отражены следующим образом:

- в настоящее время действующие и широко применяемые методы представлены в таблице 2 полужирным шрифтом;
- устаревающие, вытесняемые, объединяющиеся или иным образом утрачивающие свою актуальность методы представлены в таблице 2 светлым шрифтом.

Примечание — Эта легенда не повторяется в названии отдельного перечня данного подраздела.

5.3 Значимость безопасности и условные обозначения

Из-за очень большого числа методов пользователю настоящего стандарта дано указание в отношении безопасности их ИКТ. В таблице 2 это состояние отражено следующим образом:

- ориентированные непосредственно на обеспечение безопасности ИКТ методы обозначены символом (🔒) («замок»).

5.4 Обзор методов обеспечения доверия

В таблице 2 представлен обзор рассматриваемых методов обеспечения доверия наряду с их классификацией в соответствии со структурой, разработанной в ИСО/МЭК ТО 15443-1.

Таблица 2 — Структура методов обеспечения доверия. Краткий обзор

Раздел	Доверие — фаза→ — подход ↓	Проект/ реализация	Интеграция/ верификация	Ввод в действие/ переход	Функционирование
6.1	ИСО/МЭК 15408 — критерии оценки безопасности ИТ 🔒	→D→	→|→	→T→	→O→
6.2	TCSEC — критерии оценки доверенной компьютерной системы 🔒	→D→	→|→		→O→
6.3	ITSEC/ITSEM — критерии оценки безопасности ИТ и методология 🔒	→D→	→|→		→O→
6.4	CTCPEC — Канадские критерии оценки доверенного продукта 🔒	→D→	→|→		
6.5	KISEC/KISEM — критерии оценки информационной безопасности и методология Кореи 🔒	→D→	→|→		→O→

Продолжение таблицы 2

Раздел	Доверие — фаза→ — подход ↓	Проект/ реализация	Интеграция/ верификация	Ввод в действие/ переход	Функционирование
6.6	RAMP — фаза поддержки классификации	→D→	→|→		→O→
6.7	ERM — поддержка классификации оценки (в общем)	→D→	→|→		→O→
6.8	TTAP — программа оценки доверенной технологии	→D→	→|→		
6.9	TPEP — программа оценки доверенного продукта	→D→	→|→		
6.10	Рациональный комплексный процесс® (RUP®)	→D→	→|→		
6.11	ИСО/МЭК 15288 — процессы жизненного цикла системы	→D→	→|→	→T→	→O→
6.12	ИСО/МЭК 12207 — процессы жизненного цикла ПО	→D→	→|→	→T→	→O→
6.13	V — модель	→D→	→|→	→T→	→O→
6.14	ИСО/МЭК 14598 — оценка программного продукта	→D→			→O→
6.15	Услуги по обеспечению базовой безопасности X/Open	→D→			
6.16	SCT — тестирование строгого соответствия		→|→		
6.17	ИСО/МЭК 21827 — проектирование безопасности работы систем — модель зрелости (SSE-CMM®)	D	I	T	O
6.18	TCMM — доверенная модель технологической зрелости	D	I		
6.19	CMMI — интеграция модели технологической зрелости®	D	I	T	O
6.20	ИСО/МЭК 15504 — оценка программного процесса	D	I	T	O
6.21	CCM — модель технологической зрелости® (для ПО)	D	I		
6.22	SE-CMM® — модель технологической зрелости системного проектирования®	D	I		
6.23	TSDM — методология разработки выверенного ПО	D	I		
6.24	SdoC — заявление поставщика о соответствии	D			
6.25	SA-CMM® — модель зрелости возможностей приобретения программного обеспечения®			T	
6.26	ИСО серия 9000 — менеджмент качества	D	I	T	O

Окончание таблицы 2

Раздел	Доверие — фаза→ — подход ↓	Проект/ реализация	Интеграция/ верификация	Ввод в действие/ переход	Функционирование
6.27	ИСО 13407— сконцентрированный на человеке проект	D			
6.28	Генеалогия разработчика (в общем)	D			
6.29	ИСО/МЭК 17025 — доверие к аккредитации	D	I		
6.30	ИСО/МЭК 13335 — руководства по управлению безопасностью ИТ (GMITS)		I	T	O
6.31	BS 7799-2 — системы управления информационной безопасностью. Спецификация с руководством				O
6.32	ИСО/МЭК 17799 — практические правила управления информационной безопасностью				O
6.33	FR — исправление дефектов (в общем)				O
6.34	Базовое руководство по защите ИТ				→O→
6.35	Тестирование проникновения				→O→
6.36	Аттестация персонала (не связанная с безопасностью)				O
6.37	Аттестация персонала (связанная с безопасностью)	D	I	T	O

5.5 Методология представления

В разделе 6 представлен анализ идентифицированных методов обеспечения доверия. Поскольку многие методы обеспечения доверия связаны с различными подходами к обеспечению доверия, каждый метод должен быть представлен со своим описанием. На данном этапе сравнение методов не предусмотрено.

В подразделах раздела 6 представлен структурированный краткий обзор каждого метода обеспечения доверия, идентифицированного в данной технологической схеме.

Наименование метода отражает его суть и является полным и официальным названием метода обеспечения доверия при ссылке на него, а также при необходимости использования в качестве ссылки — символическим.

Каждый краткий обзор подразделяют на следующие составные части:

- цель: краткое отличительное назначение метода;
- описание: краткое описание метода;
- источники, описывающие: адрес/ссылку на комитеты и/или организации и документы по методу и/или стандартизации.

6 Методы обеспечения доверия

6.1 ИСО/МЭК 15408 — критерии оценки безопасности информационных технологий

→D→	→I→	→T→	→O→

6.1.1 Цель

Обеспечение согласованной схемы и подробных критериев оценки безопасности ИТ, пригодных для использования как в государственных структурах, так и для общего пользования.

6.1.2 Описание

Общие критерии разработаны по поручению правительственных учреждений, связанных с информационной безопасностью, как способ независимой оценки характеристик безопасности продуктов и систем ИКТ. Критерии были разработаны во взаимодействии с совместным техническим комитетом 1, подкомитет 27, «Методы и средства обеспечения безопасности» (СТК 1 ПК 27) и опубликованы как международный стандарт ИСО/МЭК 15408.

Общие критерии разделяют понятия «функциональные возможности безопасности» и «доверие к безопасности» и детально специфицируют методы, средства и функции, которые могут способствовать созданию уверенности в соответствии продукта безопасности целям безопасности. Конкретные методы, средства и функции доверия определены в ИСО/МЭК 15408-3 и в первую очередь (но не исключительно в этих целях) предназначены для получения доверия посредством независимой оценки или верификации. Планируется возможность верификации согласованного применения критериев оценки посредством схем национальной сертификации.

В рамках ИСО/МЭК 15408-3 методы и средства обеспечения доверия разделены на четыре области применения, называемые «классами». В пределах каждого класса определены различные методы, называемые «семействами». В каждом семействе имеются один или более уровней строгости. Уровни строгости, по которым могут применяться методы, называются «компонентами». Каждый компонент обозначает необходимые точные действия и элементы доказательства.

В рамках ИСО/МЭК 15408-3 определены несколько пакетов компонентов доверия, работающих вместе на взаимно дополняющей основе. Пакеты компонентов доверия, работающих вместе на взаимно дополняющей основе, называют «оценочными уровнями доверия».

Вспомогательная методология по применению этих критериев, общая методология оценки разрабатываются рабочей группой по общей методологии оценки, являющейся подгруппой проекта общих критериев.

6.1.3 Источники

ИСО/МЭК 15408-1; ИСО/МЭК 15408-2; ИСО/МЭК 15408-3.

Примечание — ИСО/МЭК 15408 является результатом деятельности ИСО/МЭК с совместным техническим комитетом 1, подкомитет 27, рабочая группа 3 (СТК 1/ПК 27/РГ 3) «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности»

6.2 TCSEC — критерии оценки безопасности доверенных компьютерных систем

→D→	→I→		→O→

6.2.1 Цель

Классификация или определение класса безопасности продукта компьютерной системы.

6.2.2 Описание

Критерии оценки безопасности доверенных компьютерных систем (TCSEC) являются совокупностью критериев, ранее использовавшихся для классификации или определения класса безопасности, обеспечиваемой продуктом компьютерной системы. Новые оценки с использованием TCSEC в настоящее время не проводятся, хотя разработки их ведутся. Иногда TCSEC называют «Оранжевой книгой» из-за оранжевого цвета ее обложки.

Продукт «соответствует» TCSEC при условии его оценки по «Программе оценивания доверенного продукта» (TPEP) или «Программе оценки доверенной технологии» (TTAP) на соответствие требованиям установленного класса TCSEC или если независимая оценка выявила у продукта наличие характеристик и доверия этого класса.

Класс является специфической совокупностью требований TCSEC, которым соответствует оцениваемая система. В TCSEC имеется семь классов в порядке убывания характеристик и доверия: A1, B3, B2, B1, C2, C1 и D. Следовательно, система, оцененная по классу B3, имеет больше характеристик безопасности и/или больше уверенности в должном функционировании характеристик безопасности, чем система, оцененная по классу B1. Требования для более высокого класса всегда являются расширенной

версией более низшего класса. Таким образом, система класса B2 соответствует каждому функциональному требованию класса C2 и имеет более высокий уровень доверия.

Уровнем доверия является совокупность классов (см. вопрос 11) из TCSEC [см. FAQ (часто задаваемые вопросы) концепций критериев, вопрос 1]. В «Оранжевой книге» определены четыре уровня доверия в порядке убывания доверия и уменьшения характеристик: A, B, C и D. Следовательно, система, оцененная по конкретному классу уровня доверия B, имеет больше характеристик безопасности и/или больше уверенности в должном функционировании характеристик безопасности, чем система, оцененная по конкретному классу уровня доверия C. Хотя интерпретация подсистем компьютерной безопасности (CSSI) TCSEC специфицирует критерии для различных классов D, они не отражены в самих TCSEC, которые не предъявляют требований к системам уровня доверия D. По умолчанию неклассифицированной системой является уровень доверия D.

Требованиями к различным классам являются:

Класс D: минимальная защита — резервируют оцененные системы, которые не отвечают требованиям более высокого класса.

Класс C1: необязательная защита — доверенная вычислительная база (TCB) системы класса C1 номинально удовлетворяет требования необязательной защиты посредством разделения пользователей и данных. TCB объединяет несколько видов надежных мер управления, способных осуществлять ограничения доступа на индивидуальной основе, т. е. позволяющих пользователям защищать информацию о проекте или персональные данные или предотвращать случайное считывание или разрушение своих данных другими пользователями. Предполагается, что класс C1 объединяет пользователей, обрабатывающих данные на одинаковом уровне конфиденциальности.

Класс C2: управляемая защита доступа — системы этого класса осуществляют более тщательное необязательное управление доступом, чем системы класса C1, делая пользователей индивидуально ответственными за свои действия посредством регистрационных процедур, проверки событий, связанных с безопасностью, и изоляции ресурсов.

Класс B1: мандатная защита — для систем класса B1 требуются все характеристики, необходимые для класса C2. Кроме того, должны быть в наличии: неофициальная модель политики безопасности, маркировка данных (например, секретной или частной информации) и обязательный контроль доступа к указанным субъектам или объектам. Необходимо существование потенциальных возможностей точной маркировки выдаваемой информации.

Класс B2: структурированная защита — в системах класса B2 TCB основана на четко определенной и документированной официальной модели политики безопасности, для которой требуется распространение дискреционного и мандатного контроля доступа класса B1 на все субъекты и объекты в автоматизированной системе обработки данных. Кроме того, учитываются скрытые каналы. TCB должна быть тщательным образом структурирована на критически и некритически важные в отношении защиты элементы. Интерфейс TCB должен быть определен достаточно хорошо, а проект TCB и его реализация должны позволять подвергать ее более тщательному тестированию и более детальной проверке. Механизмы аутентификации должны быть усилены, доверенная организация производства — представлена в виде поддержки функций системного администратора и оператора системы, а также предусмотрены строгие меры контроля за конфигурационным управлением. Система должна быть относительно защищена от проникновения.

Класс B3: домены безопасности — TCB класса B3 должна соответствовать требованиям того, чтобы она служила связующим звеном между всеми доступами субъектов и объектами, была защищена от неумелого обращения и была достаточно проста, чтобы подвергнуть ее анализу и тестированию. TCB структурирована так, чтобы исключить код, необязательный для осуществления политики безопасности, с применением существенного системного проектирования во время разработки проекта и реализации TCB, направленных на минимизацию ее сложности. Должна проводиться поддержка системного администратора, механизмы проверки должны распространяться на сигнальные, связанные с безопасностью события, и должна возникать потребность в процедурах восстановления систем. Система в значительной степени должна быть защищена от проникновения.

Класс A1: верифицированный проект — системы класса A1 функционально эквивалентны системам класса B3 в отсутствие дополнительных архитектурных особенностей или требований к политике безопасности. Отличительной характеристикой систем этого класса является анализ, следующий из формальной спецификации проекта и методов верификации, и полученная высокая степень доверия к правильности реализации TCB. По своему характеру это доверие является экспериментальным (опытным), начиная с официальной модели политики безопасности и официальной высокоуровневой спецификации (FTLS) проекта. FTLS является высокоуровневой спецификацией системы, записанной на формальном математическом языке для формирования гипотез из теорем (демонстрирующих соот-

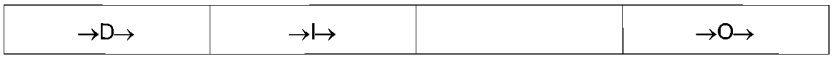
ветствие спецификации системы ее формальным требованиям) и их формального доказательства. Для соответствия расширенному проекту и анализу проекта ТСВ, необходимых для систем класса А1, требуется более строгое конфигурационное управление и формирование процедур безопасного распределения системы по местам эксплуатации. Администратору безопасности системы должна быть оказана поддержка.

6.2.3 Источники

См. [45].

Примечание — Все TCSEC, их интерпретации и руководства имеют разноцветные обложки и иногда называются «Радужной серией». TCSEC являются внутренним стандартом и продуктом Министерства обороны США.

6.3 ITSEC/ITSEM — методология и критерии оценивания безопасности информационных технологий



6.3.1 Цель

Предоставление структуры критериев и методологии оценивания безопасности ИТ для европейского рынка.

6.3.2 Описание

«Критерии оценивания безопасности информационных технологий (ITSEC)» и «Руководство по оцениванию безопасности информационных технологий (ITSEM)» находятся среди документов, предшествующих общим критериям и общей методологии оценки. Они были разработаны четырьмя европейскими странами: Францией, Германией, Нидерландами и Великобританией.

Доверие в ITSEC основано на подходе, представленном в TCSEC. Однако разделение между функциональными требованиями и требованиями доверия в ITSEC допускает большую гибкость. Требования доверия, в свою очередь, делятся на два аспекта — эффективность и правильность. Оценка эффективности включает в себя рассмотрение следующих аспектов объекта оценки (ОО):

- приемлемость функций обеспечения безопасности ОО для противодействия угрозам безопасности ОО, идентифицированным в нем;
- способность функций и механизмов обеспечения безопасности ОО объединяться на основе взаимной поддержки и формировать интегрированное и эффективное целое;
- способность механизмов обеспечения безопасности ОО противостоять прямым атакам;
- возможность на практике компрометации безопасности известными уязвимостями безопасности в конструкции ОО;
- невозможность конфигурирования или использования ОО небезопасным способом, но считающимся безопасным администратором или конечным пользователем ОО;
- возможность компрометации на практике безопасности известными уязвимостями безопасности при функционировании ОО.

Требования к эффективности доверия сосредоточены в основном на случаях, когда оценщику приходится применять собственные знания и опыт для оценки обоснованности подхода к безопасности в оцененном продукте или системе ИТ.

Требования доверия к правильности в ITSEC сосредоточены в основном на аспектах, которые должны подтверждать правильность информации разработчика относительно безопасности ИТ оцененного продукта или системы.

ITSEC различают требования к правильности конструкции и функционирования ОО. Критерии конструкции включают в себя процесс разработки с различными уровнями спецификации, начиная с высокоуровневого изложения требований, которые можно проиллюстрировать на примере архитектурного проекта, затем на примере рабочего проекта и, наконец, на примере реализации ОО. Конструктивными аспектами среды разработки, охватываемыми ITSEC, являются управление конфигурацией, языки программирования и компиляторы, а также безопасность разработки.

Далее требования к функционированию подразделяются на аспекты эксплуатационной документации с документацией пользователя и администратора и среды функционирования с доставкой и конфигурацией, запуском и функционированием.

Требования доверия к правильности в ITSEC представлены в виде шести иерархически упорядоченных уровней доверия от Е1 до Е6. От уровня к уровню дополнительные требования обеспечивают более строгое оценивание продукта и системы ИТ. В уровни доверия требования доверия к эффективности не включены. Однако информация, полученная при оценке правильности, которая должна применяться для проведения анализа уязвимостей, определена.

Дополнительно ITSEC в общих чертах намечает взаимосвязь уровней оценивания с классами ITSEC.

ITSEM основана на ITSEC, описывая, как следует оценивать ОО в соответствии с этими критериями. Специфической целью ITSEM является обеспечение наличия гармонизированного набора методов оценивания, дополняющих ITSEC.

ITSEM не основана на предшествующих документах. Она впервые представила много дополнительной информации по применению методов обеспечения доверия, в общих чертах изложенных в ITSEC, и, косвенно, методов обеспечения доверия, использованных в TCSEC и CTCPEC.

6.3.3 Источники

См. [40], [41].

Примечание — ITSEC/ITSEM являются результатом разработок Европейской комиссии, Директората главного информационного общества, отделения информации и коммуникации, BU 24 0/41, Rue de la Loi, B-1049 Брюссель.

С Директоратом главного информационного общества можно связаться через универсальный указатель ресурса http:/europa.eu.int/pol/infso/index en.htm.

6.4 CTCPEC — канадские критерии оценивания доверенного продукта



6.4.1 Цель

Предоставление системы измерений, применяемой для оценивания функциональных возможностей и доверия сервисов безопасности, предоставляемых программным или аппаратным продуктом или системой.

6.4.2 Описание

Канадские критерии оценивания доверенного продукта (CTCPEC) были разработаны со следующими тремя целями:

1) предоставление сравнительной таблицы для оценивания коммерческих продуктов;
2) предоставление основы для разработки спецификаций для доверенных компьютерных продуктов;
3) предоставление метода специфицирования доверенных продуктов при закупке.

При доверенной обработке дается определение двум типам требований:

1) специфические требования к сервисам безопасности;
2) требования доверия.

CTCPEC специфицируют требования функциональных возможностей и требования доверия по двум отдельным группам для выделения уникальных услуг по обеспечению безопасности для продуктов. Группа требований функциональных возможностей состоит из критериев конфиденциальности, целостности, доступности и подотчетности, тогда как группа требований доверия состоит из критериев доверия.

Некоторые требования доверия позволяют определить во время оценивания наличие требуемых характеристик (свойств) и их функционирование намеченным образом. Эти критерии должны применяться к совокупности компонентов, составляющих доверенный продукт, и необязательно к каждому компоненту продукта в отдельности. Следовательно, некоторые компоненты продукта могут быть совершенно ненадежны, тогда как другие могут оцениваться индивидуально по более высокому или более низкому классу оценивания, чем рассматриваемый в целом доверенный продукт. В доверенных продуктах на самом верху ранжирования устойчивость механизмов изоляции и посредничества такова, что многие из компонентов продукта могут быть совершенно ненадежны.

Требования доверия могут применяться ко всему спектру продуктов обработки электронных данных или сред обработки прикладных программ без специальной интерпретации.

6.4.3 Источники

См. [31].

Примечание — CTCPEC является стандартом для внутреннего пользования и результатом разработки Института коммуникационной безопасности (CSE), P.O.Box 9703, Terminal, Ottawa, Ontario K1G 3Z4, Canada.

6.5 KISEC/KISEM — корейские критерии и методология оценивания информационной безопасности

→D→	→I→		→O→

6.5.1 Цель

Предоставление структуры критериев и методологии оценивания безопасности для межсетевых экранов и систем обнаружения вторжения в Корее.

6.5.2 Описание

«Корейские критерии оценивания безопасности информации» (KISEC) и «Корейская методология оценивания безопасности информации» (KISEM) были разработаны в 1998 г. с тремя целями:

- обеспечение иерархической оценочной шкалы для оценивания функций безопасности межсетевых экранов и систем обнаружения вторжения;
- обеспечение метода специфицирования высоконадежных межсетевых экранов и систем обнаружения вторжения при закупке;
- накопление знаний, связанных с оцениванием безопасности, путем эксплуатации собственных критериев и методологии оценивания.

KISEC определяет функциональные требования и требования доверия к каждому из семи уровней оценивания (от К1 до К7). На каждом уровне имеется набор функциональных требований и требований доверия KISEC, которым должны соответствовать оцениваемые межсетевые экраны и системы обнаружения вторжения. KISEC имеет несколько других функциональных требований, зависящих от типа продукта, такого как межсетевые экраны и системы обнаружения вторжения. Однако требования доверия обычно используются как для межсетевых экранов, так и для систем обнаружения вторжения. Функциональные требования включают в себя идентификацию и аутентификацию, целостность, проверку безопасности, менеджмент безопасности и т. д. Требования доверия включают в себя разработку, управление конфигурацией, тестирование, эксплуатационную среду, руководящие документы и анализ уязвимостей.

Конкретный уровень определяется в соответствии с реализованными функциями безопасности и уверенности в соответствии межсетевых экранов и систем обнаружения вторжения требованиям доверия. В зависимости от функциональных требований и требований доверия оценочный уровень делится на семь уровней. Низший уровень представлен К1, высший — К7.

Ниже приведены характеристики каждого оценочного уровня:

- уровень К1 должен соответствовать минимальному уровню функций безопасности, таких как идентификация и аутентификация, для системного администратора и руководства безопасностью и т. д. Также должны быть в наличии задание по безопасности и функциональные спецификации;
- уровень К2 должен соответствовать требованиям уровня К1 и быть способным создавать и сохранять записи аудита деятельности, связанной с безопасностью. Также может потребоваться документация архитектурного проекта. Необходимо провести анализ уязвимостей и неправильного применения межсетевых экранов и систем обнаружения вторжения;
- уровень К3 должен соответствовать требованиям уровня К2 и быть способен проверять наличие любых модификаций хранимых данных внутри межсетевого экрана или системы обнаружения вторжения и переданных данных. Требуется также подробная документация по организации проектирования и конфигурационному управлению;
- уровень К4 должен соответствовать всем требованиям уровня К3 и обеспечивать функцию идентификации и аутентификации, защищающую межсетевой экран или систему обнаружения вторжения от атак методом записи и повторной передачи блоков шифрованного теста. Предлагаются также исходный код и/или документация по проектированию оборудования;
- уровень К5 должен соответствовать всем требованиям уровня К4 и обеспечивать функцию взаимной аутентификации. Необходима также формальная модель политики безопасности межсетевого экрана или системы обнаружения вторжения. Функциональные характеристики, документация по архитектурному проектированию и рабочему проекту должна оформляться в полуформальном виде;

- уровень К6 должен соответствовать требованиям уровня К5. На этом уровне должна верифицироваться согласованность между документацией рабочего проекта, исходным кодом и/или документацией по проектированию оборудования;

- уровень К7 должен соответствовать всем требованиям уровня К6. На этом уровне функциональные спецификации и документация по архитектурному проектированию должны быть записаны в формате для его синхронизации с формальной моделью политики безопасности системы.

KISEM создана на основе KISEC с целью описания, как межсетевые экраны и системы обнаружения вторжения должны оцениваться по этим критериям. Специфическим назначением KISEM является обеспечение наличия гармонизированного набора методов оценивания, дополняющих KISEC.

6.5.3 Источники

См. [50], [51].

Примечание — KISEC/KISEM является результатом разработки Агентства по информационной безопасности Кореи, 78, Karak dong, SonOПa-Gu, Seoul 138-160, Korea.

6.6 RAMP — фаза поддержания классификации

→D→	→I→		→O→

6.6.1 Цель

Обеспечение механизма распространения предыдущей классификации (доверия) TCSEC на новые версии.

6.6.2 Описание

Программа фазы поддержания классификации (RAMP) была разработана для обеспечения механизма распространения предыдущей классификации TCSEC на новую версию ранее оцененного продукта компьютерной системы. RAMP предназначена для сокращения оценочного времени и усилий, требуемых для поддержания классификации, путем использования персонала, участвующего в обслуживании продукта, с целью управления процессом внесения изменений и выполнения анализа безопасности. Таким образом, обязанность доказательства работы RAMP лежит на лицах, ответственных за обслуживание системы (т. е. поставщике), вместо группы оценивания.

В Общих критериях по оцениванию безопасности информационных технологий (CCITSE) имеются требования по сохранению существующих уровней EAL. В настоящее время разрабатывается программа, подобная RAMP, с учетом этих требований.

6.6.3 Источники

См. [32].

Примечание — RAMP является результатом разработки National Computer Security Center (NCSC), 9800 Savage Road, Fort George G. Meade, Maryland 20755-6000, USA.

6.7 ERM — поддержание классификации при оценивании (в общем)

→D→	→I→		→O→

6.7.1 Цель

Распространение полученного доверия за рамки жизненного цикла и/или периода времени, особенно после модификации.

6.7.2 Описание

После получения доверия к системе и при модификации этой системы еще потребуется дополнительное доверие к ней. Существуют схемы сохранения доверия к системе посредством незначительной модификации и, таким образом, поддержки процесса оценки (т. е. «сертификация» или «классификация»).

Поддержание классификации при оценивании является фазой оценки, следующей за фазой оценивания. Под этим термином понимается совокупность действий по поддержанию классификации, с помощью которых оценивают соответствие применяемых требований обновленных версий продукта, и позволяется составить перечень этих версий. При ERM поставщик осуществляет большую часть работы по определению поддержания ранее достигнутого рейтинга измененного продукта.

В схеме ERM имеются различные сущности с соответствующими обязанностями (поставщик, пользователь, орган по сертификации). По отношению к схеме доверия это означает сильную зависи-

мость метода обеспечения доверия, называемого «поддержание классификации при оценивании», от обеих фаз доверия — проектирование/разработка и эксплуатация.

Схемы поддержания классификации при оценивании существуют в различных формах и обычно состоят из следующих компонентов:

- применяемые требования: требования, по которым продукт должен оцениваться;
- аудит ERM: анализ доказательства RAMP, основанный на подходящем типичном образце и предназначенный для обеспечения реализации только утвержденных изменений и удовлетворительного проведения анализа безопасности. В дополнение к необходимым аудитам RAMP, проводимым VSA, группой анализа безопасности могут выполняться апериодические аудиты RAMP;
- план ERM: документ поставщика, в котором дается описание механизмов, процедур и инструментария, используемых для выполнения требований RAMP. Процедуры этого плана выполняются на фазе поддержания классификации. План поддержания классификации предлагается поставщиком и утверждается как часть процесса оценивания. Этот план может изменяться во время применения RAMP для продукта, особенно при идентификации назначенного персонала;
- анализ безопасности: проверка того, сохраняет ли предложенное изменение или совокупность изменений характеристики безопасности и доверие к исходному продукту и его последующим версиям, которые ранее поддерживались по RAMP в соответствии с приемлемыми требованиями.

Операторами RAMP обычно являются:

- группа анализа безопасности: отдельные лица (например, VSA, дополнительные оценщики), ответственные за проведение анализа, а также за представление и защиту доказательства RAMP перед комитетом по техническому надзору;
- комитет по техническому надзору: проводит главный технический анализ результатов работы, выводов и рекомендаций отдельных групп оценивания. Комитет по техническому надзору служит органом проверки качества, единообразия и последовательности оценивания.

В США ERM было формализовано как RAMP и применялось для классификации в TPEP и ИСО/МЭК 21827 (SSE-CMM).

В Великобритании ERM было формализовано как схема поддержания сертификатов и основано на ранжировании ITSEC.

Критерии оценивания ИСО/МЭК 15408 признают ERM, но предоставляют поддержание на должном уровне оценивания национальным органам, надзирающим за схемами оценивания.

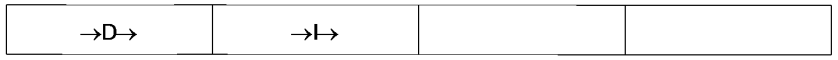
6.7.3 Источники

Программу поддержания на должном уровне оценивания США см. 6.6.

Программу поддержания на должном уровне оценивания Великобритании см. [44].

Примечание — Система поддержания сертификатов является результатом разработки Senior Executive, UK IT Security Evaluation and Certification Scheme, Certification Body, PO Box 152, Cheltenham Glos GL 52 5UF.

6.8 TTAP — программа оценки доверенных технологий



6.8.1 Цель

Создание, утверждение коммерческих средств оценивания и контроль за ними.

6.8.2 Описание

Программа оценки доверенных технологий (TTAP) является совместной разработкой Агентства национальной безопасности (АНБ) и Национального института стандартов и технологий (НИСТ) по созданию коммерческих предприятий для оценивания доверенных продуктов. TTAP формирует, утверждает коммерческие предприятия по оцениванию и надзирает за ними. В начальной стадии программа направлена на продукты со свойствами и степенями доверия, характеризуемыми общими критериями оценки безопасности информационных технологий (CCITSE).

Для проведения оценивания по TTAP организация должна быть аттестована как орган по оцениванию по TTAP (TEF). Сначала будущее TEF обращается к Совету по надзору TTAP за временным разрешением. В положительном случае будущему TEF даются полномочия на проведение пробного оценивания и данные о нем помещаются в список перспективных TEF. Затем перспективное TEF заключает договор с поставщиком и проводит пробное оценивание доверенного продукта. После пробного

оценивания статус «временное» аннулируется и TEF может проводить оценивания в соответствии с TTAP.

Надзорный совет TTAP проводит мониторинг TEF для обеспечения качества и согласованности во время оценивания. Поставщики продукции информационных технологий заключают договор с TEF и оплачивают оценивание своей продукции. После завершения оценивания продукт заносится в перечень оцененных продуктов АНБ.

6.8.3 Источники

См. [28].

Примечание — TTAP является внутренним стандартом правительства США и является разработкой Совета по надзору TTAP для передачи Агентству национальной безопасности, 9800 Savage Road, Suite 6740, Ft. Meade, Md. 20755-7640.

6.9 TPEP — программа оценивания доверенного продукта



6.9.1 Цель

Стимулирование широкой доступности доверенных продуктов обеспечения компьютерной безопасности.

6.9.2 Описание

По программе оценивания доверенного продукта (TPEP) поставщики обращаются в Агентство национальной безопасности со своим коммерческим продуктом обеспечения компьютерной безопасности с запросом на его оценивание, нацеленное на определенный уровень ранжирования доверия. Оценщики, работающие по TPEP, используют TCSEC и его интерпретации для оценки качества соответствия продукта требованиям целевого ранжирования. Результаты оценивания по TPEP публикуются ежеквартально в перечне оцененных продуктов (EPL) в разделе 4 Каталога услуг и продуктов по обеспечению безопасности информационных систем.

Конечной целью TPEP является стимулирование широкой доступности доверенных продуктов обеспечения компьютерной безопасности для владельцев данных и пользователей, желающих защитить свою секретную и/или конфиденциальную информацию. Дополнительными целями являются:

- обеспечение доступности полезных доверенных продуктов, отвечающих эксплуатационным потребностям конечного пользователя;
- обеспечение использования доверенных продуктов при конструировании внедряемой доверенной системы;
- обеспечение специального руководства по практичности доверенных продуктов;
- обеспечение специального руководства по функциональной совместимости характеристик безопасности с уровнем доверия, связанным с определенными характеристиками отдельных оцененных продуктов;
- стимулирование открытых и скоординированных деловых отношений с национальными и оборонными информационными инфраструктурами.

6.9.3 Источники

См. [46].

Примечание — TPEP была заменена программой оценки доверенных технологий. В настоящее время новые оценки с помощью TCSEC не проводятся. См. TCSEC.

TPEP является внутренним стандартом правительства США и разработкой Агентства национальной безопасности, 9800 Savage Road, Suite 6740, Ft. Meade, Md. 20755-7640.

6.10 Рациональный универсальный процесс® (RUP®)



6.10.1 Цель

Обеспечение полностью заполненной схемы жизненного цикла проектирования ПО, включая среду, процессы, действия, методы и средства, а также инструментарий.

6.10.2 Описание

Рациональный универсальный процесс®, или RUP®, является схемой процесса разработки коммерческого серийного ПО, разработанного и поддерживаемого ПО Rational®. Схема постоянно обновляется и улучшается для отражения самого последнего опыта и развития лучших практик.

В отличие, например, от ИСО 12207 «пустая» схема RUP заполнена руководством, процессами, методами, средствами, шаблонами, инструментарием и примерами, из которых можно создать конкретную схему процесса, управлять ею и улучшать ее.

Подобно производимым им программным продуктам сам RUP спроектирован и документирован с помощью универсального языка моделирования (UML). Объектной моделью RUP является универсальная модель программного процесса (USPM).

С точки зрения управления проектом RUP обеспечивает структурированный подход к распределению задач и обязанностей в рамках организации-разработчика. Он придает особое значение рассмотрению областей высокого риска на очень ранней стадии и позволяет обновлять требования по мере развития проекта, что позволяет создавать высококачественное ПО, отвечающее требованиям пользователя в рамках прогнозируемого графика и бюджета.

Действия RUP эффективно используют универсальный язык моделирования (UML) для создания и поддержания моделей, а также придания особого значения разработке и поддержке моделей — семантически ценных представлений находящегося на стадии разработки ПО, которые поддерживаются компьютерными инструментальными средствами. Эти инструментальные средства автоматизируют значительные части процесса, такого, например, как визуальное моделирование, программирование, тестирование и конфигурационное управление.

RUP представляет собой конфигурируемую схему процесса, приспособляемую для небольших групп разработчиков и для больших организаций-разработчиков. Его архитектура обеспечивает унифицированность семейства процессов и поддерживается разработочным комплектом, который сохраняет конфигурацию RUP для ее соответствия потребностям данной организации.

В RUP объединены, в частности, шесть основных лучших практик:

- интерактивная разработка ПО;
- управление требованиями;
- использование основанных на компонентах архитектур;
- визуальное моделирование ПО;
- верификация качества ПО;
- контроль за внесением изменений в ПО.

С точки зрения управления процессом и его улучшения RUP согласовывается с CMM и требованиями ИСО/МЭК 15504 на проектном уровне. При правильной реализации RUP соответствует организационным уровням 2 и 3 CMM. Он пригоден для более высокой зрелости процесса вследствие хорошего определения программного процесса и знания руководством организации технического прогресса во всех проектах.

6.10.3 Источники

См. [52].

Примечание — RUP® является разработкой группы по ПО фирмы Rational, дочерней компании корпорации IBM, Route 100, Somers, NY 10589, USA.

6.11 ИСО/МЭК 15288 — процессы жизненного цикла системы

→D→	→I→	→T→	→O→

6.11.1 Цель

Предоставление моделей, процессов и действий полного жизненного цикла любого типа сложных технических систем.

6.11.2 Описание

ИСО/МЭК 15288 является первым стандартом ИСО, связанным с процессами жизненного цикла в основном сложных систем, состоящих из аппаратных средств, человеко-машинного интерфейса и ПО.

Данный стандарт распространяется на жизненный цикл искусственных систем, охватывая период от концепции, идеи системы до изъятия ее из эксплуатации. В нем предусмотрены процессы приобретения и поставки продуктов системы и услуг, которые конфигурируются из одного или более следующих

типов системных компонентов: аппаратные средства, человеко-машинный интерфейс и ПО. Данная структура также предусматривает перечни действий, а также оценку и улучшение жизненного цикла системы и ее процессов.

Процессы, приведенные в данном стандарте, образуют всю совокупность процессов, на основе которой организации могут строить модели жизненного цикла, подходящие для продукта, видов услуг и рынков, на которых они проявляют активность. Организация в зависимости от ее назначения может выбирать и применять соответствующую подгруппу процессов для выполнения своего назначения посредством адаптации к своим целям этих процессов.

Наиболее релевантными, с точки зрения качества, процессами являются:

- процесс менеджмента качества;
- процессы интеграции, верификации и валидации;
- процессы планирования проекта, оценки и управления.

Данный стандарт может также использоваться:

- при создании условий для требуемых процессов, которые можно поддерживать инфраструктурой из обученного персонала, применяющего специальные методы, процедуры, средства и инструментарий. Эти условия используются организацией для управления своими проектами и содействия прогрессу на всех стадиях их жизненного цикла;
- для выбора, структурирования, применения и выполнения элементов созданных условий для производства продуктов и предоставления услуг;
- посредством договора или соглашения в рамках взаимодействия поставщик/покупатель по выбору процессов и действий, принятия соглашения по ним и их выполнения. Кроме того, данный стандарт может также применяться для оценки соответствия действий покупателя и поставщика пунктам соглашения.

Данный стандарт поддерживается руководством (ИСО/МЭК 19760), техническим отчетом, предназначенным для:

- применения в качестве сопроводительного документа к ИСО/МЭК 15288;
- представления рекомендаций по реализации данного стандарта.

Руководство предназначено для применения к большим и малым системам, системам, для которых требуются как большие, так и малые проектные группы, а также новым и унаследованным системам. Руководство включает в себя:

1) связи с другими документами ИСО, необходимыми как для поддержки реализации данного стандарта, так и для оценки эффективности его реализации и
2) факторы, требующие рассмотрения при реализации данного стандарта.

Руководство полезно для тех, кто:

- реализует ИСО/МЭК 15288 в организации;
- использует ИСО/МЭК 15288 для специальной системы;
- составляет стандарты организации на основе ИСО/МЭК 15288 для организации в целом или ее части.

Некоторые способы применения можно адаптировать к размерам, кадровому обеспечению проекта или типу системы. Руководство по адаптации представлено в приложении А данного стандарта и в разделе 4 настоящего стандарта. В руководстве не предусмотрено логическое обоснование требований данного стандарта.

6.11.3 Источники

См. раздел 2 ИСО/МЭК 15288.

См. [15].

Примечание — ИСО/МЭК 15288 является разработкой РГ 7/ПК 7/СТК 1 ИСО/МЭК «Информационная технология. Проектирование ПО и систем. Управление жизненным циклом».

6.12 ИСО/МЭК 12207 — процессы жизненного цикла программного обеспечения

→D→	→I→	→T→	→O→

6.12.1 Цель

Предоставление моделей, процессов и действий всего жизненного цикла систем ПО.

6.12.2 Описание

Значимость ПО как неотъемлемой составной части многих продуктов и систем определяет общую международную структуру определения установившихся практик для процессов, действий и задач ПО.

В ИСО/МЭК 12207 действия, которые могут выполняться во время жизненного цикла ПО, группируют следующим образом:

- основные процессы (процессы закупок, поставки, разработки, эксплуатации, обслуживания);
- вспомогательные процессы (процессы документирования, конфигурационного управления, создания доверия к качеству, верификации, валидации, совместной проверки, аудита, разрешения проблем);
- организационные процессы (процессы управления, инфраструктуры, улучшения, обучения).

Каждый из процессов детализирует включенные в него действия и задачи, определяющие конкретные обязанности по их выполнению, а также определяет результаты выполнения действий/задач.

Необходимо отметить, что в данном стандарте не предусмотрена конкретная модель жизненного цикла.

Процессы ИСО/МЭК 12207 представляют собой полную совокупность процессов жизненного цикла ПО. В зависимости от своего назначения организация может выбирать подходящую ей подгруппу этой совокупности. Кроме того, можно делать выбор из всех действий и адаптировать их с учетом сферы применения, размера, сложности и критичности программного продукта и самой организации.

Наиболее значимыми процессами с точки зрения качества являются процессы создания доверия к качеству, верификации, валидации, совместной проверки, аудита и решения проблем. Более того, в данном стандарте особо выделяют внутренние оценивания процесса, проводящиеся в ходе повседневной деятельности.

ИСО/МЭК 12207 предусмотрен для:

- организаций, закупающих системы, которые содержат ПО или автономный программный продукт;
- поставщиков программных продуктов;
- организаций, участвующих в эксплуатации и обслуживании ПО.

Руководством для ИСО/МЭК 12207 является технический отчет, предназначенный для конкретизации факторов, которые должны учитываться при применении ИСО/МЭК 12207 в контексте различных способов применения настоящего стандарта.

В ИСО/МЭК 12207 приводится обсуждение трех основных моделей жизненного цикла и примеры адаптации.

Руководство не содержит логическое обоснование требований ИСО/МЭК 12207.

6.12.3 Источники

См. раздел 2 ИСО/МЭК 12207.

См. [10].

Примечание — ИСО/МЭК ТО 12207 является разработкой РГ 7/ПК 7/СТК 1 ИСО/МЭК «Информационная технология. Проектирование ПО и систем. Управление жизненным циклом».

6.13 V-модель

→D→	→I→	→T→	→O→

6.13.1 Цель

Изложение в однородной и связанной форме того, что должно быть сделано, каким образом должны быть выполнены задания и какие инструментальные средства должны применяться при разработке систем ПО.

6.13.2 Описание

V-модель представлена серией общих директив (250, 251 и 252), в которых изложена модель процессов жизненного цикла, состоящая из предполагаемых к применению процедур и методов, а также функциональных требований к инструментарию, предполагаемому для применения в разработке систем ПО. Первоначально V-модель была разработана для германских федеральных вооруженных сил. V-модель была признана стандартом по разработке на международном уровне.

V-модель определяет, какие шаги должны предприниматься и какие методы применяться для выполнения задач по разработке ПО, а также какие функциональные характеристики должен иметь предназначенный для применения инструментарий. В V-модель включены модель процессов жизненного цикла, распределение методов и функциональные требования к инструментальным средствам.

V-модель жизненного цикла структурирована по трем частям:

- часть 1: положения.

В данной части содержатся обязательные положения относительно предполагаемых шагов (действий) и их результатов (продуктов);

- часть 2: дополнения относительно различных властных структур.

Данная часть существует как для вооруженных сил Германии, так и для федеральной администрации. В ней содержатся инструкции по применению модели процессов жизненного цикла в той или иной области;

- часть 3: сборник руководств.

В данной части содержится набор руководств, относящихся к конкретным темам, таким как безопасность ИКТ или использование ориентированных на объект языков.

V-модель предполагается использовать как основу для договоров, обучения и связи между участвующими сторонами. Используя документацию и глоссарий, V-модель служит основой взаимопонимания и смягчает конфликты между ними.

Положения V-модели объективны в организационном отношении. Они ограничены исключительно по технологическому процессу разработки. Следовательно, V-модель пригодна не только в государственной администрации в качестве стандарта по разработке, но и для промышленности.

Применение V-модели свободно от лицензионного платежа. Она не является частной собственностью и не защищена от копирования.

V-модель содержит правила, необходимые для создания ПО. Действительные в настоящее время критерии безопасности (ITSEC) выполняются с учетом их положений, управляющих процессом разработки посредством V-модели. Это значительно упрощает сертификацию разработанного таким образом ПО.

V-модель в совокупности со стандартами на методы и средства полностью охватывает функциональные области (разработка ПО, создание доверия к качеству, конфигурационное управление и управление проектом), является сложной, но в то же время гибкой и сбалансированной системой, обладающей широким спектром возможностей, обеспечивающей конкретную поддержку деятельности групп по наблюдению за внесением изменений, через которую проводятся необходимые улучшения и корректирующие изменения.

Влияние пользователей, необходимое для поддержания и модификации процессов V-модели, обеспечивается группой по наблюдению за внесением изменений, которая собирается раз в год совместно с представителями промышленности и властей. Эта группа обязана тщательно рассматривать все полученные запросы по внесению изменений в V-модель.

6.13.3 Источники

См. [42].

Примечание — V-модель является разработкой BWB IT 15, Postfach 7360, D-56057 Koblenz, Germany.

6.14 ИСО/МЭК 14598 — оценивание программного продукта

→D→			→O→

6.14.1 Цель

Представление метода измерения, оценки и оценивания качества программного продукта.

6.14.2 Описание

ИСО/МЭК 14598 основан на общей модели качества по ИСО/МЭК 9126. Таким образом, ИСО/МЭК 14598 представляет структуру оценивания качества всех типов программного продукта и устанавливает требования для методов его измерения и оценивания.

ИСО/МЭК 14598 предназначен для разработчиков, покупателей и независимых оценщиков, особенно отвечающих за оценивание программного продукта. Результаты оценивания, полученные при применении ИСО/МЭК 14598, могут использоваться руководителями и разработчиками/обслуживающим персоналом для определения соответствия качества оцениваемого продукта предъявляемым к нему требованиям и, при необходимости, внесения необходимых усовершенствований. Результаты оценивания могут также применяться аналитиками для установления взаимосвязей между внутренними и внешними системами измерения. Персонал, занимающийся улучшением процесса, может использовать результаты оценивания для определения возможности его улучшения посредством изучения и проверки информации о качестве продукта для проекта.

В стандартах серии ИСО/МЭК 14598 предлагает методы измерения, оценки и оценивания качества программного продукта. В стандартах серии ИСО/МЭК 14598 отсутствует описание как методов оценивания процессов изготовления ПО, так и методов прогнозирования затрат. Конечно, измерения качества программного продукта можно использовать в обеих целях.

Блок-схема процесса оценивания из ИСО/МЭК 14598 приведена на рисунке 1.



Рисунок 1 — Блок-схема процесса оценивания

6.14.3 Источники

См. раздел 2 ИСО/МЭК 9126-1; ИСО/МЭК 14598-1.

См. [1], [2], [3], [5], [6], [7], [8], [9].

Примечание — ИСО/МЭК 14598 является разработкой рабочей группы РГ 6/ПК 7/СТК 1 ИСО/МЭК «Информационная технология. Проектирование ПО и систем. Оценивание и система показателей».

6.15 Основные услуги по безопасности базовой структуры X/Open

→D→			

6.15.1 Цель

Обеспечение доверия через соответствие стандартам консорциума X/Open, сертифицированным третьими сторонами.

6.15.2 Описание

Снабжение продукции торговой маркой X/Open является еще одним типом доверия, поскольку обеспечивает доверие посредством тестирования на совместимость гарантийного обязательства продавца и торговой марки (подразумеваются средства контроля третьей стороны). Настоящий подход обеспечивает доверие к тому, что система будет удовлетворять претензии поставщика путем предоставления документированного свидетельства и применения стандартов третьей стороной.

X/Open представляет собой консорциум компаний, разрабатывающих открытые стандарты для формирования среды открытых систем, называемой «средой общих приложений (применений) (CAE)». Эта среда обеспечивает совместимость и мобильность приложений и систем. Продукты, системы и при-

ложения, соответствующие стандартам X/Open, имеют торговый знак «X/Open» для обозначения соответствия.

Присвоение торгового знака «X/Open» является процедурой, посредством которой продавец подтверждает соответствие его продукта одному или нескольким стандартам X/Open. Сертификат содержит декларацию соответствия деталей данной системы и свидетельств тестирования в поддержку претензий продавца.

Ответом X/Open на проблемы безопасности является спецификация основных услуг по безопасности X/Open (XBSS), разработанная для предоставления покупателям систем с торговым знаком «X/Open», гарантирующим, что такие системы обеспечат определенный минимальный уровень функциональных возможностей обеспечения безопасности. Фактически XBSS является профилем защиты, содержащим в основном функциональные требования безопасности и лишь некоторые требования доверия. Этот профиль определяет минимальный уровень функциональных возможностей обеспечения безопасности, которые должны обеспечиваться продуктами. XBSS также определяет специфические стандартные настройки в случаях, когда требованием является предоставление специфических избирательных вариантов обеспечения безопасности. Система для регистрации совместимой с этим профилем защиты должна обеспечивать этот или более высокий уровень безопасности.

Любая система, соответствующая определенному уровню безопасности, может маркироваться как совместимая. Детали действующей системы/операционной системы должны быть зафиксированы в декларации о соответствии. Это требует поддержки продуктами обязательных функциональных возможностей обеспечения безопасности и стандартных настроек параметров, как определено в спецификации XBSS X/Open.

Методология X/Open отличается от трех других методологий АА, поскольку она не сосредоточена на доверии, связанном с разработкой.

Спецификация XBSS содержит в основном функциональные требования, а степень доверия обеспечивается проверкой на совместимость, гарантийным обязательством продавца и торговым знаком «X/Open».

6.15.3 Источники

См. [30], [39].

Примечание — Брендинг X/Open является разработкой The Open Group, 44 Montgomery Street, Suite 960, San Francisco, CA 94104-4704, USA.

6.16 SCT — строгое тестирование соответствия

	→I→		

6.16.1 Цель

Тестирование функциональных возможностей обеспечения безопасности.

6.16.2 Описание

Строгое тестирование соответствия (требованиям безопасности) определяет метод тестирования безопасных систем по общедоступной спецификации — обычно по стандарту.

Комплексные тесты систематизированы с целью подчеркнуть реализацию тестов. Исходной точкой проведения тестов является абстрактное задание по безопасности (АЗБ), включенное в базовый стандарт по безопасности. Этим обеспечивается метод структурирования комплексных тестов и их прослеживаемость от требований безопасности через функции обеспечения безопасности и вспомогательные механизмы до испытаний этих механизмов. Тесты записаны на абстрактном уровне, соответствующем уровню абстракции базового стандарта. Затем можно задать параметры комплексному тесту для определенного типа внедрения, что обеспечивает преимущество проведения определенного объема предварительного оценивания абстрактного задания по безопасности и соответствующего комплексного теста. Таким образом обеспечивается базовый уровень охвата и уменьшается объем работы, требуемой для подготовки свидетельства, если субъектом (предметом) является реализация стандарта.

SCT является скорее тестированием функциональных возможностей, чем испытанием на прочность.

6.16.3 Источники

См. [20].

Примечание — SCT является разработкой National Physical Laboratory, Middlesex, TW 11 OLW, UK.

6.17 ИСО/МЭК 21827 — Проектирование безопасности систем — Модель зрелости процесса (SSE-CMM®)

D	I	T	→O→

6.17.1 Цель

Улучшение процессов проектирования безопасности систем организации и получение объектов с доверием к функциональным возможностям.

6.17.2 Описание

ИСО/МЭК 21827 в первую очередь сосредоточен на частях процесса (ЧП), необходимых для проектирования безопасности систем, которые называют «частями проектирования процесса». ИСО/МЭК 21827 также включает в себя ЧП, необходимые для поддержки проектов, осуществляемых в рамках частей проектирования безопасности систем, называемые «проектными ЧП», и ЧП, необходимые в рамках организации в целом для поддержки частей проектирования безопасности систем, называемых «ЧП организации».

Основное внимание в ИСО/МЭК 21827 уделяется частям проектирования безопасности систем и их действиям. ЧП SSE-CMM можно адаптировать для потребностей организации, а в область применения ИСО/МЭК 21827 могут входить конкретный проект, отдел организации или организация в целом.

ИСО/МЭК 21827 применим для любой организации, участвующей в обеспечении безопасности ИКТ или заинтересованной в ней, и может использоваться этой организацией. В число таких организаций могут входить организации, разрабатывающие как защищенные, так и незащищенные продукты и/или интегрирующие их, и организации, применяющие защищенные продукты или предоставляющие услуги по обеспечению безопасности. Таким образом, ИСО/МЭК 21827 может применяться организациями для улучшения своих процессов проектирования безопасности систем при разработке продуктов безопасности ИКТ или предоставлении услуг по обеспечению безопасности ИКТ (таких как оценка угроз или рисков) с более высоким качеством и в соответствии с графиком.

SSE-CMM является уникальной моделью, поскольку она детализирует требования по проектированию безопасности для систем обеспечения безопасности проектирования в дополнение к требованиям безопасности, которым должна соответствовать среда разработки. Более того, модель содержит ЧП для широкого ряда таких областей разработки, как определение требований безопасности, тестирование системы, анализ угроз и уязвимостей. SSE-CMM отличается от доверенной модели технологической зрелости (TCMM), специфицирующей только требования, которым должна соответствовать среда разработки организации.

ИСО/МЭК 21827 содержит ЧП, базовые практики (БП), общие практики (ОП) и уровни возможностей для описания процессов организации и определения качества осуществления организацией частей процесса (ЧП). ЧП состоят из группы родственных БП, которые сосредоточены на конкретных действиях процесса в рамках организации, тогда как ОП связаны со зрелостью всего процесса организации. ЧП, БП и ОП могут считаться требованиями, а уровни возможностей указывают на соответствие требованиям ИСО/МЭК 21827, однако эти требования относятся к конечному результату процесса, а не к тому, как этот результат достигается, не оказывая влияния на модель функционирования организации. Для каждой ЧП распределяют уровень возможностей с указанием уровня соответствия ИСО/МЭК 21827, который ранжируется от уровня 0 «Не выполнялся» до уровня 5 «Постоянно улучшается». Профиль ранжирования представлен в виде графического представления ЧП, выполняемых со связанными с ними уровнями возможностей или в виде уровня зрелости, достигнутого организацией в целом. Уровень возможностей и профили ранжирования определяются группой по оценке, проводящей оценку соответствия организаций требованиям ИСО/МЭК 21827 по методологии оценки SSE-CMM (SSAM).

Уровень возможностей демонстрирует достижение организацией минимального уровня возможностей по всем применимым ЧП (группа родственных практик). ОП являются специальными требованиями, применяемыми только к ЧП, связанным со зрелостью всего процесса и институционализацией отдельных ЧП во всей организации. Каждый последующий уровень указывает на повышение зрелости общего процесса организации и возможности выполнения ЧП в рамках организации.

В профиле ранжирования отражен уровень возможностей организации для отдельной ЧП, указывающий на ее сильные и слабые стороны. Профиль ранжирования используется для указания области, в

которой организация должна приложить усилия для улучшения своих процессов и достижения следующего более высокого уровня возможностей. Хотя изначально это не предполагалось, профиль ранжирования может стать инструментом закупки, что потребует от организации достижения различных уровней возможностей для конкретных ЧП, а не одного уровня для всех ЧП. Например, профиль закупок может обозначать уровень возможностей 2 для ЧП 1-5 и уровень 3 для ЧП 6-10.

SSE-CMM ИСО/МЭК 21827 является непрерывной моделью, которая является более гибкой и пригодной для промышленных организаций потому, что в соответствии с ней могут выбираться только подходящие ЧП, однако в случае использования многоступенчатой модели подобной TCMM сравнивать ранжирования разных организаций гораздо труднее.

Организация должна достичь для ЧП минимального уровня 2, необходимого для обеспечения удовлетворительной безопасности, так как уровня 1 недостаточно в связи с тем, что процессы подобраны специально и могут быть незавершенными. Исходя из модели SSE-CMM, это означает, что организация планирует, прослеживает выполнение ее основных практик и корректирует их в случае появления дефектов в рабочей продукции, тем самым демонстрируя повторяемость и последовательность процессов, что позволяет производить прогнозируемый продукт и, в свою очередь, являться важным фактором доверия.

6.17.3 Источники

См. раздел 2 ИСО/МЭК 21827.

См. [24] и [25].

Примечания

1 ИСО/МЭК 21827 является разработкой ИСО/МЭК СТК 1/ПК 27/РГ 3 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности».

2 Основной документ ИСО/МЭК 21827 был представлен и поддерживается Международной ассоциацией проектирования безопасности работы систем (ISSEA).

13873 Park Center Road, Suite 200, Herndon, VA 20171, USA.

1327 Upper Dwyer Hill Road, Carp, Ontario, K0A 1LO, Canada.

6.18 TCMM — доверенная модель зрелости процесса

D	I		

6.18.1 Цель

Повышение доверия к безопасности ПО организации и улучшение процессов его разработки.

6.18.2 Описание

Доверенная модель технологической зрелости (TCMM) является экспериментальным стандартом доверия к безопасности ПО, основанным на фундаментальных принципах и структуре CMM (модели технологической зрелости), разработанной Институтом программной инженерии (SEI). Хотя TCMM является специализированной моделью зрелости, она была создана путем слияния методологии разработки доверенного ПО (TSDM) и модели технологической зрелости SEI, что привело в результате к созданию многих улучшенных ключевых частей процесса (КЧП) и новых КЧП, названных «разработкой доверенного ПО», содержащей новые практики, не соответствующие ни одной из имеющихся КЧП. TCMM сосредоточена только на среде разработки и предназначена для использования в управленческой и организационной деятельности организации, что в значительной степени отличается от SSE-CMM ИСО/МЭК 21827. TCMM применима только к процессам и системам. Все процессы, связанные с разработкой ОО, находятся вне области ее применения.

TCMM содержит КЧП, ОП и уровни возможностей для описания процессов организации для определения, насколько правильно организация выполняет КЧП в соответствии с моделью SSE-CMM ИСО/МЭК 21827. Уровень возможностей присваивается организации с целью указания уровня соответствия, который находится в диапазоне от уровня 1 (исходный) до уровня 5 (оптимизирующий). Уровень 1 содержит мало КЧП, и считается, что в организации существуют специализированные процессы.

Будучи многоступенчатой моделью, уровни возможности TCMM образуют последовательность стадий для каждого уровня (кроме уровня 1), содержащего уникальный набор родственных КЧП. В отличие от непрерывной модели организации должны выполнять все КЧП для достижения соответствующего определенному уровню возможностей TCMM, однако эти стадии помогают организациям сосредоточиться на улучшении своих процессов и обеспечить четкий путь улучшения до следующего уровня возможности TCMM. Эти стадии облегчают процессы закупки и сравнений, поскольку КЧП для

каждой стадии не меняются. Будучи многоступенчатой моделью, TCMM аналогична ОК (общим критериям), однако, в отличие от ОК, сфокусированной на безопасности ОО, TCMM ограничена безопасностью среды разработки.

6.18.3 Источники

См. [26], [27], [48].

Примечание — TCMM была разработана совместно Агентством национальной безопасности (NSA) и Институтом программной инженерии (SEI). TCMM никогда не была опубликована, так как АНБ впоследствии решило поддерживать только одну из двух инициатив, которые оно финансировало.

6.19 CMMI — интеграция модели зрелости процесса®

D	I	T	O

6.19.1 Цель

Предоставление руководства по улучшению процессов организации и ее способности управлять разработкой, приобретением и обслуживанием продуктов и поддержанием услуг.

6.19.2 Описание

Назначением интеграции модели зрелости процесса® (CMMI SM) является предоставление руководства по улучшению процессов организации и ее способности управлять разработкой, приобретением и обслуживанием продуктов и поддержанием услуг. CMMI SM размещает апробированные практики в структуре, помогающей организации оценивать свою зрелость и возможности ЧП, устанавливать приоритеты для улучшения процессов организации и руководить внедрением этих улучшений.

Комплексный продукт CMMI берет начало из структуры, генерирующей множественные интегрированные модели, курсы обучения и метод оценки. По мере добавления к структуре нового материала появляются дополнительные интегрированные модели и вспомогательные материалы, включающие в себя дополнительные дисциплины.

В настоящее время имеются следующие модели:

- CMMI-SE/SW — интегрированная модель проектирования систем и ПО;
- CMMI-SE/SW/IPPD — модель разработки процесса, интегрированного продукта, проектирования систем и ПО;
- CMMI-SE/SW/IPPD/SS — модель поиска поставщиков, разработки процесса, интегрированного продукта, проектирования систем и ПО.

CMMI предназначена для поддержки улучшения процесса и продукта, снижения избыточности и устранения несовместимости при использовании отдельных автономных моделей. Ее назначение состоит в повышении эффективности, рентабельности инвестиций и производительности путем применения моделей, объединяющих такие дисциплины, как проектирование систем и ПО, неразделимые в процессе разработки систем.

Концепция проекта CMMI заключается в совершенствовании применения технологии CMM® в более широком ряду дисциплин за рамками проектирования ПО, где впервые его применение было успешным.

Концепция требует применения общей терминологии, общих компонентов и правил построения моделей зрелости возможностей, которые становятся доступны с уменьшением объема обучения и усилий по разработке процесса, необходимых для пользователей многих дисциплин. По мере разработки концепции рекомендуется ограничить начальную область применения проекта CMMI некоторыми наиболее востребованными дисциплинами до утверждения концепции. Выбор CMM проектирования ПО, систем и разработки интегрированного продукта для начальной стадии подтверждения концепции должен осуществляться представителями промышленности и государства. Комплект продуктов CMMI был спроектирован с учетом возможности его распространения как на дисциплины, так и на жизненный цикл ПО. После начала работ по распространению комплекта продуктов CMMI на процесс закупок и стал возможен охват таких дополнительных дисциплин, как проектирование систем безопасности. Решения по распространению комплекта продуктов CMMI принимаются на основе успешного применения первой версии, потребностей и поддержки сообщества пользователей и наличия участников разработки ее распространения.

Модели CMMI охватывают те же жизненные циклы, что и исходные модели (модель зрелости процесса (СММ) ПО, СММ разработки интегрированного продукта, EIA/IS 731 и модель зрелости процесса системного проектирования).

Схема CMMI спроектирована с учетом приспособления дополнительных дисциплин, и существует намерение добавить некоторые дисциплины по требованию сообщества пользователей. Процесс добавления новых дисциплин представлен в документе «Концепция операций (CONOPS) для CMMI».

А-спецификация CMMI требует согласованности и совместимости комплекта продукта CMMI с ИСО/МЭК 15504 и беспроблемного размещения дополнительных дисциплин, но не идентификации каких-либо конкретных. На сегодняшний день была добавлена дисциплина поиска поставщика.

6.19.3 Источники

См. [35], [36], [37].

Примечание — CMMI является разработкой Института программной инженерии, Carnegie — Mellon University, Pittsburgh, PA 15213-3890.

6.20 ИСО/МЭК 15504 — оценка программного процесса

D	I	T	O

6.20.1 Цель

Обеспечение структуры концепций и процессов для оценки процессов жизненного цикла ПО в соответствии с ИСО/МЭК 12207. Эта структура совместима с измерением процесса в соответствии с ИСО/МЭК 15939.

6.20.2 Описание

ИСО/МЭК 15504 совместим с моделью зрелости возможностей организации и использует измерение процесса и возможностей организации. Базовые практики подразделяют на: организацию, управление, проектирование, практики потребителя-поставщика и поддержки. ИСО/МЭК 15504 специфицирует следующую классификацию возможностей организации, осуществляющей процесс разработки:

L0 — незавершенный процесс;
L1 — выполненный процесс;
L2 — управляемый процесс;
L3 — установившийся процесс;
L4 — прогнозируемый процесс;
L5 — оптимизируемый процесс.

Классификация основана на оценке конкретного примера процесса. Все типы оценки поддерживаются. ИСО/МЭК 15504 применим к самостоятельной и независимой оценкам, а также к непрерывной и дискретной оценкам.

Уровень L3 ИСО/МЭК 15504 отражает успешную сертификацию по ИСО/МЭК 9000.

6.20.3 Источники

См. пункт 2 ИСО/МЭК 15504-1, ИСО/МЭК 15504-2, ИСО/МЭК 15504-3, ИСО/МЭК 15504-4, ИСО/МЭК 15504-5.

Примечание — ИСО/МЭК 15504 является разработкой комитета ИСО/МЭК СТК 1/ПК 7/РГ «Information technology. Software and system engineering. Process assessment».

6.21 СММ — модель СММ® (для программного обеспечения)

D	I		

6.21.1 Цель

Оценка и повышение зрелости возможностей программных процессов в организации.

6.21.2 Описание

В модели зрелости возможностей организации в отношении программных процессов описаны принципы и практики, лежащие в основе их зрелости и предназначенные для содействия занимающимся ПО организациям в повышении зрелости ее программных процессов.

Модель CMM определяет пять уровней зрелости:

Уровень 1 — начальный. Программный процесс характеризуется как произвольный, иногда даже как хаотический. Определено очень мало процессов, и успешность их выполнения зависит от индивидуальных усилий и решительных действий.

Уровень 2 — повторяемый. Установлены основные процессы управления проектом для прослеживания расходов, графика и функциональных возможностей. Существует необходимая дисциплина процесса для повторения предыдущих успехов по проектам в аналогичных применениях.

Уровень 3 — определенный. Программный процесс для деятельности по управлению и проектированию документирован, стандартизирован и интегрирован в стандартный программный процесс организации. Во всех проектах для разработки и сопровождения ПО используется утвержденный адаптированный стандартный программный процесс организации.

Уровень 4 — управляемый. Собирают детальные измерения программного процесса и качества продукта. Как программный процесс, так и продукты должны быть осмысленными в количественном отношении и управляемыми.

Уровень 5 — оптимизируемый. Непрерывное улучшение процесса осуществляется посредством количественной обратной связи от процесса, направления инновационных идей и технологий.

Считается, что прогнозируемость, эффективность программных процессов организации и управление ими улучшается по мере продвижения организации по этим пяти уровням. На сегодняшний день это мнение поддерживается эмпирическими доказательствами.

За исключением уровня 1, каждый уровень зрелости подразделяется на несколько различных КЧП, являющихся участками, на которых организации следует сосредоточиться для улучшения своего программного процесса.

КЧП на уровне 2 связаны с проблемами проекта по разработке ПО, с установлением основных средств контроля за управлением проектом. КЧП на уровне 2 являются: управление требованиями, планирование проекта по разработке ПО, прослеживание проекта по разработке ПО и контроль за ним, управление субконтрактами по разработке ПО, обеспечение доверия к качеству ПО и управление конфигурацией ПО.

В КЧП на уровне 3 рассматриваются проблемы как проекта, так и организации, поскольку организация определяет инфраструктуру и институционализирует процессы управления и проектирования ПО. КЧП на уровне 3 являются: концентрация на процессе организации, определение технологического процесса организации, программа обучения, комплексное управление разработкой ПО, проектирование программного продукта, межгрупповая координация и экспертные оценки.

КЧП на уровне 4 сосредоточены на установлении количественного согласования программного процесса и создаваемой программной продукции. КЧП на уровне 4 являются количественный менеджмент процесса и менеджмент качества ПО.

КЧП на уровне 5 охватывают проблемы, которые организации должны рассматривать при осуществлении непрерывного улучшения измеряемого программного процесса. КЧП на уровне 5 являются: предупреждение дефектов, управление изменениями в технологиях и управление изменениями процесса.

Каждая КЧП изложена с точки зрения ключевых практических ситуаций, способствующих выполнению ее цели. Ключевые практические ситуации описывают инфраструктуру и действия, способствующие эффективному выполнению институционализации ключевой части процесса.

6.21.3 Источники

См. [34].

Примечание — CMM является разработкой Института программной инженерии, Carnegie University, Pittsburgh, PA 15213-3890.

6.22 SE-CMM® — модель зрелости процесса системного проектирования®

D	I		

6.22.1 Цель

Улучшение процесса системного проектирования.

6.22.2 Описание

В модели зрелости процесса системного проектирования® (SE-CMM®) изложены основные элементы процесса системного проектирования организации, которые должны быть в наличии для обеспечения качественного системного проектирования.

Кроме того, SE-CMM служит эталоном при сравнении фактических действий по системному проектированию с этими основными элементами. Работа по разработке SE-CMM была инициирована в августе 1993 г. в ответ на запросы промышленности в оказании помощи для согласования и опубликования модели, аналогичной CMM, для сообщества, занимающегося системным проектированием. Конструкторские работы явились результатом сотрудничества нескольких организаций, включая Институт программной инженерии.

Работы в этой области в настоящее время являются частью интеграции модели зрелости процесса (CMMI).

6.22.3 Источники

См. [21] и [22].

Примечание — SE-CMM® является разработкой Института программной инженерии Carnegie University, Pittsburgh, PA 15213-3890.

6.23 TSDM — методология разработки доверенного программного обеспечения

D	I		

6.23.1 Цель

Обеспечение доверия посредством присвоения уровней доверия политике управления, средствам контроля окружающей среды и ее управления, а также системному проектированию.

6.23.2 Описание

Методология разработки доверенного ПО (TSDM) была разработана отделом стратегической оборонной инициативы (SDIO) в середине 80-х годов для повышения доверия к ПО путем интенсификации процесса разработки.

Вследствие оцененного размера (миллионы строк программы) предложенных проектов SDIO обычная частота программных ошибок сделала бы системы неработоспособными. При анализе доверенного ПО было сделано предположение, что улучшения процесса разработки могут снизить частоту появления программных ошибок.

Каждая характеристика процесса разработки ПО была проверена с целью выявления потенциальных слабых мест. Результатом этого анализа стало формулирование 25 принципов доверия.

TSDM определяет принципы доверия в отчете от 2 июля 1993 г. В нем содержится обоснование каждого принципа доверия, набор требований к соответствию, а также идентификация приемлемых классов доверия. Кроме того, данный документ определяет перечень связанных с ним требований, описывающих действия, аналогичные действиям, рассматриваемым в принципе доверия, и предоставляет перечень полезных ссылок для принципа доверия.

25 принципов доверия можно сгруппировать в следующие четыре области, связанные с общим процессом разработки ПО:

- политика в области управления (принципы доверия 1—6);
- средства контроля окружающей среды (принципы доверия 7—10);
- управление окружающей средой (принципы доверия 11—14);
- проектирование ПО (принципы доверия 15—25).

Каждый из принципов доверия измеряется пятью уровнями TSDM:

T1 (минимальное доверие);

T2 (умеренное доверие);

T3 (предпочтительное доверие);

T4 (вредоносная атака);

T5 (идеальное доверие).

TSDM предлагает измерение доверия к ПО/информации. Для специального плана разработки ПО (SDP) требуются приемлемые практики TSDM, предназначенные для выполнения. Применение приемлемых практик обусловлено тем, что в SDP используются методы определения соответствия TSDM наряду с результатами анализа рисков для группы проектирования ПО.

При оценке функциональных возможностей ПО важно понять, как определяется и прослеживается соответствие TSDM с помощью таких стандартов анализа проектирования ПО, как модель технологической зрелости (CMM) Института программной инженерии. Для оценки издержек, связанных с обучением членов группы проектирования ПО по программе TSDM, требуются определенные знания. Наконец, необходимо знание повторного использования ПО и совокупности исходных параметров ПО.

Примечание — Для интеграции CMM и TSDM была сформирована группа из представителей Агентства национальной безопасности и Института программной инженерии. Полученная в результате ее деятельности доверенная модель технологической зрелости (TCMM) является основой для проведения оценивания функциональных возможностей доверенного ПО.

6.23.3 Источники

См. [29] и [47].

6.24 SdoC — декларация поставщика о соответствии

D			

6.24.1 Цель

Заявление о соответствии продукта, процесса или услуги нормативным документам под ответственность поставщика и обоснование этого соответствия.

6.24.2 Описание

Данный подход формализует обязательство разработчика по отношению к его продукту посредством декларации поставщика о соответствии (SDoC). Для систем безопасности ИКТ эта декларация должна включать утверждения о соответствии безопасности систем. В руководстве для поставщика и конечных пользователей должна быть определена требуемая структура и содержание функциональных возможностей обеспечения безопасности.

Существуют схемы SDoC для многих элементов продукции ИКТ, а в Европе SDoC уже являются обязательными при определении соответствия продуктов электромагнитной совместимости (EMC) и низковольтной дифференциальной схемы LVD. Однако в отличие от других случаев, подобно ИСО 9000 и другим документам по качеству ПО, эргономике, защите окружающей среды и т. д., SDoC является добровольной.

До сих пор декларация о соответствии аспектам безопасности не рассматривалась. Однако большинство поставщиков выполняют огромный объем работы по специфицированию, проектированию, тестированию/гарантированию и документированию функциональных возможностей обеспечения безопасности, которая не видна конечному пользователю, тогда как другие поставщики проводят лишь минимальное тестирование. Адекватные утверждения поставщиков в отношении безопасности повысят степень прозрачности и сопоставимости для конечного пользователя, выбирающего надежную продукцию.

Более того, утверждения о соответствии требованиям безопасности ИКТ в SDoC будут способствовать большей сосредоточенности поставщиков и конечных пользователей на безопасности ИКТ. Коммерческие организации больше чем когда-либо зависят от проблем рынка, и это служит дальнейшим шагом к стимулированию обеспечения аспектов безопасности на экономичной и добровольной основе.

В родственном стандарте ИСО/МЭК специфицируются общие критерии для структуры вспомогательной документации, упрочивающей, упрощающей и стимулирующей уверенность в декларации поставщика о соответствии, как определено ИСО/МЭК 17050.

6.24.3 Источники

См. [11], [12], [13].

Примечание — SdoC является разработкой ISO/Casco WG 24 Committee on conformity assessment — Supplier's declatartion of conformity and its supporting documentation.

6.25 SA-CMM® — модель зрелости возможностей приобретения программного обеспечения®

		T	

6.25.1 Цель

Эталонное тестирование и улучшение процесса приобретения ПО.

6.25.2 Описание

Модель зрелости возможностей приобретения ПО® (SA-CMM®) является моделью эталонного тестирования и улучшения процесса приобретения ПО. Архитектура модели аналогична модели зрелости возможностей для ПО (SW-CMM), но с акцентом на проблемы приобретения и потребности

лости возможностей для ПО (SW-CMM), но с акцентом на проблемы приобретения и потребности отдельных лиц и групп, планирующих действия по приобретению ПО и управляющих ими. Каждый уровень зрелости обозначает возможности процесса и имеет несколько КЧП. Каждая часть КЧП имеет цели, общие признаки и организационные методы, предназначенные для институционализации установившейся практики. Совместными усилиями государственных организаций и Института программной инженерии и промышленности группа специалистов по приобретению вначале разработала, а затем провела контрольные испытания и спланировала внедрение SA-CMM. КЧП SA-CMM® приведена в таблице 3.

Поскольку значительный объем работ по моделированию процесса приобретения ПО был выполнен армией, ВМФ, ВВС и другими федеральными формированиями, в настоящем стандарте были объединены и уточнены лучшие результаты этих работ, и созданная SW-CMM была использована в качестве архитектурной модели.

Таблица 3 — Ключевая часть процесса SA-CMM®

Уровень	Сосредоточение	Ключевая часть процесса
5 Оптимизированный	Непрерывное улучшение процесса	Инновационное управление процессом. Непрерывное улучшение процесса
4 Количественный	Количественное управление	Количественное управление приобретением. Количественное управление процессом
3 Определенный	Стандартизация процесса	Программа обучения. Менеджмент рисков приобретения. Управление исполнением контракта. Управление выполнением проекта. Требования пользователя. Определение и обеспечение процесса
2 Повторяемый	Основное управление проектом	Переход на поддержку. Оценивание. Прослеживание и надзор за исполнением контракта. Управление выполнением проекта. Разработка требований и запрос на предложение к руководству. Планирование приобретения ПО
1 Начальный	Компетентный персонал	

6.25.3 Источники

См. [38].

Примечание — SA-CMM® является разработкой Института программной инженерии, Carnegie Mellon University, PA 15213-3890).

6.26 Серия ИСО 9000 — менеджмент качества



6.26.1 Цель

Обеспечение организаций структурой менеджмента качества и предоставление возможности сертификации ее успешного внедрения.

6.26.2 Описание

ИСО 9000 является стандартом менеджмента качества, содержащим 20 пунктов, связанных с высокими уровнями качества, которым организация должна соответствовать перед получением регистрации по ИСО 9000. Первоначально разработанный для промышленных организаций данный стандарт может применяться для организаций, разрабатывающих ПО, но для этого потребуется его более подробное толкование. По этой причине для того, чтобы ИСО 9001 можно было использовать для разработки, поставки и сопровождения ПО, с целью избежания трудностей и неясностей было разработано

руководство ИСО 9000-3. ИСО 9000-3 содержит 22 пункта, разработанных специально для области разработки ПО. Поскольку эти пункты более специфичны для ПО, их уровень достаточно высок для того, чтобы требовать дальнейшей интерпретации ИСО 9000 для применения к какой-либо организации, и в них не учитывается безопасность информационных технологий. Следует обратить внимание на то, что ИСО 9000-3 ограничивается ПО, тогда как ИСО 9001 и ИСО/МЭК 15408, кроме программных продуктов и систем, применимы также к аппаратным средствам.

Соответствие ИСО 9000 определяется независимыми аудиторами, проверяющими руководство по качеству и технологические процессы организации, а также проводящими опрос персонала. Сертификат ИСО 9000 предлагается только специфической организации, например, компании. Этим он отличается от модели SSE-CMM по ИСО/МЭК 21827, которая может оцениваться для отдельной группы или проекта в рамках компании или организации.

ИСО 9001 охватывает бóльшую область применения, чем требования ИСО/МЭК 15408, от принятия концепции продукта до его вывода из эксплуатации. Это означает, что организации, желающей быть зарегистрированной по ИСО 9001 с целью экономии времени на оценку, придется внедрить систему управления качеством, охватывающую больше областей, чем требуется для оценки по ИСО/МЭК 15408. Эта дополнительная работа по обеспечению соответствия требованиям ИСО 9000 может быть неоправданна.

Важно отметить, что ИСО 9000-3 является лишь руководством, и для получения регистрации организация должна соответствовать требованиям ИСО 9001.

6.26.3 Источники

См. раздел 2 ИСО 9000, ИСО 9001, ИСО/МЭК 90003 (пересмотр ИСО 9000-3).

Примечания

1 ИСО 9000 и ИСО 9001 являются разработкой комитета ИСО ТК 176 «Менеджмент качества и гарантия качества» со следующими подкомитетами:

ИСО ТК 176/ПК 1 «Менеджмент качества и гарантия качества. Концепции и терминология»;

ИСО ТК 176/ПК 2 «Менеджмент качества и гарантия качества. Системы управления качеством. Вспомогательные технологии»;

ИСО ТК 176/ПК 3 «Менеджмент качества и гарантия качества. Вспомогательные технологии».

2 ИСО/МЭК 90003 является разработкой комитета ИСО/МЭК СТК 1/ПК 7/РГ 18 «Информационная технология. Проектирование систем и программного обеспечения. Менеджмент качества».

6.27 ИСО 13407 — ориентированное на человека проектирование (HCD)

D			

6.27.1 Цель

Получение посредством ориентированного на человека проектирования более работоспособного, доступного для обучения использованию и приемлемого во всех отношениях продукта для снижения рисков безопасности, связанных с функционированием системы.

6.27.2 Описание

Процессы ориентированного на человека проектирования интерактивных систем ИСО 13407 объединены стандартом, разработанным РГ6 ПК4 ТК 159/ИСО, в котором дано разъяснение преимуществ, получаемых посредством большего ориентирования жизненного цикла интерактивных систем на человека, и приведены процессы, необходимые для ориентирования жизненного цикла на человека. Модель процессов ориентированного на человека жизненного цикла, представленная в настоящем стандарте, является структурированным и формализованным определением ориентированных на человека процессов, изложенных в ИСО 13407. ИСО 13407 полезен для специалистов в области оценки и улучшения программных процессов и тех, кто знаком с процессом моделирования или участвует в нем.

Модель, представленная в данном стандарте, применяет формат, присущий моделям оценки процесса. Эти модели описывают процессы, предназначенные для выполнения организацией с целью достижения поставленных целей. Процессы в настоящей модели описаны в формате, определенном в ИСО 15504 в контексте оценки программного процесса. Хотя модель оценки процесса в основном применяется для измерения эффективности выполнения организацией процессов, включенных в модель, подобные модели могут использоваться как в качестве описания того, что может потребоваться для проектирования и разработки эффективных процессов управления проектом и организационных процессов.

Модель зрелости возможностей (UMM), основанная на ИСО 13407, описывает семь процессов, каждый из которых определен набором базовых практик. Эти базовые практики определены. Каждому процессу определен набор рабочих продуктов. В ИСО/МЭК 15504 приведено краткое описание шкалы оценки зрелости процессов, изложены основные принципы применения модели, дана форма записи и описано ее применение, а также представлены отображения базовых практик на процессы в SPICE (программа моделирования с ориентацией на интегральные схемы), CMM и SE-CMM. Модель процессов соответствует требованиям ИСО/МЭК 15504.

Что касается разработчиков систем и ПО, применение ориентированного на человека подхода дает в результате более работоспособный, доступный для обучения использованию и приемлемый продукт и приносит большее удовлетворение пользователю. Ориентированное на человека проектирование может снижать риски безопасности, связанные с эксплуатацией системы. Ориентированные на человека процессы требуют больших вложений на ранних стадиях жизненного цикла, но, как оказалось, сокращают расходы не только на обслуживание, но и на разработку. В частности, ориентированные на человека процессы снижают риск неожиданных изменений требований и связанных с переделкой и инсталляцией риски.

Целью ориентированного на человека подхода является напоминание разработчику и владельцу об интерактивной системе о том, что система предназначена в основном для использования, а не для доставки или закупки. Ориентированные на человека процессы позволяют разработчикам и владельцам анализировать поведение системы в процессе ее эксплуатации и оценивать ее качество и доверие к ней в процессе работы. Ориентированные на человека процессы учитывают условия использования и среду, в которой будет использоваться интерактивная система. Ориентированные на человека процессы связаны с интегрированной системой, компонентами которой являются ПО и аппаратные средства. Ориентированные на человека системы оказывают поддержку пользователям и побуждают их к обучению. Преимущества обучения могут включать в себя: повышение производительности, улучшение качества работы, сокращение поддержки и времени обучения и повышение доверия к функционированию.

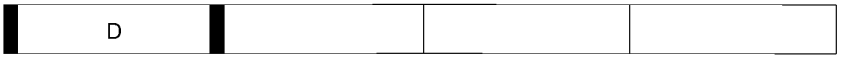
6.27.3 Источники

См. раздел 2 ИСО/МЭК 15504-1.

См. [4].

Примечание — ИСО 13407 является разработкой комитета РГ6/ПК4/ИСО ТК 159 «Эргономика. Эргономика взаимодействия человек — машина. Ориентированные на человека процессы проектирования интерактивных систем».

6.28 Характеристика разработчика (в общем)



6.28.1 Цель

Использование прежнего успешного опыта и доли успешных попыток как показателя качества программных средств защиты данных.

6.28.2 Описание

Характеристика разработчика предполагает метод определения приемлемости свидетельства, основанный на подтверждении идентичности автора свидетельства, используя предыдущую долю успешных попыток (т. е. достижений), которые были получены отдельным лицом/организацией при разработке, эксплуатации и проверке продуктов и систем безопасности. Характеристика может основываться на подтверждении идентичности какого-либо отдельного лица или организации, представивших это свидетельство. Более того, характеристика может классифицироваться на основании ролей отдельного лица/организации как характеристика разработчиков, оценщиков и утверждающих лиц.

Предыстория может быть формализована в рамках коллектива, занимающегося обеспечением безопасности ИКТ. Будучи формализованной или нет, эта характеристика является источником информации, используемой в данный момент, хотя на более неформальной основе, такой как «доверие»; многие продукты/системы выбираются на основе репутации разработчика или интегратора.

Вариантом характеристики, серьезно рассматриваемым в некоторых инстанциях, является характеристика доверия к разработчику. Доверие к разработчику подразумевает проведение разработчиком тестирования и оценки внутри фирмы и формулирование утверждения о доверии, основанного на внутренних процедурах фирм. Отметка разработчика о доверии не может обеспечить такой же уровень дове-

рия, как тестирование независимой третьей стороной, но некоторые стороны считают, что разработка схемы распознавания доверенных разработчиков может соответствовать многим коммерческим требованиям.

6.28.3 Источники

См. [43].

Примечание — Формализацию понятия «Предыстория разработчика» можно найти в таких методах гарантии процессов, как CMM (см. 6.21) и ИСО/МЭК 15504 (см. 6.20), в «Аттестации персонала» (см. 6.36 и 6.37) и в Декларации поставщика о соответствии (см. 6.24).

6.29 ИСО/МЭК 17025 — доверие к аттестации

D	I		

6.29.1 Цель

Целью обеспечения доверия к аттестации является гарантирование сопоставимости всех процедур и результатов оценки для обеспечения соответствия всем релевантным стандартам, а также гарантирование объективности и нейтральности.

6.29.2 Описание

Сопоставимость всех процедур и результатов оценки для обеспечения соответствия всем релевантным стандартам, а также объективность и нейтральность образуют основу доверия к аттестации. Для процедуры обеспечения доверия к аттестации требуются средства оценки с целью предоставления доказательства соответствия условиям и квалификационным требованиям.

Согласно ИСО/МЭК 17025 требованиями по аттестации являются:

a) 1 Соблюдение соответствующих частей ИСО/МЭК 17025 (включая доказательство компетентности для всей области безопасности ИКТ).

b) 2 Доказанная техническая компетентность в конкретной области оценки (если необходимо, в нескольких областях оценки).

Следовательно, процедура аттестации, приведенная в таблице 4, объединяет базовую аттестацию (соблюдение требований в дополнение к пункту 1 перечисления a) и, по меньшей мере, одну процедуру лицензирования [соблюдение требований в дополнение к пункту 2, перечисления b)].

Таблица 4 — Процедура аттестации

Поле лицензирования 1	Поле лицензирования 2	Поле лицензирования *n*
Базовая аккредитация в соответствии с ИСО/МЭК 17025		

Средства оценки, используемые физическими или юридическими лицами по частному праву, могут быть аттестованы по соглашению по аттестации, достигнутому между сертификационной организацией и оператором. Предварительное условие для аттестации заключается в том, что эти оценочные организации не могут участвовать в разработке, изготовлении или продаже на рынке продукции, подлежащей оценке. Следовательно, в принципе это не препятствует возможности аттестации так называемых «лабораторий поставщика».

В качестве основы процесса аттестации данный стандарт специфицирует общие критерии технической компетентности испытательных лабораторий, включая поверочные лаборатории, независимо от рассматриваемой отрасли. ИСО/МЭК 17025 предназначен для использования испытательными лабораториями и их сертификационными организациями, а также другими органами, связанными с признанием компетентности испытательных лабораторий. Этот набор критериев пополняется в случае применения к конкретному сектору безопасности ИКТ.

Примечание — Оценка независимой третьей стороной по «Общим критериям» по ИСО/МЭК 15408 проводится сертифицированными и лицензированными оценочными организациями в соответствии с требованиями ИСО/МЭК 17025.

6.29.3 Источники

См. [11] и [12].

Примечание — ИСО 13407 является разработкой РГ24 ИСО/КАСКО Комитет по оценке соответствия. Оценка и аттестация.

6.30 ИСО/МЭК 13335 — менеджмент безопасности информационных и телекоммуникационных технологий

	I	T	O

6.30.1 Цель

Предоставление общего руководства по оценке и менеджменту рисков безопасности.

6.30.2 Описание

ИСО/МЭК 13335 состоит из серии стандартов и технических отчетов для обеспечения руководства, но не для принятия решений по аспектам управления безопасностью информационных и телекоммуникационных технологий (ИТТ). Лица, отвечающие за безопасность ИКТ в рамках организации, должны уметь адаптировать материал ИСО/МЭК 13335 для удовлетворения ее специфических потребностей. Основным назначением ИСО/МЭК 13335 является:

1) определение и описание понятий, связанных с управлением безопасностью ИТТ;

2) идентификация взаимосвязей между управлением безопасностью ИКТ и менеджментом ИКТ в целом;

3) представление нескольких моделей, которые могут использоваться для разъяснения понятия «безопасность ИТТ»;

4) предоставление общего руководства по менеджменту безопасностью ИТТ (РМБИТТ).

МБИТТ описывает основные понятия, лежащие в основе оценки риска и менеджмента риска, включая терминологию и общий процесс оценки и менеджмента рисков.

МБИТТ разработано для управления проблемами информационной безопасности в целом с учетом таких вопросов, как технические, физические, процедурные и административные меры управления. МБИТТ не только является основой оказания помощи организации в разработке и улучшении собственной архитектуры информационной безопасности, но и предназначено для установления общности между организацией.

МБИТТ обеспечивает структуру менеджмента безопасности ИТТ. МБИТТ содержит обсуждение высокоуровневых понятий об управлении безопасностью ИТТ и вводит общие требования к анализу и менеджменту риска и методы осуществления этого анализа и менеджмента.

Процесс менеджмента риска, определенный в разрабатываемой части 2 МБИТТ, требует внедрения соответствующих мер управления и предлагает конкретные меры управления, выбранные из ИСО/МЭК 17799 или из Руководства по защите базы ИТ.

МБИТТ из ИСО/МЭК 13335 находится на стадии пересмотра и частичного изменения предыдущих и действующих РМБИТ. По завершении этого процесса РМБИТ может включить следующие части под общим наименованием «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент безопасности информационных и телекоммуникационных технологий»:

- часть 1. Концепции и модели менеджмента безопасности информационных и телекоммуникационных технологий;
- часть 2. Методы и средства менеджмента рисков безопасности информационных и телекоммуникационных технологий.

ИСО/МЭК 13335-1:2004 отменяет и заменяет ИСО/МЭК 13335-1:1996 и ИСО/МЭК ТО 13335-2:1997. Он также включает в себя ИСО/МЭК ТО 13335-5:2001.

ИСО/МЭК 13335-2 отменяет и заменяет ИСО/МЭК ТО 13335-3:1998 и ИСО/МЭК ТО 13335-4:2000.

ИСО/МЭК ТО 13335 включает в себя следующие части под общим наименованием «Информационная технология. Руководство по менеджменту безопасности ИТ»:

- часть 3. Методы менеджмента безопасности ИТ;
- часть 4. Выбор защитных мер;
- часть 5. Руководство по менеджменту безопасности сети.

6.30.3 Источники

См. раздел 2 ИСО/МЭК 13335-1, ИСО/МЭК ТО 13335-2, ИСО/МЭК ТО 13335-3, ИСО/МЭК ТО 13335-4, ИСО/МЭК ТО 13335-5, ИСО/МЭК 17799.

См. [33].

Примечания

1 ИСО/МЭК 13335 является результатом разработки РГ 1/ПК 27/ТО 1 ИСО/МЭК «Информационная технология. Методы и средства обеспечения безопасности. Требования, услуги по обеспечению безопасности и руководства».

2 ИСО/МЭК 13335 к моменту издания ИСО/МЭК 15443-2 находился на стадии пересмотра, включая реструктуризацию и изменение наименования. Планировалось, что новые части ИСО/МЭК 13335, ранее имевшие наименование «Руководства по менеджменту безопасности ИТ», будут носить название «Менеджмент безопасности информационных и телекоммуникационных технологий», МБИКТ.

6.31 BS 7799-2 — системы менеджмента информационной безопасности. Спецификация с руководством по применению

			О

6.31.1 Цель

Формирование требований по созданию и менеджменту эффективной системы менеджмента информационной безопасности (СМИБ).

6.31.2 Описание

В BS 7799-2 подробно излагаются требования по созданию, внедрению, эксплуатации, мониторингу, проверке, поддержанию и улучшению документированной СМИБ в контексте общих деловых рисков организации. В нем также определены требования по внедрению мер управления безопасностью, адаптированные для потребностей отдельных организаций и их подразделений.

СМИБ, разработанная с помощью BS 7799-2, учитывает общие деловые риски организации при определении адекватных и пропорциональных мер управления безопасностью для защиты информационных активов и обеспечения доверия потребителей и других заинтересованных сторон. Учет общих деловых рисков организации и обеспечение доверия потребителей и других заинтересованных сторон должно поддерживать и усиливать конкурентное преимущество, увеличивать денежный поток, прибыльность, улучшать правовое соответствие и коммерческий имидж организации.

Для эффективного функционирования организация должна идентифицировать многие виды своей деятельности и управлять ими. Любая совокупность видов деятельности, использующая ресурсы, может рассматриваться как процесс, преобразующий входные данные в выходные. Часто выходные данные одного процесса непосредственно формируют входные данные последующего процесса. Применение системы процессов в рамках организации, наряду с идентификацией и взаимодействиями этих процессов и руководством ими, можно назвать «процессным подходом».

BS 7799-2 использует процессный подход, чтобы подчеркнуть для своих пользователей важность:

a) знания требований безопасности деловой информации и необходимости формирования политики и целей информационной безопасности;

b) внедрения и эксплуатации мер управления в контексте менеджмента общих деловых рисков организации;

c) мониторинга и анализа функционирования и эффективности СМИБ;

d) постоянного улучшения на основе объективного измерения.

Основной моделью процесса, применяемой BS 7799-2, является модель «планирование — осуществление — проверка — действие» (PDCA), которую можно найти во многих стандартах технологических процессов.

6.31.3 Источники

См. [53].

Примечания

1 BS 7799-2 является разработкой BSI (Британский институт стандартов), 389 Chiswick High Road, London W4 4AL, United Kingdom.

2 BS 7799-2 был опубликован в качестве национального стандарта AS/NZS-2 — 2003 в Австралии и Новой Зеландии.

6.32 ИСО/МЭК 17799 — практические правила менеджмента информационной безопасности

			О

6.32.1 Цель

Создание структуры, позволяющей фирмам разрабатывать, внедрять и измерять эффективную практику управления безопасностью, как правило, на уровне организации.

6.32.2 Описание

ИСО/МЭК 17799 является международным стандартом, включающим в себя передовой опыт в области информационной безопасности. Впервые он был опубликован как BS 7799 до принятия ИСО/МЭК 17799 посредством ускоренной процедуры с использованием общедоступной спецификации. Первоначально он был разработан в ответ на требование со стороны промышленности по созданию общей структуры, позволяющей фирмам разрабатывать, внедрять и измерять эффективную практику управления безопасностью и обеспечивать доверие к торговле между фирмами. ИСО/МЭК 17799 основан на передовом опыте в области информационной безопасности ведущих британских и международных коммерческих предприятий и получил широкое международное признание.

ИСО/МЭК 17799 является сводом правил для качественного управления информационной безопасностью. Родственный BS 7799-2:1999 является спецификацией систем менеджмента информационной безопасности. Стандарт применялся как спецификация требований к системе менеджмента, в сравнении с которыми можно оценивать организацию на соответствие и последующую сертификацию. BS 7799-2 публиковался как национальный стандарт в других странах.

ИСО/МЭК 17799 может применяться ко всей информации независимо от вида носителей, на которых она хранится и передается, или места ее размещения. Каждое коммерческое предприятие нуждается в системе постоянного менеджмента рисков ее информации, и данный стандарт представляет собой руководство по лучшим доступным мерам управления. Важно, чтобы соответствующие меры и цели управления выбирались с использованием процесса оценки риска и применения правильности уровня управления.

В ИСО/МЭК 17799 установлены следующие меры управления, определяющие хорошую практику обеспечения безопасности в промышленном секторе:

- политика информационной безопасности;
- организация безопасности;
- классификация активов и управление ими;
- личная безопасность;
- физическая и экологическая безопасность;
- компьютерное и сетевое управление;
- управление доступом к системе;
- разработка и обслуживание систем;
- планирование непрерывности бизнеса;
- соответствие.

6.32.3 Источники

См. раздел 2 ИСО/МЭК 17799.

См. [53].

Примечание — ИСО/МЭК 17799 является разработкой рабочей группы РГ 1/ПК 27/СТК 1 ИСО/МЭК «Информационная технология. Методы и средства обеспечения безопасности. Требования, услуги по обеспечению безопасности и рекомендации».

6.33 FR — исправление дефектов (в общем)

			O

6.33.1 Цель

Получение целесообразной информации о дефектах и сбоях и их исправление, когда продукт находится на стадии внедрения или эксплуатации.

6.33.2 Описание

При внедрении или эксплуатации продукта неисправности и дефекты подвергают информационную систему опасности неправильного срабатывания и/или атаки. На этой стадии следует выполнять следующие правила:

- оператор должен поддерживать систему в безопасном состоянии, например, применяя системы обнаружения, обновляя свою систему с помощью новейших патчей или посредством временно́го ограничения ее функциональных возможностей;
- оператор должен направлять информацию об атаках и сбоях в соответствующие инстанции, например, разработчику, в центр борьбы с чрезвычайными ситуациями, администратору, пользователям;

- разработчик должен отвечать за свои продукцию и системы, выдавая соответствующие рекомендации всем потенциально заинтересованным пользователям, разрабатывая и распределяя «заплатки» для исправления сбоев/дефектов, угрожающих безопасности. Следует применять систему распределения программных средств защиты данных.

Все обязанности должны быть формализованы, например, ответственность разработчика за свои продукты и услуги, своевременную коррекцию ошибок, а также разрешение всех проблем пользователя и обязанность за распределение «заплаток» всем пользователям после разрешения проблемы одного из них.

Исправление дефектов обычно считается независимым от поддержки рейтинга оценки.

«Заплатками» являются программы, устраняющие ошибки или слабые места в ПО, а также одним из наиболее распространенных методов исправления дефектов в системе защиты. Однако инсталляция новейших поставляемых продавцом «заплаток» не является идеальным решением проблем безопасности, так как:

- непрерывный поток «заплаток» может быстро «затопить» администраторов, которые и так обременены другими административными задачами;

- даже после установки организацией всех новейших «заплаток» новые атаки, например, через Интернет, могут продолжиться;

- при обнаружении новых атак и опубликовании их в Интернете большое число сетей немедленно становится уязвимым для этих атак, пока будут создаваться и устанавливаться новые «заплатки». До тех пор, пока не будет создана эффективная «заплатка» для противодействия новой атаке, могут пройти недели или месяцы, и пораженные серверы останутся открытыми для атак;

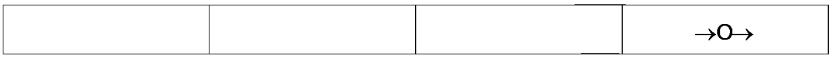
- организации могут поддерживать свою осведомленность о новых «заплатках» посредством мониторинга рекомендаций в области безопасности в отношении угроз или распространенных атак. Также рекомендации выдаются различными организациями и обычно ссылаются на какую-либо «заплатку» или работу, в результате которой упомянутая уязвимость будет ликвидирована;

- действия по исправлению ошибок обычно объединены в методы, которые представлены в ИСО/МЭК 15408 или СММ.

6.33.3 Источники

Примечание — Источником рекомендаций в области безопасности является группа компьютерной «скорой помощи» университета Карнеги-Меллона.

6.34 Руководство по базовой защите информационных технологий



6.34.1 Цель

Обеспечение набора практических мер безопасности для систем ИКТ, которые в случае с обычной организацией адекватны и достаточны для выполнения требований по защите и которые также могут быть модифицированы для более жестких требований по защите.

6.34.2 Описание

Базовая защита ИТ с помощью соответствующего применения мер безопасности, связанных с организацией, персоналом, инфраструктурой и техническими требованиями, предназначена для обеспечения такого уровня безопасности систем ИКТ, который адекватен и достаточен для выполнения требований по защите обычной организации и может служить основой для применений ИКТ, требующих высокой степени защиты. В этом отношении руководство по базовой защите ИТ рекомендует такие элементы, которые объединяются в комплексы мер безопасности для типичных конфигураций ИКТ, угрожающих условий и организационных требований.

Для подготовки настоящего руководства немецкое Агентство по информационной безопасности предполагало использование сценариев рисков на основе общеизвестных угроз и уязвимостей. Для противодействия этим угрозам был разработан постоянно обновляемый структурированный комплекс мер безопасности. Следовательно, пользователям надо только обеспечить постоянное и полное внедрение рекомендуемых мер. Организация процесса внедрения в виде контрольного списка позволяет экономно реализовывать требования по защите обычных ИКТ.

Политики безопасности организации могут ссылаться на общие меры руководства по базовой защите ИТ. Таким образом, базовая защита ИТ становится основой соглашения по мерам, отвечающим обычным требованиям защиты.

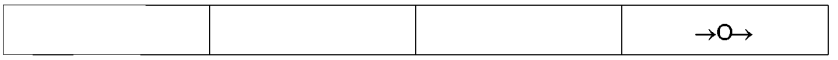
Однако обобщенные подходы, используемые для базовой защиты, нельзя сразу применять к системам ИКТ, требующим более высоких уровней защиты. Необходимо обеспечить, чтобы в случаях применения ИКТ, требующих более высоких уровней защиты, отдельные способы анализа безопасности применений ИКТ проводились бы в дополнение к усовершенствованию базовой защиты ИКТ. Это приведет к получению более специфических результатов по выбору и/или разработке дополнительных, качественно более эффективных мер в дополнение к существующим мерам базовой защиты ИКТ. При этом в свою очередь повышается стоимость/эффективность базовой защиты ИКТ.

Для обеспечения удовлетворительной базовой защиты ИТ недостаточно даже на основе руководства по базовой защите ИТ только один раз разработать политику безопасности системы. Точнее, проектирование, внедрение и мониторинг мер безопасности ИКТ являются циклическими требованиями и также могут инициироваться нарушениями безопасности. Задача обеспечения удовлетворительной базовой защиты ИТ имеет большое значение и должна решаться руководством агентства/фирмы. В поддержку решения этой задачи руководство по базовой защите ИТ должно предложить план действий.

6.34.3 Источники

См. [33].

6.35 Испытание проникновением



6.35.1 Цель

Испытание эффективности внедренных функций обеспечения безопасности попыткой преодоления мер безопасности.

6.35.2 Описание

Испытание проникновением проводится для анализа эффективности функций обеспечения безопасности. Испытание проникновением проводится после успешного завершения тестов на корректность. Испытание проникновением распространяется на продукты, которые являются правильными, но не защищены.

Целью испытания проникновением является обнаружение уязвимостей продукта. Уязвимости подразделяют на уязвимости в конструкции и эксплуатационные уязвимости. Возможными уязвимостями являются вредоносные части продукта или скрытые каналы. Уязвимости могут появляться непосредственно при запуске системы или позднее, при введении в ее действие специальных входных данных. Последний сценарий позволяет осуществлять запланированные атаки на систему в любое время ее функционирования. Уязвимости могут появляться непосредственно при запуске системы или позднее, при введении в систему специальных входных данных. Следовательно, все части продукта должны помечаться как потенциально опасные. Уязвимости активизируются в основном редкими и неожиданными чаще всего неявными (скрытыми) входными данными.

План и методики испытания проникновением специфицируются на основе результатов анализа безопасности продукта. Анализ безопасности является подтверждением наличия уязвимости без проведения испытания проникновением. В плане испытаний специфицируются атаки, которые должны быть включены в методики испытаний. Испытание проникновением является попыткой обойти функции защиты продукта. Проникновение является результатом успешного использования уязвимости.

Стратегиями «черного ящика» в испытании проникновением являются обнаружение «троянского коня», генерирование критических входных данных и мониторинг утверждений. Стратегии генерирования критических входных данных включают в себя усечение входного потока данных, переполнение входного буфера и добавление ненужных данных к входным, ввод вредоносных команд и тестирование в предельных режимах. Стратегии «прозрачного ящика» включают в себя применение плохо специфицированного, использованного и документированного кода, внесение неисправностей и основанный на коде мониторинг утверждений.

6.35.3 Источники

См. [49].

6.36 Аттестация персонала (в общем)

			О

6.36.1 Цель

Обеспечение квалификации персонала, достаточной для выполнения стадии эксплуатации систем ИКТ.

6.36.2 Описание

Аттестация персонала является организационным процессом, обеспечивающим доверие к персоналу и поддержание этого доверия (например, посредством обеспечения и гарантирования непрерывного обучения).

Аттестация персонала, адаптированная к эксплуатации ИКТ, включает в себя гарантирование приемлемого для ИКТ обучения, квалификации и опыта. Аттестация может также включать в себя гарантирование физических возможностей, психологической стабильности и моральных качеств отдельного лица применительно к эксплуатации ИКТ, особо учитывая аспект безопасности. Опыт в области обеспечения безопасности ИКТ может послужить дополнением к общей квалификации в области ИКТ и быть ее частью.

Существует большое число видов аттестации в области ИКТ, которые могут обеспечить определенную степень гарантии безопасности функционирования систем ИКТ.

Аттестованные в области ИКТ лица должны сообщать о повышении своей компетентности и производительности работодателям, коллегам и клиентам. С другой стороны, аттестация может способствовать карьере специалиста, обеспечивая дополнительное доверие к ИКТ.

Аттестация в области ИКТ может проводиться следующими лицами и организациями:

- работодателем, сосредоточиваясь на эксплуатационных требованиях ИКТ;
- производителем, сосредоточиваясь в основном на продукции и услугах ИКТ;
- третьей стороной, сосредоточиваясь на потребностях рынка или требованиях потребителя.

Примечание — Международные стандарты по аттестации персонала имеются в других технических областях, но окончательно не введены в область ИКТ.

Крупные работодатели и государство могут иметь подробные правила внутренней аттестации в области ИКТ, которые могут основываться на соответствующих разделах руководства для работников.

Поощряемая крупными производителями сертификация продукции ИКТ стала методом разработки норм в отношении компетентности в области индустрии компьютеризации и идентификации лиц, ставших специалистами в части этих норм. Примерами влияния системы сертификации на компетентность специалистов компании и компанию в целом являются:

- дипломированный инженер по системам корпорации «Майкрософт»;
- администратор баз данных корпорации Oracle;
- сертифицированный сетевой администратор;
- сертифицированный инженер по NetWare;
- сертификаты компании «Cisco Systems».

В быстро изменяющихся областях технологий аттестация в области ИКТ сторонней организацией возникла как образовательный процесс, конкурирующий с высшим образованием. После завершения такого образовательного процесса выдаются сертификаты, а не дипломы, без уведомления правительства и контроля с его стороны. Исследования показали, что 80 % предложений работы в сфере ИКТ содержат требования к образованию без требований университетских дипломов.

Аттестация в области ИКТ сторонней организацией имеет целью гарантирование и совершенствование новейших специальных знаний. Многие органы по оценке или аттестации с их сертификатами являются транснациональными организациями.

Третьими сторонами, предлагающими аттестацию в области ИКТ, являются, например:

- A+® аттестация (Computer Tech Industry Associate);
- Институт аттестации специалистов по компьютерам;
- Национальная ассоциация инженеров по системам связи.

Аттестация типа A+® приведена ниже в качестве примера аттестации в области ИКТ.

Для того чтобы получить аттестацию типа A+, необходимо выдержать два экзамена. Экзамены имеют целью определение необходимой компетентности для специалиста по ИТ начального уровня или

технического специалиста сервисной службы ИТ с объемом знаний, эквивалентным по меньшей мере 500 часам практического опыта работы в лаборатории или в полевых условиях.

В качестве основы для успешной сдачи экзаменов предлагаются для изучения следующие учебные материалы:

- экзамен А+ «Core Hardware» касается в основном аппаратных средств с элементной базой фирмы Intel или совместимой аппаратурой ПК:

1.0 Основные положения по операционным системам,
2.0 Инсталляция, конфигурация и модификация,
3.0 Диагностика и обнаружение неисправностей,
4.0 Сети

- экзамен А+ «Технологии ОС» связан со средой Microsoft DOS/Windows:

1.0 Инсталляция, конфигурация и модификация,
2.0 Диагностика и обнаружение неисправностей,
3.0 Профилактическое обслуживание,
4.0 Материнская плата/процессоры/память,
5.0 Принтеры,
6.0 Организация базовой сети.

6.36.3 Источники

Информация и услуги по аттестации обычно доступны через инициатора и руководителей аттестации.

6.37 Аттестация персонала (в части безопасности)

D	I	T	O

6.37.1 Цель

Обеспечение безопасности функционирования ИКТ с помощью сертифицированных администраторов, операторов и аудиторов, связанных с безопасностью.

6.37.2 Описание

Аттестация персонала в области безопасности ИКТ является специфической формой аттестации персонала (см. 6.36), т. е. обеспечения осведомленности персонала в области безопасности. Аттестация персонала в области безопасности обеспечивает прохождение персоналом такого обучения и подготовки, которые могут потребоваться для:

- обеспечения необходимых знаний и информации для качественного выполнения функций безопасности;
- способствования пониманию политик и требований программы обеспечения информационной безопасности и их важности для обеспечения безопасности организации или национальной безопасности;
- внушения необходимости постоянной осведомленности о требованиях безопасности и ее поддержании, а также об угрозах со стороны разведки;
- стимулирования высокой степени мотивации для поддержки целей программы.

Существуют несколько таких видов сертификатов, обеспечивающих различные степени доверия к безопасности функционирования системы ИКТ, как:

- сертифицированный специалист в области систем информационной безопасности (CISSP)®;
- специалист-практик в области безопасности систем (SSCP)™;
- дипломированный аудитор информационных систем (CISA)™;
- сертифицированный специалист по защите (CPP);
- программа сертификации начальника по информационным технологиям Министерства обороны;
- информационная безопасность KickStart Глобальной сертификации доверия к информации;
- основные элементы безопасности первого уровня Глобальной сертификации доверия к информации;
- модули предметной области второго уровня Глобальной сертификации доверия к информации;
- инженер по безопасности Глобальной сертификации доверия к информации.

В дальнейшем CISSP используется в качестве примера аттестации в области безопасности.

Аттестация CISSP была предназначена для признания совершенного владения международным стандартом по информационной безопасности и знания общей совокупности знаний.

Экзамен на аттестацию CISSP состоит из 250 вопросов с разными вариантами ответов. У кандидатов есть для сдачи экзамена не более шести часов. В экзамен, относящийся к общей совокупности знаний, включены следующие десять вариантов теста безопасности информационных систем:

- системы и методология управления доступом;
- разработка систем и приложений;
- планирование непрерывности бизнеса;
- криптография;
- право, расследования и этика;
- безопасность работы;
- физическая защита;
- архитектура и модели безопасности;
- практики менеджмента безопасности;
- безопасность Интернета, сетей и коммуникаций.

6.37.3 Источники

Информация и услуги по аттестации обычно доступны через инициатора и руководителей данной аттестации.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 9000	IDT	ГОСТ Р ИСО 9000—2001 «Системы менеджмента качества. Основные положения и словарь»
ИСО 9001		ГОСТ Р ИСО 9001—2001 «Системы менеджмента качества. Требования»
ИСО/МЭК 9126-1	—	*
ИСО/МЭК 12207	—	ГОСТ Р ИСО/МЭК 12207—99 «Информационная технология. Процессы жизненного цикла программных средств»
ИСО/МЭК ТО 13335-1	IDT	ГОСТ Р ИСО/МЭК 13335-1—2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий»
ИСО/МЭК ТО 13335-2	—	*
ИСО/МЭК ТО 13335-3	IDT	ГОСТ Р ИСО/МЭК 13335-3—2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий»
ИСО/МЭК ТО 13335-4	IDT	ГОСТ Р ИСО/МЭК 13335-4—2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер»
ИСО/МЭК ТО 13335-5	IDT	ГОСТ Р ИСО/МЭК 13335-5—2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети»
ИСО/МЭК 14598-1	—	*
ИСО/МЭК 15939	—	*
ИСО/МЭК 15288	IDT	ГОСТ Р ИСО/МЭК 15288—2005 «Информационная технология. Системная инженерия. Процессы жизненного цикла систем»
ИСО/МЭК 15408-1	IDT	ГОСТ Р ИСО/МЭК 15408-1—2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»
ИСО/МЭК 15408-2	IDT	ГОСТ Р ИСО/МЭК 15408-2—2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»
ИСО/МЭК 15408-3	IDT	ГОСТ Р ИСО/МЭК 15408-3—2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности»
ИСО/МЭК 15504-1	—	*
ИСО/МЭК 15504-2	—	*
ИСО/МЭК 15504-3	—	*
ИСО/МЭК 15504-4	—	*
ИСО/МЭК 15504-5	—	*

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 17799	IDT	ГОСТ Р ИСО/МЭК 17799—2006 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности»
ИСО/МЭК 21827	MOD	ГОСТ Р ИСО/МЭК 21827—2010 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование безопасности систем. Модель зрелости процесса»
ИСО/МЭК 90003	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов:

- IDT — идентичные стандарты;
- MOD — модифицированные стандарты.

Библиография

[1] ISO/IEC TR 9126-2 Software engineering — Product quality — Part 2: External metrics

[2] ISO/IEC TR 9126-3 Software engineering — Product quality — Part 3: Internal metrics

[3] ISO/IEC TR 9126-4 Software engineering — Product quality — Part 4: Quality in use metrics

[4] ISO 13407 Human-centred design processes for interactive systems

[5] ISO/IEC 14598-2 Software engineering — Product evaluation — Part 2: Planning and management

[6] ISO/IEC 14598-3 Software engineering — Product evaluation — Part 3: Process for developers

[7] ISO/IEC 14598-4 Software engineering — Product evaluation — Part 4: Process for acquirers

[8] ISO/IEC 14598-5 Information technology — Software product evaluation — Part 5: Process for evaluators

[9] ISO/IEC 14598-6 Software engineering — Product evaluation — Part 6: Documentation of evaluation modules

[10] ISO/IEC TR 15271 Information technology — Guide for ISO/IEC 12207

[11] ISO/IEC 17024 Conformity assessment — General requirements for bodies operating certification of persons

[12] ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories
Note: EN ISO 17025 is identical to CEN/CENELEC EN ISO 17025.
Note: ISO/IEC 17025 replaces ISO Guide 25 and CEN/CENELEC EN 45001.

[13] ISO/IEC 17050-1 Conformity assessment — Supplier's declaration of conformity — Part 1: General requirements

[14] ISO/IEC 17050-2 Conformity assessment — Supplier's declaration of conformity — Part 2: Supporting documentation

[15] ISO/IEC TR 19760 Systems engineering — Guide for ISO/IEC 15288 (System Life Cycle Processes)

[16] ISO/IEC 25000 Software Engineering — Software Product Quality Requirements and Evaluation (SQuaRE) — Guide to SquaRE (presently FCD)

[17] ISO/IEC 25020 Software and System Engineering — Software quality requirements and evaluation (SQuaRE) — Quality measurement — Measurement reference model and guide (presently CD)

[18] ISO/IEC 25021 Software and System Engineering — Software Product Quality Requirements and Evaluation (SQuaRE) — Measurement Primitives (presently CD)

[19] ISO/IEC 25030 Software engineering — Software quality requirements and evaluation (SQuaRE) — Quality requirements (presently CD)

[20] SCT. Strict Conformance Testing
NPL Report, March 1997. (National Physical Laboratory, Teddington, Middlesex TW11 OLW, UK)

[21] A Systems Engineering Capability Maturity Model (SE-CMM Model), Version 1.1
(CMU/SEI-95-MM-003), November 1995. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.
Note: The model may be available as
gost.e-ecolog.ru

[22] A Description of the Systems Engineering Capability Maturity Model Appraisal Method (SE-CMM Method), Version 1.1 A
(CMU/SEI-96-HB-004), March 1996. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA
Note: The model may be available as gost.e-ecolog.ru

[23] Capability Maturity Model® for Software (SW-CMM®) v1.1
National Technical Information Service (NTIS), US Department of Commerce, Springfield, VA 22161, USA

[24] System Security Engineering Capability Maturity Model, Model Description (SSE-CMM Model), Version 2.0
April 1, 1999 ISSEA, 13873 Park Center Road, Suite 200, Herndon, VA 20171, USA.
Note: The latest version is available at gost.e-ecolog.ru

[25] System Security Engineering Capability Maturity Model, Appraisal Methodology (SSE-CMM Method), Version 2.0
April 16, 1999. ISSEA, 13873 Park Center Road, Suite 200, Herndon, VA 20171, USA.
Note: The latest version is available at gost.e-ecolog.ru

[26] Trusted Capability Maturity Model, Version 2.0
NSA, June 20, 1996 (unreleased US Government document)

[27] A Tailoring of the CMM for the Trusted Software Domain
Kitson, David H in Proceedings of the Seventh Annual Software Technology Conference. Salt Lake City, Utah, April 9-14, 1995

[28] Trust Technology Assessment Program (TTAP)
Note: Information may be available at gost.e-ecolog.ru

[29] Trusted Software Methodology (volumes 1 and 2)
SDI-S-SD-91-000007, June 17, 1992. US Dept. of Defense, Strategic Defense Initiative Organization, Washington, D.C.

[30] Practical Guide to the Open Brand
Ref. X981. The Open Group, 44 Montgomery, Street, Suite 960, San Francisco, CA 94104-4704, USA
Note: The guide may be available as gost.e-ecolog.ru

[31] Canadian Trusted Computer Product Evaluation Criteria, Version 3.0
(NITSM 8/93 and CID 09/19), 1993. Communications Security Establishment, P.O. Box 9703, Terminal, Ottawa, Ontario K1G 3Z4, Canada

[32] Rating Maintenance Phase Program (RAMP), Doc Vers. 2, 1995
NCSC-TG-013-95, Library No. S-242,047, National Computer Security Center (NCSC), 9800 Savage Road, Fort George G. Meade, Maryland 20755-6000, USA
Note: The document may be available as
gost.e-ecolog.ru

[33] IT Baseline Protection Manual
ISBN 3-88784-915-9. Bundesanzeiger-Verlag, Postfach 10 05 34, 50455 Koln, Germany.
Note: Up-to-date versions of this manual may also be available on-line at gost.e-ecolog.ru

[34] Capability Maturity Model for Software CMU/SEI-91-TR-24,
August 1991, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213—3890.
Note: The document may be available as
gost.e-ecolog.ru

[35] Capability Maturity Model ® Integration for the systems engineering and software engineering integrated model, CMMI-SE/SW Version 1.1
Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213—3890.
Note: The document may be available as gost.e-ecolog.ru

[36] CMMISM for Systems Engineering/Software Engineering/Integrated Product and Process Development, Version 1.1, Staged Representation CMMI-SE/SW/IPPD, V1.1, Staged, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890.
Note: The document may be available as
gost.e-ecolog.ru

[37] CMMISM for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1, Staged Representation
CMMI-SE/SW/IPPD/SS, V1.1, Staged, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.
Note: The document may be available as
gost.e-ecolog.ru

[38] Software Acquisition Capability Maturity Model® (SA-CMM®), Version 1.03
March 2002. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.
Note: The document may be available as
gost.e-ecolog.ru

[39] X/Open Baseline Security Services (XBSS) Document Number C529, ISBN 1-85912-136-5, December 1995. The Open Group, 44 Montgomery, Street, Suite 960, San Francisco, CA 94104-4704, USA.
Note: The document may be available at gost.e-ecolog.ru

[40] Information Technology Security Evaluation Criteria (ITSEC), version 1.2 Office for Official Publications of the EC, June 1991. Document may be obtained by: gost.e-ecolog.ru

[41] Information Technology Security Evaluation Manual (ITSEM), version 1.0 Office for Official Publications of the EC, September 1993. Document may be obtained by: gost.e-ecolog.ru

[42] V-Model — Development Standard for IT Systems, VM 1997 IABG, EinsteinstraBe 20, D-85521 Ottobrunn, Germany. Document may be obtained by: gost.e-ecolog.ru

[43] A Head Start on Assurance in Proceedings of an Invitational Workshop on Information Technology (IT) Assurance and Trustworthiness, March 21-23, 1994, NISTIR 5472. National Security Agency, 9800 Savage Road, Suite 6740, Ft. Meade, MD 20755-7640, USA.

[44] UK Certificate Maintenance Scheme, Issue 1.0
31 July 1996, Certification Body, PO Box 152, Cheltenham, Glos GL52 5UF, UK.

Note: The document may be available as
gost.e-ecolog.ru

[45] Trusted Computer System Evaluation Criteria (TCSEC), 1985
DOD 5200.28-STD, Library No. 8225,711, US Dept. of Defense.
Document may be obtained by: gost.e-ecolog.ru

[46] Trusted Product Evaluation Program (TPEP)
Information may be obtained by: gost.e-ecolog.ru

[47] A Trusted Software Development Methodology
J. Watson and E. Amoroso, in Proc. 13th Natl. Computer Security Conf, Oct. 1990, pp. 717—727

[48] Insider Threat Mitigation Report
in Final Report of the Insider Threat Integrated Process Team, IPT April 24, 2000. Insider Threat Integrated Process Team, Department of Defense, USA

[49] State of the Practice of Intrusion Detection Technologies
CMU/SEI-99-TR-028 ESC-TR-99-028, January 2000. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, USA.
Note: The document may be available as gost.e-ecolog.ru

[50] Korea Information Security Evaluation Criteria (KISEC)
Ministry of Information and Communication, Republic of Korea, February 1998

[51] Korea Information Security Evaluation Methodology (KISEM)
Ministry of Information and Communication, Republic of Korea, November 1998

[52] Philippe Kruchten, The Rational Unified Process — An Introduction Addison-Wesley-Longman, Reading, MA, USA

[53] BS 7799-2:2002 Information security management systems — Specification with guidance for use BSI (British Standards Institution), Customer Services, 389 Chiswick High Road, London W4 4AL, United Kingdom

УДК 681.324:006.354 ОКС 35.040 IDT

Ключевые слова: информационная технология, безопасность информационных технологий, методы обеспечения доверия

Редактор *В.Н. Колысов*
Технический редактор *Н.С. Гришанова*
Корректор *М.В. Бучная*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 28.12.2012. Подписано в печать 04.02.2013. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 6,05. Уч.-изд. л. 5,50. Тираж 96 экз. Зак. 109.

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