ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 21827— 2010

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Проектирование систем безопасности. Модель зрелости процесса

ISO/IEC 21827:2008
Information technology — Security techniques — Systems Security Engineering —Capability Maturity Model (SSE-CMM)
(IDT)

Издание официальное

Москва
Стандартинформ
2015

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»)

2 ВНЕСЕН Техническим комитетом по стандартизации № 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 30 сентября 2010 г. № 291-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 21827:2008 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем защиты. Модель зрелости возможностей (SSE-CMM)» [ISO/IEC 21827:2008 «Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model (SSE-CMM)»].

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

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2015

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
2 Нормативные ссылки ... 1
3 Термины и определения ... 1
4 Вводная информация ... 4
4.1 Основание для разработки ... 4
4.2 Значимость проектирования безопасности ... 5
4.3 Согласованность ... 5
5 Структура документа ... 6
6 Архитектура модели ... 6
6.1 Проектирование безопасности ... 6
6.2 Обзор процесса проектирования безопасности ... 8
6.3 Описание архитектуры модели SSE-CMM® ... 12
6.4 Итоговая схема ... 17
7 Базовые практики обеспечения безопасности ... 18
7.1 PA01 - Управление мерами безопасности ... 21
7.2 PA02 - Оценка воздействия ... 24
7.3 PA03 - Оценка риска безопасности ... 27
7.4 PA04 - Оценка угроз ... 30
7.5 PA05 - Оценка уязвимостей ... 32
7.6 PA06 - Создание аргумента доверия ... 35
7.7 PA07 - Координация безопасности ... 38
7.8 PA08 - Мониторинг состояния безопасности ... 40
7.9 PA09 - Предоставление входных данных по безопасности ... 45
7.10 PA10 - Обозначение потребности в безопасности ... 48
7.11 PA11 - Верификация и подтверждениесостояние безопасности ... 52
Приложение А (справочное) Общие практики ... 55
Приложение В (справочное) Базовые практики проекта и организации ... 56
Приложение С (справочное) Концепции модели зрелости возможностей ... 98
Приложение D (справочное) Общие практики ... 104
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации ... 116
Библиография ... 117

0 Введение

0.1 Общие положения

Многие организации используют проектирование безопасности в разработке компьютерных программ, таких как операционные системы, а также функций обеспечения выполнения требований безопасности и управления безопасности, ПО, ПО для обмена данными или прикладных программ.

Следовательно, разработчики продукта, системные интеграторы и даже специалисты в области безопасности нуждаются в соответствующих методах и практических приемах. Некоторые из этих организаций имеют дело с высокоуровневыми задачами (например, функциональным использованием или системной архитектурой), другие сосредоточены на низкоуровневых задачах (например, проектировании или выборе механизма), третьи занимаются и тем, и другим. Организации могут специализироваться на определенной технологии или конкретной области деятельности (например, в области океанологии).

Модель SSE-CMM® предназначена для всех подобных организаций и случаев применения. Применение модели SSE-CMM® не подразумевает, что то или иное направление деятельности лучше другого или требуется какое-либо конкретное направление деятельности. Использование модели SSE-CMM® не должно отрицательно воздействовать на основное направление деловой деятельности конкретной организации.

Некоторые способы проектирования безопасности применяются на основе направления деловой деятельности организации. Кроме того, организации может потребоваться рассмотрение взаимосвязей между различными практическими приемами в границах модели с целью определения их применимости. Приведенные ниже примеры демонстрируют способы, какими многие организации могут применять модель SSE-CMM® для разработки программного обеспечения, систем, оборудования или эксплуатации.

Настоящий стандарт связан со стандартами серии ИСО/МЭК 15504, в частности с ИСО/МЭК 15504-2, поскольку они оба касаются технологического прогресса и оценки развития функциональных возможностей. Однако ИСО/МЭК 15504 сосредоточен конкретно на процессах создания и эксплуатации ПО, тогда как модель SSE-CMM предназначена для обеспечения безопасности.

Настоящий стандарт особенно тесно связан с новыми версиями ИСО/МЭК 15504, в частности с ИСО/МЭК 15504-2:2004, и согласуется с его принципами и требованиями.

Провайдеры услуг, связанных с безопасностью

Для определения возможностей технологического процесса (далее просто процесса) организации, проводящей оценки рисков, применяются несколько групп практических приемов. Для разработки или интеграции любой системы может потребоваться оценка способности организации определять и анализировать уязвимости системы безопасности, а также оценка эксплуатационных воздействий. Для эксплуатации любой системы может потребоваться оценка способности организации осуществлять мониторинг состояния безопасности системы, идентификацию, анализ уязвимостей и угроз безопасности, а также оценка воздействий, возникающих в процессе эксплуатации системы.

Разработчики мер противодействия

Когда группа разработчиков занимается разработкой мер противодействия угрозам безопасности, возможности технологического процесса организации характеризуются комбинацией практических приемов модели SSE-CMM®. Модель содержит практические приемы определения и анализа уязвимостей безопасности, оценки функциональных воздействий и предоставления входных данных и руководств другим задействованным группам специалистов (таким, как группа специалистов по программному обеспечению). Группа, предоставляющая услугу по разработке мер противодействия, должна знать взаимосвязи между этими практическими приемами.

Разработчики продукта

Модель SSE-CMM® содержит практические приемы, направленные на обеспечение понимания потребностей заказчика в области безопасности. Для их определения требуется взаимодействие с заказчиком. В случае с продуктом «заказчик» является общим понятием, поскольку продукт разрабатывается априори независимо от потребностей конкретного заказчика. Если потребуется, в качестве гипотетического заказчика может использоваться группа маркетинга продукции.

Специалисты - практики по проектированию безопасности признают, что методы ее разработки столь же разнообразны, как и сами продукты. Однако существуют несколько проблем, связанных с продукцией и проектами, о которых известно, что они оказывают воздействие на то, как продукты проектируются, изготавливаются, доставляются и обслуживаются. Особое значение для модели SSE-CMM® имеют:

- тип клиентской базы (продукты, системы или услуги);
- требования доверия (высокие в сравнении с низкими);

- поддержка как разрабатывающих, так и эксплуатационных организаций.

Ниже обсуждаются отличия между двумя разными клиентскими базами, различные степени требований доверия и воздействия каждого из этих различий в модели SSE-CMM®. Они представлены в качестве примера того, как организация или отрасль промышленности может определить, соответствует ли SSE-CMM® условиями конкретной окружающей среды.

Специфика отраслей промышленности

Каждая отрасль промышленности имеет свою особую культуру, терминологию и стиль общения. Минимизируя различия между должностями и последствия несовершенства структуры организации, ожидается, что концепции SSE-CMM® могут быть легко преобразованы любыми отраслями промышленности для своих нужд и внедрены в информационную систему.

0.2 Как следует использовать SSE-CMM®

Модель SSE-CMM® и метод ее применения (то есть оценочный метод) предназначены для использования в качестве:

- инструмента проектных организаций для оценки практических приемов проектирования безопасности и определения улучшений;
- метода, посредством которого организации, оценивающие проектирование безопасности, такие как органы сертификации и экспертные организации по оценке, могут упрочить доверие к ее потенциальным возможностям в качестве вклада в формирование доверия к безопасности продукта или системы;
- стандартного механизма оценки клиентами возможностей проектирования безопасности провайдером.

Область оценки должна определяться оценивающей организацией и, если это необходимо, обсуждаться с экспертом по оценке.

Методы оценки могут использоваться организацией при применении модели в целях самосовершенствования и выборе поставщиков, если пользователи модели и оценочных методов в достаточной мере осведомлены о надлежащем применении модели и присущих ей ограничениях. Дополнительная информация по использованию оценки технологических процессов содержится в ИСО/МЭК 15504-4:2004 «Информационная технология-Оценка технологических процессов - Часть 4: Руководство по применению для усовершенствования процессов и определения функциональных возможностей процессов».

0.3 Преимущества применения SSE-CMM®

Общей тенденцией обеспечения безопасности является переход от защиты правительственной информации к более широкому спектру задач, включая защиту финансовых операций, контрактов, персональных данных и Интернета. Эта тенденция привела к соответствующему распространению продукции, систем и услуг, сохраняющих и защищающих информацию. Продукция и системы обеспечения безопасности обычно поступают на рынок двумя путями: через длительное и дорогостоящее оценивание и без него. В первом случае надежная продукция часто попадает на рынок уже после снабжения ее системами безопасности, когда текущие угрозы для нее уже не страшны. Во втором случае приобретающая сторона и пользователи должны полагаться исключительно на утверждения разработчика или оператора о безопасности продукта или системы. Более того, услуги по проектированию безопасности по сложившейся традиции часто предоставлялись на основе принципа «пусть покупатель будет бдителен».

Данная ситуация требует от организации более продуманного проектирования безопасности. В частности, для производства и эксплуатации систем безопасности и надежной продукции необходимы следующие качества:

- непрерывность – знания, полученные в ходе предшествующей деятельности, используются в последующей деятельности;
- повторяемость – способ обеспечения повторения в проектах успешных работ;
- результативность – способ оказания помощи как разработчикам, так и оценщикам в повышении эффективности их труда;
- доверие – обеспечение уверенности в рассмотрении потребностей в безопасности.

Для выполнения этих требований необходим механизм, направляющий организации на понимание и усовершенствование своих действий по проектированию безопасности. Учитывая эти запросы, модель SSE-CMM® разработана с целью развития существующей практики проектирования безопасности для повышения качества и доступности защищенных систем, надежной продукции и услуг по проектированию безопасности, а также снижения затрат на их поставку.

В частности, предполагается получение следующих преимуществ.

Для проектных организаций.

Проектные организации включают в себя системных интеграторов, разработчиков прикладных программ, продавцов продукции и провайдеров услуг. Преимуществами применения модели SSE-CMM® в этих организациях являются:

- экономия средств вследствие уменьшения числа исправлений в ходе повторяющихся прогнозируемых процессов и практик;
- уверенность в надлежащем осуществлении функциональных возможностей, особенно при выборах источника;
- направленность на повышение компетентности (зрелости) организации.

Для приобретающих организаций.

Приобретающие стороны включают в себя организации, приобретающие системы, продукцию и услуги у внешних/внутренних источников, а также конечных пользователей. Для этих организаций преимущества от применения модели SSE-CMM® состоят в:

- снижении рисков (для функционирования, стоимости, плана) выбора неквалифицированного участника торгов;
- уменьшении числа претензий вследствие единообразия оценок, основанных на промышленном стандарте;
- прогнозируемости уровеня доверия к продукту или услуге с высокой повторяемостью.

Для оценивающих организаций

Оценивающие организации включают в себя органы сертификации и аккредитации систем, органы оценки и органы по аттестации. Для этих организаций преимущества от применения SSE-CMM® состоят в:

- возможности повторного использования результатов оценки процесса независимо от изменений системы или продукта;
- доверии к проектированию безопасности и его интеграции в другие дисциплины;
- доверии к доказательству, основанному на потенциальных возможностях и уменьшающему объем работ, связанных с оцениванием безопасности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Проектирование систем безопасности. Модель зрелости процесса

Information technology. Security techniques. Systems security engineering. Capability maturity model

Дата введения 2011—09—01

1 Область применения

Настоящий стандарт содержит подробное описание модели проектирования систем безопасности – зрелости функциональных возможностей (SSE-CMM®). SSE-CMM® является эталонной моделью процесса, сосредоточенной на требованиях по реализации безопасности в системе или серии взаимосвязанных систем, которые являются доменом безопасности информационных технологий (БИТ). В границах домена БИТ сосредоточена на процессах, используемых для обеспечения БИТ и, более конкретно, на зрелости этих процессов. Модель SSE-CMM® не предполагает навязывание конкретной организации заданного процесса, не говоря об определенной методологии. Скорее имеется в виду, что организации используют модель SSE-CMM®, если в них не применяются процессы, основанные на каком-либо другом руководстве по БИТ. Область применения настоящего стандарта охватывает:

- действия по проектированию безопасности для защищенного продукта или выверенной системы, включающие полный жизненный цикл, состоящий из определения понятия, анализа требований, проектирования, разработки, интеграции, установки, эксплуатации, обслуживания и вывода из эксплуатации;
- требования к разработчикам продукта, разработчикам и интеграторам безопасных систем, организациям, предоставляющим услуги по обеспечению компьютерной безопасности и проектированию безопасности;
- организации по проектированию безопасности всех типов и масштабов, от коммерческих до правительственных и академических.

Использование SSE-CMM® для оценки и улучшения возможностей проектирования безопасности не означает, что его следует осуществлять без применения других технических дисциплин. Наоборот, модель SSE-CMM® способствует интеграции с учетом того, что обеспечение безопасности распространяется на все технические дисциплины (например, системы, программное обеспечение и аппаратные средства), и определяет компоненты модели для решения таких задач. Общий признак «координация практических приемов» признает необходимость интегрирования безопасности во все дисциплины и группы, участвующие в проекте, или во всю организацию. Аналогично в области процесса «координация безопасности» приводится определение цели и описываются механизмы, предназначенные для использования при координировании действий по проектированию безопасности.

2 Нормативные ссылки

В настоящем стандарте использованы ссылка на международный стандарт ИСО/МЭК 15504-2 2003 Информационная технология. Оценка процесса. Часть 2. Проведение оценки (ISO/IEC 15504-2, Information technology — Process assessment — Part 2: Performing an assessment).

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **учетность (подотчетность, отслеживаемость)** (accountability): Свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта.

[ИСО/МЭК 7498-2:1989]

3.2 **аккредитация** (accreditation): Формальное заявление назначенного утверждающего органа о принятии системы для эксплуатации в определенном режиме безопасности с использованием заданного набора мер безопасности.

Примечание - Данное определение в основном применяется в области безопасности в целом; в ИСО наиболее широко применяемым определением является следующее: процедура, посредством которой официальный орган формально признает компетентность организации или лица выполнять определенные задачи.

[ИСО/МЭК Руководство 2]

Издание официальное

3.3 **оценка** (assessment): Верификация продукта, системы или услуги на соответствие требованиям стандарта, используя метод оценки, для установления соответствия и определения степени доверия.

Примечание - Адаптировано с ИСО/МЭК ТО 15443-1:2005.

3.4 **актив** (asset): Всё, что имеет ценность для организации.

[ИСО/МЭК ТО 13335-1:1996]

3.5 **доверие** (assurance): Основание для создания уверенности в том, что продукт отвечает своим целям безопасности.

Примечания

1 Адаптировано с ИСО/МЭК 15408-1:2005.

2 Данное определение в основном применяется в области безопасности в целом; в ИСО наиболее широко применяемым определением является следующее: «деятельность, приводящая в результате к утверждению, которое дает уверенность в том, что продукт, процесс или услуга соответствуют установленным требованиям».

[ИСО/МЭК Руководство 2].

3.6 **аргумент доверия** (assurance argument): Совокупность структурированных заявлений о доверии, подтвержденных доказательствами и аргументацией, четко демонстрирующих, каким образом были удовлетворены потребности в доверии.

3.7 **заявление о доверии** (assurance claim): Утверждение или поддержка утверждения того, что система удовлетворяет требованиям безопасности.

Примечание - В заявлениях учитываются как прямые угрозы (например, защищенность данных системы от атак посторонних лиц), так и косвенные (например, наличие у кода системы минимума дефектов).

3.8 **свидетельство доверия** (assurance evidence): Данные, на которых может базироваться обоснование заявления о доверии или заключение о нем.

Примечание - Свидетельство может состоять из наблюдений, результатов тестирования, результатов анализа и оценок.

3.9 **аутентичность** (authenticity): Свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

Примечания

1 Аутентичность применяется к таким логическим объектам, как пользователи, процессы, системы и информация.

2 Адаптировано из ИСО/МЭК ТО 13335-1:1996.

3.10 **доступность** (availability): Свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта.

[ИСО/МЭК 7482-2:1989]

3.11 **база** (baseline): Спецификация или продукт, формально проанализированный, согласованный и впоследствии служащий в качестве основы для дальнейших разработок, который может быть изменен только посредством формальных процедур управления изменениями.

[IEEE-Std.610]

3.12 **сертификация** (certification): Изложенный в письменной форме процесс проведения всеобъемлющего оценивания функциональных возможностей обеспечения безопасности и других мер защиты системы для определения степени, в которой проект системы и его реализация удовлетворяют требованиям безопасности.

Примечание - Данное определение в основном применяется в области безопасности в целом; в ИСО наиболее широко применяемым определением является следующее: «процедура, посредством которой третья сторона дает письменные заверения, что продукт, процесс или услуга соответствуют установленным требованиям».

[ИСО/МЭК Руководство 2]

3.13 **конфиденциальность** (confidentiality): Свойство, позволяющее не давать право на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам.

[ИСО/МЭК 7498-2:1989]

3.14 **последовательность** (consistency): Степень единообразия, стандартизации и отсутствия противоречий в документах, частях системы или компонентах.

[IEEE-Std.610]

3.15 **правильность** (correctness): Состояние продукта или системы, демонстрирующее их соответствие установленным требованиям безопасности.

3.16 **заказчик** (customer): Получатель продукта, предоставленного поставщиком.

Примечания

1 В договорных ситуациях заказчик называется «покупателем».

2 Заказчик может быть, например, непосредственным потребителем, пользователем или покупателем.

3 Заказчик может быть ее сотрудником или сторонним для организации.

[ИСО 9000:2005] и [ИСО/МЭК 15504-1:2004].

3.17 **эффективность** (effectiveness): Свойство системы или продукта, показывающее, насколько хорошо оно обеспечивает безопасность в контексте их предполагаемой или фактической эксплуатации.

3.18 **инженерная группа** (engineering group): Совокупность лиц (как руководителей, так и инженерно-технического персонала), ответственных за действия по проекту или в организации, связанные определенной технической дисциплиной.

Примечание - Технические дисциплины включают в себя: аппаратные средства, программное обеспечение, управление конфигурированием программного обеспечения, доверие к качеству программного обеспечения, а также системы, их тестирование и безопасность.

3.19 **свидетельство** (evidence): Непосредственно измеряемые характеристики процесса и/или продукта, свидетельствующие, что конкретное действие удовлетворяет установленному требованию.

3.20 **целостность** (integrity): Свойство обеспечения безопасности достоверности и полноты информации и методов обработки.

3.21 **техническое обслуживание** (maintenance): Процесс модифицирования системы или компонента после доставки с целью исправления дефектов, улучшения рабочих и других характеристик или адаптации к изменившимся условиям.

[IEEE-Std.610]

3.22 **методология** (methodology): Совокупность стандартов, процедур и вспомогательных методов, определяющих детальный подход к разработке продукта или системы.

3.23 **профиль преодоления защиты** (penetration profile): Определение действий по преодолению защиты.

3.24 **процедура** (procedure): Письменное описание хода действия, осуществляемого для выполнения данной задачи.

[IEEE-Std.610]

3.25 **процесс** (process): Совокупность взаимосвязанных действий по преобразованию входных данных в выходные.

Примечание - Адаптировано с ИСО/МЭК 15288:2002.

3.26 **надежность** (reliability): Свойство поддержания постоянного режима и получения непротиворечивых результатов.

[ИСО/МЭК ТО 13335-1:1996]

3.27 **остаточный риск** (residual risk): Риск, сохраняющийся после внедрения мер безопасности.

[ИСО/МЭК ТО 13335-1:1996]

Примечание - Данное определение отличается от определения, применяемого в Руководстве 73 ИСО/МЭК.

3.28 **риск** (risk): Потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей актива или группы активов.

[ИСО/МЭК ТО 13335-1:1996]

Примечание - Данное определение отличается от определения, применяемого в Руководстве 73 ИСО/МЭК.

3.29 **анализ риска** (risk analysis): Процесс идентификации рисков безопасности, определения их величины и областей, нуждающихся в применении мер безопасности.

[ИСО/МЭК ТО 13335-1:1996]

Примечание - Данное определение отличается от определения, применяемого в Руководстве 73 ИСО/МЭК.

3.30 **менеджмент риска** (risk management): Процесс оценки и определения величины риска, а также установления уровня риска, приемлемого для организации.

[ИСО/МЭК ТО 13335-1:1996]

Примечание - Данное определение отличается от определения, применяемого в Руководстве 73 ИСО/МЭК.

3.31 **политика безопасности** (security policy): Правила, указания и практические приемы, определяющие то, как активы, включая информацию ограниченного доступа, управляются, защищаются и распределяются внутри организации и ее систем, в особенности те, которые воздействуют на системы и связанные с ними элементы.

3.32 **требования, связанные с безопасностью** (security related requirements): Требования, оказывающие непосредственное влияние на безопасное функционирование системы и обязывающие соблюдать установленную политику безопасности.

3.33 **система:** Отдельный, различимый физически, существующий логический объект, имеющий определенное назначение, полностью состоящий из интегрированных взаимодействующих компонентов, каждый из которых в отдельности не соответствует указанному общему назначению.

Примечания

1 Адаптировано с ИСО/МЭК 15288:2002.

2 Толкование значения слова «система» часто упрощается использованием связанных с ним существительных или прилагательных (например «система продуктов», «авиационная система»). В качестве альтернативы слово «система» можно заменить зависящим от контекста синонимом (например «продукт», «самолет»), хотя в будущем это может исказить первоначальный смысл этой фразы.

3 Для удовлетворения различным требованиям во время ее жизненного цикла системе могут потребоваться другие системы. Например, автоматизированной системе может потребоваться система концептуализации, разработки, изготовления, эксплуатации, поддержки и удаления.

3.34 **угроза** (threat): Потенциальные возможности, намерения и методы атаки противника, другое обстоятельство или событие, возникнувшие внутри или вовне организации, которые могут нанести ущерб информации, программе или системе или заставить их причинить ущерб другой информации, программе или системе.

3.35 **носитель угрозы** (threat agent): Источник и/или инициатор преднамеренных или случайных исходящих от человека угроз.

3.36 **проверка достоверности** (validation): Подтверждение выполнения установленных требований к конкретному использованию по назначению посредством проверки и предоставление объективных доказательств.

Примечание - Адаптировано с ИСО/МЭК 15288:2002.

3.37 **верификация** (verification): Подтверждение путем проверки и предоставление объективных доказательств выполнения установленных требований.

Примечание - Адаптировано с ИСО/МЭК 15288:2002:2002.

3.38 **уязвимость** (vulnerability): Слабое место актива или группы активов, которое может быть подвержено воздействию угрозы.

3.39 **рабочий продукт** (work product): Артефакт, связанный с выполнением процесса.

[ИСО/МЭК 15504-1:2004]

Примечание - Рабочий продукт может использоваться, производиться или изменяться процессом.

4 Вводная информация

В модели зрелости функциональных возможностей проектирования безопасности систем (SSE-CMM®) представлены необходимые характеристики процесса проектирования безопасности организации, которые должны обеспечивать высокое качество проектирования безопасности.

SSE-CMM® не предписывает каких-либо конкретных процессов или последовательности действий, а представляет собой совокупность практических приемов, в основном применяемых в промышленности. Эта модель является стандартной для практического проектирования систем безопасности, охватывающих:

- весь жизненный цикл системы безопасности, включающий в себя действия по разработке, эксплуатации, обслуживанию и выводу из эксплуатации;
- управленческую, организационную и конструкторскую деятельность организации;
- одновременные (параллельные) взаимодействия с другими дисциплинами, такими как система, программное обеспечение, человеческий фактор и испытательная техника, управление, эксплуатация и обслуживание системы;
- взаимодействие с другими организациями, включая приобретение, менеджмент систем, сертификацию, аттестацию и оценивание.

В описании SSE-CMM® представлено общее изложение принципов и архитектуры, на которых она основана, общий вид модели, предложения по ее надлежащему применению, практические приемы, включенные в модель, и описание атрибутов модели. В описании также содержатся требования, используемые для разработки модели. Оценочный метод SSE-CMM® описывает процесс и инструменты оценивания возможностей организации по проектированию системы безопасности и сопоставления с SSE-CMM®.

4.1 Основание для разработки

Как заказчики, так и поставщики заинтересованы в совершенствовании разработки продуктов, систем и услуг в области безопасности. В области проектирования безопасности содержатся несколько общепринятых принципов, но в настоящее время в ней отсутствует комплексная основа оценивания практических приемов проектирования безопасности. Определяя подобную основу, SSE-CMM® предоставляет способ измерения и улучшения эффективности применения принципов проектирования безопасности.

Необходимо подчеркнуть, что проектирование безопасности является уникальной дисциплиной, требующей уникальных знаний, навыков и процессов, гарантирующих разработку особой SSE-CMM® для проектирования безопасности. Это не противоречит исходному условию, что проектирование безопасности осуществляется в контексте системного проектирования. Фактически, четко определенная и

общепринятая деятельность по системному проектированию позволит осуществлять на практике проектирование безопасности при всех обстоятельствах.

Современное статистическое управление процессом предлагает возможность производства более качественной продукции более рентабельным образом путем придания особого значения качеству процессов их производства и зрелости организационных практических приемов, присущих этим процессам. Большая эффективность процессов гарантируется при условии увеличения стоимости и времени, необходимых для разработки безопасных систем и высоконадежной продукции. Эксплуатация и обслуживание безопасных систем основаны на процессах, объединяющих людей и технологии.

Целью проекта является продвижение проектирования безопасности как определенной, зрелой и измеряемой дисциплины. SSE-CMM® и оценочные методы разрабатываются с целью обеспечения:

- направленных инвестиций в инструменты проектирования безопасности, обучение, определение процессов, практические приемы менеджмента и внесение усовершенствований инженерными группами;
- основанного на потенциальных возможностях доверия (то есть кредитоспособности, основанной на доверии к зрелости практических приемов и процессов обеспечения безопасности, применяемых инженерными группами);
- подбора квалифицированных проектировщиков систем безопасности посредством дифференциации претендентов по уровням их потенциальных возможностей и связанных с ними программируемых рисков.

4.2 Значимость проектирования безопасности

С усилением зависимости общества от информации защита этой информации становится все более значимой. Для сохранения и защиты информации требуются различные продукты, системы и услуги. Значимость проектирования безопасности расширилась от использования, связанного в первую очередь с защитой правительственной информации ограниченного доступа, до более широкого использования, включающего финансовые операции, контракты, персональную информацию и Интернет. Эта тенденция в существенной степени повысила значимость проектирования безопасности.

4.3 Согласованность

SSE-CMM® разрабатывалась более чем 50 организациями, многие из которых являются многонациональными корпорациями. В разработке проекта участвовали представители Австралии, Канады, Европы и США. Кроме того, проект SSE-CMM® всегда стремился к расширению круга участников путем использования различных мест проведения мероприятий, включая презентации, и применение выставочные стенды, а также веб-сайт gost.e-ecolog.ru

Участники были организованы в руководящую группу и несколько рабочих групп. Большая часть разработки осуществлялась рабочими группами, в то время как руководящая группа отвечала за общий ход процесса и утверждение отдельных частей проекта.

Модель SSE-CMM® разрабатывалась посредством консенсуса. Все организации-участники могли посылать своих представителей на заседания рабочих групп и большинство из них именно так и поступали. Статьи рассылались электронной почтой другим членам рабочей группы в перерывах между заседаниями. Заседания проводились ежемесячно и на них обсуждались, пересматривались и согласовывались вносимые предложения. Результаты всех необходимых голосований фиксировались в протоколах заседаний рабочих групп на каждом заседании. Затем эти документы сохранялись.

Каждая версия модели SSE-CMM® вначале утверждалась рабочей группой, занимающейся разработкой. Затем она просматривалась и утверждалась руководящей группой. После этого версия модели отсылалась группе «главных рецензентов», собранной из представителей сообщества, связанного с безопасностью ИТ, для проведения анализа и критического разбора. Затем каждая версия публиковалась для общественного рассмотрения и получения замечаний и предложений. На основе замечаний и предложений главных рецензентов и сообщества в целом руководящая группа определяла последнюю редакцию этой версии модели SSE-CMM®.

Модель SSE-CMM® в первый раз утверждалась на уровне рабочей группы, второй раз на уровне руководящей группы, в третий раз на уровне главных рецензентов и, наконец, на уровне сообщества. Таким образом, по существу применялись три уровня утверждения.

Дополнительное утверждение и консенсус достигались в ходе проведения контрольных экспертиз результатов применения модели в различных заданных областях. Рабочая группа альтернативного гарантирования Проекта Общих Критериев провела анализ модели SSE-CMM® на ее применимость в качестве альтернативы получения доверия путем оценивания и представила в проект замечания и предложения, относящиеся к безопасности систем ИТ.

Каждая публикация модели анализировалась группой независимых рецензентов, которые не участвовали в ее разработке. Их замечания были собраны, проанализированы и включены в модель. Наконец, каждая версия этого документа подвергалась общественному изучению и критическому анализу на двух международных семинарах, а полученные замечания были рассмотрены и учтены.

5 Структура документа

Предпосылки создания документа и основания для его разработки обсуждаются в разделе 4. Архитектура модели SSE-CMM® и роль проектирования безопасности систем рассматриваются в разделе 6. Составные области процесса проектирования безопасности и базовые практики подробно рассматриваются в разделе 7. Уровни зрелости функциональных возможностей и общие практики изложены в приложении А, тогда как в приложении В описаны области организационного процесса и проекта и базовые практики. Концепции модели зрелости функциональных возможностей изложены в приложении С.

6 Архитектура модели

Модель SSE-CMM® представляет собой совокупность лучших практических приемов проектирования безопасности. Для понимания данной модели требуется исходная информация по этому проектированию. Данный раздел предлагает высокоуровневое описание проектирования безопасности, а также того, каким образом архитектура модели отражает это основное понятие.

6.1 Проектирование безопасности

6.1.1 Понятие проектирования безопасности

Стремление к всеобъемлющей взаимосвязи и совместимости сетей, компьютеров, прикладных программ и даже предприятий непрерывно повышает роль безопасности. Основное внимание к обеспечению безопасности сместилось с защиты правительственной информации ограниченного пользования к области более широкого применения, включая финансовые операции, контракты, персональные данные и Интернет. В результате необходимо, чтобы потенциальные области, нуждающиеся в защите, рассматривались и определялись для каждого направления использования. Примерами таких областей являются конфиденциальность, целостность, доступность, подотчетность, неприкосновенность частной жизни и доверие.

Смещение направленности задач обеспечения безопасности повышает значимость проектирования безопасности. Оно становится все более важной дисциплиной и должно превратиться в ключевой компонент согласованных действий инженерных групп, состоящих из специалистов в разных дисциплинах. Проектирование безопасности применимо к разработке, интеграции, эксплуатации, управлению и развитию систем и приложений, а также к разработке, доставке и модернизации продукции. Вопросы безопасности должны учитываться при определении, руководстве и модернизации безопасности предприятий и процессов деловой деятельности. Проектирование безопасности может осуществляться в системе, продукте или в виде услуги.

6.1.2 Описание проектирования безопасности

Проектирование безопасности является развивающейся дисциплиной. По существу согласие по точному определению понятия «проектирование» пока не достигнуто. Однако возможно несколько обобщений. Так, одними из целей проектирования безопасности являются:

- обеспечение понимания рисков безопасности предприятия;
- установление уравновешенной (сбалансированной) совокупности требований безопасности в соответствии с идентифицированными рисками;
- преобразование требований безопасности в руководство по безопасности с целью интеграции в деятельность, относящуюся к другим дисциплинам, участвующим в проекте, и в описание конфигурации или функционирования системы;
- создание уверенности или доверия к правильности и эффективности механизмов обеспечения безопасности;
- определение допустимости воздействий на эксплуатацию, обусловленных остаточными уязвимостями в системе или в процессе ее эксплуатации (то есть определение остаточных рисков);
- объединение усилий всех инженерных дисциплин с целью общего понимания надежности системы.

6.1.3 Организации, связанные с проектированием мер безопасности

Деятельность по проектированию безопасности практикуется различными типами организаций, такими как:

- разработчики;
- продавцы продукции;
- интеграторы;
- покупатели (приобретающая организация или конечный пользователь);
- организации, оценивающие безопасность (органы сертификации систем, оценки продукции и аккредитации эксплуатации);
- доверенные третьи стороны (орган сертификации);
- консультирующие организации/провайдеры услуг.

6.1.4 Жизненный цикл проектирования безопасности

Деятельность по проектированию безопасности осуществляется на всех этапах жизненного цикла, включая этапы:

- создания концепции;
- разработки;
- производства;
- эксплуатации;
- поддержки;
- изъятия из эксплуатации.

6.1.5 Проектирование безопасности и другие дисциплины

Деятельность по проектированию безопасности связана со многими другими дисциплинами, включая:

- проектирование предприятий;
- системное проектирование;
- проектирование программного обеспечения;
- инженерную психологию;
- технику связи;
- испытательную технику;
- администрирование системы.

Примечания

1 В отношении системного проектирования дополнительную информацию, рассматривающую задачи безопасности с точки зрения систем, можно найти в ИСО/МЭК 15288:2002.

2 В отношении проектирования программного обеспечения дополнительную информацию, рассматривающую задачи безопасности с точки зрения программного обеспечения, можно найти в ИСО/МЭК 12207:1995.

Деятельность по проектированию безопасности должна быть скоординирована со многими сторонними логическими объектами, поскольку доверие и приемлемость остаточных эксплуатационных воздействий устанавливаются совместно с разработчиком, интегратором, покупателем, пользователем, независимым оценщиком и другими группами. Именно эти необходимые взаимодействия между различными организациями делают проектирование безопасности особенно сложным.

6.1.6 Специализации в области проектирования безопасности

В то время как проектирование безопасности и безопасность ИТ очень часто являются ведущими дисциплинами в условиях обеспечения безопасности деловой деятельности, нельзя игнорировать другие более традиционные дисциплины обеспечения безопасности, такие как физическая защита и защита персонала. Если необходимо получить наиболее эффективные и действенные результаты при выполнении своей работы, к проектированию безопасности следует привлекать эти и многие другие специальные второстепенные дисциплины. В перечне, приведенном ниже, приведено несколько примеров специальных второстепенных дисциплин, связанных с безопасностью:

- эксплуатационная безопасность, связанная с безопасностью условий эксплуатации и поддержанием этой безопасности;
- информационная безопасность, относящаяся к информации и поддержанию безопасности информации во время ее обработки;
- сетевая безопасность, включающая в себя защиту аппаратных средств, программного обеспечения и протоколов, включая передаваемую по сетям информацию;
- физическая защита, подразумевающая защиту зданий и физических местоположений;
- защита персонала, связанная с людьми, их надежностью в работе и осведомленностью о задачах безопасности;
- административная безопасность, связанная с административными аспектами безопасности и безопасности в административных системах;
- коммуникационная безопасность (безопасность содержания и трафика информации), связанная с передачей информации между доменами безопасности, в частности защитой информации при ее передаче через средство сообщения;
- защита от побочных электромагнитных излучений и наводок, связанная с помехами, создаваемыми всеми ЭВМ, которые могут передавать информацию за пределы доменов безопасности;

- компьютерная безопасность, относящаяся конкретно к безопасности вычислительных устройств всех типов.

6.2 Общее понятие о процессе проектирования безопасности

Модель SSE-CMM® разделяет проектирование безопасности на три основные части: риск, проектирование и формирование доверия (см. рисунок 1). Поскольку эти части никак не зависят друга от друга, можно рассматривать их в отдельности. На самом простом уровне процесс обнаружения рисков идентифицирует угрозы, присущие разрабатываемому продукту или системе, и определяет их приоритеты. Процесс проектирования безопасности функционирует наряду с другими инженерными дисциплинами для определения задач, инициированных угрозами и реализации их решений. Наконец, процесс формирования доверия обеспечивает уверенность в решениях задач безопасности и передает эту уверенность заказчикам.

Вместе эти три части служат достижению цели получения надлежащих результатов в процессе проектирования безопасности.

6.2.1 Риск

Основной целью проектирования безопасности является снижение риска. Оценка риска является процессом выявление проблем, которые ранее не встречались. Риски оцениваются путем изучения вероятности реализации угрозы и уязвимости и рассмотрения потенциального воздействия непредусмотренного инцидента (см. рисунок 2). С этой вероятностью связан фактор неопределенности, который изменяется в зависимости от определенной ситуации. Это значит, что вероятность появления угрозы безопасности можно предсказать только в определенных пределах. Кроме того, воздействие, оцененное для конкретного риска, также имеет связанную с ним неопределенность, поскольку непредусмотренный инцидент может оказаться не таким, как предполагалось. Так как факторы могут иметь большую степенью неопределенности, связанную с точностью их прогнозирования, планирование и обоснование обеспечения безопасности может быть сильно затруднено. Одним из путей рационального решения этой задачи является внедрение методов обнаружения непредусмотренного инцидента.

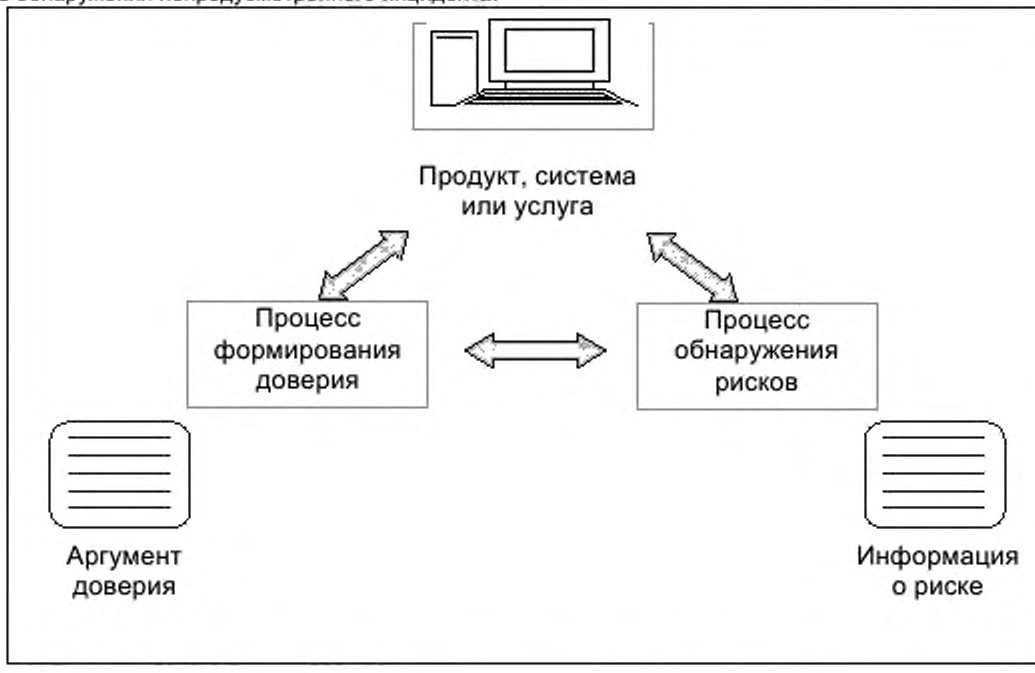

Рисунок 1 - Процесс проектирования безопасности, состоящий из трех основных частей

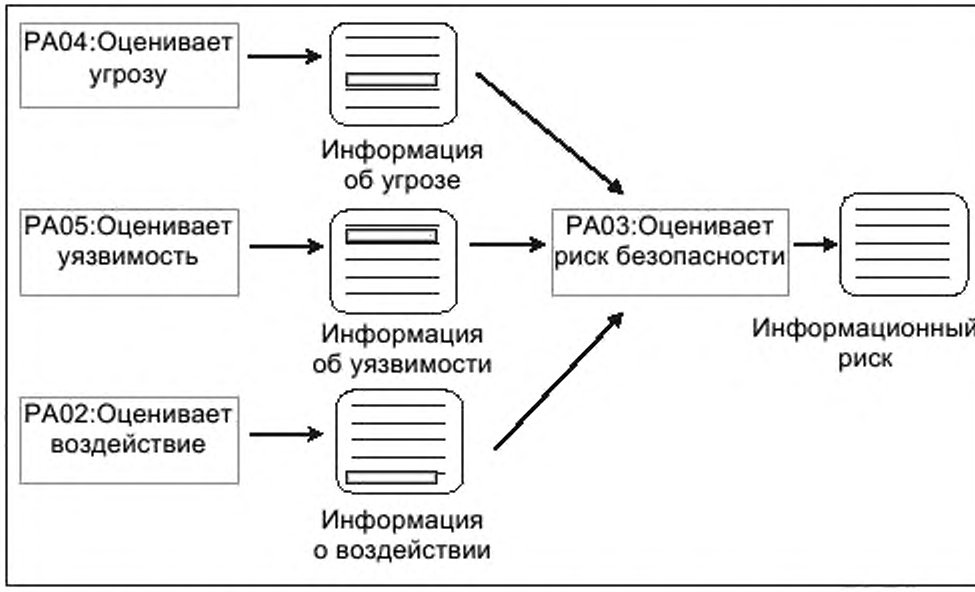

Рисунок 2 - Процесс обнаружения риска, включающего в себя угрозы, уязвимости и воздействие

Непредусмотренный инцидент состоит из трех компонентов: угрозы, уязвимости и воздействия. Уязвимостями являются свойства актива, которые имеют слабые места и могут использоваться угрозой. При отсутствии угрозы или уязвимости непредусмотренного инцидента риска не будет. Менеджментом риска являются все действия, которые надо скоординировать для управления действиями по менеджменту риска в организациях и контроля за ними. Это подразумевает установление приемлемого уровня риска для организации и, соответственно, идентификацию, анализ, оценивание и обработку риска. Управление риском является важной частью управления безопасностью.

Риски обрабатывают посредством внедрения мер безопасности, которые могут учитывать угрозу, уязвимость, воздействие и сам риск. Однако обработка всех рисков или полная нейтрализация последствий реализации какого-либо определенного риска практически неосуществимо. Большей частью это является следствием высокой стоимости обработки рисков и связанными с ней неопределенностями. Следовательно, всегда должен приниматься во внимание некоторый остаточный риск. При высокой степени неопределенности принятие риска становится крайне проблематичным вследствие неточного характера риска. Одной из немногих областей, контролируемых лицом, принявшим риск, является неопределенность, связанная с системой. Области процесса SSE-CMM® включают в себя действия организации-провайдера, обеспечивающие анализ угроз, уязвимостей, воздействий и связанного с ними риска.

Примечание - Упорядоченность областей процесса является строго алфавитном, основанной на наименованиях областей процесса. Это делается с целью предотвращения возможности сделать вывод о какой-либо последовательности или приоритетах в упорядоченности областей процесса.

6.2.2 Проектирование

Проектирование безопасности, подобно другим дисциплинам проектирования, является процессом, который осуществляется посредством использования концепции, проекта, реализации, теста, ввода в эксплуатацию, обслуживания и вывода из эксплуатации. С помощью этого процесса специалисты в области безопасности должны тесно сотрудничать с другими подразделениями группы системного проектирования. В модели SSE-CMM® особое внимание придается тому, что специалисты в области безопасности являются частью большой группы и должны координировать свои действия со специалистами по другим дисциплинам. Это помогает обеспечивать неотъемлемость процесса обеспечения безопасности от большего процесса, а не рассматривать его как отдельный и обособленный вид деятельности.

Используя информацию по вышеизложенному процессу обнаружения риска и другую информацию о требованиях системы, соответствующих законов и политик, специалисты в области безопасности вместе с заказчиком определяют потребности в мерах безопасности (см. рисунок 3). После этого они определяют конкретные требования и отслеживают их выполнение.

Процесс принятия решений по проблемам безопасности в основном включает в себя установление возможных альтернатив и их последующую оценку с целью определения, какая из них является самой многообещающей. Трудность интегрирования этой деятельности в остальной процесс проектирования заключается в том, что решения невозможно принять на основе только соображений безопасности. Необходимо также учитывать широкий набор других соображений, включая стоимость, производительность, технический риск и удобство эксплуатации. Обычно эти решения надо обобщать для минимизации необходимости повторного обращения к этим проблемам. Проводимые анализы также формируют существенную основу для работы по обеспечению доверия.

Позднее, в ходе жизненного цикла систем безопасности, специалист в области безопасности вызывается для подтверждения правильности конфигурации продукции и систем в отношении осознанных рисков, обеспечивая защиту функционирования системы от новых рисков.

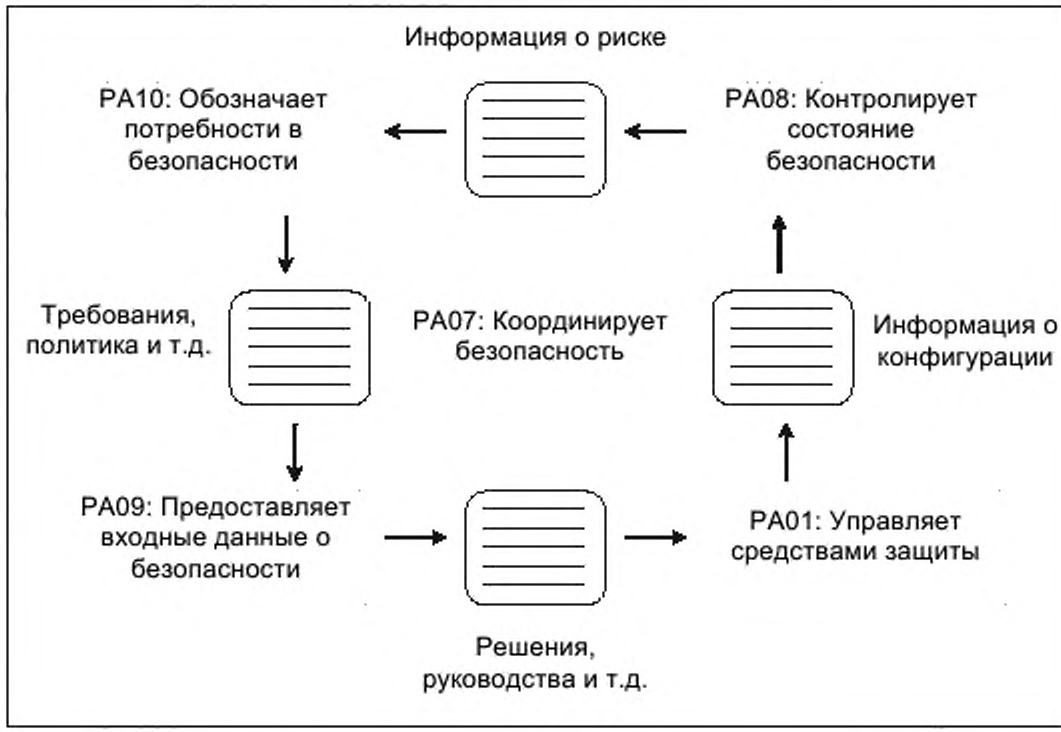

Рисунок 3 - Безопасность, являющаяся неотъемлемой частью общего процесса проектирования

6.2.3 Доверие

Доверие определяется как степень уверенности в удовлетворении требований безопасности [1]. Оно является очень важным результатом проектирования безопасности. Существует много форм доверия. Модель SSE-CMM® содействует одному аспекту, а именно уверенности в повторяемости результатов процесса проектирования безопасности. Основанием для этой уверенности является наличие большей вероятности повторения результатов зрелой организацией, чем недостаточно зрелой (см. рисунок 4). Детальная взаимосвязь между различными формами доверия является целью проводимого анализа.

Доверие не добавляет каких-либо дополнительных мер безопасности для противодействия рискам, связанным с безопасностью, но обеспечивает уверенность в том, что уже внедренные меры безопасности снизят ожидаемые риски.

Доверие можно также рассматривать как уверенность в том, что меры безопасности функционируют должным образом. Эта уверенность основана на качествах правильности и эффективности. Правильность можно рассматривать как свойство выполнения мерами безопасности требований так, как это было запланировано. Эффективность можно рассматривать как свойство обеспечения мерами безопас-

ности степени безопасности, адекватной потребностям заказчика. Интенсивность процесса также играет определенную роль, но она смягчается уровнем защиты и искомым доверием.

Доверие часто передается в виде аргумента. Аргумент включает в себя совокупность утверждений о свойствах системы. Эти утверждения поддерживаются доказательством. Доказательство часто имеет форму документации, разработанной во время стандартной деятельности по проектированию безопасности.

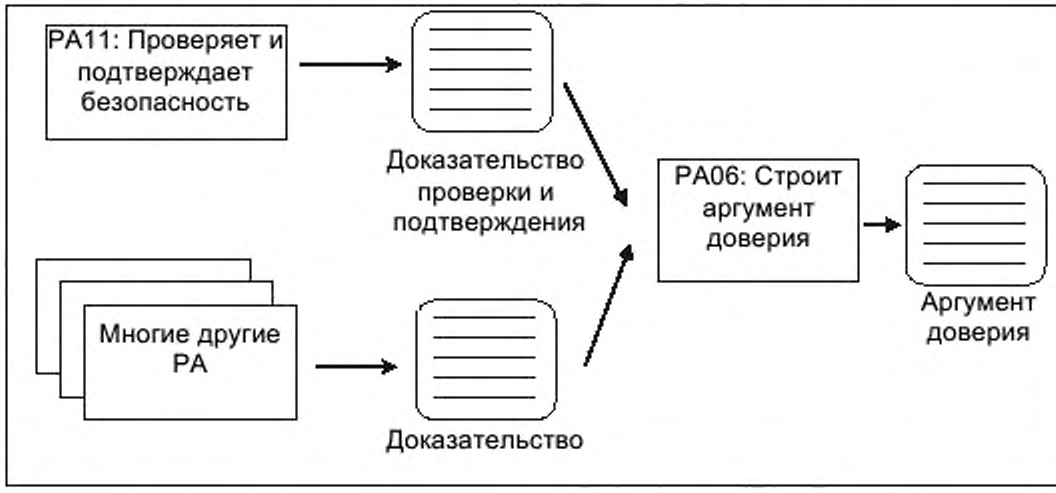

Рисунок 4 - Процесс формирования доверия, производящий аргумент, который создает уверенность

Действия модели SSE-CMM® сами по себе включают получение относящегося к доверию свидетельства. Например, документация процесса может указывать на то, что разработка последовала за четко определенным и зрелым процессом проектирования, который постоянно совершенствуется. Проверка безопасности и подтверждение достоверности играют большую роль в формировании надежности продукта или системы.

Многие образцы продуктов, включенные в рамки области процесса, оказывают содействие свидетельству или образуют его часть. Современное статистическое управление процессом предлагает возможность получения продукции с большей степенью качества и доверия более рациональным и воспроизводимым образом, сосредоточивая внимание на процессе ее производства. На процесс также оказывает влияние и содействует ему зрелость (развитость) практических приемов организации.

6.3 Описание архитектуры модели SSE-CMM®

Архитектура модели SSE-CMM® спроектирована для определения зрелости процесса проектирования безопасности организации во всем объеме проектирования безопасности. Целью создания архитектуры является четкое отделение его основных характеристик от характеристик менеджмента и институционализации. Для обеспечения этого разделения модель имеет две величины, называемые «домен» и «возможности» и описанные ниже.

Важно, что SSE-CMM® не предполагает необходимости выполнения какого-либо процесса, описанного в модели какой-нибудь определенной группой в рамках организации. Модель также не требует применения новейшего метода или методологии проектирования безопасности. Однако она требует наличия в организации процесса, включающего в себя базовые практики обеспечения безопасности, изложенные в модели. Организация может создавать собственный процесс и организационную структуру, так или иначе отвечающие их бизнес-целям.

6.3.1 Базовая модель

SSE-CMM® имеет две величины, «домен» и «возможность». Из двух величин величина «домен», возможно, более легка для понимания. Эта величина состоит из всех практических приемов, которые в

совокупности определяют проектирование безопасности. Эти практические приемы называются «базовыми практиками». Структура и содержание этих «базовых практик» обсуждаются ниже.

Величина «возможность» представляет собой практические приемы, демонстрирующие возможности менеджмента и институционализации процесса. Эти практические приемы называются «общими практиками», поскольку они применяются в широком диапазоне доменов. Общие практики представляют действия, которые должны осуществляться как часть базовых практик.

Взаимосвязь между базовыми и общими практиками показана на рисунке 5. Существенной частью проектирования безопасности является идентификация уязвимостей безопасности системы. Это действие представлено базовой практикой 05.02 «Идентификация уязвимостей безопасности системы».

Одним способом определения способности организации выполнять какие-либо действия является проверка наличия у нее процесса распределения ресурсов для действий, которые, по ее утверждению, она выполняет. Эта «характеристика» развитой (зрелой) организации отражена в общей практике 2.1.1 «Распределение ресурсов» модели SSE-CMM®.

Объединение общих и базовых практик обеспечивает способ проверки возможности организации выполнять определенную деятельность. Здесь заинтересованная сторона может задать вопрос: «ваша организация выполняет распределение ресурсов для идентификации уязвимостей безопасности системы?». Если ответом является «Да», опрашивающий узнает немного о возможностях организации.

Ответы на все вопросы, возникающие при объединении всех общих практик со всеми базовыми, дают хорошую картину возможностей проектирования безопасности.

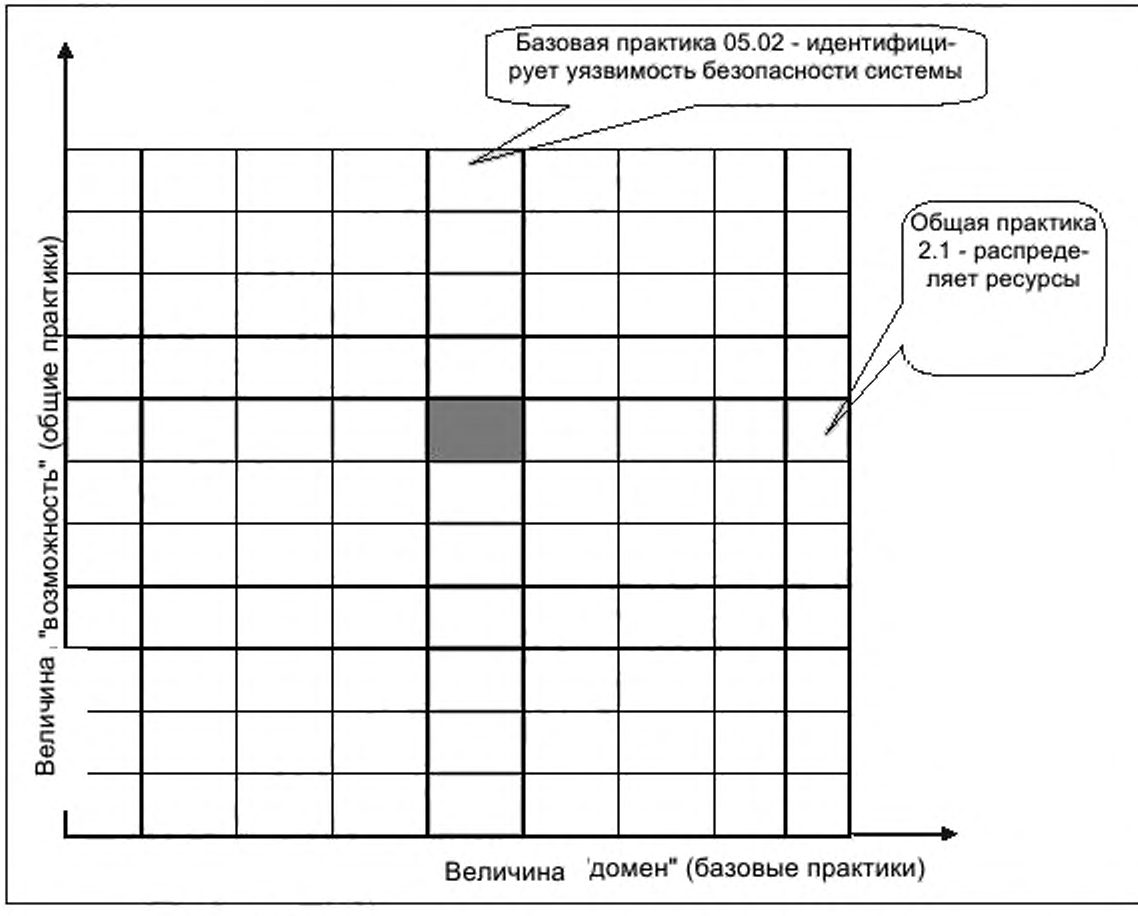

Рисунок 5 - Модель, оценивающая каждую область процесса в сопоставлении с каждым общим признаком

6.3.2 Базовые практики

Модель SSE-CMM® состоит из 129 базовых практик, организованных в 22 областях процесса. Из них 61 базовая практика, организованные в 11 областях процесса, охватывает все главные области проектирования безопасности. Остальные 68 практик, организованных в 11 областях процесса, относятся к доменам проекта и организации. Эти практики были выведены из модели зрелости функциональных возможностей модели CMM® средств программирования и системного проектирования и требуются для обеспечения условий и поддержки областей процесса проектирования безопасности систем. Общие практические приемы обеспечения безопасности были собраны из большого количества существующих материалов, результатов практической деятельности и практического опыта. Выбранные практические приемы протестированы и отражают имеющийся передовой опыт организаций, занимающихся проектированием безопасности.

Определение базовых практик проектирования безопасности осложняется наличием многих различных названий действий, которые по существу одинаковы. Некоторые из этих действий применяются позднее в жизненном цикле на разном уровне абстракции или обычно выполняются лицами на различных должностях. Однако нельзя считать, что организация получила базовую практику, если она применяется только на этапе проектирования или на одном уровне абстракции. Следовательно, модель SSE-CMM® игнорирует эти различия и определяет основной набор практических приемов, которые необходимы в деятельности по качественному проектированию безопасности.

Базовая практика:

- применяется в течение жизненного цикла предприятия;
- не накладывается на другие базовые практики;
- представляет собой «передовой опыт» по обеспечению безопасности;
- не является простым отражением самой современной технологии;
- применяется множественными методами в многочисленных, связанных с деятельностью ситуациях;
- не обозначает конкретный метод или инструмент.

Базовые практики были организованы в области процесса таким образом, чтобы они соответствали широкому спектру организаций, занимающихся проектированием безопасности. Существует много способов разделить домен проектирования безопасности на области процесса. Кто-то может попытаться смоделировать реальную обстановку, создавая области процесса, согласующиеся с услугами по проектированию безопасности. В других стратегиях делается попытка идентифицировать концептуальные зоны, образующие стандартные блоки проектирования безопасности. Модель SSE-CMM® создает компромисс между этими разными целями в текущей совокупности областей процесса.

Каждая область процесса имеет ряд целей, которые представляют собой предполагаемое состояние организации, успешно выполняющей базовые практики области процесса. Организация, выполняющая базовые практики области процесса, также должна добиваться этих целей.

Область процесса:

- объединяет родственные действия в одной части для удобства использования;
- связана с важными услугами по проектированию безопасности;
- может реализовываться во многих контекстах организаций и продуктов;
- может усовершенствоваться как отдельный процесс;
- может усовершенствоваться группой с аналогичной заинтересованностью в процессе;
- включает в себя все базовые практики, которые требуются для выполнения целей данной области процесса.

Ниже приведены одиннадцать частей процессов модели SSE-CMM® проектирования безопасности систем. Следует отметить, что они перечислены в алфавитном порядке во избежание представления о том, что области процесса упорядочены по этапам или областям жизненного цикла. Эти области процесса (PA) и определяющие их базовые практики (BP) изложены в разделе 7 и перечислены ниже:

- PA01 управляет средствами защиты;
- PA02 оценивает воздействие;
- PA03 оценивает риск безопасности;
- PA04 оценивает угрозу;
- PA05 оценивает уязвимость;
- PA06 формирует аргумент доверия;
- PA07 координирует задачи безопасности;
- PA08 проводит мониторинг состояния безопасности;
- PA09 предоставляет входные данные по безопасности;
- PA10 обозначает потребности в безопасности;

- PA11 проверяет и подтверждает состояние безопасности.

Модель SSE-CMM® также включает в себя одиннадцать областей процесса, связанных с проектными и организационными приемами. Эти области процесса были адаптированы к модели SSE-CMM®. Эти области процесса и определяющие их базовые практики изложены в приложении В и перечислены ниже:

- PA12 обеспечивает качество;
- PA13 управляет конфигурацией;
- PA14 управляет проектным риском;
- PA15 осуществляет мониторинг и управляет технической деятельностью;
- PA16 планирует техническую деятельность;
- PA17 определяет процесс системного проектирования организации;
- PA18 совершенствует процесс системного проектирования организации;
- PA19 управляет развитием производственных линий;
- PA20 управляет средой поддержки системного проектирования;
- PA21 постоянно обеспечивает практические навыки и знания;
- PA22 осуществляет сотрудничество с поставщиками.

Примечание - Изложение этих областей процесса помещено в приложение с целью способствования синхронизации с ИСО/МЭК 15288:2002 в будущем.

6.3.3 Общие практики

Общие практики представляют собой действия, применимые ко всем процессам. Эти практики связаны с процессами менеджмента, измерения и институционализации. В общем, общие практики применяются во время оценки возможностей организации осуществлять процесс.

Общие практики сгруппированы в логические области, называемые «Общие признаки», которые организованы в пять «Уровней возможностей», представляющих возрастающие функциональные возможности организации. В отличие от базовых практик величины «домен» общие практики измерения возможностей упорядочены в соответствии с их зрелостью. Следовательно, общие практики, указывающие на более высокие уровни функциональных возможностей процесса, расположены в верхней части величины «возможность».

Общие признаки предназначены для описания основных изменений в типичном способе выполнения организацией технологических процессов (в данном случае домен проектирования безопасности). Каждый общий признак имеет один или несколько практических приемов. Самым низким общим признаком является уровень «1.1 Базовые практики выполнены». Этот общий признак просто проверяет, выполняет ли организация все базовые практики в той или иной области процесса.

Следующие общие признаки имеют общие практики, помогающие определить, насколько качественно проект управляет и улучшает каждую область процесса в целом. Общие практики, изложенные в приложении А, сгруппированы для выявления основных изменений процесса выполнения проектирования безопасности. Несколько принципов применения общих практик указаны в таблице 1.

Таблица 1 - Принципы измерения возможностей

Принцип	Способ выражения в SSE-CMM®
Вам следует сделать «это» перед тем, как вы сможете управлять «этим»	Уровень «Выполненный Неформально» относится к тому, осуществляет ли организация процесс, объединяющий базовые практики
Следует знайть, что происходит с проектом (где находится продукция!) перед определением процессов в объеме организации	Уровень «Запланированный и Отслеженный» относится к задачам определения, планирования и выполнения на уровне проекта
Используйте лучшее из того, что вы узнали из ваших проектов, для создания проектов в масштабе организации	Уровень «Четко Определенный» относится к упорядоченной подгонке определенных процессов на уровне организации
Вы не сможете измерить «это», пока не узнаете, что «это» значит	Хотя важно начать сбор и использование основных мер измерения проекта заранее (то есть на уровне «Запланированный и Отслеженный»), измерение и использование данных не ожидается в масштабе организации до тех пор, пока не будут достигнуты уровни «Четко Определенный и Управляемый»
Управление с измерением значимо только тогда, когда вы измеряете правильные вещи	Уровень «Управляемый Количественно» относится к измерениям, связанным с целями деловой деятельности организации

Окончание таблицы 1

Принцип	Способ выражения в SSE-CMM®
Культура постоянного улучшения требует основания надежной практики менеджмента, определенных процессов и измеримых целей	Уровень «Постоянное улучшение» использует все улучшения практики менеджмента с предыдущих уровней, затем выделяет культурные сдвиги, которые поддержат полученные достижения

Приведенные ниже общие признаки представляют собойхарактеристики зрелого проектирования безопасности, необходимые для достижения каждого уровня. Эти общие признаки и определяющие их общие практики изложены в приложении А.

Уровень 1:

1.1Базовые практики выполнены.

Уровень 2:

2.1 Планирование выполнения.

2.2 Упорядоченное выполнение.

2.3 Проверка выполнения.

2.4 Отслеживание выполнения.

Уровень 3:

3.1 Определение стандартного процесса.

3.2 Выполнение заданного процесса.

3.3 Координация практических приемов.

Уровень 4:

4.1 Определение измеримых целей обеспечения качества.

4.2 Объективное управление выполнением.

Уровень 5:

5.1 Улучшение организационных возможностей;

5.2 Улучшение эффективности процесса.

Модель SSE-CMM® не подразумевает наличие конкретных требований по выполнению общих практик. В основном организация может по своему усмотрению планировать, отслеживать, определять свои процессы и управлять ими в любом виде и в любой последовательности. Однако, поскольку некоторые общие практики более высокого уровня зависят от общих практик более низкого уровня, организациям рекомендуется поработать с общими практиками более низкого уровня перед тем, как пытаться достичь более высоких уровней.

6.3.4 Уровни возможностей

Существует несколько путей группирования практических приемов в общие признаки, а общих признаков - в уровни возможностей. Нижеследующее обсуждение касается этих общих признаков.

Упорядочивание общих признаков исходит из того, что реализация и институционализация некоторых практических приемов выигрывают от присутствия других приемов. Это особенно справедливо, если практические приемы являются общепризнанными. До того, как организация сможет определить, адаптировать и эффективно использовать конкретный процесс, отдельные проекты должны иметь некоторый опыт управления функционированием этого процесса. Например, организация должна вначале попробовать применить процесс оценки на проекте перед институционализацией специфического процесса оценки всей организации. Однако некоторые аспекты реализации и институционализации должны рассматриваться в совокупности (не по очереди), поскольку они работают вместе в направлении усиления возможностей.

Общие признаки и уровни возможностей имеют значение как при проведении оценки, так и при усилении возможностей процесса организации. В случае оценки, когда организация имеет несколько общих признаков, реализованных на определенном уровне возможностей заданного процесса, организация обычно функционирует на самом низком уровне этого процесса. Например, организация, выполняющая все, кроме одной, общие практики Уровня 2 некоторой области процесса должна получить категорию Уровня 1. Организация не может получить все преимущества от внедрения общего признака на какой-либо данный уровень возможностей, если не были внедрены общие признаки на более низких уровнях возможностей. Группа по оценке должна учитывать это при оценке отдельных процессов организации.

В случае с улучшением возможностей объединение практических приемов в уровни возможностей обеспечивает для организации план действий по улучшению, если она захочет усилить свои возможно-

сти в отношении какого-либо конкретного процесса. По этим причинам практические приемы модели SSE-CMM® сгруппированы в общие признаки, которые упорядочены уровнями возможностей.

Каждая область процесса должна оцениваться на предмет определения ее уровней возможностей. Это указывает на то, что различные области процесса могут и возможно будут находиться на различных уровнях возможностей. Тогда организация сможет использовать эту специфическую для процесса информацию как средство его улучшения. При установлении приоритетов и последовательности действий по улучшению процессов организации необходимо учитывать свои бизнес-цели.

Бизнес-цели являются основной мотивацией интерпретации такой модели, как SSE-CMM®. Но существует основной порядок действий и основные принципы, которые приводят в действие логическую последовательность типичных действий по улучшению. Этот порядок выражен в общих признаках и общих практиках аспекта уровней возможностей архитектуры SSE-CMM®.

Модель SSE-CMM® состоит из пяти уровней, представленных на рисунке 6 и подробно изложенных в приложении А.



процесса (PA). В приведенной ниже таблице приводится соответствие уровней возможностей модели SSE-CMM® уровням по ИСО/МЭК 15504-2:2003.

Таблица 2 - Соответствие величины «возможность» структуре измерений

Величина «возможность» модели SSE-CMM®	Структура измерений ИСО/МЭК 15504-2:2003
[В SSE-CMM® не определен однозначно, а подразумевается]	Уровень 0: незавершенный процесс
Уровень возможностей 1 Выполнен неформально	Уровень 1: выполненный процесс
Общий признак 1.1 Базовые практики выполнены	РА 1.1 Характеристика выполнения процесса
Уровень возможностей 2 Запланированный и отслеженный	Уровень 2: управляемый процесс
Общий признак 2.1 Планирование выполнения Общий признак 2.4 Отслеживание выполнения	РА 2.1 Характеристика управления выполнением
Общий признак 2.2 Упорядоченное выполнение Общий признак 2.3 Проверка выполнения	РА 2.2 Характеристика управления рабочим изделием
Уровень возможностей 3 Вполне определенный	Уровень 3: установленный процесс
Общий признак 3.1 Определение стандартного процесса Общий признак 3.2 Выполнение заданного процесса	РА 3.2 Характеристика ресурса процесса

Окончание таблицы 2

Величина «возможность» модели SSE-CMM®	Структура измерений ИСО/МЭК 15504-2:2003
[Специально здесь не рассматриваются, но рассматриваются в последующих общих практиках] ОПП 2.1.1 Распределяет ресурсы ОПП 2.1.2 распределяет обязанности ОПП 2.1.5 Обеспечивает обучение	РА 3.2 Характеристика ресурса процесса
Общий признак 3.3 Координирует практические приемы	*[Прямой эквивалент отсутствует]*
Уровень возможностей 4 Количественно контролируется	Уровень 4: прогнозируемый процесс
Общий признак 4.1 Определение измеримых целей обеспечения качества	РА 4.1 Характеристика измерений
Общий признак 4.2 Объективное управление выполнением	РА 4.2 Характеристика управления процессом
Уровень возможностей 5 Постоянно улучшает	Уровень 5: оптимизация процесса
Общий признак 5.1 Улучшение возможностей организации	РА 5.2 Характеристика постоянного улучшения
Общий признак 5.2 Повышение эффективности процесса	РА 5.1 Характеристика изменения процесса

6.3.6 Взаимосвязь с ИСО/МЭК 15288:2002

В настоящем стандарте модель SSE-CMM® была разработана за рамками обычной среды ИСО/МЭК. Это означает существование отличий в использовании терминологии и построении между ИСО/МЭК 21827 и ИСО/МЭК 15288:2002. Кроме того, ИСО/МЭК 21827 нацелен на разработку другой области и дисциплины, а именно проектирования безопасности, что неизбежно ведет к появлению некоторых различий, являющихся второстепенными и упоминаемых только при необходимости. Однако основные концепции и подходы, используемые ИСО/МЭК 21827 и ИСО/МЭК 15288:2002, очень похожи.

Некоторые примеры взаимосвязи этих стандартов:

- области процесса ИСО/МЭК 21827 непосредственно связаны с процессами ИСО/МЭК 15288:2002;
- практические приемы ИСО/МЭК 21827 непосредственно связаны с действиями ИСО/МЭК 15288:2002;
- рабочие документы ИСО/МЭК 21827 имеют непосредственное отношение к результатам применения ИСО/МЭК 15288:2002;
- описания процесса ИСО/МЭК 21827 идентичны описаниям процесса ИСО/МЭК 15288:2002.

Основные взаимосвязи областей процесса ИСО/МЭК 21827 с процессами ИСО/МЭК 15288:2002 приведены в таблице 3.

Примечания

1 Строка с многочисленными «X» указывает на то, что заданный процесс ИСО/МЭК 15288:2002 перекрывается более чем одной областью процессов ИСО/МЭК 21827.

2 Столбец с многочисленными «X» указывает, что определенная область процесса ИСО/МЭК 21827 перекрывается более чем одним процессом ИСО/МЭК 15288:2002.

6.4 Итоговая схема

Данная схема представляет собой модель на высоком уровне абстракции. Специалист-практик предупреждается, что каждая область процесса состоит из нескольких базовых практик, которые подробно изложены в разделе 7 и приложении В. Каждый общий признак состоит из нескольких общих практик, которые подробно изложены в приложении В. Каждой отдельной организации предоставляется выбор комбинации областей процесса. Итоговая схема взаимосвязей областей процесса с общими признаками представлена на рисунке 7.

7 Базовые практики обеспечения безопасности

Настоящий раздел содержит практические приемы, считающиеся необходимыми при проведении основного проектирования безопасности (то есть базовые практики). При этом области процесса не пронумерованы в каком-то особом порядке, поскольку модель не предписывает какой-либо конкретный процесс или последовательность процессов.

Организацию можно оценить по любой отдельной области процесса или комбинации областей процесса. Однако вместе области процесса предназначены для охвата всех базовых практик проектирования безопасности, а между областями процессов имеется много взаимосвязей. В настоящее время модель SSE-CMM® включает в себя 11 областей процесса, связанных с безопасностью, каждая из которых содержит несколько базовых практик. Каждая область процесса определена в последующих подразделах.

Общий формат областей процесса показан на рисунке 8. В кратком описании содержится беглый обзор их назначения. Каждая область процесса разделяется на несколько базовых практик. Базовые практики считаются обязательными элементами (то есть они должны успешно реализовываться для выполнения назначения области

Таблица 3 - Взаимосвязь областей процесса ИСО/МЭК 21827 с процессами ИСО/МЭК 15288:2002

15288 Процессы	21827 Части процесса																							
Приобретение	РА01	РА02	РА03	РА04	РА05	РА06	РА07	РА08	РА09	РА10	РА11	РА12	РА13	РА14	РА15	РА16	РА17	РА18	РА19	РА20	РА21	РА22	Примечание
Поставка										X												X	
Управление средой	X																		X	X			
Управление инвестициями																							ЭО
Управление системой																	X	X					
Управление ресурсами																	X				X	X	
Планирование проекта																X							
Оценка проекта															X								
Управление проектом												X			X								
Принятие решений										X													
Менеджмент риска														X									
Управление конфигурацией													X										

Окончание таблицы 3

15288 Процессы	21827 Части процесса																							
Приобретение	РА01	РА02	РА03	РА04	РА05	РА06	РА07	РА08	РА09	РА10	РА11	РА12	РА13	РА14	РА15	РА16	РА17	РА18	РА19	РА20	РА21	РА22	Примечание
Управление информацией																							
Определение запроса акционера										X													
Анализ требований			X						X	X	X												
Проектирование архитектуры									X														
Реализация																							ЭО
Проверка интеграции											X												ЭО
Переход																							ЭО
Подтверждение											X												
Функционирование								X											X				
Обслуживание	X								X														

Удаление	X																					
Примечания		Э О		Э О	Э О																	
Условные обозначения	X - Есть взаимосвязь между частью процесса и процессом												ЭО – Эквивалент отсутствует									

	РА 01 – Управляет средствами защиты	РА 02 – Оценивает воздействие РА 03 – Оценивает риск воздействия	РА 04 – Оценка угрозы	РА 05 – Оценка уязвимости	РА 06 – Создание аргумента доверия РА 07 – Координация безопасности	РА 08 – Мониторинг состояния безопасности	РА 09 – Предоставляет входные данные по безопасности	РА 10 – Обозначает потребности безопасности РА 11 – Проверяет и подтверждает состояние безопасности	РА 12 – Обеспечивает качество	РА 13 – Управляет конфигурациями РА 14 Управляет рисками проекта	РА 15 – Контролирует техническую деятельность и управляет	РА 16 – Активирует техническую деятельность	РА 17 – Определяет процесс проектирования безопасности РА 18 – Улучшает процесс проектирования безопасности организации	РА 19 – Управляет средой производственной линии	РА 20 – Управляет средой поддержки проектирования систем и знания	РА 21 – Обеспечивает требуемые навык	РА 22 – Координирует деятельность с поставщиками
5.2 Повышение эффективности процесса																	
5.1 Повышение возможностей организации																	
4.2 Объективное управление выполнением																	
4.1 Определение измеряемых целей обеспечения качества																	
3.3 Координация практических приемов																	
3.2 Выполнение заданных процессов																	
3.1 Определение стандартного процесса																	
2.4 Отслеживание выполнения																	
2.3 Проверка выполнения																	
2.2 Упорядоченное выполнение																	
2.1 Запланированное выполнение																	
Общие признаки	**Области процесса проектирования безопасности**								**Области процесса проекта и организации**								

Рисунок 7 – Итоговая схема взаимосвязей областей процесса с общими признаками

процесса, который они поддерживают). Каждая базовая практика подробно описана в соответствии с кратким изложением области процесса. Цели определяют желательный конечный результат реализации области процесса.

7.1 PA01 - Управляет мерами безопасности

7.1.1 Область процесса

7.1.1.1 Краткое описание

Назначением области процесса «Управление мерами безопасности» является обеспечение того, что заданный уровень безопасности, интегрированный в проект системы, фактически достигнут разработанной в результате системой, находящейся в рабочем состоянии.

PA01 – Название области процесса (в форме глагол — существительное). Краткое описание - Краткий обзор области процесса. Цели – Перечень желательных результатов реализации этой области процесса. Перечень базовых практик – Перечень с номером и названием каждой базовой практики. Примечания к области процесса – Все другие примечания к данной области процесса BP.01.01 Название базовой практики (в форме глагол-существительное). Описательное имя – Предложение, описывающее базовую практику. Описание – Общее представление о данном практическом приеме. Примеры результатов деятельности – Перечень примеров предполагаемого выпуска продукции. Примечание – Все другие замечания о данной базовой практике – см. BP.01 02...

Рисунок 8 – Формат области процесса

7.1.1.2 Цели:

- правильные конфигурация и использование мер безопасности.

7.1.1.3 Перечень базовых практик

BP.01.01 — Определяет обязанности и подотчетность по мерам безопасности и обеспечивает информирование о них каждого сотрудника организации.

BP 01.02 — Управляет конфигурацией мер безопасности системы.

BP.01.03 — Управляет программами обеспечения осведомленности, подготовки и обучения для всех пользователей и администраторов.

BP.01.04 — Управляет периодическим обслуживанием и администрированием служб безопасности и механизмов контроля.

7.1.1.4 Примечания к данной области процесса

В данной области процесса применяются действия, требуемые для управления и обслуживания механизмов контроля безопасности среды проектирования и автоматизированной системы. Далее эта область процесса способствует тому, чтобы уровень безопасности со временем не понизился. Управление мерами безопасности какого-либо нового устройства должно интегрироваться с уже имеющимися мерами безопасности.

7.1.2 Базовая практика 01.01 (BP.01.01) – Определяет обязанности в области безопасности

Данная базовая практика определяет обязанности и подотчетность для мер безопасности и информирует о них каждого сотрудника организации.

7.1.2.1 Описание

Некоторые аспекты безопасности могут управляться в рамках обычной структуры менеджмента, в то время как для других требуется более специализированный менеджмент.

Процедуры должны обеспечивать подотчетность лиц с возложенными на них обязанностями и их полномочия на проведение каких-либо действий. Необходимо также обеспечить, чтобы любые принятые меры безопасности были понятны и применялись последовательно. Кроме того, они должны обеспечивать передачу информации о любой принятой структуре не только лицам в рамках самой структуры, но и всей организации.

7.1.2.2 Примеры результатов деятельности:

- схема структуры безопасности организации – определяет сотрудников организации, связанных с безопасностью, и их должность;

- документация с описанием функций, связанных с обеспечением безопасности – описывает каждую из должностей в организации, связанных с безопасностью, и связанные с ней обязанности;

- документация с описанием обязанностей по безопасности – подробно описывает каждую из обязанностей по безопасности, включая ожидаемые выходные данные и способ их анализа и использования;

- документация с подробным описанием подотчетности по безопасности – определяет лицо, подотчетное за связанные с безопасностью вопросы, гарантируя его ответственность за все риски;

- документация с подробным описанием полномочий в области безопасности – определяет, что разрешено делать каждому сотруднику организации.

7.1.2.3 Примечания

Некоторые организации создают рабочую группу по проектированию безопасности, ответственную за решение связанных с ней вопросов. Другие организации определяют руководителя рабочей группы, ответственного за обеспечение достижения целей, связанных с безопасностью.

7.1.3 BP.01.02 - Управляет конфигурацией безопасности

Управляет конфигурацией средств обеспечения безопасности системы.

7.1.3.1 Описание

Конфигурация всех технических средств, связанных с обеспечением безопасности, нуждается в управлении. Эта базовая практика признает, что безопасность системы в огромной степени зависит от многих взаимосвязанных компонентов (аппаратных средств, программного обеспечения и процедур) и что обычные практические приемы управления конфигурацией не могут охватить взаимосвязанные зависимости, необходимые для обеспечения безопасности систем.

7.1.3.2 Примеры результатов деятельности:

- записи обо всех обновлениях программного обеспечения – отслеживают лицензии, серийные номера и информацию по всему программному обеспечению и обновлениях программного обеспечения системы, включая дату обновления, ответственное лицо и описание изменения;

- записи обо всех задачах распределения – содержат описание любой проблемы, встретившейся во время распределения программного обеспечения, и способ ее решения;

- конфигурация безопасности системы – база данных, описывающая текущее состояние аппаратного и программного обеспечения и средств связи системы, включая их местоположение, назначенных для работы с ними лиц и связанную с ними информацию;

- изменения конфигурации безопасности системы – база данных, описывающая все изменения конфигурации безопасности системы, включая имя лица, внесшего изменение, описание изменения, причину изменения и время внесения изменения;

- - периодическое документирование распространения программного обеспечения, гарантирующего отсутствия скрытых модулей с неизвестными функциями, – приводят описание последнюю деятельность по распределению выверенного программного обеспечения, отмечая любые встреченные трудности и все элементы деятельности;

- изменения в требованиях, связанные с безопасностью, – отслеживает любые изменения в требованиях к системе, внесенные по причинам, связанным с безопасностью, или влияющим на безопасность, чтобы убедиться в преднамеренности этих изменений и их воздействий;

- изменения в проектной документации, связанные с безопасностью, - отслеживает любые изменения в проектировании системы, внесенные по причинам, связанным с безопасностью или влияющим на безопасность, чтобы убедиться в преднамеренности этих изменений и их воздействий;

- внедрение средств обеспечения безопасности – описывает внедрение средств обеспечения безопасности в систему, включая детали конфигурации внедрения;

- анализ безопасности – описывает текущее состояние средств обеспечения безопасности системы относительно намеченного внедрения контроля,

- удаление контроля – описывает процедуру удаления или блокирования средств защиты, включая планы перехода.

7.1.3.3 Примечания

Данная базовая практика включает в себя создание при необходимости конфигураций средств обеспечения безопасности. Однако фактическая задача по выбору конфигурации средства обеспечения безопасности, по-видимому, должна выполняться при внедрении этого средства. Сохранение приемлемой конфигурации средств обеспечения безопасности в любой системе является сложной задачей, особенно в большой распределенной системе. Некоторые аспекты самой конфигурации имеют жизненно важное значение для поддержания безопасности. Эффективная безопасность требует регистрации определенной информации, связанной с механизмами управления безопасностью, которые являются частью системы и обычно не используются другими дисциплинами. Аналогично, предлагаемые изменения в существующей системе должны подвергаться оценке с целью определения их воздействия на общее состояние безопасности системы.

Требуются процедуры обеспечения идентичности всех копий определенного модуля программного обеспечения или приложения и того, что они являются соответствующей версией, особенно в распределенной среде. Кроме того, особенно в случае распределения программного обеспечения по всей сети, важно убедиться в том, что программное обеспечение не было нарушено во время распределения. Эти требования применяются ко всему программному обеспечению.

Данная базовая практика должна обеспечивать выполнение программным обеспечением только намеченных функций, сохранение эталонной версии программного обеспечения; идентичность всех копий программного обеспечения, подтверждение обновлений, известность и сохранение конфигурации средств обеспечения безопасности.

7.1.4 BP.01.03 - Управляет программами по обеспечению осведомленности, подготовке и обучению

Управляет программами по обеспечению осведомленности, подготовке и обучению всех пользователей.

7.1.4.2 Описание

Осведомленность, подготовка и обучение в области безопасности всего персонала нуждается в управлении так же, как осведомленность, подготовка и обучение в других областях.

7.1.4.2 Примеры результатов деятельности:

- анализ пользователем учебного материала в области безопасности - описывает эффективность, применимость и важность осведомленности и учебного материала в области обеспечения безопасности;
- журналы регистрации проведения подготовки, обучения и повышения квалификации и их результатов – отслеживает обеспечение осведомленности пользователя в области безопасности организации и системы;
- периодические повторные оценки уровня знаний, компетентности и подготовки пользователей в отношении безопасности – анализирует осознание сотрудниками организации задач безопасности и определяет возможные области, на которых следует сосредоточиться в будущем;
- каталоги учебных и образовательных материалов – набор учебных материалов в области безопасности, который может использоваться повторно во всей организации. Может быть объединен с другими учебными материалами организации.

7.1.4.3 Примечания

В данном контексте термин «пользователи» применяется в отношении не только тех лиц, которые непосредственно работают с системой, но и всех лиц, прямо или косвенно получающих информацию от системы, плюс все руководство.

Крайне важно, чтобы пользователи знали цели и задачи обеспечения безопасности и определенного механизма или средства обеспечения безопасности. Кроме того, важно, чтобы пользователи знали, как правильно пользоваться тем или иным механизмом или средством обеспечения безопасности. Таким образом, для пользователей требуется начальная подготовка и периодическая переподготовка в случае внедрения новых механизмов и средств обеспечения безопасности. От всех пользователей требуется осведомленность о безопасности, для обеспечения которой необходимо обучение по использованию механизмов обеспечения безопасности, а для небольшого количества пользователей требуются более глубокие знания в области безопасности и таким образом, эти пользователи являются кандидатами на получение образования в этой области.

7.1.5 BP.0104 - Управляет услугами по обеспечению безопасности и механизмами управления

Осуществляет периодическое обслуживание и администрирование услуг по обеспечению безопасности и механизмов управления.

7.1.5.1 Описание

Общее управление услугами по обеспечению безопасности и механизмами обеспечения безопасности идентично управлению другими услугами и механизмами. Оно включает в себя защиту услуг и механизмов от повреждений, случайных или преднамеренных, в соответствии с юридическими требованиями и требованиям политики.

7.1.5.2 Примеры результатов деятельности:

- журналы учета состояния оборудования и административные журналы – фиксирование обслуживания, проверок целостности и регламентных проверок, выполненных на механизмах защиты системы;

- периодический анализ с целью обслуживания и административные осмотры – содержит анализ последних действий по администрированию и обслуживанию системы безопасности;

- неисправности, внесенные в процессе администрирования и обслуживания – отслеживает проблемы администрирования и обслуживания с целью определения мест, где требуются дополнительные усилия;

- исключения из администрирования и обслуживания – содержит описания исключений, сделанных в процедурах администрирования и обслуживания, включая основание для исключения и его срок действия;

- перечень информации ограниченного доступа – приводит различные типы информации в системе и способ ее защиты;

- перечень носителей ограниченного доступа – описывает различные типы носителей, используемых для хранения информации, и способ защиты каждого из них;

- удаление секретной информации, перевод в более низкую категорию секретности и ликвидация – описывает процедуры предупреждения появления ненужных рисков в случае понижения степени секретности информации, при удалении секретной информации с носителей или их ликвидации.

7.1.5.3 Примечания

Примерами этих услуг являются идентификация и аутентификация (И/А); посредничество при осуществлении доступа и управление доступом; распределение ключей.

Каждая услуга по обеспечению безопасности должна включать в себя установление соответствующих параметров безопасности, их соблюдение, мониторинг и анализ соблюдения, а также корректировку параметров.

Эти требования особенно применимы к таким услугам по обеспечению безопасности, как идентификация и аутентификация, для поддержания пользователей и данных аутентификации и управления доступом для поддержания прав доступа.

Программное обеспечение и данные, принадлежащие организации, определены как информационные активы, представляющие подгруппу активов. Для некоторых активов требуется удаление их частей ограниченного доступа для обеспечения возможности использования остальной части активов в менее секретных целях. Удаление секретной информации обеспечивает выдачу информации лицам по принципу обеспечения необходимого знания. Этого можно достичь посредством понижения категории секретности информации или выборочного удаления специальной информации ограниченного доступа.

Электронные носители могут сохранять остаточные следы информации даже после наложения на нее другой информации. Может потребоваться удаление секретной информации с некоторых носителей перед использованием их для менее секретных целей. После завершения полезного времени жизни носителя его можно ликвидировать способом, наиболее соответствующим степени секретности остаточной информации, которая может обуславливать необходимость ликвидации этого носителя. Некоторые организации не разрешают использовать носители повторно для менее секретной информации. Специфические детали требований удаления, перевода на более низкую категорию и ликвидации секретной информации зависят от конкретной организации и применяемых ею инструкций.

7.2 PA02 – Оценивает воздействия

7.2.1 Область процесса

7.2.1.1 Краткое описание

Назначением области является идентификация воздействий, вызывающих опасения по отношению к системе, и оценки вероятности возникновения воздействий. Воздействия могут быть материальными, например, такими как потеря доходов или финансовые санкции, и нематериальными, такими как потеря репутации и доброго имени.

7.2.1.2 Цели:

- определение и характеризация воздействия рисков на безопасность системы.

7.2.1.3 Перечень базовых практик

BP.02.01 Определение, анализ и назначение приоритетов функциональных и деловых возможностей или возможностей выполнения целевых задач, используемых системой.

BP.02.02 Определение и составление спецификации активов системы, поддерживающих ключевые функциональные возможности или цели безопасности системы.

BP.02.03 Выбор показателя воздействия, используемого для этой оценки.

BP.02.04 При необходимости определения взаимосвязи между выбранной системой мер этой оценки и коэффициентами преобразования показателей.

BP.02.05 Определение и снятие характеристик воздействий.

BP.02.06 Мониторинг текущих изменений в воздействиях.

7.2.1.4 Примечания к области процесса

Воздействие является результатом (следствием) нежелательного инцидента, созданного намеренно или случайно и оказывающего негативное влияние на активы. Последствиями могут быть уничтожение определенных аспектов, нанесение ущерба системам ИТ и потеря конфиденциальности, целостности, доступности, подотчетности, аутентичности или надежности. Возможные косвенные последствия включают в себя финансовые убытки и потерю доли рынка или имиджа компании. Измерение воздействий позволяет установить соответствие между результатами нежелательного инцидента и стоимостью мер безопасности для защиты от него. Следует принимать во внимание частоту возникновения нежелательных инцидентов. Это имеет особое значение, когда объем ущерба, наносимого при каждом возникновении инцидента, невелик, но совокупное воздействие многочисленных инцидентов может привести к нанесению значительного ущерба. Оценка результатов воздействий является важным элементом оценки рисков и выбора мер безопасности.

Информация о воздействиях, получаемая в этой области процесса, предназначена для использования базовой практики PA03 наряду с информацией об угрозах от PA04 и информацией об уязвимостях от PA05. Несмотря на то, что действия по сбору информации об угрозах, уязвимостях и воздействиях были объединены в отдельные области процесса, они являются взаимозависимыми. Целью сбора информации о воздействиях является обнаружение комбинаций угрозы, уязвимости и воздействия, которые считаются достаточно рискованными для обоснования применения определенного действия. Следовательно, поиск воздействий должен в определенной степени определяться наличием соответствующих угроз и уязвимостей.

7.2.2 BP.02.01 - Назначает приоритеты функциональным возможностям

Определение, анализ и назначение приоритетов функциональных и деловых возможностей или возможностей выполнения целевых задач, используемых системой.

7.2.2.1 Описание

Определение, анализ и назначение приоритетов руководящих указаний по эксплуатации, деловой деятельности или выполнению целевых задач. Следует принимать во внимание стратегии бизнеса, которые влияют на воздействия, которым может подвергаться организация, и смягчают их. Это в свою очередь может повлиять на последовательность рассмотрения рисков при других практических приемах и в других частях процесса. Следовательно, необходимо учитывать эти влияния при изучении потенциальных воздействий. Эта практика связана с действиями PA10.

7.2.2.2 Примеры результатов деятельности:

- указатели приоритетов системы и модификаторы воздействий
- краткая характеристика возможностей системы - описывает функциональные возможности системы и их значимость для выполнения назначения системы.

7.2.2.3 Примечания

Функциональные и информационные активы могут интерпретироваться по их ценности и критичности в определенной среде. Ценностью могут быть: функциональная значимость, засекречивание, уровень конфиденциальности и другие средства обозначения воспринимаемой ценности актива для намеченного функционирования и использования системы. Критичность может интерпретироваться как воздействие на функционирование системы, человеческую жизнь, эксплуатационные расходы и другие критические факторы, когда используемая функция компрометируется, модифицируется или недоступна в условиях эксплуатации. Ценность актива может быть также определена относительно его требованиям безопасности. Например, ценность может быть определена как конфиденциальность списка клиентов, доступность межофисной связи или целостность информации о списочном составе. Многие активы являются нематериальными или неявными в противоположность явным. Выбранный метод оценки рисков должен учитывать то, как определяется ценность функциональных возможностей и активов, и назначаются их приоритеты.

7.2.3 BP.02.02 - Идентифицирует активы системы

Идентификация и характеристика активов системы, которые поддерживают ключевые функциональные возможности или цели обеспечения безопасности системы.

7.2.3.1 Описание

Идентифицирует ресурсы системы и данные, необходимые для поддержки целей обеспечения безопасности или ключевых возможностей (функциональные, деловые функции или функции по выпол-

нению целевых задач) системы. Определяет каждый из этих активов путем оценки его значимости при предоставлении такой поддержки в рамках установленной среды.

7.2.3.2 Примеры результатов деятельности:

- анализ произведенных активов – содержит идентификацию произведенных активов и их значимости для функционирования системы;
- анализ активов системы - содержит идентификацию активов системы и их значимости для функционирования системы.

7.2.3.3 Примечания

Активы толкуются расширительно для включения в систему людей, среду, технические средства и инфраструктуру. Активы также включают в себя данные и ресурсы. Под этим подразумевается не только информация, но также системы (например, связь, поиск данных, приложения и печатные ресурсы). Важность этих активов можно определить как их значимость для ценности и критичности возможностей, которые они поддерживают в определенной среде. В некоторых случаях этой практикой является анализ работы областей процесса от PA09 и PA11.

7.2.4 BP.02.03 - Выбирает способы измерения воздействия

Выбор способов меры измерения при оценке степени воздействия.

7.2.4.1 Описание

Для определения степени воздействия можно использовать различные способы измерения. Полезно заранее определять способы измерения для использования в конкретной рассматриваемой системе.

7.2.4.2 Примеры результатов деятельности:

- выбранные способы измерения степени воздействия.

7.2.4.3 Примечания

Ограниченный набор согласованных способов измерения минимизирует трудности работы с расходящимися измерениями. Количественные и качественные измерения степени воздействия можно осуществлять различными способами, такими как:

- определение финансовых расходов;
- установление эмпирической шкалы строгости (например, от 1 до 10);
- использование прилагательных из стандартного списка (например, низкая, средняя, высокая).

7.2.5 BP.02.04 – Определяет взаимодействия способов измерения

При необходимости определяет взаимосвязь между способами измерения, выбранными для этой оценки, и коэффициентами преобразования способов измерения.

7.2.5.1 Описание

Некоторые воздействия требуют оценки посредством различных измерений. Для обеспечения согласованного подхода ко всем случаям подвергания воздействию во время его оценки необходимо установить взаимосвязь между различными измерениями. «Подвергание» считается комбинация угрозы, уязвимости и воздействия, которая может причинить значительный вред. В некоторых случаях измерения необходимо объединить для получения единого обобщенного результата. Следовательно, надо установить подход к требованиям обобщения. При использовании качественных измерений следует также установить правила руководства комбинацией качественных факторов на этапе объединения.

7.2.5.2 Примеры результатов деятельности:

- перечни взаимодействий измерений воздействий – описывают взаимосвязи между измерениями;
- правила объединения измерений воздействий – описывают правила объединения измерений воздействий.

7.2.5.3 Примечания

В качестве примера может служить воздействие метеора, разрушившего здание, где одним потенциальным воздействием могут быть расходы на восстановление здания - 100000 долларов. Другим воздействием может быть лишение крова до восстановления здания - шесть месяцев. Эти два воздействия можно объединить, если установлена стоимость предоставления приюта в месяц - 250 долларов в месяц. Тогда общее воздействие в этом случае будет оценено в 101500 долларов.

7.2.6 BP.02.05 – Определяет и характеризует воздействия

Определение и характеристика воздействия нежелательных инцидентов посредством или нескольких измерений, или объединенного измерения по выбору.

7.2.6.1 Описание

Начав с активов и возможностей, идентифицированных в BP.02.01 и BP.02.02, определяет наносящие ущерб последствия. Для каждого актива они могут включать в себя несанкционированное раскрытие, модификацию, потерю и/или уничтожение. Воздействия на возможности могут включать в себя прерывание, задержку или понижение устойчивости к внешним факторам.

После создания относительно полного перечня воздействий их можно характеризовать с помощью измерений, определенных в BP.02.03 и BP.02.04. Для этого шага может потребоваться изучение актуарных таблиц, сборников и других источников. Для каждого актива следует учитывать связанную с ним неопределенность измерений.

7.2.6.2 Примеры результатов деятельности:

- перечни подверганий воздействиям – перечень потенциальных воздействий и соответствующих им измерений.

7.2.6.3 Примечания

Оценку воздействий проводят на основе их измерений, определенных в BP.02.03, а воздействия объединены на основе правил, установленных в BP.02.04. В большинстве случаев существует некая неопределенность, связанная с измерениями, и вероятность появления специфического воздействия на них в определенной среде. В целом, полезнее держать факторы неопределенности отдельно, чтобы в случае принятия мер по уточнению рабочих данных можно было увидеть, уточняются ли сами данные или связанная с ними неопределенность.

7.2.7 BP.02.06 – Осуществляет мониторинг воздействий

Осуществление мониторинга текущих изменений в воздействиях.

7.2.7.1 Описание

Воздействия на любую позицию или ситуацию имеют динамичный характер. Новые воздействия могут стать действующими, а характеристики существующих воздействий могут измениться. Следовательно, важно постоянно контролировать как новые, так и уже существующие воздействия и регулярно корректировать возможность появления новых воздействий. Эта базовая практика тесно связана с обобщенной деятельностью по мониторингу в BP.08.02.

7.2.7.2 Примеры результатов деятельности:

- отчеты по мониторингу воздействий – описывают результаты мониторинга воздействий;
- отчеты об изменениях в воздействиях – описывают изменения в воздействиях.

7.2.7.3 Примечания

Из-за возможности изменения в воздействиях деятельность по оценке воздействий должна быть повторяющейся и проводиться несколько раз для различных условий. Однако повторение оценки воздействий не должно подменять мониторинг воздействий.

7.3 PA03 – Оценивает риск безопасности

7.3.1 Область процесса

7.3.1.1 Краткое описание

Назначением области процесса по оценке риска безопасности является идентификация, анализ и оценивание рисков безопасности системы в определенных условиях (среде). Данная область процесса сосредоточена на выявлении этих рисков, основанном на общепринятом знании того, каким образом возможности и активы уязвимы для угроз. Конкретно эта деятельность включает в себя определение и оценку вероятности появления подверганий. Данный комплекс действий выполняется в любое время в ходе жизненного цикла системы для поддержки решений, связанных с разработкой, обслуживанием и эксплуатацией системы в известной среде.

7.3.1.2 Цели:

- достижение понимания риска безопасности, связанного с эксплуатацией системы в определенной среде;
- назначение приоритетов рискам в соответствии с установленной методологией.

7.3.1.3 Перечень базовых практик

BP.03.01 Выбор методов, технологии и критериев, по которым идентифицируются, анализируются, оцениваются и сравниваются риски безопасности для системы в определенной среде.

BP.03.02 Идентификация угроз/уязвимостей/подвергания воздействиям.

BP.03.03 Оценка рисков, связанных с возникновением факта незащищенности

BP.03.04 Оценка общей неопределенности, связанной с риском незащищенности.

BP.03.05 Упорядочивание рисков по приоритетам.

BP.03.06 Постоянный контроль текущих изменений в диапазоне рисков и изменений их характеристик.

7.3.1.4 Примечания к области процесса

Риском безопасности является вероятность реализации воздействия нежелательного инцидента. Будучи связанным с проектными рисками, касающимися расходов и графика, риск безопасности имеет дело конкретно с защитой активов и возможностей системы от воздействий.

Оценивание риска всегда включает в себя фактор неопределенности, который изменяется в зависимости от конкретной ситуации. Это означает, что вероятность можно предсказать только в определенных пределах. Кроме того, воздействие, оцененное для определенного риска, также имеет некую неопределенность, поскольку нежелательный инцидент может оказаться ожидаемым. Таким образом, большинство факторов имеют неопределенность в отношении точности связанных с ними прогнозов. Во многих случаях эти неопределенности могут быть значительными. Это в огромной мере затрудняет планирование и обеспечение безопасности.

Все, что может уменьшить связанную с конкретной ситуацией неопределенность, очень важно. Поэтому так важно доверие, которое косвенно снижает риски системы.

Информация о риске, предоставляемая этой областью процессов, зависит от информации об угрозе от PA04, информации об уязвимости от PA05 и информации о воздействии от PA02. Несмотря на то, что действия по сбору информации об угрозах, уязвимостях и воздействиях были сгруппированы в различных частях процесса, они взаимосвязаны. Цель заключается в нахождении комбинаций угрозы, уязвимости и воздействия, которые считаются достаточно рискованными для обоснования принятия мер. Информация о риске формирует основу определения потребности в безопасности в PA10 и входных данных по безопасности, предоставляемых PA09.

Поскольку условия риска подвержены изменениям, они должны периодически контролироваться с тем , чтобы убедиться в поддержании постоянной осведомленности о риске, создаваемом этой областью процессов.

7.3.2 BP.03.01 – Выбирает метод анализа риска

Выбор методов, технологий и критериев, по которым идентифицируют, анализируют, оценивают и сравнивают риски безопасности для системы в определенной среде и назначают их приоритеты.

7.3.2.1 Описание

Данная практика определяет метод идентификации рисков безопасности для системы в определенной среде способом, который позволяет анализировать, оценивать и сравнивать их. Эта практика должна включать в себя схему категорирования и назначения приоритетов рискам на основе существующих угроз, эксплуатационных функций, установленных уязвимостей системы, потенциальных потерь, требований безопасности или задачных областей процесса.

7.3.2.2 Примеры результатов деятельности:

- метод идентификации риска описывает подход к идентификации риска;
- метод оценки риска описывает подход к анализу и оцениванию рисков;
- форматы оценки риска - описывает формат документирования и отслеживания рисков, включающего их описание, значимость и зависимости.

7.3.2.3 Примечания

Можно использовать уже существующий метод, адаптированный метод или метод, специфический для функциональных аспектов и определенной среды системы. Методология, применяемая для оценки риска, должна согласовываться с методологиями, выбранными для оценки угроз, уязвимостей и воздействий.

7.3.3 BP.03.02 – Идентифицирует подвергания

Идентификация трех факторов подвергания: угрозам/уязвимостям/воздействиям.

7.3.3.1 Описание

Целью выявления незащищенности является распознавание того, какая из угроз и уязвимостей вызывает опасение, и определение воздействия появления угрозы и уязвимости. Эту незащищенность следует учитывать при выборе мер безопасности для защиты системы.

7.3.3.2 Примеры результатов деятельности:

- перечни видов незащищенности системы – описывает незащищенность системы.

7.3.3.3 Примечания

Эта базовая практика зависит от выходных данных об угрозах, уязвимостях и областей процесса, связанного с рисками.

7.3.4 BP.03.03 – Оценивает риск подвергания

Оценка рисков, связанных с каждым подверганием.

7.3.4.1 Описание

Определяет последствия и вероятность появления каждого подвергания, объединяет эти значения для получения оценки риска и оценивает риск в сопоставлении с заранее определенными критериями.

7.3.4.2 Примеры результатов деятельности:

- перечень рисков подвергания – перечень расчетных рисков.

7.3.4.3 Примечание

Вероятность подвергания является комбинацией вероятности угрозы и вероятности уязвимости. Во многих случаях необходимо также учитывать вероятность определенной или обобщенной величины или силы воздействия. Во всех случаях будет присутствовать связанная с измерениями неопределенность. Полезнее хранить факторы неопределенности раздельно, чтобы в случае принятия мер по уточнению рабочих данных можно было увидеть, уточнятся ли сами данные или связанная с ними неопределенность. Это часто может воздействовать на стратегии, принятые для рассмотрения рисков. Эта базовая практика использует данные о вероятности, собранные в BP.04.05, BP.05.03 и BP.02.05, для оценки воздействия реализации подвергания или с помощью множественных или обобщенных измерений по выбору.

7.3.5 BP.03.04 – Оценивает общую неопределенность

Оценивание общей неопределенности, связанной с подверженностью рискам.

7.3.5.1 Описание

Каждый риск обладает неопределенностью. Общая неопределенность риска является накоплением неопределенностей, идентифицированных для угроз, уязвимостей и воздействий и их характеристик в BP.04.05. BP.05.03 и BP.02.05. Эта базовая практика тесно связана с действиями PA06, поскольку доверие может использоваться для изменения неопределенности и в некоторых случаях уменьшать ее.

7.3.5.2 Примеры результатов деятельности:

- подверженность риску с соответствующей неопределенностью – перечень рисков, демонстрирующий меру риска наряду с мерой неопределенности.

7.3.5.3 Примечания

Если неопределенность не сохраняется отдельно от вероятности появления подвергания, то применение мер безопасности может не принести ожидаемых результатов или привести к смягчению последствий реализации риска, когда фактически в этом нет необходимости.

7.3.6 BP.03.05 – Назначает приоритеты рискам

Упорядочивает риски посредством назначения приоритетов.

7.3.6.1 Описание

Идентифицированные риски следует упорядочивать на основе приоритетов организации, вероятности их появления, неопределенности, связанной с ними, и имеющихся денежных средств. Можно также использовать их комбинации. Риск может снижаться, передаваться, приниматься или его можно избегать. Снижение может касаться угрозы, уязвимости и воздействия или самого риска. Действия должны выбираться с учетом потребностей заинтересованных сторон, как показано в PA10, приоритетов деловой деятельности и общей архитектуры системы.

7.3.6.2 Примеры результатов деятельности:

- перечень приоритетов рисков – перечень, назначающий приоритеты рискам;
- перечень требований к мерам безопасности – перечни возможных мер безопасности, которые могут смягчить риски;
- обоснование назначения приоритетов – описание схемы назначения приоритетов.

7.3.6.3 Примечания

Этот этап может быть очень сложным и часто требует многократного повтора. Меры безопасности могут относиться к многократным рискам или многократным угрозам, уязвимостям и воздействиям. Этот аспект может изменять эффективное упорядочение рассматриваемых рисков. Следовательно, эта область процесса тесно связана с PA10 и PA09.

7.3.7 BP.03.06 – Осуществляет мониторинг рисков и их характеристик

Осуществление мониторинга изменений в диапазоне рисков и их характеристиках.

7.3.7.1 Описание

Диапазон рисков, применимый к любой позиции и ситуации, имеет динамичный характер. Новые риски могут стать действующими, а характеристики существующих рисков могут измениться. Следовательно, важно осуществлять мониторинг как существующих рисков, так и их характеристик, а также проверять новые риски на постоянной основе. Эта базовая практика тесно связана с обобщенной деятельностью по мониторингу в BP.08.02.

7.3.7.2 Примеры результатов деятельности:

- отчеты о мониторинге рисков – отчеты, описывающие диапазон действующих рисков;
- отчеты об изменениях рисков – описывают функциональные возможности системы и их значимость для выполнения целей системы.

7.3.7.3 Примечания:

Действия по оценке риска в определенных средах из-за возможности изменения рисков должны выполняться несколько раз. Однако повторение оценки рисков не должно подменять их мониторинг. Следует отметить, что термин «диапазон» используется для обозначения новых рисков, а термин «характеристики» относится к свойствам существующих идентифицированных рисков.

7.4 PA04 - Оценивает угрозы

7.4.1 Область процесса

7.4.1.1 Краткое описание

Назначением области процесса «Оценка угроз» является идентификация угроз безопасности и их характеристик.

7.4.1.2 Цели:

- идентификация и определение характеристик угроз безопасности.

7.4.1.3 Перечень базовых практик

BP.04.01 Идентификация соответствующих угроз, исходящих от естественного источника.

BP.04.02 Идентификация соответствующих угроз, исходящих от искусственных источников, случайных или преднамеренных.

BP.04.03 Определение соответствующих единиц измерения и диапазонов в определенной среде.

BP.04.04 Оценка возможностей и мотивации агента (носителя) угрозы в отношении угроз, исходящих от искусственных источников.

BP.04.05 Оценка вероятности появления события, связанного с угрозой.

BP.04.06 Мониторинг текущих изменений диапазона угроз и изменений их характеристик.

7.4.1.4 Примечания к области процесса

Для выполнения оценки угрозы можно использовать различные методы и технологии. Важным фактором определения методологии для использования является то, как она будет согласовываться и работать с методологиями, применяемыми на других участках выбранного процесса оценки риска.

Информация об угрозах, полученная от этой области процесса, предназначена для использования в PA03 наряду с информацией об уязвимостях от PA05 и воздействиях от PA02. Несмотря на то, что действия по сбору информации об угрозах, уязвимостях и воздействиях были объединены в отдельные области процесса, они являются взаимозависимыми. Целью сбора информацииявляется обнаружение комбинаций угрозы, уязвимости и воздействия, которые считаются достаточно рискованными для обоснования действия. Следовательно, поиск угроз должен в определенной степени руководствоваться наличием соответствующих уязвимостей и воздействий.

Вследствие подверженности изменениям воздействий должны периодически подвергаться мониторингу с целью обеспечения постоянного поддержания осведомленности о них, полученной с помощью этой области процесса.

При отслеживании функционирования этой области процесса анализ тенденций, существующий среди различных общих практических приемов, может указать на удовлетворение аргументу доверия (см. PA06).

7.4.2 BP.04.01 – Идентифицирует естественные угрозы

Идентифицирование угроз, происходящих от естественных источников.

7.4.2.1 Описание

Естественные угрозы исходят от землетрясений, цунами и торнадо. Однако не все угрозы природного происхождения могут возникать повсеместно. Например, цунами не может появиться в центре

большого континента. Следовательно, важно определить, какие угрозы естественного происхождения могут возникнуть в конкретном месте.

7.4.2.2 Примеры результатов деятельности:

- применимые таблицы естественных угроз – таблицы, документирующие характер и вероятность естественных угроз.

7.4.2.3 Примечания:

Большую часть информации, требуемую для этой оценки, можно получить из статистических таблиц и баз данных возникновения природных явлений. Из-за ценности этой информации ею надо пользоваться с осторожностью, поскольку она может быть в значительной степени обобщенной, и, следовательно, для применения в конкретной среде может потребоваться ее интерпретация.

7.4.3 BP.04.02 – Идентифицирует искусственные угрозы

Идентифицирование угроз, исходящих от искусственных источников, как случайных, так и преднамеренных.

7.4.3.1 Описание

Для угроз, исходящих от искусственных источников, требуется несколько иной подход. Существуют два основных типа искусственных угроз: исходящие от случайных источников и угрозы, являющиеся результатом преднамеренного воздействия. Некоторые искусственные угрозы не могут применяться в определенных средах. Они не должны рассматриваться в дальнейшем анализе.

7.4.3.2 Примеры результатов деятельности:

- описания сценариев угроз – описания действий угроз;
- оценки серьезности угроз – измерения вероятности, связанной с какой-либо угрозой.

7.4.3.3 Примечания

В некоторых случаях распознаванию преднамеренной угрозы может помочь разработка сценария, описывающего возможность появления угрозы. Общие базы данных искусственных угроз должны подвергаться оценке на предмет завершенности и уместности.

7.4.4 BP.04.03 – Определяет единицы измерения угроз

Определение подходящих единиц и диапазонов измерения в определенной среде.

7.4.4.1 Описание

Для большинства естественных и многих искусственных угроз имеются связанные с ними единицы измерения. Примером является шкала Рихтера для землетрясений. В большинстве случаев полный диапазон единиц измерения не применим в каком-либо конкретном месте. Следовательно, уместно установить максимум, а в некоторых случаях минимум, масштабность или частоту возникновения события, которое может возникнуть в определенном месте.

7.4.4.2 Примеры результатов деятельности:

- таблица угроз с соответствующими единицами и диапазонами измерения.

7.4.4.3 Примечания:

При отсутствии единицы измерения для определенной угрозы следует создать единицу измерения, приемлемую для того или иного места. Если это применимо, соответствующий диапазон и единица измерения должны быть описаны в проверяемых терминах.

7.4.5 BP.04.04 – Оценивает возможности носителя угрозы

Оценка возможностей и мотивации носителя угроз, исходящих от искусственного источника.

7.4.5 1 Описание

Данная область процесса связана с определением потенциальной способности и возможности потенциального противника осуществлять успешную атаку против системы. Данная способность подразумевает осведомленность противников об атаках (например, имеют ли они подготовку/знания). Возможностью является степень вероятности того, что компетентный противник может действительно осуществить атаку (например, имеет ли он достаточно ресурсов).

7.4.5.2 Примеры результатов деятельности:

- описания носителей угрозы – описания и оценки возможностей.

7.4.5.3 Примечания

Преднамеренные искусственные угрозы в значительной степени зависят от возможностей носителя угрозы и ресурсов, находящихся в его распоряжении. Таким образом, сравнительно неопытный хакер, имеющий доступ к инструментарию гораздо более опытных и квалифицированных хакеров, представляет собой довольно опасную угрозу, но не настолько опасную, как опытные хакеры. Однако совсем неопытный хакер также может нанести непреднамеренный ущерб, что вряд ли сделает опытный хакер. Кроме возможностей носителя угрозы, необходимо учитывать оценку ресурсов, имеющихся у носителя, наряду с его мотивацией к выполнению действий, на которую может повлиять вероятная оценка носителем угрозы привлекательности объекта (актива).

Для достижения желаемой цели носитель угрозы может наносить множественные атаки последовательно или параллельно. Необходимо рассмотреть результат множественных атак, проводимых последовательно или параллельно. Выполнению этой задачи может содействовать разработка сценариев угроз.

7.4.6 BP.04.05 – Оценивает вероятность угроз

Оценка вероятности появления события угрозы.

7.4.6.1 Описание

Оценивает степень вероятности возникновения события, связанного с угрозой. При проведении этой оценки надо учитывать многие факторы от случайного возникновения природного явления до случайных действий отдельного лица. Многие из этих факторов не поддаются оценке или измерению. В целях отчетности желательно иметь согласованную систему показателей по этому вопросу.

7.4.6.2 Примеры результатов деятельности:

- оценка вероятности события, связанного с угрозой - отчет о вероятности возникновения события, связанного с угрозой.

7.4.6. Примечания

Данная оценка представляет собой сложное вычисление, поскольку многие факторы содержат изменяющиеся вероятности. С любой оценкой вероятности связан фактор неопределенности, связанный с ее точностью и достоверностью. О неопределенности оцененной вероятности следует сообщать отдельно с целью избежания возможной путаницы. Во всех случаях будет существовать неопределенность, связанная с измерениями и вероятностью. Обычно предпочтительно сохранять факторы неопределенности, которые являются составными выражениями, отдельно для того, чтобы при принятии мер по уточнению рабочих данных можно было увидеть, уточняются ли сами данные или неопределенность, связанная с этими данными.

7.4.7 BP.04.06 – Осуществляет мониторинг угроз и их характеристик

Осуществление мониторинга текущих изменений в диапазоне угроз и изменений их характеристик.

7.4.7.1 Описание

Диапазон угроз, применимый к любому месту и ситуации, имеет динамический характер. Новые угрозы могут стать действующими, а характеристики существующих угроз — измениться. Таким образом, важно постоянно контролировать как существующие угрозы, так и их характеристики и регулярно корректировать новые угрозы. Эта базовая практика тесно связана с общей деятельностью по мониторингу в BP.08.02.

7.4.7.2 Примеры результатов деятельности:

- отчеты о мониторинге угроз – документы, описывающие результаты мониторинга угроз;
- отчеты об изменениях угроз - документы, описывающие изменения в спектре угроз.

7.4.7.3 Примечания

Поскольку угрозы в определенных средах могут изменяться, действия по оценке угроз следует проводить многократно. Однако повторение оценки угроз не заменяет мониторинга угроз.

7.5 PA05 – Оценивает уязвимости

7.5.1 Область процесса

7.5.1.1 Краткое описание

Назначением области процесса «Оценка уязвимостей» является идентификация и определение уязвимостей безопасности системы. Эта область процесса включает в себя анализ активов системы, определение специфических характеристик и обеспечение оценки общей уязвимости системы. Термины,

связанные с риском безопасности и оценкой уязвимости, используются во многих контекстах по разному. Для данной модели термин «уязвимость» относится к аспекту системы, который можно использовать в целях, отличных от намеченных первоначально, а именно: слабые места, пробелы в безопасности или ошибки при реализации в рамках системы, которые могут быть использованы угрозой. Эти уязвимости не зависят от какой-либо определенной угрозы или атаки. Эта совокупность видов деятельности осуществляется в любое время жизненного цикла системы для поддержки решения о разработке, обслуживании и эксплуатации системы в пределах известной среды.

7.5.1.2 Цели:

- осведомленность об уязвимостях безопасности системы в пределах определенной среды.

7.5.1.3 Перечень базовых практик

ВР.05.01 Выбирает методы, технологии и критерии, по которым идентифицируются уязвимости безопасности системы в определенной среде и определяются их характеристики.

ВР.05.02 Идентификация уязвимостей безопасности системы.

ВР.05.03 Сбор данных, связанных со свойствами уязвимостей.

ВР.05.04 Оценка уязвимостей системы и обобщение уязвимостей, являющихся результатом конкретных уязвимостей и их комбинаций.

ВР05.05 Проведение мониторинга текущих изменений соответствующих уязвимостей и их характеристик.

7.5.1.4 Примечания к данной области процесса

Анализ и практические приемы, связанные с данной областью процессов, часто являются «бумажной работой». Обнаружение уязвимостей системы активными средствами и способами является еще одним методом, который дополняет другие методы анализа уязвимостей, но не подменяет их. Эти активные методы можно рассматривать как специализированный вид анализа уязвимостей. Этот вид анализа может быть полезен при подтверждении уязвимости безопасности системы после ее значительного обновления или идентификации уязвимости системы в случае соединения двух систем. В некоторых случаях активный анализ уязвимости требуется для подтверждения правильности состояния безопасности системы и улучшения осознания и понимания имеющихся уязвимостей безопасности. Активный анализ, иногда называемый испытанием на проникновение, является процессом, посредством которого специалисты по безопасности пытаются обмануть средства защиты системы. Обычно они работают при тех же ограничениях, которые налагаются на обычных пользователей, но имеют всю проектную документацию и документацию по внедрению. Процесс атаки на безопасность не истощает ресурсы, а сдерживается их ограниченностью (время, деньги, персонал и т.д.).

Информация об уязвимостях, полученная от этой области процесса, предназначена для использования в РА03 наряду с информацией об угрозах из РА04 и воздействиях из РА02. Несмотря на то, что действия по сбору информации об угрозах уязвимостях и воздействиях были объединены в отдельные области процесса, они являются взаимозависимыми. Целью является обнаружение комбинаций угрозы, уязвимости и воздействия, которые считаются достаточно рискованными для обоснования действия. Следовательно, поиск уязвимостей должен в определенной степени руководствоваться наличием соответствующих угроз и воздействий.

Вследствие подверженности уязвимостей изменениям они должны периодически контролироваться с целью обеспечения постоянного поддержания осведомленности о них, полученной с помощью этой области процесса.

При отслеживании функционирования этой области процесса анализ тенденций, существующих среди различных общих практических приемов, может указать на удовлетворение аргументу доверия (см. РА06).

7.5.2 ВР.05.01 – Выбирает метод анализа уязвимости

Выбираются методы, технологии и критерии, по которым идентифицируются уязвимости безопасности системы в определенной среде и определяются их характеристики.

7.5.2.1 Описание

Эта базовая практика определяет метод установления уязвимостей безопасности способом, позволяющим их идентифицировать и характеризовать. Это может включать в себя схему категорирования уязвимостей и назначения им приоритетов на основе угроз и их вероятностей, эксплуатационных функций требований безопасности и других проблемных зон (при их наличии). Определение глубины анализа позволяет специалистам по безопасности и заказчику определять целевые системы, предназначенные для использования, и их полноту. Анализ должен проводиться по известной и зафиксированной конфигурации в течение заранее согласованного и заданного периода времени. Методология анализа должна

включать в себя ожидаемые результаты. Следует четко формулировать конкретные цели анализа.

7.5.2.2 Примеры результатов деятельности:

- метод анализа уязвимостей – определяет метод обнаружения и изучения уязвимостей безопасности системы, включая анализ, отчетность и процесс отслеживания;
- форматы анализа уязвимостей – описывает формат результатов анализа уязвимостей для обеспечения стандартизированного подхода;
- методология и методика атак – включает цели и метод проведения тестирования атак;
- процедуры атак – подробные этапы проведения тестирования атак;
- планы атак – включает ресурсы атак, график и описание их методологии;
- изучение проникновения – анализ и реализация сценариев атак, направленные на идентификацию неизвестных уязвимостей;
- сценарии атак – описание конкретных атак, которые будут предприниматься.

7.5.2.3 Примечания

Метод анализа уязвимостей может быть действующим, адаптированным или специфическим для эксплуатационных аспектов и определенной среды системы. Он часто основывается на методологии анализа риска, выбранной из РА03, или дополняет ее. Следует отметить, что разъяснение угроз, возможностей и значений может быть не предусмотрено, и в этом случае необходимо сузить область применения методологии или принять набор подходящих допущений.

Метод анализа уязвимостей может быть качественным или количественным. Он часто включает в себя отражение вероятности существования уязвимости. Результаты атак могут передаваться в письменном отчете, но сами атаки могут быть продемонстрированы.

Для идентификации уязвимостей существует по крайней мере два принципиально различных метода. Один из них основан на анализе, другой - на тестировании. Основанный на тестировании метод удобен для идентификации существующих уязвимостей, для которых есть известная угроза, включенная в набор тестов. Основанный на анализе метод является лучшим для идентификации новых уязвимостей и уязвимостей, недоступных для использования непосредственно, но которые могут стать доступными после разрешения какой-то другой проблемы. Другими вариантами, которые следует учитывать при выборе методологии идентификации уязвимостей, являются качественный и количественный методы. Следует также учитывать возможность осуществления контроля полноты анализа и тестирования.

7.5.3 ВР.05.02 – Идентифицирует уязвимости

Идентификация уязвимостей безопасности системы.

7.5.3.1 Описание

Уязвимости системы можно обнаружить как в связанных с обеспечением безопасности частях системы, так и в частях, не связанных с ней. Во многих случаях оказывается, что не связанные с безопасностью механизмы, поддерживающие функции безопасности или работающие во взаимодействии с механизмами безопасности, имеют используемые уязвимости. Методологии сценариев атак, разработанной в ВР.05.01, надо следовать до тех пор, пока уязвимости не подтвердятся. Все обнаруженные уязвимости системы должны фиксироваться.

7.5.3.2 Примеры результатов деятельности:

- перечень уязвимостей – описывает уязвимость системы для различных атак;
- профиль проникновения - включает в себя результаты тестирования атак (например, уязвимости).

7.5.3.3 Примечания

В данном практическом приеме уязвимости рассматриваются как внутренне присущие системе без учета вероятности каких-либо угроз. Приоритеты упорядочения таких уязвимостей могут быть назначены в соответствии с результатами анализа угрозы. Невоспроизводимые атаки усложняют задачу разработки контрмер.

Уязвимости идентифицируются частично на основе рисков с назначенными приоритетами из РА03, и приоритетов деловой деятельности и целей, обозначенных в РА10. Кроме того, надо учитывать активы, упоминаемые в РА02.

7.5.4 ВР.05.03 – Собирает данные об уязвимостях

Сбор данных, связанных со свойствами уязвимостей. Назначением этой базовой практики является сбор данных, связанных с указанными свойствами. В некоторых случаях уязвимость может иметь единицы измерения аналогичные единицам, связанным с угрозами (см. ВР.04.03). Легкость использования уязвимости и вероятность существования уязвимости следует определять и фиксировать.

7.5.4.2 Примеры результатов деятельности:

- таблицы свойств уязвимости – таблицы, документирующие характеристики продукта или системы.

7.5.4.3 Примечания

Большая часть данных, собранных во время этой деятельности, будет использоваться позднее для выполнения PA03. Поэтому важно, чтобы данные собирались и хранились в формате, пригодном для использования PA03. Во всех случаях будет существовать неопределенность, связанная с измерениями и вероятностями. Обычно удобнее хранить неопределенность отдельно, так, чтобы при принятии мер по уточнению данных можно было видеть, уточняются ли сами данные или связанная с ними неопределенность.

7.5.5 BP.0504 – Синтезирует уязвимость системы

Оценка уязвимости системы и объединение уязвимостей, вытекающих из конкретных уязвимостей и их комбинаций.

7.5.5.1 Описание

Анализирует, какие уязвимости или комбинации уязвимостей создают проблемы для системы. Анализ должен определять дополнительные характеристики уязвимости, такие как вероятность использования уязвимости и возможность ее успешного использования. В результаты анализа можно также включить рекомендации по рассмотрению синтезированных уязвимостей.

7.5.5.2 Примеры результатов деятельности:

- отчет об оценке уязвимостей – включает в себя количественное или качественное описание уязвимостей, которые создают проблемы для системы, включая вероятность атаки, вероятность ее успеха и ее воздействие;
- отчеты об атаках – документируют результаты и их анализ, включая обнаруженные уязвимости, возможность их использования и любые рекомендации.

7.5.5.3 Примечания

Результаты анализа и осуществления атаки должны регистрироваться. Любые обнаруженные уязвимости и возможность их использования должны идентифицироваться и документироваться достаточно подробно, чтобы заказчик мог принять решение о принятии контрмер.

7.5.6 BP.05.05 – Осуществляет мониторинг уязвимостей и их характеристик

Проведение мониторинга текущих изменений в соответствующих уязвимостях и их характеристиках.

7.5.6.1 Описание

Диапазон уязвимостей применим повсеместно, а ситуация является динамичной. Новые уязвимости могут стать действующими, а характеристики существующих уязвимостей могут изменяться. Поэтому важно проводить мониторинг существующих уязвимостей и их характеристик, а также постоянно проверять новые уязвимости. Эта практика тесно связана с общей деятельностью по мониторингу в BP 08.02.

7.5.6.2Примеры результатов деятельности:

- отчеты о мониторинге уязвимостей – документы, описывающие результаты действий по мониторингу уязвимостей;
- отчеты об изменениях уязвимостей - документы, описывающие новые или изменившиеся уязвимости.

7.5.6.3 Примечания

Из-за возможности изменения уязвимостей действия по их оценке должны проводиться несколько раз в определенных средах. Однако они не должны заменять мониторинг уязвимостей.

7.6 PA06 – Создает аргумент доверия

7.6.1 Область процесса

7.6.1.1 Краткое описание

Назначением области процесса является однозначное сообщение о том, что требования безопасности заказчика удовлетворены. Аргументом доверия является набор установленных целей доверия, поддерживаемых свидетельством, которое можно получить от различных источников и уровней абстракции.

Этот процесс включает в себя идентификацию и определение связанных с доверием требований, получение свидетельства и деятельность по проведению анализа и дополнительных связанных со свидетельством действий, необходимых для поддержки требований к доверию. Кроме того, свидетельства, полученные в результате этих действий, собираются, объединяются в пакеты и готовятся к презентации.

7.6.1.2 Цели:

- рабочая продукция и процессы предоставляют собой четкое доказательство удовлетворения требованиям безопасности заказчика.

7.6.1.3 Перечень базовых практик

ВР.06.01 Определяет цели обеспечения доверия к безопасности.

ВР.06.02 Определяет стратегию обеспечения доверия для работы со всеми целями обеспечения доверия.

ВР.06.03 Определяет меры измерения для мониторинга целей обеспечения доверия к безопасности.

ВР.06.04 Идентифицирует и контролирует свидетельства доверия к безопасности.

ВР.06.05 Проводит анализ свидетельства доверия к безопасности.

ВР.06.06 Предоставляет аргумент доверия к безопасности, демонстрирующий удовлетворение требованиям безопасности заказчика.

7.6.1.4 Примечания к данной области процесса

Действия по созданию аргумента доверия включают в себя управление идентификацией, планированием, пакетированием и представлением свидетельства доверия к безопасности.

При отслеживании функционирования этой области процесса анализ тенденций между различными базовыми практиками может указать на удовлетворение аргумента доверия.

7.6.2 ВР.06.01 – Определяет цели обеспечения доверия

Определение целей обеспечения доверия к безопасности.

7.6.2.1 Описание

Для угроз, исходящих от искусственных источников, требуется несколько иной подход. Существуют два основных типа искусственных угроз: те, которые исходят от случайных источников и те, которые являются результатом преднамеренного воздействия. Некоторые искусственные угрозы не могут применяться в определенных средах. Они не должны рассматриваться в дальнейшем анализе.

Определение новых и модификация существующих целей обеспечения доверия к безопасности координируются со всеми связанными с безопасностью группами проектных организаций и группами, являющимися сторонними для этой организации (например, заказчиком, органом сертификации систем, пользователем).

Цели обеспечения доверия к безопасности обновляются для отражения происходящих изменений. Примеры изменений, требующих модификации целей обеспечения доверия к безопасности, включают в себя изменения степени приемлемости риска заказчиком, органом сертификации систем или пользователем и изменения в требованиях или их трактовках.

О целях обеспечения доверия к безопасности должно быть сообщено для избежания двусмысленности. Включается или (при необходимости) разрабатывается приемлемое объяснение этих целей.

7.6.2.2 Примеры результатов деятельности:

- формулировка целей обеспечения доверия к безопасности – определяет требования заказчика к степени уверенности в характеристиках безопасности системы.

7.6.2.3 Примечания

В случаях, когда конкретное утверждение необязательно, полезно цели обеспечения доверия сформулировать или связать с конкретным утверждением о доверии, которое должно быть получено или удовлетворено. Это помогает устранить неверные толкования и неясности.

7.6.3 ВР 06.02 – Определяет стратегию обеспечения доверия

Определение стратегии обеспечения доверия к безопасности для выполнения ее целей.

7.6.3.1 Описание

Целью стратегии обеспечения доверия к безопасности является планирование и обеспечение правильной реализации целей безопасности. Свидетельство, полученное посредством реализации этой стратегии, должно обеспечить приемлемую степень уверенности в адекватности мер защиты системы менеджмента риска безопасности. Эффективное управление связанными с обеспечением доверия действиями достигается посредством разработки и установления в обязательном порядке стратегии обеспечения доверия к безопасности. Ранняя идентификация и определение связанных с обеспечением до-

верия требований крайне важны для получения необходимого подтверждающего свидетельства. Знание требований заказчика к доверию и мониторинг их выполнения посредством постоянной внешней координации обеспечивает удовлетворение высоких требований доверия к качеству обеспечения безопасности.

7.6.3.2 Примеры результатов деятельности:

- стратегия обеспечения доверия к безопасности – описывает план выполнения целей обеспечения доверия к безопасности заказчика и определяет ответственные стороны.

7.6.3.3 Примечания

Стратегия обеспечения доверия к безопасности координируется со всеми группами проектирования безопасности в организации и сторонними группами (например, заказчиком, органом сертификации систем, пользователем), как определено в PA07.

7.6.4 BP.06.03 – Определяет измерения безопасности

Определение измерений для мониторинга целей обеспечения доверия к безопасности.

7.6.4.1 Описание

Измерения используются для облегчения принятия решений, улучшения функционирования и подотчетности посредством сбора, анализа соответствующих связанных с функционированием данных и путем сообщения о них. Целью измерения рабочих характеристик является мониторинг состояния процессов обеспечения безопасности и способствование усовершенствованию этих процессов с применением корректирующих действий, основанных на полученных измерениях. Применение измерений упрощает мониторинг осуществления стратегии обеспечения доверия и, следовательно, поддерживает аргумент доверия.

7.6.4.2 Примеры результатов деятельности:

- перечень измерений, согласующихся с целями и стратегиями обеспечения доверия.

7.6.4.3 Примечания

Измерения должны быть количественными по своему характеру и выражаться числами и практическими данными. Они должны быть финансово разумными и соответствовать стоимости проекта (например, расходы на сбор данных не должен превышать ценности собранных данных). Измерения должны проверяться представителями третьей стороны на предмет согласованности результатов. Некоторые измерения могут применяться для анализа тенденций изменения и сообщать об изменениях воздействий за период времени. Результирующие измерения должны быть полезными для принятия решений о месте сосредоточения усилий по реализации проекта. Они должны собираться на самом низком уровне и не делиться по другому формату. Наконец, измерения должны быть хорошо определены с помощью таких характеристик, как частота, формулы, доказательство и показатели. Для данной базовой практики рекомендуется знать измерения, требуемые для оценки других влияний (например, на правительство, на промышленность и т.д.).

7.6.5 BP.06.04 – Управляет свидетельствами доверия

Идентификация свидетельства доверия к безопасности и управление им.

7.6.5.1 Описание

Свидетельства доверия к безопасности собираются согласно определению в стратегии обеспечения безопасности посредством взаимодействия со всеми областями процессов проектирования безопасности для идентификации свидетельств на различных уровнях абстракции. Эти свидетельства контролируются для обеспечения широкого применения рабочей продукции и ее соответствия целям обеспечения безопасности.

7.6.5.2 Примеры результатов деятельности:

- архив информации свидетельства доверия к безопасности – хранит все доказательства, полученные в процессе разработки, тестирования и использования. Может существовать в виде базы данных, справочника по инжинирингу, тестовых результатов или журнала доказательств.

7.6.5.3 Примечания

Рабочую документацию по доверию можно получить из информации о системе, архитектуре, проекте, реализации, процессе разработки, физической среде разработки и физической среде эксплуатации. Идентификация свидетельств доверия и управление ими способствует сбору данных более высокого качества и повышению эффективности передачи результатов анализа более широкой аудитории,

обеспечивая объективный механизм постоянного измерения и улучшения функционирования и результатов общих процессов обеспечения безопасности.

7.6.6 BP.06.05 – Анализирует свидетельства

Проведение анализа свидетельства доверия к безопасности.

7.6.6.1 Описание

Анализ свидетельств доверия к безопасности проводится для обеспечения уверенности в том, что собранные доказательства отвечают целям обеспечения безопасности, таким образом, удовлетворяя требованиям безопасности заказчика. Анализ свидетельства доверия определяет достаточную степень адекватности и полноты процессов проектирования и верификации безопасности для принятия решения об удовлетворительности реализации характеристик и механизмов обеспечения безопасности. Кроме того, свидетельства подвергаются анализу для гарантирования полноты и правильности артефактов проектирования по отношению к основной системе. В случае недостаточности или неадекватности свидетельства доверия этот анализ может обусловить исправления в системе результатов деятельности по обеспечению безопасности и в процессах, поддерживающих цели обеспечения безопасности.

7.6.6.2 Примеры результатов деятельности:

- результаты анализа свидетельства доверия – идентифицируют и обобщают сильные и слабые места доказательств в архиве информации.

7.6.6.3 Примечания

Некоторые свидетельства доверия можно получить только из объединения других объектов системного проектирования или вывести из обобщения других видов доверия.

7.6.7 BP.06.06 – Предоставляет аргумент доверия

Предоставление аргумента доверия к безопасности, демонстрирующего удовлетворение требований заказчика.

7.6.7.1 Описание

Общий аргумент доверия разрабатывается для демонстрации соответствия целям обеспечения доверия к безопасности и представляется заказчику. Аргументом доверия является совокупность установленных целей обеспечения доверия, поддерживаемых комбинацией свидетельств доверия, которые можно вывести из многих уровней абстракции. Аргумент доверия должен анализироваться на предмет наличия недостатков в изложении свидетельства, а также недостатков в выполнении целей обеспечения доверия к безопасности.

7.6.7.2 Примеры результатов деятельности:

- аргумент доверия с поддерживающим доказательством - структурированная совокупность целей обеспечения доверия, поддерживаемая различными компонентами свидетельства доверия.

7.6.7.3 Примечания

Высокоуровневый аргумент доверия может заключаться в том, что были выполнены цели соответствующих критериев. Другие вероятные части аргумента доверия могут касаться того, как были рассмотрены угрозы активам системы. Каждая из целей обеспечения доверия поддерживается соответствующим достаточным доказательством для соответствия критерию доказанности. Аргумент доверия может использоваться заказчиком, органом сертификации безопасности систем и пользователями.

7.7 PA07 - Координирует безопасность

7.7.1 Область процесса

7.7.1.1 Краткое описание

Назначением этой области процесса является обеспечение осведомленности всех сторон о действиях по проектированию безопасности и вовлечение их в эти действия. Эта деятельность является критически важной, поскольку проектирование безопасности нельзя успешно реализовать изолированно. Данная координация включает поддержание открытого обмена информацией между персоналом проекта и сторонними группами. Для координации и передачи решений о инжиниринге безопасности и рекомендаций между этими сторонами и рабочими группами могут использоваться различные механизмы, включая служебные записки, документацию, сообщения по электронной почте.

7.7.1.2 Цели:

- все члены проектной группы осведомлены о действиях по проектированию безопасности и участвуют в них в объеме, необходимом для выполнения своих функций;
- решения и рекомендации, связанные с безопасностью, сообщаются и координируются.

7.7.1.3 Перечень базовых практик

BP.07.01 Определяет цели и взаимодействие при координации действий по проектированию безопасности.

BP.07.02 Определяет механизмы координации для проектирования безопасности.

BP.07.03 Содействует координации проектирования безопасности.

BP.07.04 Использование определенных механизмов для координации решений и рекомендаций, связанных с безопасностью.

7.7.1.4 Примечания к данной области процесса

Данная область процесса гарантирует неотделимость проектирования безопасности от общей деятельности по проектированию. Специалисты по безопасности должны быть частью всех основных проектных и рабочих групп. Особенно важно, чтобы группы по проектированию безопасности систем устанавливали взаимосвязи с другими инженерно-техническими группами на раннем этапе жизненного цикла процесса проектирования, когда принимаются важные решения. Данная область процесса проектирования может быть одинаково применима как к организациям-разработчикам, так и к эксплуатирующим организациям.

При отслеживании функционирования этой области процесса, анализ тенденций среди различных базовых практик может указать на соответствие аргументу доверия (см. PA06).

7.7.2 BP.07.01 – Определяет цели координации

Определение целей и взаимосвязей координации проектирования безопасности.

7.7.2.1 Описание

Многие рабочие группы должны быть осведомлены о действиях по проектированию безопасности и участвовать в них. Цели обмена информацией между этими группами определяются структурой проекта, информационными потребностями и требованиями проекта. Устанавливаются взаимосвязи с другими группами и их обязательства в отношении друг друга. Успешные взаимосвязи могут принимать различные формы, но должны быть признаны всеми сторонами-участниками.

7.7.2.2 Примеры результатов деятельности:

- соглашения по совместному использованию информации – описывают процесс совместного использования информации рабочими группами, определяя участвующие стороны, носители информации, формат, ожидаемые результаты и частоту обмена информацией;
- членство в рабочих группах и планы – описывают рабочие группы организации, включая членство в них, должности членов групп, цели, планы работ и материально-техническое обеспечение;
- организационные нормы – описывают процессы и процедуры обмена связанной с безопасностью информации между различными рабочими группами и заказчиком.

7.7.2.3 Примечания

Цели координации и ее взаимосвязи должны определяться в проекте как можно раньше для создания достаточно хороших каналов обмена информацией. Все инженерно-технические группы должны определять роли специалистов по безопасности в повседневной работе (например, участие в процессах анализа, в обучении, оценке проектов). Невыполнение вышеупомянутого увеличивает риск пропуска какого-нибудь ключевого аспекта обеспечения безопасности.

7.7.3 BP.07.02 – Определяет механизмы координации

Определение механизмов координации для проектирования безопасности.

7.7.3.1 Описание

Существует много способов совместного использования решений и рекомендаций по проектированию безопасности всеми инженерно-техническими группами. Эти действия определяют различные способы координирования действий по обеспечению безопасности проекта.

Нет ничего необычного в наличии многочисленного персонала, связанного с безопасностью и работающего над одним и тем же проектом. В этой ситуации все специалисты по безопасности должны работать над понятной всем целью. Действия по определению областей взаимодействия, выбору механизмов обеспечения безопасности, обучению и разработке должны проводиться так, чтобы обеспечить должное функционирование каждого элемента безопасности в автоматизированной системе. Кроме того, все инженерно-технические группы должны понимать действия по проектированию безопасности для осуществления интеграции безопасности в систему. Заказчик также должен быть осведомлен о событиях и действиях, связанных с безопасностью, для обеспечения соответствующего определения требований.

7.7.3.2 Примеры результатов деятельности:

- планы обмена информацией - включают в себя информацию, предназначенную для совместного использования: время совещаний, процессы и процедуры, которые будут использоваться членами рабочих групп и в других группах;

- требования к инфраструктуре связи – определяют инфраструктуру и нормы, необходимые для совместного использования информации членами рабочих групп и в других группах;

- образцы для составления отчетов совещаний, сообщений, справок - описывают формат для различных документов с целью обеспечения стандартизации и эффективности работы.

7.7.3.3 Примечания

Отсутствуют.

7.7.4 BP.07.03 – Содействует координации

Способствование координации проектирования безопасности.

7.7.4.1 Описание

Успешность взаимосвязей зависит от качественной организации групповой работы. Взаимодействие различных групп с разными приоритетами может привести к конфликтам разного рода. Данная базовая практика обеспечивает продуктивное разрешение спорных вопросов.

7.7.4.2 Примеры результатов деятельности:

- процедуры разрешения конфликтов – определяют подход к разрешению конфликтов как в рамках объектов организации, так и между ними;

- повестки дня совещаний, цели, элементы действий – излагают темы, обсуждаемые на совещании, выделяя для рассмотрения цели и элементы действий;

- отслеживание элементов действий – определяет план работы и принятия решений по объектам действий, включая обязанности, график и очередность выполнения.

7.7.4.3 Примечания

Отсутствуют.

7.7.5 BP.07.04 – Координирует решения и рекомендации по безопасности

Использование определенных механизмов для координаций решений и рекомендаций, связанных с безопасностью.

7.7.5.1 Описание

Назначением данной базовой практики является распространение решений и рекомендаций среди различных специалистов по безопасности, других инженерно-технических групп, сторонних объектов и причастных сторон.

7.7.5.2 Примеры результатов деятельности:

- решения – передача связанных с безопасностью решений заинтересованным группам посредством отчетов о совещаниях, памятных записок, протоколов рабочих групп, электронной почты, руководств по безопасности и электронных досок объявлений;

- рекомендации – передача связанных с безопасностью рекомендаций заинтересованным группам посредством отчетов о совещаниях, памятных записок, протоколов рабочих групп, электронной почты, руководств по безопасности и электронных досок объявлений.

7.7.5.3 Примечания

Отсутствуют.

7.8 PA08 – Осуществляет мониторинг состояния безопасности

7.8.1 Область процесса

7.8.1.1 Краткое описание

Назначением области процесса «Мониторинг состояния безопасности» является идентификация всех нарушений безопасности, попыток нарушения и ошибок, которые могут привести к нарушению безопасности. Проводится мониторинг как внутренних, так и внешних сред организации на наличие всех факторов, которые могут оказать воздействие на безопасность системы.

7.8.1.2 Цели:

- обнаружение и отслеживание как внутренних, так и внешних связанных с безопасностью событий;

- реагирование на инциденты в соответствии с установленной политикой;

- идентификация и обработка изменений состояния безопасности в соответствии с целями безопасности.

7.8.1.3 Перечень базовых практик

BP.08.01 анализирует документацию о событиях с целью определения причины события, его развития и возможных будущих событиях.

BP.08.02 осуществляет мониторинг изменений угроз, уязвимостей, воздействий, рисков и среды.

BP.08.03 идентифицирует соответствующие инциденты безопасности.

BP.08.04 осуществляет мониторинг результативности и функциональной эффективности мер безопасности.

BP.08.05 анализирует состояние безопасности системы с целью обнаружения необходимых изменений.

BP.08.06 управляет реагированием на соответствующие инциденты безопасности.

BP.08.07 обеспечивает должную защиту объектов, связанных с мониторингом безопасности.

7.8.1.4 Примечания к области процесса

Состояние безопасности указывает на готовность системы и ее среды к обработке текущих угроз и уязвимостей, а также любого воздействия на систему и ее активы. Данная область процесса включает в себя действия PA05 и PA03. Собранные данные о внутренней и внешней средах анализируются как в их собственном контексте, так и в отношении других данных, которые могут быть результатом событий, имевших место до обсуждаемого события, одновременно с ним или после него. Область процесса относится как к конкретной среде, предназначенной для системы, так и к среде, в которой система разрабатывается. Любой конкретной системе приходится функционировать совместно с существующими системами, что может повлиять на ее общую безопасность, поэтому эти существующие системы тоже должны быть включены в мониторинг.

При отслеживании функционирования этой области процесса, анализ тенденций между различными базовыми практиками может указывать на удовлетворенность аргументу доверия (см. PA06).

7.8.2 BP.08.01 – Анализирует записи о событиях

Анализ записей о событиях для определения причины отдельного события, его развития, а также о вероятных будущих событиях.

7.8.2.1 Описание

Исследует записи отображения процесса и записи событий (комплекты журнальных записей) на наличие связанной с безопасностью информации. Представляющие интерес события следует идентифицировать наряду с факторами, используемыми для корреляции событий среди множественных записей. Множественные записи событий затем можно объединить в одну запись.

7.8.2.2 Примеры результатов деятельности:

- описания каждого события – определяют источник, воздействие и значимость каждого обнаруженного события;
- составляющие журнальные записи и их источники – записи связанных с безопасностью событий из различных источников;
- параметры идентификации событий – описывают, какие события собираются различными частями системы, а какие нет;
- перечень всех текущих опасных состояний в отдельном журнале – идентифицирует все запросы на действие на основе записей в отдельном журнале;
- перечень всех текущих опасных состояний отдельных событий - идентифицирует все запросы на действие на основе событий, сформированных из записей во многих журналах;
- периодический отчет обо всех опасных состояниях, имевших место - синтезирует перечни сигналов опасности из нескольких систем и осуществляет предварительный анализ;
- краткое содержание журналов и их анализ – проводит анализ последних сигналов опасности и сообщает результаты для широкого потребления.

7.8.2.3 Примечания

Многие контрольные журналы могут содержать информацию, связанную с отдельным событием. Это особенно характерно для распределенной или сетевой среды. Часто событие оставляет след во многих узлах сети. Для обеспечения ценности отдельных записей и способствования ими полному пониманию события и его поведения надо обобщить отдельные журнальные записи или объединить их в отдельную запись о событии.

Можно проводить анализ как единичных, так и множественных записей. Для анализа множественных записей одинакового вида часто применяются методы статистического или анализа тенденций изменений. Анализ множественных записей различного вида можно проводить на журнальных записях или записях (объединенных) о них, хотя анализ множественных записей о событиях обычно проводится на одинаковом виде событий.

Сигналы тревоги (то есть, запросы на действие, основанные на единичном появлении события) должны быть определены для журнальных записей и объединенных записей о событиях. В анализ также надо включать журнальные записи и записи о событиях в среде разработки.

7.8.3 BP.08.02 – Осуществляет мониторинг изменений

Проводение мониторинга изменений в угрозах, уязвимостях, воздействиях, рисках и среде.

7.8.3.1 Описание

Ведет поиск любых изменений, которые могут положительно или отрицательно повлиять на эффективность текущего состояния безопасности.

Реализованная для любой системы безопасность должна касаться угроз, уязвимостей, воздействий и рисков, поскольку они связаны с внутренней и внешней средой системы. Все они не являются статичными, и их изменения влияют как на эффективность, так и на целесообразность безопасности системы. Угрозы, уязвимости, воздействия и риски должны постоянно контролироваться на предмет внесения изменений, а изменения анализироваться с целью оценки их значимости для эффективности безопасности.

7.8.3.2 Примеры результатов деятельности:

- сообщение об изменениях – идентифицирует все внешние и внутренние изменения, способные повлиять на состояние безопасности системы;
- периодическая оценка значимости изменений – проводит анализ изменений состоянии безопасности для определения степени их воздействия и необходимости реагирования на них.

7.8.3.3 Примечания

Как внутренние и внешние источники, так и среды разработки и эксплуатации должны проверяться.

При обнаружении изменений необходимо реагировать на них путем оценки анализа риска или его части (см. PA03).

7.8.4 BP.08.03 – Идентифицирует инциденты безопасности

Идентификация инцидентов, связанных с безопасностью.

7.8.4.1 Описание

Определяет, наличие связанного с безопасностью инцидента, идентифицирует его детали и при необходимости сообщает о них. Связанные с безопасностью инциденты можно обнаружить с помощью ретроспективных данных о событиях, данных о конфигурации системы, средств интеграции и другой системной информации. Так как некоторые инциденты возникают в течение длительного периода времени, по-видимому, анализ должен включать в себя сравнение состояний безопасности за этот период.

7.8.4.2 Примеры результатов деятельности:

- перечень инцидентов и их определения – идентифицирует общие инциденты безопасности и описывает их с целью облегчения распознавания;
- инструкции по реагированию на инциденты – описывают соответствующее реагирование на возникающие инциденты безопасности.
- отчеты об инцидентах – описывают возникший инцидент в деталях, включая источник инцидента, любой ущерб от него, реагирование на него и требуемые дальнейшие меры в его отношении;
- отчеты о каждом обнаруженном событии вторжения – описывают каждое обнаруженное событие вторжения и предоставляют все необходимые детали, включая источник инцидента, любой ущерб от него, реагирование на него и требуемые дальнейшие меры в его отношении;
- периодические сводки об инцидентах – предоставляют сводку о последних инцидентах безопасности, отмечая тенденции, области, требующие усиления безопасности, и возможную экономию в расходах от понижения степени безопасности, в то же время не забывая о возможности повышения степени риска.

7.8.4.3 Примечания

Инциденты безопасности могут возникнуть как в среде разработки, так и в среде эксплуатации. Эти инциденты могут воздействовать на разрабатываемую или функционирующую системы различными путями. Преднамеренные технические атаки со стороны хакеров или вредоносных кодов (вирусов, сетевых червей и т.д.) обусловливают различный подход к защите от случайных событий. Для обнаружения этих атак требуется анализ состояния и конфигурации системы. Следует подготавливать, тестировать и задействовать соответствующие планы реагирования. Многие атаки требуют быстрого, заранее определенного реагирования для минимизации последующего распространения ущерба. В некоторых случаях нескоординированные реагирования могут лишь ухудшить ситуацию. В необходимых случаях реагирование идентифицируется и определяется с помощью BP.08.06.

7.8.5.BP.08.04 – Осуществляет мониторинг мер безопасности

Проведение мониторинга функционирования и функциональной эффективности мер безопасности.

7.8.5.1 Описание

Проверка функционирования мер безопасности с целью обнаружения в нем изменений.

7.8.5.2 Примеры результатов деятельности:

- периодическое краткое изложение состояния мер безопасности – описывает состояние имеющихся мер безопасности с целью обнаружения возможного нарушения их конфигурации или других проблем;
- периодические сводки о состоянии мер безопасности – предоставляют сводку о состоянии имеющихся мер безопасности, отмечая тенденции, требуемые усовершенствования и возможную экономию в расходах вследствие понижения степени безопасности.

7.8.5.3 Примечания

Меры безопасности, защищающие среды разработки и эксплуатации, должны постоянно контролироваться. Многие меры безопасности после долгого использования могут находиться в неадекватном или неэффективном состоянии. Многим из них предъявляются требования в отношении их текущего состояния, эффективности и обслуживания. Все три аспекта следует периодически проверять.

7.8.6 BP.08.05 – Анализ состояния безопасности

Анализ состояния безопасности системы для определения необходимости внесения изменений.

7.8.6.1 Описание

Состояние безопасности системы подвержено изменениям, основанным на среде угроз, функциональных требованиях и конфигурации системы. Эта практика повторно исследует основания для формирования безопасности и требований безопасности, предъявляемых к другим дисциплинам.

7.8.6.2 Примеры результатов деятельности:

- анализ безопасности – содержит описание текущей среды рисков безопасности, существующего состояния безопасности и анализ совместимости этих двух факторов;
- анализ приемлемости рисков – заявление соответствующего утверждающего органа о приемлемости риска, связанного с эксплуатацией системы.

7.8.6.3 Примечания

Анализ состояния безопасности должен проводиться исходя из текущей операционной обстановки и произошедших изменений. Если другие события, подобные изменениям, не инициировали детальный анализ безопасности, он должен инициироваться, основываясь на периоде времени, прошедшем после последнего анализа. Инициированные временем анализы должны согласовываться с соответствующими политикой и правилами. Анализ должен приводить к переоценке адекватности текущей безопасности и целесообразности текущего уровня приемлемости риска. Анализ должен основываться на подходе организаций к оценке безопасности (см. PA05). Аналогично анализу среды эксплуатации должна периодически анализироваться среда разработки, в которой создаются системы. Фактически среду разработки следует рассматривать как рабочую среду для разработки систем.

7.8.7 BP.08.06 – Управляет реагированием на инциденты безопасности

Управление реагированием на инциденты безопасности.

7.8.7.1 Описание

Во многих случаях постоянная доступность систем является критически важной. Многие события предотвратить нельзя, поэтому очень большое значение имеет способность реагировать на нарушение безопасности. Для чрезвычайного плана требуется определение максимального допустимого периода простоя системы; идентификация необходимых элементов функциональности системы, определение и разработка стратегии и плана восстановления; тестирование и выполнение плана.

В некоторых случаях неожиданные ситуации могут включать в себя реагирование на инциденты и активное контактирование с враждебными агентами (например, вирусами, хакерами и т.д.).

7.8.7.2 Примеры результатов деятельности:

- указатель приоритетов восстановления системы – содержит описание порядка, в котором функции системы должны быть защищены и восстановлены в случае возникновения вызывающего отказы инцидента;
- программа испытаний – содержит даты периодического тестирования системы для обеспечения рабочего состояния функций, связанных с обеспечением безопасности;
- результаты испытаний – описывают результаты периодического тестирования и меры поддержания безопасности системы;
- план регламентных работ – содержит даты обслуживания всей системы, включая модернизацию и профилактику, и обычно интегрируется в программу испытаний;
- отчеты об инцидентах – описывают возникший инцидент со всеми сопутствующими деталями, включая источник инцидента, любой ущерб, наносимый им, принятые против него меры и дальнейшие необходимые действия;
- периодические анализы – описывают процедуру периодического анализа безопасности системы, включая лицо, проводящее анализ, какие проверки делаются в ходе анализа и содержание результатов;
- чрезвычайные планы – определяют максимально приемлемое время простоя системы, важнейшие элементы системы, стратегию и план восстановления системы, возобновления деловой деятельности, управления ситуацией, а также процедуры тестирования и выполнения плана.

7.8.7.3 Примечания

Будущие события нельзя предопределить, но, если только они не способны вызвать хаос, они должны быть управляемыми. Если ситуация выходит за рамки заранее определенного сценария, она передается на более высокий уровень принятия решений руководством бизнеса.

7.8.8 BP 08.07 - Защищает объекты мониторинга безопасности

Обеспечение защиты объектов, связанных с мониторингом безопасности.

7.8.8.1 Описание

Если от результатов действий по мониторингу ничего не может зависеть, их ценность невелика. Эти действия включают в себя изолирование и архивирование соответствующих журналов, отчетов о результатах проверок и соответствующих анализов.

7.8.8.2 Примеры результатов деятельности:

- перечень всех архивированных журналов и связанных с ними периодов хранения – определяет место хранения объектов мониторинга безопасности и время их возможного уничтожения;
- периодические результаты выборочных проверок, которые должны быть представлены в архиве – перечисляют недостающие отчеты и определяют соответствующую реакцию на это;
- использование архивированных журналов - определяет пользователей архивированных журналов, включая время и цель доступа к информации, и любые комментарии;
- периодические результаты тестирования достоверности и применимости произвольно выбранных архивированных журналов – анализируют произвольно выбранные журналы и определяет их полноту, корректность и пригодность для обеспечения должного мониторинга безопасности системы.

7.8.8.3 Примечания

Большинство действий по мониторингу, включая аудит, дают результаты. Эти результаты можно обработать сразу или зафиксировать для дальнейшего анализа и обработки. Содержание журналов следует составлять так, чтобы облегчить понимание произошедшего во время инцидента и обнаружить изменения в тенденциях. Регистрацией выходных данных следует управлять в соответствии с применяемой политикой и положениями. Журналы должны быть достоверными и защищенными от фальсификации или случайного нанесения ущерба. После заполнения всего журнала его заменяют новым. При замене журнала все ненужные записи следует удалить и выполнить необходимые действия по его сокращению. Журналы должны опечатываться с тем, чтобы какие-либо изменения не остались незамеченными, и архивироваться в течение установленного периода времени.

7.9 PA 09 – Предоставляет входные данные по безопасности

7.9.1 Область процесса

7.9.1.1 Краткое описание

Назначением области процесса «Предоставление входных данных по безопасности» является предоставление архитекторам, проектировщикам, конструкторам или пользователям системы нужной им информации о безопасности. Эта информация включает в себя архитектуру безопасности, проект или альтернативы внедрения безопасности и руководство по безопасности. Входные данные разрабатываются, анализируются, предоставляются и координируются соответствующими сотрудниками организации на основе требований безопасности, определенных в PA01.

7.9.1.2 Цели:

- все проблемы системы в отношении безопасности анализируются и решаются в соответствии с целями безопасности;
- все члены проектной группы имеют достаточное понятие о безопасности для выполнения своих функций;
- решение отражает представленные входные данные по безопасности.

7.9.1.3 Перечень базовых практик

BP.09.01 Используется проектировщиками, разработчиками и пользователями для обеспечения общего ознакомления причастных сторон с потребностями по вводу данных по безопасности.

BP.09.02 Определяет ограничения безопасности и соображения, необходимые для обоснованного выбора в области проектирования безопасности.

BP.09.03 Определяет альтернативные решения проблем проектирования, связанных с безопасностью.

BP.09.04 Анализирует альтернативы и назначает им приоритеты, используя связанные с безопасностью соображения и ограничения.

BP.09.05 Предоставляет руководство по обеспечению безопасности другим инженерно-техническим группам.

BP.09.06. Предоставляет руководство по обеспечению безопасности пользователям и администраторам автоматизированной системы.

7.9.1.4 Примечания к области процесса

Данная область процесса предоставляет входные данные по безопасности для поддержки действий по проектированию и реализации системы. Основное внимание уделяется тому, насколько безопасность является неотъемлемой частью разработки какой-либо системы, но это не является самоцелью. Каждая базовая практика использует входные данные самой проектной организации, выдает конкретные результаты, связанные с безопасностью, и передает эти результаты проектной организации. Установленные процессы применимы к разработке новых систем или к эксплуатации и обслуживанию имеющихся.

Данная область процесса включает в себя входные данные по безопасности, относящиеся как к разработке (для проектировщиков и конструкторов), так и эксплуатации (для пользователей и администраторов). Кроме того, объединение действий по обеспечению безопасности проектирования и реализации в одну область процесса подчеркивает, что эти действия в значительной степени идентичны, но находятся на разных уровнях абстракции. Область применения альтернативных решений распространяется как на архитектуру всей системы, так и на ее отдельные компоненты. Некоторые аспекты требований безопасности воздействуют скорее на среду, в которой разрабатывается система, чем на саму систему.

Все базовые практики в рамках этой области процесса могут быть повторяющимися и применяться в кратных точках по всему жизненному циклу системы.

При отслеживании выполнения этой области процесса анализ тенденций между различными базовыми практиками указывает на соответствие аргументу доверия (см. PA06).

7.9.2 BP.09.01 – Обеспечивает понимание требований к входным данным по безопасности

Используется проектировщиками, разработчиками и пользователями для обеспечения общего понимания соответствующими сторонами требований к входным данным по безопасности.

7.9.2.1 Описание

Проектирование безопасности координируется с другими дисциплинами для определения типов входных данных по безопасности, значимых для этих дисциплин.

Входные данные по безопасности включают в себя любой вид руководства, проектов, документов или идей, связанных с безопасностью, которые могут рассматриваться другими дисциплинами. Входные данные могут принимать различные формы, включая документы, памятные записки, электронную почту, обучение и консультирование.

Эти входные данные основаны на потребностях, определенных в PA10. Например, для специалистов по программному обеспечению может потребоваться разработка набора правил безопасности. Некоторые входные данные связаны скорее со средой, чем с системой.

7.9.2.2 Примеры результатов деятельности:

- согласование между проектированием и другими дисциплинами – определяет, как проектирование безопасности обеспечивает входные данные для других дисциплин (например, в форме документов, памятных записок, обучения и консультирования);
- описания требуемых входных данных – стандартные определения для каждого из механизмов предоставления входных данных по безопасности.

7.9.2.3 Примечания

Цели обеспечения доверия могут оказывать влияние на специфические потребности безопасности, особенно для таких факторов, как взаимозависимости. Эти цели также могут содержать дополнительное обоснование потребностей безопасности. В этом случае проектирование безопасности должно обеспечить другие дисциплины руководством по получению соответствующего свидетельства.

7.9.3 BP 09.02 – Определяет ограничения и соображения в области обеспечения безопасности

Определение ограничений и соображений в области обеспечения безопасности, требуемых для осуществления обоснованного выбора при проектировании.

7.9.3.1 Описание

Назначением этого практического приема является определение всех ограничений и соображений в области обеспечения безопасности, требуемых для осуществления обоснованного выбора при проектировании. Группа проектирования безопасности проводит анализ для определения любых ограничений и соображений в области обеспечения безопасности в отношении требований, проекта, реализации, конфигурации и документации. Ограничения могут определяться в любое время в течение жизненного цикла системы. Они могут определяться на многих различных уровнях абстракции. Следует отметить, что эти ограничения могут быть или позитивными (всегда применяются) или негативными (никогда не применяются).

7.9.3.2 Примеры результатов деятельности:

- критерии проектирования безопасности - ограничения и соображения в области обеспечения безопасности, необходимые для принятия решений в отношении общего системного проектирования или изделий;
- правила внедрения безопасности - ограничения и соображения в области обеспечения безопасности, применимые для реализации системы или продукта (например, применение специальных механизмов, стандартов кодирования);
- требования к документации – идентификация специальной документации, требуемой для поддержания требований безопасности (например, руководство для администратора, руководство для пользователя, специальная проектная документация).

7.9.3.3 Примечания

Эти ограничения и соображения используются для идентификации связанных с безопасностью альтернатив BP.09.03 и предоставления руководства по проектированию безопасности BP09.05. Основным источником ограничений и соображений являются относящиеся к безопасности требования, определенные в PA10.

7.9.4 BP.09.03 – Определяет альтернативы безопасности

Определение решений задач проектирования, связанных с безопасностью.

7.9.4.1 Описание

Назначением этой практики является определение альтернативных решений задач проектирования, связанных с безопасностью. Этот процесс является повторяющимся и пре-

образует связанные с безопасностью требования в их выполнение. Эти решения могут быть в виде, например, архитектуры, модели или прототипа. Эта практика включает в себя разбиение (декомпозицию), анализ и повторное составление связанных с безопасностью требований, пока не будут найдены эффективные альтернативные решения.

Примеры результатов деятельности:

- архитектура системы в отношении безопасности – описывает на абстрактном уровне взаимосвязи между ключевыми элементами архитектуры системы способом, удовлетворяющим требованиям безопасности;

- проектная документация по безопасности – включает в себя подробности об активах и потоке информации в системе, а также описание функций системы, которые реализуют безопасность или связаны с ней;

- модели безопасности – формальное представление политики безопасности, принятой в системе; оно должно определять совокупность правил и практических приемов, которые регулируют на то, как система управляет информацией, защищает и распределяет ее; иногда правила выражаются в точных математических терминах;

- архитектура системы – сосредоточена на аспектах безопасности архитектуры системы, описывающей принципы, основные концепции, функции и услуги, и то, как они связаны с безопасностью системы;

- анализ доверия (взаимосвязи и зависимости мер защиты) – описание того, как взаимодействуют и зависят друг от друга механизмы безопасности и услуги по ее обеспечению для обеспечения эффективности безопасности системы в целом; определяет те области, где могут потребоваться дополнительные меры безопасности.

7.9.4.3 Примечания

Альтернативы решений включают в себя решения по архитектуре, проекту и реализации. Эти связанные с безопасностью альтернативы должны согласовываться с ограничениями и соображениями, ранее определенными в BP.09.02. Альтернативы также являются частью компромиссных сравнений BP.09.04. Эта деятельность связана с предоставлением руководства по проектированию безопасности, поскольку после выбора предпочтительной альтернативы возникает потребность в руководстве для других дисциплин проектирования.

7.9.5 BP.09.04 – Анализирует варианты проектирования безопасности

Анализ альтернатив проектирования и назначение им приоритетов с помощью ограничений и соображений, касающихся безопасности.

7.9.5.1 Описание

Назначением этой практики является анализ альтернатив проектирования и назначение им приоритетов. Используя ограничения и соображения в области безопасности, ранее определенные в BP.09.02, специалисты по безопасности могут оценить каждую альтернативу проектирования и выдать рекомендацию инженерно-технической группе. Эти специалисты могут также рассмотреть возможность предоставления руководства по проектированию для других инженерно-технических групп.

Эти альтернативы проектирования не ограничиваются альтернативами безопасности, определенными в BP.09.02, а могут также включать в себя альтернативы из других дисциплин.

7.9.5.2 Примеры результатов деятельности:

- результаты изучения компромиссов и рекомендации – включает в себя анализ всех альтернатив проектирования с учетом ограничений и соображений в области безопасности, представленных в BP.09.02;

- результаты комплексного изучения компромиссов – результаты принятия различных решений, принятых в течение жизненного цикла продукта, системы или процесса, уделяя особое внимание областям, где требования безопасности могли быть снижены для выполнения других целей (например, стоимость, функциональные возможности).

7.9.5.3 Примечания

Отсутствуют.

7.9.6 BP.09.05 – Предоставляет руководство по проектированию безопасности

Предоставляет руководство по обеспечению безопасности инженерно-техническим группам

7.9.6.1 Описание

Назначением этой базовой практики является разработка связанного с безопасностью руководства и предоставление его инженерно-техническим группам. Руководство по проектированию безопасности используется инженерно-техническими группами для принятия решений о выборе архитектуры, проекта и реализации системы.

7.9.6.2 Примеры результатов деятельности:

- рекомендации по архитектуре – определяют принципы и ограничения, которые будут содействовать разработке архитектуры системы, отвечающей требованиям безопасности;

- рекомендации по проекту - определяет принципы и ограничения, управляющие системным проектированием;

- рекомендации по реализации - определяют принципы и ограничения, управляющие реализацией системы;

- рекомендации по архитектуре безопасности – определяют принципы и ограничения, которые определяют свойства безопасности системы;

- основные принципы защиты – высокоуровневое описание способа обеспечения безопасности, включая автоматизированные, физические и административные механизмы и персонал;

- принципы, стандарты проектирования – ограничения пути системного проектирования (например, наименьший уровень привилегий, изоляция средств обеспечения безопасности;

- стандарты кодирования – ограничения по реализации системы.

7.9.6.3 Примечания

Объем требуемого руководства и степень детализации зависят от знания, опыта или осведомленности других инженерно-технических работников в области безопасности. Во многих случаях большая часть руководства может относиться скорее к среде разработки, чем к разрабатываемой системе.

7.9.7 BP.09.06 - Предоставляет руководство по безопасности

Предоставление руководства по безопасности пользователям и администраторам автоматизированной системы.

7.9.7.1 Описание

Назначением этой практики является разработка связанного с безопасностью руководства и представление его пользователям и администраторам системы. В этом руководстве пользователям и администраторам сообщается, что необходимо сделать для безопасной установки, конфигурирования, эксплуатации системы и вывода ее из эксплуатации. Для реализации этой возможности разработку руководства по безопасности следует начинать в самом начале жизненного цикла системы безопасности.

7.9.7.2 Примеры результатов деятельности:

- руководство для администратора – описание функций администратора и привилегий при безопасной установке, конфигурирования, эксплуатации системы и вывода ее из эксплуатации;

- руководство для пользователя – описание механизмов обеспечения безопасности, предоставляемых системой, и инструкции по их применению;

- профиль безопасности – среда безопасности (угрозы, политика организации), цели обеспечения безопасности (противодействие угрозам), функциональные требования и требования доверия к безопасности; обоснование того, что системы, разработанные по этим требованиям, отвечают поставленным целям;

- инструкции по конфигурированию систем - инструкции по конфигурированию системы для обеспечения соответствия ее функционирования целям безопасности.

7.9.7.3 Примечания

При разработке систем среда разработки считается средой эксплуатации.

7.10 PA10 – Определяет требования безопасности

7.10 Область процесса

7.10.1.1 Краткое описание

Назначением практики "Определение требований безопасности" является однозначное определение требований, связанных с безопасностью системы. Область процесса "Определение потребностей в безопасности" включает определение основы безопасности в системе, с целью обеспечения соответствия всем правовым требованиям и требованиям политики и организации к безопасности. Эти требования изменяются в соответствии с существующими условиями безопасности системы, средой безопасности системы организации и комплекса целей обеспечения безопасности. Для системы определен набор связанных с безопасностью требований, который становится основой проектирования безопасности в рамках системы.

7.10.1.2 Цели

Обеспечение общего понимания требований безопасности всеми сторонами, включая заказчика.

7.10.1.3 Перечень базовых практик

BP.10.01 обеспечивает понимание требований заказчика к безопасности.

BP.10.02 определяет законы, политики, стандарты, внешние воздействия и ограничения, обуславливающие функционирование системы.

BP.10.03 определяет назначение системы с целью определения контекста безопасности.

BP.10.04 обеспечивает ориентированное на безопасность высокоуровневое представление о функционировании системы.

BP.10.05 представляет высокоуровневые цели, определяющие безопасность системы.

BP.10.06 определяет набор согласованных формулировок, определяющих защиту, которую надо реализовать в системе.

BP.10.07 получает согласие о том, что установленные требования безопасности удовлетворяют требованиям заказчика.

7.10.1.4 Примечания к области процесса

Эта область процесса охватывает действия, определяющие все аспекты безопасности информационной системы в целом (например, физический, функциональный, процедурный). Базовые практики учитывают то, как определяются и сочетаются потребности в безопасности с совокупностью требований, связанных с безопасностью, которые используются в проектировании, разработке, верификации, функционировании и обслуживании системы. В большинстве случаев необходимо принимать во внимание существующую среду и связанные с ней потребности в безопасности. Полученная и произведенная этой областью процесса информация собирается, уточняется, используется и корректируется в течение всего проекта (особенно в PA09) с целью обеспечения рассмотрения потребностей заказчика.

При отслеживании функционирования этой области процесса анализ тенденций между различными базовыми практиками может показать, удовлетворен ли аргумент доверия (см. PA06).

7.10.2 BP.10.01 – Обеспечивает понимание потребностей заказчика в обеспечении безопасности

Обеспечение понимания потребностей заказчика в безопасности.

7.10.2.1 Описание

Назначением этой практики является сбор информации, необходимой для полного понимания потребностей заказчика в безопасности. На эти потребности оказывает влияние важность риска безопасности для заказчика. Целевая среда, в которой должна функционировать система, также влияет на потребности заказчика в отношении безопасности.

7.10.2.2 Примеры результатов деятельности:

- формулировка потребностей заказчика в обеспечении безопасности - описание защиты, требуемой заказчиком.

7.10.2.3 Примечания

Термин «заказчик» часто относится к конкретному получателю продукта, системы или услуги или к гипотетическому получателю, определенному на основании изучения рынка или предназначения продукта. Может понадобиться идентификация разных групп заказчиков и проведение различий между ними. Например, у обычных пользователей могут быть потребности, отличные от потребностей администраторов.

7.10.3 BP.10.02 – Определяет применимые законы, политики и ограничения

Определяет законы, политики, стандарты, внешние воздействия и ограничения, обусловливающие работу системы.

7.10.3 1 Описание

Назначением этой практики является обобщение всех воздействий, оказывающих влияние на безопасность системы. При определении применимости идентифицируются законы, положения, политики и торговые стандарты, управляющие целевой средой системы. Необходимо определить приоритет между глобальными и локальными политиками. Требования безопасности, предъявляемые к системе ее заказчиком, должны быть определены, а их последствия для безопасности - выделены отдельно.

7.10.3.2 Примеры результатов деятельности:

- ограничения безопасности – законы, положения, политики и другие ограничения, влияющие на безопасность системы;
- профиль безопасности – среда безопасности (угрозы, политика организации), цели обеспечения безопасности (например, противодействие угрозам); функциональные требования и требования доверия к безопасности; обоснование соответствия систем, разработанных по этим требованиям, поставленным целям.

7.10.3.3 Примечания

Требуется особое внимание при пересечении системой множественных физических областей. Существует возможность возникновения конфликта между законами и положениями, приемлемыми для

разных стран и разных видов деловой деятельности. В качестве области процесса идентификации конфликты должны быть определены, сведены к минимуму и по возможности разрешены.

7.10.4 BP.10.03 – Определяет контекст безопасности системы

Определение назначения системы с целью определения контекста безопасности.

7.10.4.1 Описание

Назначением этой практики является определение степени воздействия среды системы на безопасность. Это подразумевает понимание назначения системы (например, интеллектуальная, финансовая, медицинская). Сценарии выполнения заданий и операций оцениваются из соображений безопасности. На этом этапе требуется высокоуровневое понимание угрозы, которой может подвергаться система. Эксплуатационные и функциональные требования оцениваются на предмет возможных воздействий на безопасность. Также анализируются эксплуатационные ограничения, с точки зрения их последствий для состояния безопасности.

Среда может также включать в себя средства сопряжения с другими организациями и системами с целью определения периметра безопасности системы. Определяется местонахождение элементов средств сопряжения внутри периметра безопасности или за его пределами.

Многие факторы, являющиеся внешними для организации, тоже в разной степени влияют на потребности организации в обеспечении безопасности. Эти факторы включают политическую ориентацию и ее изменения, разработки технологий, экономические влияния, глобальные события и действия по ведению информационной войны. Поскольку ни один из этих факторов не является статичным, они требуют мониторинга и периодической оценки потенциального воздействия их изменений.

7.10.4.2 Примеры результатов деятельности:

- среда ожидаемой угрозы – любые известные или предполагаемые угрозы активам систем, нуждающимся в защите; включает в себя носителя угрозы (квалификация, имеющиеся ресурсы, мотивация), атаку (метод, используемые уязвимости, благоприятные возможности), актив;
- цель оценки – описание системы или продукта, чьи свойства безопасности подлежат оценке (тип, предполагаемое применение, основные свойства, ограничения по применению).

7.10.4.3 Примечания

Периметр безопасности системы необязательно идентичен границам системы (например, периметр безопасности может содержать помещение, в котором находится система и работающий с ней персонал, тогда как границы системы могут проходить по человеко-машинному интерфейсу). Этот расширенный периметр безопасности позволяет рассматривать физические меры как эффективные защитные меры для управления доступом в дополнение к чисто техническим мерам.

7.10.5 BP.10.04 – Фиксирует ориентированное на безопасность представление о функционировании системы

Фиксация ориентированного на высокоуровневую безопасность представления о функционировании системы.

7.10.5.1 Описание

Назначением этой практики является разработка ориентированного на высокоуровневую безопасность представления о предприятии, включая роли, обязанности, информационный поток, активы, защиту персонала и физическую защиту. Данное описание должно включать обсуждение возможности управления предприятием в рамках ограничений требований системы. Этот взгляд на систему обычно предусматривается в концепции обеспечения безопасности операций и должен включать представление об архитектуре, процедурах и среде системы, ориентированное на высокоуровневую безопасность.

. На этом этапе также фиксируются требования, связанные со средой разработки системы.

7.10.5.2 Примеры результатов деятельности:

- концепция обеспечения безопасности операций - ориентированное на высокоуровневую безопасность представление системы (роли, обязанности, активы, информационный поток, процедуры);
- концептуальная архитектура безопасности - концептуальное представление архитектуры безопасности (см. BP.09.03).

7.10.5.3 Примечания

Отсутствуют.

7.10.6 BP.10.05 – Фиксирует высокоуровневые цели обеспечения безопасности

Фиксация высокоуровневых целей, определяющих безопасность системы.

7.10.6.1 Описание

Назначением этой практики является определение целей, которые должны выполняться для обеспечения адекватной безопасности системы в ее среде эксплуатации.

7.10.6.2 Примеры результатов деятельности:

- политика безопасности функционирования/среды эксплуатации – правила, указания и практические приемы, руководящие управлением, защитой и распределением активов в рамках организации и за ее пределами;

- политика безопасности системы - правила, указания и практические приемы, руководящие управлением, защитой и распределением активов в системе или продукте.

7.10.6.3 Примечания

Цели безопасности по возможности не должны зависеть от какого-либо конкретного ее внедрения. Если имеются какие-либо конкретные ограничения из-за существующей среды, их следует рассматривать в PA09, когда определяются ограничения и соображения по информированному выбору проектирования. Цели безопасности должны, как минимум, учитывать доступность, подотчетность, аутентичность, конфиденциальность, целостность и требования к надежности системы и информации.

7.10.7 BP.10.06 – Определяет связанные с безопасностью требования

Определяет последовательный набор требований, определяющих защиту, предназначенную для внедрения в систему.

7.10.7.1 Описание

Назначением этой практики является определение требований к системе, связанных с безопасностью. Практика должна обеспечивать согласованность каждого требования с применяемой политикой, правовыми нормами, стандартами, требованиями безопасности и ограничениями системы. Эти требования должны полностью определять потребности системы в безопасности, включая требования, представляемые нетехническими средствами. Обычно для изучения всех аспектов необходимо определить или обозначить логические или физические границы целевой задачи. Требования должны соответствовать целям системы или быть связаны с ней. Обеспечение безопасности должно, по возможности, минимизировать любое воздействие на характеристики и функциональные возможности системы. Связанные с безопасностью требования должны обеспечивать основу для оценки безопасности системы в ее целевой среде.

7.10.7.2 Примеры результатов деятельности:

- связанные с безопасностью требования - требования, оказывающие непосредственное воздействие на безопасное функционирование системы и обеспечивающие соответствие установленной политике;

- таблица прослеживаемости – отображение соответствия потребностей в безопасности требованиям, решениям (например, по архитектуре, проекту, реализации), тестам и результатам тестов.

7.10.7.3 Примечания

Многие требования применимы к многочисленным дисциплинам, поэтому лишь несколько требований связаны исключительно с безопасностью. Следовательно, для этой области процесса требуется большая степень координации с другими дисциплинами для получения именно того, что является требованиями системы. Действия, связанные с этой взаимосвязью, описаны в PA07.

7.10.8 BP.10.07 – Заключает соглашение по безопасности

Заключение соглашения о согласовании установленных требований безопасности с потребностями заказчика.

7.10.8.1 Описание

Назначением этой практики является достижение согласия между заинтересованными сторонами по требованиям безопасности. В случаях с обобщенной группой заказчиков вместо одного заказчика требования должны соответствовать совокупности целей. Установленные требования безопасности должны быть полным и последовательным отражением управления политикой, правовых норм и потребностей заказчика. Проблемы необходимо определить и проработать до получения согласия сторон.

7.10.8.2 Примеры результатов деятельности:

- утвержденные цели обеспечения безопасности – сформулированное намерение противодействовать идентифицированным угрозам и/или следовать установленным политикам безопасности (утвержденным заказчиком);

- основа связанных с безопасностью требований – минимальный набор связанных с безопасностью требований, согласованных всеми сторонами-участниками (в частности с заказчиком) в качестве установленных контрольных точек.

7.10.8.3 Примечания

Важно обеспечить реальное понимание всеми заинтересованными сторонами того, о чем было достигнуто соглашение, и это понимание является одинаковым для всех. Особая осторожность требуется для обеспечения идентичности содержания (смысла) требований безопасности для всех участников процесса.

7.11 PA11 – Верифицирует и проверяет достоверность безопасности

7.11.1 Область процесса

7.11.1.1 Краткое описание

Назначение области процесса «Верификация и проверка достоверности безопасности» является обеспечение верификации и проверки достоверности решений в отношении безопасности. Решения верифицируются, исходя из требований безопасности, архитектуры и проекта, посредством наблюдения, демонстрации, анализа и тестирования. Достоверность решений проверяется исходя из оперативных потребностей заказчика в безопасности.

7.11.1.2 Цели:

- решения удовлетворяют требованиям безопасности;
- решения удовлетворяют потребностям заказчика в безопасности.

7.11.1.3 Перечень базовых практик

BP.11.01 Определяет решение для его верификации и подтверждения.

BP.11.02 Определяет метод и уровень строгости верификации и проверки достоверности каждого решения.

BP.11.03 Проверяет, выполняет ли решение требования, связанные с более высоким уровнем абстракции.

BP.11.04 Проверяет достоверность решения, показывая, что оно удовлетворяет потребностям, связанным с предыдущим уровнем абстракции, и в конечном счете, удовлетворяет потребностям заказчика в безопасности.

BP.11.05 Собирает результаты верификации и проверки достоверности для других инженерно-технических групп.

7.11.1.4 Примечания к области процесса

Данная область процесса является важной частью верификации и проверки достоверности системы и присутствует на всех уровнях абстракции. Архитектуры и проекты безопасности обычно имеют иерархическую структуру, где каждый последующий уровень содержит больше деталей о проекте, чем предыдущий. Решения включают в себя все - от оперативных концепций до архитектур и реализации, и охватывают всю информационную систему, включая среду и процедуры.

В интересах получения объективных результатов группа верификации и проверки достоверности должна работать отдельно от инженерно-технических групп; однако она может тесно сотрудничать с ними. Результаты верификации и проверки достоверности могут передаваться инженерно-техническим группам в любое время в ходе жизненного цикла решения. Верификация и проверка достоверности иногда связаны с понятиями правильности и эффективности.

При отслеживании функционирования этой области процесса анализ тенденций между различными базовыми практиками может показать, удовлетворен ли аргумент доверия (см. PA06).

7.11.2 BP.11.01 – Определяет цели верификации и проверки достоверности

Определяет решение для его верификации и проверки достоверности.

7.11.2.1 Описание

Назначением этой практики является определение целей верификации и проверки достоверности. Верификация дает оценку правильность реализации решения, тогда как проверка достоверности демонстрирует эффективности решения. При этом подразумевается координация действий всех инженерно-технических групп в течение всего жизненного цикла.

7.11.2.2 Примеры результатов деятельности:

- планы верификации и проверки достоверности – определение действий по верификации и проверке достоверности (включает в себя предназначенные для верификации и проверки достоверности ресурсы, график выполнения и результаты какой-либо деятельности).

7.11.2.3 Примечания

Значительная часть продукции может верифицироваться и проверяться на достоверность в широком диапазоне абстракции и сложности. Это подразумевает требования, проекты, архитектуры, реализацию, элементы аппаратных средств и программного обеспечения и планы испытаний. Рабочая продукция, связанная с эксплуатацией и обслуживанием системы, также может верифицироваться и проверяться на достоверность, включая конфигурацию системы, пользовательскую документацию, учебные материалы и планы реагирования на инциденты.

7.11.3 BP.11.02 – Определяет метод верификации и проверки достоверности

Определение метода и уровеня строгости верификации и проверки достоверности каждого решения.

7.11.3.1 Описание

Назначением этой практики является определение уровня строгости и метода верификации и проверки достоверности каждого решения. Определение метода включает в себя выбор способа верификации и проверки достоверности каждого требования. Уровень строгости должен указывать, насколько тщательными должны быть верификация и проверка достоверности, и связана с результатами проведения стратегии обеспечения доверия из PA06. Например, для некоторых проектов для проверки соответствия требованиям может быть достаточно беглой проверки, а для других потребоваться более строгая проверка.

Эта методика может также включать в себя средство поддержки отслеживаемости от оперативных потребностей заказчика в безопасности до требований безопасности, принятия решений, проверки достоверности и результатов этой проверки.

7.11.3.2 Примеры результатов деятельности:

- планы испытаний, анализа, демонстрации и наблюдения – определение предполагаемых методов верификации и проверки достоверности (например, тестирование, анализ) и уровня строгости (например, формальность или неформальность методов);
- методика испытаний – определение этапов проведения тестирования каждого решения;
- метод отслеживаемости – описание способа отслеживаемости результатов верификации и проверки достоверности до потребностей заказчика и требований безопасности.

7.11.3.3 Примечания

Метод верификации и проверки достоверности безопасности должен быть совместим с методом верификации и проверки достоверности всей системы. Для этого требуется значительная степень координации и взаимодействия. Связанные с координацией действия описаны в PA07.

7.11.4 BP.11.03 - Проводит верификацию

Верификация выполнения предпринятым действиям требований, связанных с более высоким уровнем абстракции.

7.11.4.1 Описание

Назначением этой практики является верификация правильности решения о необходимых действиях демонстрацией выполнения этим решением требований, связанных с более высоким уровнем абстракции, включая требования доверия, определенные как результат PA06. Существует много методов верификации требований, включая тестирование, анализ, наблюдение и демонстрацию. Предназначенный к применению метод определен в BP.11.02. Проверяются как отдельные требования, так и требования системы в целом.

7.11.4.2 Примеры результатов деятельности:

- необработанные данные тестов, анализа, демонстрации и наблюдения – результаты применения всех методов верификации соответствия решения требованиям;
- сообщения о проблемах – несоответствия, обнаруженные при верификации соответствия решения требованиям.

7.11.4.3 Примечания

Отсутствуют.

7.11.5 BP.11.04 – Проводит проверку достоверности

Проверка достоверности решения путем демонстрации соответствия решения требованиям, связанным с более высоким уровнем абстракции, в конечном счете, удовлетворяя потребности заказчика в безопасности.

7.11.5.1 Описание

Назначением этой практики является проверка достоверности соответствия решения потребностям, связанным с более высоким уровнем абстракции. Проверка достоверности демонстрирует эффективность соответствия решения этим потребностям. Существует много путей проверки достоверности соответствия этим требованиям, включая тестирование решения в эксплуатационной или демонстрационной среде. Предполагаемый к применению метод определен в ВР.11.02.

7.11.5.2 Примеры результатов деятельности:

- сообщения о проблемах – несоответствия, обнаруженные при верификации соответствия решения требованиям;
- несоответствия – области, где решение не соответствует потребностям в безопасности;
- неэффективные решения – решения, не удовлетворяющие потребностям заказчика в безопасности.

7.11.5.3 Примечания

Эта практика связана с отслеживаемостью.

7.11.6 ВР.11.05 – Предоставляет результаты верификации и проверки достоверности

Обобщение результатов верификации и проверки достоверности для инженерно-технических групп.

7.11.6.1 Описание

Назначением этой практики является сбор и представление результатов верификации и проверки достоверности. Эти результаты должны представляться простым и понятным способом. Результаты необходимо прослеживать, чтобы не утратить способности отслеживаемости от потребностей к требованиям, решению и результатам испытаний.

7.11.6.2 Примеры результатов деятельности:

- результаты испытаний - документация с выходными данными тестирования;
- таблица отслеживаемости - отображение соответствия потребностей в безопасности требованиям, решениям (например, по архитектуре, проекту, реализации), тестам и результатам тестов.

7.11.6.3 Примечания

Отсутствуют.

Приложение А
(справочное)

Общие практики

Общие практики определены в ИСО/МЭК 15504-2:2003. Первоначальное содержание этого приложения было перенесено в новое приложение D, которое тоже является справочным. Оно сохранено в целях обратной совместимости.

Приложение В
(справочное)

Базовые практики для областей процесса «Проект» и «Организация»

В.1 Общая часть

Модель SSE-CMM® включает в себя области процесса «Проект» и «Организация», заимствованные из модели SE-CMM®). Эти области процесса являются важными элементами SSE-CMM® и играют важную роль в интерпретации общих практик.

Каждая область процесса включает в себя раздел «Соображения по вопросам безопасности», в котором представлены некоторые соображения по применению этой части в среде проектирования безопасности. В данном разделе также даются ссылки, связанные с областями процессов модели SSE-CMM.

В.2 Общие соображения по вопросам безопасности

Кроме конкретных соображений в таблице интерпретации по каждой области процесса в последующие разделы включены общие соображения по проектированию безопасности для всех областей процесса «Проект» и «Организация».

В.2.1 Проектный риск в сравнении с риском безопасности

В областях процесса «Проект» и «Организация» используется термин «риск». В этих случаях ссылка на «проектный риск» означает риск, связанный с успешным выполнением проекта с учетом вопросов, относящихся к расходам и графику выполнения. Области процесса проектирования безопасности системы рассматривают действия с «риском безопасности» как определение допустимости эксплуатационных воздействий, являющихся следствием остаточных рисков безопасности. Результаты оценок рисков безопасности могут обеспечить входные данные для действий, связанных с проектными рисками, и влиять на них, хотя области процесса «Проект» и «Организация» не учитывают менеджмент рисков безопасности, ссылка на который имеется в области процесса «Проектирование».

В.2.2 Применимость к этапу эксплуатации

Хотя формулировка «Проект» и «Организация» областей процесса кажутся применимыми только к разработке, они равным образом применимы и к этапу эксплуатации и поддержания жизненного цикла. В целях улучшения или оценки эти области процесса следует интерпретировать на основе перспективы их применимости для организации. В области «соображения по вопросам безопасности» отмечены несколько исключений.

В.2.3 Проектирование безопасности в сравнении с системным проектированием

Термин « системное проектирование « применяется на всем протяжении областей процесса «Проект» и «Организация» (например, «Улучшает процессы системного проектирования организации»). Эти области процесса повсеместно находят широкое применение. Когда области процесса используются в контексте проектирования безопасности, термин «системное проектирование» следует заменить на термин «проектирование безопасности». В областях процесса следует также учитывать перспективы проектирования безопасности путем проведения интеграции этих мер в другие инженерные дисциплины.

В.2.4 Взаимосвязи при проектировании

Взаимосвязь между системным проектированием и проектированием безопасности указана для каждой области процесса. Следует отметить большое число взаимосвязей между различными областями процессов (в этих разделах указаны только основные взаимосвязи).

В.3 PA12 – Обеспечивает качество

В.3.1 Область процесса

B.3.1.1 Соображения безопасности

Область процесса PA06 связана с обеспечением качества. Доверие можно считать специфическим типом качества, связанным с безопасностью.

B.3.1.2 Краткое описание

Назначением области процесса « Обеспечение качества» является рассмотрение не только качества системы, но и качества процесса, используемого для формирования системы, и степени, в которой проект следует заданному процессу. Основная концепция этой области процесса заключается в том, что высококачественные системы можно получить только при условии наличия процесса постоянного измерения и улучшения качества. Кроме того, этот процесс надо поддерживать в течение всего жизненного цикла. Ключевыми аспектами процесса, требуемого для разработки высококачественных систем, являются измерение, анализ и корректирующие действия.

B.3.1.3 Цели:

- определение и измерение качества процесса;
- получение ожидаемого качества рабочего продукта.

B.3.1.4 Перечень базовых практик

Последующий перечень содержит следующие базовые практики, являющиеся неотъемлемыми элементами качественного системного проектирования:

BP.12.01 - определяет требования к качеству каждого рабочего продукта.

BP.12.02 - обеспечивает следование процессу системного проектирования во время жизненного цикла.

BP.12.03 - оценивает меры измерения качества рабочего продукта в сравнении с требованиями к качеству этого продукта.

BP.12.04 - определяет качество процесса системного проектирования, используемого в проекте.

BP.12.05 - анализирует измерения качества для разработки рекомендаций по повышению качества или соответствующим корректирующим действиям.

BP.12.06 - обеспечивает участие работников в идентификации проблем с качеством и сообщение о них.

BP.12.07 - инициирует действия в отношении идентифицированных проблем с качеством и возможностей повышения качества.

BP.12.08 - создает механизм или группу механизмов для выявления потребности в корректирующих действиях в отношении процессов и продукции.

B.3.1.5 Примечания к области процесса.

Успешная программа обеспечения качества требует интеграции усилий всех членов проектной группы и вспомогательных подразделений. Эффективные процессы являются механизмом обеспечения качества и уменьшения зависимости от проверок готовых продуктов и доработок.

Это не означает, что лица, управляющие качеством рабочих продуктов и процессов и/или его обеспечивающие, полностью ответственны за качество готовых результатов деятельности. Напротив, основная ответственность за «создание» качества лежит на его создателях. Процесс менеджмента качества помогает обеспечивать серьезное изучение всех его аспектов и воздействие на них со стороны организации, а также их отражение в ее продукции. Это повышает уверенность разработчиков, руководства и заказчиков в качестве системы.

Типы отклонений от качества, которые могут рассматриваться в этой области процесса, могут включать в себя техническое содержание, например, такое как определенные значения производных или распределенных требований, и проблемы оформления (например, предпочитает ли заказчик инструкции по применению изделия в печатном или электронном виде). Расходы выше запланированных и отставания от графика тоже могут считаться дефектами и требуют внимания.

Организации могут пожелать определить отклонения от ожидаемых значений технических и других вопросов в приращениях, соответствующих обязательствам организации по графику (например, если организация обязалась поставлять или производить какой-либо продукт в течение данной недели, то целесообразно измерять или определять ее достижения путем еженедельного измерения отклонений от графика).

При прослеживании функционирования этой области процесса анализ тенденций, существующих среди различных базовых практик, может указать на соответствие аргументу доверия (см. PA06).

Тема и содержание области процесса 12 «Обеспечение качества» рассматриваются в разделе «Процесс управления проектом» ИСО/МЭК 15288:2002.

B.3.2 BP.12.01 – Определяет требования к качеству рабочей продукции

Определение требований к качеству каждого рабочего продукта.

B.3.2.1 Описание

Для различных типов рабочей продукции и разных конкретных рабочих продуктов могут предъявляться различные требования к качеству. Эти требования должны идентифицироваться при определении рабочего продукта.

B.3.2.2 Примеры результатов деятельности:

- требования к качеству рабочей продукции;
- перечни общих требований к качеству рабочей продукции.

B.3.2.3 Примечания

Отсутствуют.

B.3.3 BP.12.02 – Осуществляет мониторинг соответствия заданному процессу

Обеспечение следования заданному процессу системного проектирования во время жизненного цикла системы.

B.3.3.1 Описание

Обеспечивает выполнение проекта в соответствии с процессом системного проектирования. Соответствие должно проверяться через регулярные промежутки времени. Отклонения от заданного процесса и воздействие каждого отклонения должны оцениваться и фиксироваться.

B.3.3.2 Примеры результатов деятельности:

- зафиксированные отклонения от заданного процесса системного проектирования;
- зафиксированное воздействие отклонений от заданного процесса системного проектирования;
- справочник по качеству (на бумаге или электронный).

B.3.3.3 Примечания

Мониторинг заданного процесса можно проводить несколькими способами (например, назначенный аудитор/наблюдатель может участвовать во всех действиях процесса (или их выборочном проценте) или наблюдать за ними или он может проверять все рабочие продукты (или их выборочные партии) в процессе их производства).

B.3.4 BP.12.03 – Измеряет качества рабочего продукта

Оценка мер измерения качества рабочего продукта и проведение их сравнения с требованиями к его качеству.

B.3.4.1 Описание

Измерение характеристик рабочего продукта, связанных с соответствием требованиям и стандартам, правильностью и своевременностью, служит показателем качества системы. Измерения должны оценивать соответствие рабочего продукта требованиям проектирования заказчика и техническим требованиям. Измерения продукта должны также способствовать изолированию проблем процесса разработки системы.

B.3.4.2 Примеры результатов деятельности:

- оценка качества продукта;
- сертификация качества продукта.

B.3.4.3 Примечания

Примеры методов измерения качества рабочего продукта включают в себя:
- статистическое управление процессом измерения продукта в различных точках процесса разработки;
- измерение полной совокупности результатов процесса и сравнение с такими требованиями, как:
1) значение спецификации,
2) запланированное значение,
3) поле допуска,
4) продемонстрированное значение,
5) продемонстрированное техническое отклонение,
6) текущая оценка,
7) расчетное техническое отклонение.

B.3.5 BP.12.04 – Измеряет качество процесса

Измерение качества процесса системного проектирования, используемого проектом.

B.3.5.1 Описание

Процесс, используемый для создания качественной продукции, имеет такое же значение, как и качество продукта. Важно иметь процесс разработки системы, проверяемый измерением, чтобы можно было идентифицировать признаки ухудшения заранее, до завершения производства конечного рабочего продукта, когда выявляется его несоответствие требованиям. Таким образом, наличие измеряемого процесса может привести к уменьшению отходов производства и повышению производительности.

B.3.5.2 Примеры результатов деятельности:

- сертификация качества процесса.

B.3.5.3 Примечания

Примеры инструментария, предназначенного для измерения процесса, включают в себя:
- схему технологического процесса: может использоваться для определения предназначенных для измерения характеристик и идентификации потенциальных источников отклонения в дополнение к определению процесса;
- статистическое управление параметрами процесса;
- проектирование экспериментов.

B.3.6 BP.12.05 – Анализирует измерения качества

Проведение анализа качества посредством измерений с целью разработки рекомендаций по повышению качества или при необходимости корректирующих действий.

B.3.6.1 Описание

Тщательная проверка всех имеющихся данных о продукции, процессе и выполнении проекта может выявить причины проблем. В последствии эта информация будет способствовать усовершенствованию процесса и повышению качества продукта.

B.3.6.2 Примеры результатов деятельности:

- анализ отклонений;

- анализ отказов;
- отчеты о дефектах;
- тенденции в области качества системы;
- рекомендации по корректирующим действиям;
- графики (диаграммы) причин и следствия.

B.3.6.3 Примечания

Примеры измерений, способствующих повышению качества, включают в себя:
- анализ тенденций, таких как определение проблем калибровки (настройки) оборудования, приводящих к постепенному изменению параметров продукта;
- оценка стандартов на предмет продолжения применения конкретных стандартов после изменения технологии или процесса.

B.3.7 BP.12.06 - Обеспечивает участие

Обеспечение участия работников в выявлении проблем с качеством и сообщении о них.

B.3.7.1 Описание

Разработка рабочего продукта высокого качества с помощью обязательного процесса обеспечения качества требует сосредоточения и внимания всего участвующего в процессе персонала. Следует поощрять идеи по повышению качества и проводить совещания, позволяющие каждому сотруднику свободно поднимать вопросы по качеству.

B.3.7.2 Примеры результатов деятельности:

- условия стимулирования качества;
- собранные входные данные и предложения сотрудников.

B.3.7.3 Примечания

Среда качества может создаваться:
- группами, работающими с процессом;
- группой обеспечения качества с цепью информирующих инстанций, независимых от проекта;
- независимый канал сообщений о проблемах с качеством.

B.3.8 BP.12.08 – Инициирует действия по повышению качества

Инициирование действий, связанных с выявленными проблемами с качеством и возможностями повышения качества.

B.3.8.1 Описание

Для постоянного улучшения качества необходимо планировать и осуществлять определенные действия. Следует идентифицировать и корректировать некоторые аспекты процесса разработки системы, что включает в себя минимизацию громоздких или бюрократических систем.

B.3.8.2 Примеры результатов деятельности:

- рекомендации по улучшению процесса системного проектирования;
- план по повышению качества;
- модифицированные варианты процесса.

B.3.8.3 Примечания

Для эффективной реализации действий по повышению качества необходимы входные данные и согласие группы разработчиков продукта.

B.3.9 BP.12.08 – Выявляет потребности в корректирующих действиях

Установление механизма или набора механизмов для выявления потребности процессов или продуктов в корректирующих действиях.

B.3.9.1 Описание

Такой механизм должен быть доступен в течение жизненного цикла продукта (от разработки до производства и использования заказчиком). Механизмы могут включать в себя онлайновые системы передачи информации, семинары, периодические проверки, группы по работе с заказчиком и т.д.

B.3.9.2 Примеры результатов деятельности:

- действующая база данных или архив, содержащие установленные потребности и улучшения процесса и продукта;
- четко прописанные процессы, методы и способы введения установленных потребностей в базу данных или архив;
- установленные потребности в улучшении процесса;
- установленные потребности в улучшении продукта;
- отчет о неисправностях.

B.3.9.3 Примечания

Данная базовая практика является критичной для обеспечения эффективного использования системного проектирования на этапах производства, эксплуатации и обслуживания жизненного цикла.

Этой базовой практикой определяются потребности в корректирующих действиях. Корректирующие действия см. в PA15.

Отчеты о неисправностях также используются этой базовой практикой из PA11.

B.4 PA – Управляет конфигурацией

B.4.1 Область процесса

B.4.1.1 Соображения безопасности

В BP.13.02 в определении уровня элементов конфигурации, идентифицированных для системы/проекта, должна учитываться степень детализации, требуемая для целей обеспечения доверия в PA06.

Область процесса «Управление конфигурацией» представляет доказательство для PA01. Выбранная система управления конфигурацией также должна управляться в соответствии с PA01.

B.4.1.2 Краткое описание

Назначением области процесса «Управление конфигурацией» является сохранение данных об идентифицированных элементах конфигурации и их состоянии, а также анализ изменений в системе и элементах ее конфигурации и управление этими изменениями. Управление конфигурацией системы включает в себя представление точных и современных данных о конфигурациях и их состоянии для разработчиков и заказчиков.

Эта область процесса применима ко всем рабочим продуктам, находящимся под управлением конфигурацией. Примерный набор результатов деятельности, которые можно передать под управление конфигурацией, может включать в себя элементы конфигурации программного обеспечения, логическое обоснование проекта, требования, файлы данных о продукте или исследования коммерческой деятельности.

B.4.1.3 Цели:

- поддержание контроля над конфигурациями рабочего продукта.

B.4.1.4 Перечень базовых практик

В приведенном ниже перечне содержатся базовые практики, являющиеся существенными элементами качественного системного проектирования:

BP.13.01 принимает решение о соответствующем методе управления конфигурацией.

BP.13.02 идентифицирует неделимые элементы управления конфигурацией.

BP.13.03 поддерживает архив баз данных рабочей продукции.

BP.13.04 управляет изменениями в установленных элементах конфигурации.

BP.13.05 сообщает состояние данных о конфигурации, предлагаемых изменениях и информацию о доступе причастным группам.

B.4.1.5 Примечания к данной области процесса

Функция управления конфигурацией способствует отслеживаемости, позволяя прослеживать обратно через иерархию требований любой системы в любую точку жизненного цикла конфигурирования. Отслеживаемость признана частью практик в PA10.

В случае использования практик этой области процесса для управления требованиями, об изменениях в этих требованиях следует сообщать заказчику или его доверенному лицу посредством PA10.

При прослеживании функционирования этой области процесса анализ тенденций, существующих среди различных базовых практик, может указать на соответствие аргументу доверия (см. PA06).

Тема и содержание PA13 рассматриваются в разделе «Процесс управления конфигурацией» ИСО/МЭК 15288:2002.

B.4.2 BP.13.01 – Устанавливает метод управления конфигурацией

Принятие решения по соответствующему методу управления конфигурацией.

B.4.2 Описание

Три основные компромиссные соображения оказывают воздействие на структуру и стоимость управления конфигурацией и включают в себя:

- степень детализации, с которой идентифицируются элементы конфигурации;
- ситуацию, когда элементы конфигурации передаются под управление конфигурацией;
- уровень формализации, требуемый для процесса управления конфигурацией.

B.4.2.2 Примеры результатов деятельности:

- рекомендации по идентификации элементов конфигурации;
- временная шкала передачи элементов конфигурации под управление конфигурацией;
- выбранный процесс управления конфигурацией;
- описание выбранного процесса управления конфигурацией.

B.4.2.3 Примечания

Примерные критерии выбора элементов конфигурации на соответствующем уровне рабочего продукта включают в себя:

- потребность поддержания средств сопряжения на управляемом уровне;
- уникальные требования пользователя, такие как замена элементов в ходе эксплуатации;
- новые и модифицированные проекты;
- ожидаемую скорость изменения.

Эти критерии влияют на уровень обозримости в конструкторских работах.

Примерные критерии для определения момента передачи рабочих продуктов под управление конфигурацией включают в себя:

- часть жизненного цикла разработки, в котором находится проект;
- готовность элемента системы для тестирования;
- выбранный уровень формализации;
- ограничения по стоимости и производственному графику;
- требования заказчика.

Примерные критерии для выбора процесса управления конфигурацией включают в себя:

- часть жизненного цикла разработки;
- воздействие изменения в системе на другие рабочие продукты;
- воздействие изменения в системе на имеющиеся или субдоговорные рабочие продукты;
- воздействие изменения в системе на программный график и финансирование;

- управление требованиями.

B.4.3 BP.13.02 – Идентифицирует элементы конфигурации

Идентификация неделимых элементов для управления конфигурацией.

B.4.3.1 Описание

Элементом конфигурации является один или более рабочий продукт, который рассматривается как неделимый элемент для управления конфигурацией. Выбор рабочих продуктов для управления конфигурацией должен основываться на критериях, установленных в выбранной стратегии управления конфигурацией. Элементы конфигурации должны выбираться на уровне, приносящем пользу разработчикам и заказчикам, что не является чрезмерным административным грузом для разработчиков.

B.4.3.2 Примеры результатов деятельности:

- конфигурация рабочего продукта;
- идентифицированные элементы конфигурации.

B.4.3.3 Примечания

Требования к элементам конфигурации в области управления требованиями могут варьироваться от отдельных требований до групп требований.

Элементы конфигурации системы, которые подлежат замене в условиях эксплуатации, должны иметь обозначение, указывающее на возможность его замены в условиях эксплуатации.

B.4.4 BP.13.03 - Сохраняет базы рабочей продукции

Поддержка архива баз рабочей продукции.

B.4.4.1 Описание

Данная практика создает и поддерживает архив информации о конфигурации рабочей продукции. Обычно он состоит из собранных данных и описания элементов конфигурации. Он может также включать в себя установленную процедуру осуществления добавлений к базе, удалений из нее или ее модификаций наряду с процедурами отслеживания, аудита и учета данных о конфигурации. Другой целью сохранения данных конфигурации является обеспечение следов аудита обратно к исходным документам в любой точке жизненного цикла системы.

B.4.4.2 Примеры результатов деятельности:

- база данных принятия решений;
- база конфигураций;
- таблица отслеживаемости.

B.4.4.3 Примечания

В случае с элементами конфигурации аппаратных средств ее данные состоят из спецификаций, чертежей, данных изучения коммерческой деятельности и т.д. Оптимальные данные конфигурации можно сохранять в электронном формате для упрощения их обновлений и внесения изменений во вспомогательную документацию.

Элементы конфигурации обычно включают в себя файлы исходных кодов, требования и проектные данные, а также планы и результаты испытаний.

B.4.5 BP.13.04 – Управляет изменениями

Управляет изменениями в установленных элементах конфигурации.

B.4.5.1 Описание

Поддерживает управление базой конфигураций рабочих продуктов. Уравнение включает в себя отслеживание конфигурации каждого из элементов конфигурации и, при необходимости, утверждение новой конфигурации и обновление базы.

Выявленные проблемы, связанные с рабочим продуктом или запросами на изменение рабочего продукта, анализируются для определения будущего воздействия изменения на этот рабочий продукт, график выполнения программы и ее стоимость, а также на другие продукты. Если предложенное изменение рабочего продукта принимается на основе анализа, определяется график внедрения изменения в рабочий продукт и другие, связанные с ним области.

Изменения элементов конфигурации публикуются после проверки и формального утверждения изменений конфигурации. Изменения не являются официально признанными, пока они не опубликованы.

B.4.5.2 Примеры результатов деятельности

Новые базы рабочей продукции.

B.4.5.3 Примечания

Механизмы управления изменениями можно адаптировать по категориям изменений (например, процесс утверждения изменений элементов, не влияющих на другие элементы, должен быть короче).

B.4.6 BP.13.05 – Сообщает о состоянии конфигураций

Сообщение данных о состоянии конфигурации, предложенных изменениях и информации о доступе для причастных групп.

B.4.6.1 Описание

Информирует причастные группы о состоянии данных о конфигурации при внесении каких-либо изменений в это состояние. Сообщения о состоянии должны включать в себя информацию о времени обработки принятых изменений в элементах конфигурации, а также соответствующих рабочих продуктах, подвергнувшихся воздействию этих изменений. Доступ к данным о состоянии конфигурации должны предоставляться разработчикам, заказчикам и другим причастным группам.

B.4.6.2 Примеры результатов деятельности:

- сообщения о состоянии конфигурации.

B.4.6.3 Примечания

Примерами действий по передаче информации о состоянии конфигурации являются:
- предоставление разрешения доступа санкционированным пользователям;
- представление копий баз санкционированным пользователям.

B.5 PA14 - Управляет проектными рисками

B.5.1 Область процесса

B.5.1.1 Соображения безопасности

Область процесса «Менеджмент проектных рисков» относится к риску, связанному с успешным завершением проекта, с учетом вопросов, связанных со стоимостью и графиком выполнения. Области процесса проектирования выполняют действия, связанные с риском безопасности, путем определения допустимости функциональных воздействий остаточных рисков безопасности. Результаты действий, связанных с риском безопасности, могут обеспечить входные данные для выполнения действий по менеджменту проектных рисков.

При рассмотрении вопросов безопасности необходимо учитывать PA07.

B.5.1.2 Краткое описание

Назначением части «Менеджмент проектных рисков» является идентификация, оценка, мониторинг и снижение рисков для обеспечения успешности действий по проектированию систем и общих техниче-

ских работ. Эта область процесса распространяется на весь жизненный цикл проекта. Аналогично областям процесса PA16 и PA15 сфера применения этой области включает в себя как действия по системному проектированию, так и общие технические работы по проекту, поскольку работа по системному проектированию не может считаться успешной, пока не будут положительно оценены общие технические работы.

B.5.1.3 Цели:

- идентификация, понимание и снижение рисков для программы.

B.5.1.4 Перечень базовых практик

Приведенный ниже перечень содержит базовые практики, являющиеся неотъемлемыми элементами качественного системного проектирования:

BP.14.01 разрабатывает план действий по менеджменту рисков, который является основой для идентификации, оценки, смягчения последствий реализации и мониторинга рисков в течение срока жизни проекта.

BP.14.02 идентифицирует проектные риски путем изучения целей проекта с учетом альтернатив и ограничений и определения потенциальных отказов.

BP.14.03 оценивает риски и определяет возможность их возникновения и последствий реализации.

BP.14.04 получает формальное признание оценки проектных рисков.

BP.14.05 реализует действия по снижению рисков.

BP.14.06 проводит мониторинг рисков с целью получения желаемых результатов.

B.5.1.5 Примечания к области процесса

Все работы по разработке систем имеют присущие им риски, которые иногда распознать нелегко. Особенно важно на самой ранней стадии определить вероятность возникновения известных рисков и наличие неизвестных. Неудовлетворительный менеджмент рисков часто считается основной причиной неудовлетворенности заказчиков, расходов и нарушения графика работ. Раннее обнаружение и смягчение последствий реализации рисков снижает расходы на смягчение последствий реализации рисков на более продвинутой стадии разработки систем.

Важно отметить различие между видами рисков, анализом и методом менеджмента (рисков). Качественный менеджмент рисков проводится по трем направлениям (например, анализ риска разработчика в первую очередь касается метода менеджмента, то есть, предварительной оценки прибыли и рынка, тогда как анализ риска пользователем в основном касается видов рисков и анализа, то есть, выполнения задачи и достижения цели).

При отслеживании функционирования этой области процесса анализ тенденций, существующих среди различных основных практических приемов, может указать на соответствие аргументу доверия (см. PA06).

Тема и содержание PA14 рассматриваются в разделе «Процесс менеджмента рисков» ИСО/МЭК 15288:2002. Важно осознать, что ни PA14, ни раздел «Процесс менеджмента рисков» ИСО/МЭК 15288:2002 не имеют отношения к рискам безопасности, но сосредоточены исключительно на рисках функционирования проекта.

B.5.2 BP.14.01 – Разрабатывает метод менеджмента рисков

Разработка плана действий по менеджменту рисков, который является основой для идентификации, оценки, снижения и мониторинга рисков в течение срока жизни проекта.

B.5.2.1 Описание

Назначением данной практики является разработка эффективного плана по руководству действиями по менеджменту проектных рисков. Составные части плана должны включать в себя определение членов группы менеджмента рисков и их обязанностей; график регулярных действий по менеджменту рисков, методов и инструментов, которые будут использованы при идентификации и смягчении рисков, а также методы прослеживания и управления действиями по смягчению рисков. План должен также предусматривать оценку результатов менеджмента рисков.

B.5.2.2 Примеры результатов деятельности:

- план менеджмента рисков.

B.5.2.3 Примечания

Примеры методов менеджмента рисков включают в себя:
- использование спирального метода менеджмента, когда цели следующего цикла и цели всего проекта периодически разъясняются и документируются;
- формальную идентификацию и анализ рисков в начале каждого цикла, а также разработку методов смягчения рисков;
- анализ прогресса, достигнутого в смягчении последствий реализации каждого риска, в конце каждого цикла.

B.5.3 BP.14.02 – Идентифицирует риски

Идентификация проектных рисков путем изучения целей проекта по отношению к альтернативам, ограничениям и идентификации потенциальных отказов.

B.5.3.1 Описание

Системное изучение целей планов проекта (включая зависимости от деятельности или события) и требования системы с целью определения вероятных областей затруднений и потенциальных отказов в этих областях. При идентификации потенциальных рисков на основании прошлого опыта следует учитывать источники риска. Эта деятельность осуществляется в ходе PA16. Установление критических зависимостей разработки и проведение отслеживающих и корректирующих действий осуществляется в PA15.

B.5.3.2 Примеры результатов деятельности

- перечень идентифицированных рисков.

B.5.3.3 Примечания

Примеры действий по идентификации рисков включают в себя:
- разработку общей схемы классификации или систематики рисков для их категорирования. Эта систематика содержит предысторию рисков каждой категории, включая вероятности возникновения (какие элементы системы создают больше рисков), расчетную себестоимость устранения последствий и стратегии смягчения. Эта практика очень удобна для улучшения оценивания рисков и при повторном использовании успешного снижения рисков;
- сосредоточение ресурсов снижения и средства управления на элементах системы, наиболее способствующих риску;
- сбор всей информации, обозначающей цели проекта и системного проектирования, альтернативные технологические стратегии, ограничения и критерии успеха. Обеспечение четкого определения целей проекта и системного проектирования. Документирование элементов, которые могут препятствовать корректировке целей, по каждому альтернативному методу, предложенному для выполнения целей; этими элементами являются риски. Следование этой процедуре приводит к формированию перечня рисков по каждому альтернативному методу. Следует отметить идентичность некоторых рисков во всех альтернативных методах;
- проведение опроса технического и управленческого персонала с целью раскрытия предположений (допущений) и решений, приводящих к появлению рисков. Использование исторических данных аналогичных проектов для определения проблемных областей в аналогичных контекстах.

B.5.4 BP.14.03 – Оценивает риски

Оценка рисков и определение возможности возникновения и последствий реализации рисков.

B.5.4.1 Описание

Оценивание возможности потенциальных потерь (или выгоды) и последствий в случае возникновения ранее идентифицированных рисков. Анализирует риски в отдельности и устанавливает взаимосвязи

между разными отдельными рисками. В методологии анализа следует учитывать такие факторы, как возможность отказа вследствие зрелости и сложности технологий.

B.5.4.2 Примеры результатов деятельности:

- оценка риска.

B.5.4.3 Примечания

Примеры действий по оценке риска включают в себя:

- разработку норм оценивания возможности и стоимости возникновения риска. Возможные нормы ранжируются от простых шкал типа «высокая - средняя (умеренная) - низкая» до количественных шкал в долларах и вероятности до десятой доли процента;
- установление технических норм для проекта на основе его масштаба, длительности выполнения, общей подверженности рискам, области функционирования системы и потребительской среды предприятия [группа Charette, A.B., последние публикации, 89].

B.5.5 BP.14.04 – Анализирует оценки рисков

Получение формального признания оценки проектных рисков.

B.5.5.1 Описание

Анализирует адекватность оценки рисков и принимает решение продолжать, изменять или отменять действия, связанные с риском. Этот анализ должен включать в себя усилия по смягчению последствий реализации потенциальных рисков и вероятность успеха этих усилий.

B.5.5.2 Примеры результатов деятельности:

- стратегия смягчения последствий реализации рисков.

B.5.5.3 Примечания

Примеры действий по анализу оценки рисков включают в себя:

- проведение совещания всех заинтересованных сторон внутри компании с представлением оценки рисков. Представление возможных стратегий смягчения последствий реализации по каждому риску с целью создания ощущения контроля над рисками;
- получение согласия от участников совещания о приемлемости оценок рисков и о том, что никакие очевидные стратегии смягчения не были не рассмотрены.

B.5.6 BP.14.05 – Осуществляет смягчение последствий реализации рисков

Осуществление действий по смягчению последствий реализации рисков.

B.5.6.1 Описание

Действия по смягчению последствий реализации рисков могут включать в себя смягчение последствий при возникновении риска или уменьшение размера ущерба, который риск нанесет в случае его возникновения. По особо опасным рискам могут быть одновременно инициированы различные виды деятельности по смягчению последствий их реализации.

B.5.6.2 Примеры результатов деятельности:

- план по смягчению последствий реализации риска.

B.5.6.3 Примечания

Примеры действий по смягчению последствий реализации рисков включают в себя следующее действие:

- создание прототипа или модели системы, которые можно тестировать на соответствие этому требованию. Этот тип стратегии смягчения последствий реализации риска уменьшает возможность возникновения риска;
- разработка альтернативных планов интеграции с другими сроками для подсистемы повышенного риска. В случае возникновения риска (то есть, если подсистема не готова вовремя) его воздействие на общий график будет слабее. Этот тип стратегии смягчения последствий реализации рисков ослабляют последствия возникновения риска;
- использованиее заранее предопределенные базы (объект ссылки для рисков) для инициирования действий по смягчению последствий реализации рисков.

B.5.7 BP.14.06 – Отслеживает смягчение последствий реализации рисков

Проведение мониторинга действий по смягчению рисков для обеспечения получения желаемых результатов.

B.5.7.1 Описание

Регулярно исследует результаты проведенного смягчения последствий реализации рисков с целью их измерения и определяет успешность смягчения.

B.5.7.2 Примеры результатов деятельности:

- состояние рисков;
- систематика рисков.

B.5.7.3 Примечания

Для проекта с графиком разработки длительностью около шести месяцев проводят переоценку рисков каждые две недели. Проводят также переоценку вероятности и последствий каждого возникновения риска.

B.6 PA15 – Осуществляет мониторинг технических работ и управление ими

B.6.1 Область процесса

B.6.1.1 Соображения безопасности

Области процесса PA08 и PA01 следует учитывать как во время проектно-конструкторских работ, так и эксплуатации системы.

Для рассмотрения вопросов безопасности следует использовать PA07.

B.6.1.2 Краткое описание

Назначением области процесса «Мониторинг технических работ и управление ими» является обеспечение адекватной наглядности конкретного процесса и рисков. Наглядность способствует своевременному проведению корректирующих действий при значительном отличии качества функционирования от запланированного.

Область процесса «Мониторинг технических работ и управление ими» включает в себя руководство, отслеживание и анализ выполнения, результатов и рисков проекта, а также их анализ в сравнении с документированными оценками, обязательствами и планами. Документированный план используется в качестве основы для отслеживания действий и рисков, сообщения о состоянии и пересмотра планов.

B.6.1.3 Цели:

- мониторинг технических работ и управление ими.

B.6.1.4 Перечень практик

Приведенный ниже перечень содержит базовые практики, являющиеся неотъемлемыми элементами качественного системного проектирования:

BP.15.01 руководит техническими работами в соответствии с планами технического управления.

BP.15.02 отслеживает фактическое использование ресурсов по отношению к планам технического управления.

BP.15.03 отслеживает качество функционирования (рабочие характеристики) по отношению к установленным техническим параметрам.

BP.15.04 проверяет качество функционирования по отношению к планам технического руководства.

BP.15.05 анализирует проблемы, возникающие при отслеживании и проверке технических параметров с целью определения корректирующих действий.

BP.15.06 предпринимает корректирующие действия при отличии фактических результатов от запланированных.

B.6.1.5 Примечания к области процесса

Аналогично PA16 данная область процесса применяется в технической деятельности по проекту, а также для работ по проектированию.

Прогресс в первую очередь определяется сравнением фактических работ, объемов рабочей продукции, затрат и графика с планом, когда выбранные рабочие продукты готовы в выбранных контрольных точках. При определении невыполнения плана принимаются корректирующие меры. Эти меры могут включать в себя пересмотр планов для отражения фактических достижений и перепланирование оставшейся работы или осуществление действий по улучшению технических характеристик и смягчению последствий реализации рисков.

При отслеживании функционирования этой области процесса анализ тенденций, существующих среди различных базовых практик, может указать на соответствие аргументу доверия (см. PA06).

Тема и содержание области процесса 15 рассматриваются в двух процессах ИСО/МЭК 15288:2002. а именно «Процесс управления проектом» и «Процесс оценки риска».

B.6.2 B.P.15.01 – Руководство техническими работами

Направление технических работ в соответствии с планами технического руководства.

B.6.2.1 Описание

Выполняет планы технического руководства, разработанные в области процесса «Планирование технических работ». Данная практика включает в себя техническое руководство всеми конструкторскими работами по проекту.

B.6.2.2 Примеры результатов деятельности:

- матрица ответственности;
- разрешения на выполнение работ.

B.6.2.3 Примечания

Эффективное техническое руководство включает в себя использование соответствующих механизмов связи и своевременной передачи технической информации всем заинтересованным сторонам. Весь процесс технического руководства должен регистрироваться для сохранения основы принятия решений и мер различного рода.

B.6.3 BP.15.02 – Отслеживает ресурсы для проекта

Отслеживание фактического использования ресурсов и его соответствия планам технического руководства.

B.6.3.1 Описание

Предоставляет текущую информацию по использованию ресурсов в ходе выполнения проекта с целью корректировки работ и планов (в случае необходимости).

B.6.3.2 Примеры результатов деятельности:

- использование ресурсов.

B.6.3.3 Примечания

Отслеживание затрат включает в себя сравнение фактических затрат со сметой расходов, документированных в плане проекта, для выявления потенциального профицита и дефицита затрат.

B.6.4 B.P.15.03 – Отслеживание технических параметров

Отслеживание качества функционирования и его соответствия установленным техническим параметрам.

B.6.4.1 Описание

Фактическое качество функционирования проекта и его продуктов отслеживается измерением технических параметров, заданных в плане технического руководства. Эти измерения сравниваются с пороговыми значениями, заданными в плане технического руководства, с тем, чтобы предупреждения о проблемах могли быть сообщены руководству.

B.6.4.2 Примеры результатов деятельности:

- профиль технического управления качеством функционирования.

B.6.4.3 Примечания

Пример практики: для каждого технического параметра определяют по эталонному анализу действия, которые будут использоваться для проведения измерения. Задействуют лиц, неподконтрольных руководителю проекта, для проведения объективных измерений методом эталонного анализа. Периодически проводят эталонный анализ и сравнивают полученные измерения с запланированными значениями параметров.

B.6.5 BP.15.04 – Проверяет качество выполнения проекта

Качество выполнения проекта и его продуктов проверяют периодически и в случае превышения допусков по параметрам. Результаты анализа измерений технических характеристик проверяют наряду с другими показателями выполнения и утверждают планы корректирующих действий.

B.6.5.2 Примеры результатов деятельности:

- запросы на изменение плана технического руководства;
- утвержденные корректирующие действия.

B.6.5.3 Примечания

Примерами анализа качества выполнения являются:
- проведение совещания всех участников проекта внутри организации с целью представления результатов анализа качества выполнения и предложения корректирующих действий;
- составление отчета о состоянии, который является основанием для проведения совещания по анализу проекта.

B.6.6 BP.15.05 – Анализирует проблемы, связанные с проектом

Анализ проблем, возникающих при отслеживании и проверке технических параметров, для определения корректирующих действий.

B.6.6.1 Описание

Новые проблемы, связанные с проектом, возникают часто и регулярно в течение всего жизненного цикла проекта. Для управления качеством выполнения проекта критически важными являются своевременное обнаружение, анализ и отслеживание этих проблем.

B.6.6.2 Примеры результатов деятельности:

- анализ проблем выполнения проекта;

- утвержденные корректирующие действия.

B.6.6.3 Примечания

Новая информация объединяется со статистическими данными по проекту. Определяются тенденции, наносящие вред проекту, наряду с новыми проблемами, обозначающими риски для успешности проекта. При необходимости получаются более подробные данные по спорным проблемам и тенденциям. Для анализа часто требуются средства моделирования и имитации, а также заключения сторонних экспертов.

B.6.7 BP.15.06 – Принимает корректирующие меры

Принятие корректирующих мер при наличии указаний технических параметров на будущие проблемы или если фактические параметры отличаются от запланированных.

B.6.7.1 Описание

Корректирующие меры после их утверждения осуществляют посредством перераспределения ресурсов, изменения методов и процедур или повышения точности выполнения имеющихся планов. При необходимости внесения изменений в план технического руководства задействуют практические приемы области процесса PA16.

B.6.7.2 Примеры результатов деятельности:

- перераспределение ресурсов;
- изменения в методах и процедурах;
- заявки на изменения.

B.6.7.3 Примечания

Данная практика охватывает меры, которые могут потребоваться для предотвращения возможных проблем или корректировки выявленных. Возможные меры, принимаемые в этом практическом приеме, разнообразны и многочисленны.

B.7 PA16 – Планирует технические работы

B.7.1 Область процесса

B.7.1.1 Соображения безопасности

Область процесса PA надо учитывать, особенно во время выполнения BP.16.05 в течение всего жизненного цикла проекта и выполнения BP.16.06 для поддержки эффективного взаимодействия с заказчиками и поставщиками.

B.7.1.2 Краткое описание

Назначением части проекта «Планирование технических работ» является разработка планов, представляющих собой основу для составления графика, калькуляции, отслеживания и обсуждения характера и области применения технических работ, задействованных в разработке, изготовлении, использовании и ликвидации системы. Действия по системному программированию должны быть интегрированы в комплексное техническое планирование общего проекта.

Часть проекта « Планирование технических работ» включает в себя разработку оценок предполагаемых работ, получение необходимых обязательств от смежных групп и определение плана выполнения работ.

B.7.1.3 Цели:

- планирование всех аспектов технических работ.

B.7.1.4 Перечень базовых практик

В последующем перечне содержатся базовые практики, являющиеся существенными элементами качественного системного проектирования:

BP.16.01 идентифицирует ресурсы, критические для успешной реализации технической стороны проекта.

BP.16.02 разрабатывает оценки факторов, влияющих на значимость и техническую осуществимость проекта.

BP.16.03 составляет сметы всех технических ресурсов, требуемых для проекта.

BP.16.04 определяет предполагаемый технологический процесс для проекта.

BP.16.05 определяет технические действия для всего жизненного цикла проекта.

BP.16.06 определяет специфические процессы поддержки эффективного взаимодействия с заказчиком (заказчиками) и поставщиком (поставщиками).

BP.16.07 разрабатывает технологический график для всего жизненного цикла проекта.

BP.16.08 устанавливает технические параметры с пороговыми значениями для проекта и системы.

BP.16.09 использует информацию, собранную при планировании, для разработки планов технического руководства, которые послужат основой для отслеживания выдающихся аспектов проекта и работ по инжинирингу систем.

BP.16.10 анализирует планы технического руководства со всеми задействованными группами и отдельными лицами и получает обязательства групп.

B.7.1.5 Примечания к области процесса

Планирование начинается с осознания масштаба предполагаемых работ наряду с ограничениями, рисками и целями, которые определяют и ограничивают проект. Процесс планирования включает в себя шаги по оценке объемов рабочей продукции, необходимых ресурсов, составлению графика, изучению рисков и обсуждению обязательств. Для создания плана, который устанавливает соответствие между качеством, затратами и графиком выполнения, может потребоваться итерирование этих шагов.

При отслеживании функционирования этой области процесса анализ тенденций, существующих среди различных базовых практик, может указать на удовлетворение аргументу доверия (см. PA060).

В приведенном ниже перечне содержатся базовые практики, являющиеся существенными элементами качественного системного проектирования:

Тема и содержание области процесса PA16 рассматриваются в разделе «Процесс планирования» проекта ИСО/МЭК 15288:2002.

B.7.2 BP.16.01 - Идентифицирует критические ресурсы

Идентификация ресурсов, критических для успешного выполнения проекта.

B.7.2.1 Описание

Критическими называются ресурсы, необходимые для успешного выполнения проекта, которые могут быть недоступны для выполнения проекта. Критические ресурсы могут включать в себя персонал со специальными навыками, инструментарий, оборудование или данные. Критические ресурсы можно идентифицировать путем анализа задач проекта и графиков выполнения и путем сравнения данного проекта с аналогичными.

B.7.2.2 Примеры результатов деятельности:

- идентифицированные критические ресурсы.

B.7.2.3 Примечания

Практический пример: проверяют графики выполнения проекта и рассматривают виды ресурсов, требуемых в каждой точке жизненного цикла. Проверяют и дополняют этот перечень с учетом инженерного состава, требуемого для синтезирования системы и рабочей продукции.

B.7.3 BP.16.02 – Оценивает область действия проекта

Разработка оценок факторов, влияющих на значимость и техническую осуществимость проекта.

B.7.3.1 Описание

Область применения и масштаб одного проекта можно определить разложением системы на составные элементы, идентичные элементам других проектов. Затем оценку масштаба можно скорректировать по таким факторам, как различие по сложности, или по другим параметрам.

Для начального определения масштаба проекта анализ аналогичных проектов часто предоставляет наиболее доступную информацию. По мере увеличения объема информации по данной системе эти оценки совершенствуются.

B.7.3.2 Примеры результатов деятельности:

- оценки области действия системы;
- число исходных строк кода;
- число электронных карт (плат);
- число больших фальсификатов;
- число кубических ярдов материала, предназначенного для перемещения.

B.7.3.3 Примечания

Практический пример: проводят анализ наличной документации и опрос персонала проекта с целью определения основных технических ограничений и допущений. Определяют методические подходы самого высокого уровня и факторов, которые могут препятствовать успешному выполнению работ по системному проектированию. Идентифицируют основные технические параметры и оценивают приемлемый диапазон каждого параметра.

B.7.4 BP.16.03 – Оценивает стоимость проекта

Разработка оценок стоимости всех технических ресурсов, необходимых для проекта.

B.7.4.1 Описание

Для качественного управления проектом необходима подробная оценка стоимости проекта независимо от запроса заказчика. Оценки стоимости проекта осуществляются посредством определения трудовых и материальных затрат и затрат на субподрядчика на основе графика выполнения и установленной области проведения работ. Сюда включаютпрямые и косвенные издержки (такие как стоимость инструментов, обучения, специальных испытаний и вспомогательных операций). В отношении расходов на зарплату применяют исторические параметры или модели затрат для преобразования рабочих часов в доллары, основываясь на сложности работ, инструментария, наличия квалификации и опыта, графиках, прямых нормах и нормах накладных расходов. На основе идентифицированных рисков создают соответствующие резервы.

B.7.4.2 Примеры результатов деятельности:

- общие расходы на зарплату с учетом уровня квалификации работников и графика выполнения;
- стоимость материалов;
- стоимость субконтрактов;
- стоимость инструментария;
- стоимость обучения;
- вспомогательное логическое обоснование.

B.7.4.3 Примечания

Перед оценкой расходов необходимо собрать значительный объем информации о проекте, например, такой как область действия, график выполнения и материальные единицы. Для определения статей

издержек, которые иначе могут быть пропущены, можно использовать перечни других проектов и исторические данные о них. Хорошими источниками этого вида информации являются отчеты о несоответствии и документация об «уроках, извлеченных из ошибок».

B.7.5 BP.16.04 – Определяет технологический процесс проекта

Определение технологического процесса, предполагаемого для использования в процессе.

B.7.5.1 Описание

На самом высоком уровне технологический процесс должен соответствовать модели жизненного цикла, основанной на характеристиках проекта, характеристиках организации и стандартном процессе организации. Типичные модели жизненного цикла включают в себя модель типа «водопад», эволюционно спиральную модель и инкрементную модель. В определение процесса включают действия процесса, входные данные, выходные данные, последовательности и измерения качества процесса и рабочих продуктов.

B.7.5.2 Примеры результатов деятельности:

- выбранный системный технологический процесс для проекта.

B.7.5.3 Примечания

Формируют и сохраняют план технического руководства, определяющий взаимосвязь с внутренними и сторонними организациями (например, субподрядчиком) при выполнении технических работ. Включаютмодель запланированного жизненного цикла в проект и конкретные события проекта.

B.7.6 BP.16.05 - Определяет технические действия

Определение технических действий для всего жизненного цикла проекта.

Действия по проектному и системному проектированию могут быть выбраны из соответствующих стандартов, передового опыта отрасли промышленности, базовых моделей, таких как SSE-CMM®, или прошлого опыта организации.

B.7.6.2 Примеры результатов деятельности:

- определенные технические действия.

B.7.6.3 Примечания

Для разработки перечня действий и получения уверенности в его завершенности по возможности используют записи, отображающие процесс аналогичных проектов. При планировании используют принцип «бегущей волны». Этот принцип применяется скорее для более точного определения действий в ближайшем будущем, чем действий, выполняемых гораздо позже.

Пример практического приема: по системному программированию действия, запланированные на следующие три месяца, планируются с продолжительностью каждого действия приблизительно две недели. Продолжительность действий, запланированные на срок от 3 до 12 месяцев, должны быть около одного месяца. Действия, которые начнутся позже, чем через год, могут иметь продолжительность около двух месяцев каждое. Для технических действий, не относящихся к системному программированию, при работе с другими дисциплинами в соответствии с областью процессов PA09 используют аналогичный метод.

B.7.7 BP.16.06 – Определяет средства взаимодействия проекта

Определение специфических процессов поддержки эффективного взаимодействия с заказчиком (заказчиками) и поставщиком (поставщиками).

B.7.7.1 Описание

Средства взаимодействия проекта включают в себя все средства взаимодействия с организациями и отдельными лицами, которые необходимы для успешного выполнения проекта, невзирая на то, являются ли они членами проектной группы. Виды взаимодействия включают в себя обмен информацией, постановку задач и поставки. Методы и процессы взаимодействия (включая средства управления) устанавливают в интересах взаимодействующих сторон.

B.7.7.2 Примеры результатов деятельности:

- установленные процессы для средств взаимодействия проекта.

B.7.7.3 Примечания

Определяют группы, принадлежащие вашей организации, и группы, являющиеся для нее сторонними, которым следует взаимодействовать по проекту для обеспечения успешности его выполнения. Для каждой группы используют базовые практики PA09 для определения и реализации каждого средства взаимодействия в отношении механизмов взаимодействия, частоты взаимодействия и механизмов решения проблемы.

B.7.8 BP.16.07 – Разрабатывает график выполнения проекта

Разработка технических графиков для всего жизненного цикла проекта.

B.7.8.1 Описание

Графики выполнения проекта включают в себя разработку системы и ее компонентов, получение приобретенных изделий, обучение и подготовку условий поддержки проектирования. Графики разрабатываются на основе проверяемых моделей работ и данных об идентифицированных задачах. При этом надо учитывать взаимозависимость задач и наличие приобретенных изделий. В графики следует также включать время простоя, соответствующее идентифицированным рискам. Все причастные стороны должны проанализировать график и придерживаться его.

B.7.8.2 Примеры результатов деятельности:

- графики выполнения проекта.

B.7.8.3 Примечания

Графики обычно включают в себя как контрольные точки заказчика, так и технические контрольные точки.

Пример практического приема: в рамках ограничений проекта (договорные ограничения, выбор времени для операций на рынке, предоставляемые заказчиком входные данные и т.д.) определяют расширения системы, соответствующие общему методологическому подходу. С точки зрения пользователя каждое расширение должно повышать возможности системы. Определяют дополнительные рабочие часы, необходимые для разработки каждого расширения.

Для составления графика использования ресурсов с равномерной интенсивностью выбирают даты окончания каждого расширения пропорционально объему работы, требуемой для разработки расширения. Строят подробные графики технических действий в рамках каждого расширения путем упорядочения действий с самого начала расширения и учета зависимостей между действиями.

Для обусловленного событиями графика нагрузка обычно является неравномерной. Для действий некритического пути может возникнуть необходимость корректировки продолжительности действий, их упорядочения или дат начала действий с целью избежания недопустимого истощения ресурсов.

B.7.9 BP.16.8 - Устанавливает технические параметры

Установление технических параметров с пороговыми значениями для проекта и системы.

B.7.9.1 Описание

Устанавливает ключевые технические параметры, которые можно будет отслеживать по всему жизненному циклу проекта, и которые будут служить показателями выполнения процесса в отношении соответствия конечным техническим целям. Ключевые технические параметры могут быть определены через взаимодействие с заказчиком, требования заказчика, изучение рынка сбыта, прототипы, идентифицированные риски или прошлый опыт аналогичных проектов. Каждый технический параметр, предназначенный для отслеживания, должен иметь пороговое или допустимое значение, при превышении которого должны приниматься какие-либо корректирующие меры. Для ключевых технических параметров должны быть заранее запланированы оценки, назначенные для выполнения в удобных точках графика выполнения проекта.

B.7.9.2 Примеры результатов деятельности:

- технические параметры;
- пороговые значения технических параметров.

Примерами технических параметров являются следующее:
- грузоподъемность самолета;
- разрешающая способность датчика;
- масса переносного радиоприемника;
- пробег автомобиля на единицу расхода горючего;
- искажения на видеомониторе.

B.7.9.3 Примечания

Пример практического приема: определяют аспекты системы, являющиеся главными движущими силами функционирования системы. Разрабатывают показатель для каждого аспекта, который можно отслеживать во время разработки системы.

B.7.10 BP.16.09 – Разрабатывает план технического руководства

Используют информацию, собранную при планировании действий, для разработки планов технического руководства, которые будут служить основой для отслеживания основных аспектов проекта и работ по системному проектированию.

B.7.10.1 Описание

Создают и поддерживают интегрированный план руководства, определяющий взаимодействие проекта со всеми внутренними и сторонними организациями (например, субподрядчиками), выполняющими технические работы.

B.7.10.2 Примеры результатов деятельности

План технического руководства.

B.7.10.3 Примечания

Планы технического руководства обычно включают в себя:
- планы по разработке системы;
- планы взаимодействия с другими организациями (например, субподрядчиками), выполняющими технические работы.

B.7.11 BP.16.10 – Анализирует и утверждает планы проекта

Проведение анализа планов технического руководства группами исполнителей и отдельными лицами и принимает групповое обязательство.

B.7.11.1 Описание

Целью анализа планов проекта является обеспечение полного и безусловного понимания технологического процесса, ресурсов, графика и информационных требований группами исполнителей и отдельными лицами по всему проекту. Входные данные по плану проекта запрашиваются у всех ответст-

венных подразделений организации и персонала проекта. По возможности входные данные объединяют для формирования группового права собственности на планы. Если входные данные отклоняют или изменяют, лицо, предоставившее эти данные, извещают об этом. Промежуточные и завершенные планы проекта распределяют для анализа. От всех групп, входящих в проектную группу, следует получить обязательство по планам проекта.

B.7.11.2 Примеры результатов деятельности:

- проблемы взаимодействия между дисциплинами/группами;
- риски;
- входные данные для планов проектов;
- замечания по плану проекта,
- проблемы и решения по плану проекта.

B.7.11.3 Примечания

Группы исполнителей и отдельные лица выполняют следующую работу:
- проектирование программного обеспечения;
- проектирование аппаратных средств;
- производство;
- руководство (управление);

а также функции:
- заказчиков;
- пользователей;
- партнеров;
- субподрядчиков.

Пример практического приема: определяют вопросы, на которые каждая группа должна ответить в ходе ее проверки (вопросы могут быть разными для разных групп). Сообщают группам о порядке проведения проверки. Предоставляют группам планы технического руководства и в заранее определенное время встречаются с ними для обсуждения их замечаний. Составляют перечень проблем по этим замечаниям и работают над каждым проблемой до ее разрешения.

B.8 PA17 – Определяет процесс системного проектирования организации

B.8.1 Область процесса

B.8.1.1 Соображения безопасности

Для данной области процесса применяют термин «системное проектирование». Однако эта область процесса имеет широкое применение и термин «системное проектирование» можно заменить термином «проектирование безопасности» при оценке технических возможностей обеспечения безопасности организации.

Базовые практики нужны для осуществления интеграции проектирования безопасности с системным проектированием и другими инженерными дисциплинами. Таким образом, при определении процесса проектирования безопасности следует принимать во внимание область процесса PA07.

B.8.1.2 Краткое описание

Назначением области процесса «Определение процесса системного проектирования организации» является формирование стандартных процессов системного проектирования организации и управление ими. Эти процессы впоследствии могут быть адаптированы проектом с целью создания уникальных процессов, которые будут использоватны проектом при разработке систем или продуктов.

Область процесса «Определение процесса системного проектирования организации» включает в себя определение, накопление (сбор) и поддержание процесса, отвечающего бизнес-целям организации, а также проектирование, разработку и документирование активов для процесса системного проектирования. Активы включают в себя примеры процессов, составные части процессов, относящуюся к процессу документацию, архитектуры процесса, правила адаптации процесса и измерения процесса.

B.8.1.3 Цели

Определение стандартного процесса системного проектирования для организации.

B.8.1.4 Перечень базовых практик

В приведенном ниже перечне содержатся базовые практики, являющиеся существенными элементами качественного системного проектирования:

BP.17.01 определяет цели осуществления процесса системного проектирования на основе бизнес-целей организации.

BP.17.02 собирает и поддерживает активы для процесса системного проектирования.

BP.17.03 разрабатывает четко определенный стандартный процесс системного проектирования для организации.

BP.17.04 определяет рекомендации по адаптации стандартного процесса системного проектирования организации для использования в разработке заданного процесса проекта.

B.8.1.5 Примечание к области процесса

В данную область процесса входят начальные действия по сбору и поддержанию активов для процесса, включая стандартный процесс системного проектирования организации. Процедуры усовершенствования активов и стандартного процесса системного проектирования организации изложены в PA18.

При отслеживании функционирования этой области процесса анализ тенденций, существующих среди различных базовых практик, может указать на соответствие аргументу доверия (см. PA06).

Тема и содержание области процесса PA17 «Определение процесса системного проектирования организации» рассматриваются в процессах ИСО/МЭК 15288:2002, а именно «Управление жизненным циклом системы» и некоторых действиях «Процесса управления ресурсами».

B.8.2 BP.17.01 – Устанавливает цель процесса

Установление целей процесса системного проектирования организации на основе бизнес-целей организации.

B.8.2.1 Описание

Процесс системного проектирования организации функционирует в контексте деловой деятельности, и это должно быть признано однозначно для институционализации стандартной практики организации. При установлении целей процесса необходимо учитывать финансовые и людские ресурсы, качество и проблемы маркетинга, значимые для успеха деловой деятельности.

B.8.2.2 Примеры результатов деятельности:

- цели процесса системного проектирования организации;
- требования к процессу системного проектирования организации;
- требования к библиотеке активов для процесса организации;
- библиотека активов для процесса.

B.8.2.3 Примечания

Установление целей может включать в себя определение критериев принятия компромиссных решений по функционированию процесса, основанные на связанных с деловой деятельностью проблемах производительности, качества и маркетинга.

B.8.3 BP.17.02 – Собирает активы процесса

Сбор и поддержание активов процесса системного проектирования.

B.8.3.1 Описание

Информацию, собранную во время действий по определению процесса, как на уровне организации, так и на уровне проекта, следует сохранять (например, в библиотеке активов процесса), предоставлять лицам, участвующим в работе по адаптации и разработке проекта, и поддерживать так, чтобы она соответствовала действительности.

B.8.3.2 Примеры результатов деятельности:

- инструкции по использованию библиотеки активов процесса;
- проектные спецификации библиотеки активов процесса;
- активы процесса.

B.8.3.3 Примечания

Назначением библиотеки активов процесса является хранение и предоставление активов процесса, которые проекты сочтут полезными для определения процесса разработки систем. Она должна содержать примеры уже определенных процессов и измерений процесса. После определения стандартного процесса системного проектирования организации он должен быть добавлен к библиотеке активов процесса наряду с рекомендациями по адаптации этого процесса.

Обычно активы процесса включают в себя:

- стандартный процесс системного проектирования организации;
- утвержденные или рекомендованные жизненные циклы разработки;
- процессы проекта вместе с измерениями, собранными во время осуществления процессов;
- руководства и критерии для адаптации стандартного процесса системного проектирования организации;
- связанную с процессом справочную документацию;
- измерения процесса проекта.

B.8.4 BP.17.03 – Разрабатывает процесс системного проектирования организации

Разработка четко определенного стандартного процесса системного проектирования для организации.

B.8.4.1 Описание

Стандартный процесс системного проектирования организации разрабатывается с помощью средств (возможностей) библиотеки активов процесса. В ходе выполнения задачи по разработке могут потребоваться новые активы, которые необходимо добавлять к библиотеке активов. Стандартный процесс системного проектирования организации должен находиться в библиотеке активов процесса.

B.8.4.2 Примеры результатов деятельности:

- стандартный процесс системного проектирования организации;
- входная информация для обучения;
- входные данные для улучшения процесса системного проектирования.

B.8.4.3 Примечания

Стандартный процесс системного проектирования должен включать в себя средства сопряжения с другими определенными процессами организации. Кроме того, необходимо приводить ссылочные материалы, используемые для определения процесса системного проектирования (например, военные стандарты, стандарты ИИЭР).

Для разработки стандартного процесса системного проектирования организация может идентифицировать все элементы или действия своего процесса системного проектирования. Организация должна оценивать элементы процесса в отношении согласованности входных и выходных данных, излишних действий и недостающих активов. Необходимо решить проблему несогласованности между элементами процесса и предусмотреть возможность упорядочения и верификации. Полученный в результате процесс должен быть четко определенным.

Четко заданный процесс включает в себя:

- критерии готовности;
- входные данные;
- стандарты и процедуры;
- механизмы верификации:

1) сравнительные исследования,

2) выходные данные,
3) критерии завершения [2].

B.8.5 BP.17.04 – Определяет рекомендации по адаптации

Определение рекомендаций по адаптации стандартного процесса системного проектирования организации для использования в проекте при разработке заданного процесса проекта.

B.8.5.1 Описание

Поскольку стандартный процесс системного проектирования организации не может подходить для каждой ситуации, связанной с проектом, требуются рекомендации по его адаптации. Рекомендации должны разрабатываться для большого разнообразия ситуаций, в то же время не давая возможности проектам обойти нормы или значимые практические приемы, предписанные политикой организации, которая полежит строгому соблюдению.

B.8.5.2 Примеры результатов деятельности

Рекомендации по адаптации стандартного процесса системного проектирования организации.

B.8.5.3 Примечания

Рекомендации должны способствовать адаптации стандартного процесса системного проектирования организации к таким контекстуальным переменным, как предметная область проекта, стоимость, график выполнения и компромиссные решения по качеству, опыт персонала проекта, класс компьютера; техническая трудность проекта и т.д.

B.9 PA18 – Усовершенствует процессы системного проектирования организации

B.9.1 Область процесса

B.9.1.1 Соображения безопасности

В области процесса «Усовершенствование процесса системного проектирования организации» применяется термин «системное проектирование». Однако эта область процесса находит очень широкое применение, и термин «системное проектирование» заменяется термином «проектирование безопасности» при оценке потенциальных возможностей проектирования безопасности организации. Кроме того, базовые практики должны рассматривать возможность интеграции проектирования безопасности с дисциплинами системного проектирования.

B.9.1.2 Краткое описание

Назначением области процесса «Усовершенствование процесса системного проектирования организации» является получение конкурентного преимущества путем постоянного повышения эффективности и производительности процесса системного проектирования, используемого организацией. Это подразумевает совершенствование знания процессов организации в контексте бизнес-целей организации, анализ функционирования процессов, детальное планирование и внесение усовершенствований в эти процессы.

B.9.1.3 Цели:

- планирование и внедрение усовершенствований в стандартный процесс системного проектирования.

B.9.1.4 Перечень базовых практик

Приведенный ниже перечень содержит базовые практики, необходимые для качественного системного проектирования:

BP.18.01 оценивает действующие процессы в организациии, с целью получения данных об их сильных и слабых сторонах.

BP.18.02 планирует усовершенствования процессов организации на основе анализа воздействия этих потенциальных усовершенствований на достижение целей процессов.

BP.18.03 изменяет стандартный процесс системного проектирования организации для отражения заданных усовершенствований.

BP.18.04 сообщает об усовершенствованиях процесса соответствующим действующим проектам и другим задействованным группам.

B.9.1.5 Примечания к области процесса

В данной области процесса приведены продолжающиеся действия по измерению и улучшению эффективности процессов системного проектирования в организации. Первичный сбор активов для процесса организации и определение представлены в PA17.

Руководство по усовершенствованию стандартного процесса можно получить из различных источников, включая извлеченные уроки, применение общих практик и оценки стандартного процесса в сравнении с SSE-CMM®. Полученный профиль уровней возможностей в сравнении с областями процессов укажет на области процесса, наиболее нуждающиеся в усовершенствовании. Полезно включение в эти области процесса общих практик.

При отслеживании функционирования данной области процесса анализ тенденций, существующих среди различных основных практических приемов, может указать на удовлетворение аргументу доверия (см. PA06).

Тема и содержание PA18 рассматривается в действиях «Процесса управления жизненным циклом системы» в ИСО/МЭК 15288:2002.

B.9.2 BP.18.01 – Оценивает процесс

Оценка действующих процессов с целью получения данных об их сильных и слабых сторонах.

B.9 2.1 Описание

Оценивает действующие процессы с целью получения данных об их сильных и слабых сторонах.

B.9 2.2 Примеры результатов деятельности:

- профили развитости (зрелости) процессов;
- анализы эффективности процесса;
- данные оценок;
- анализ просчетов.

B.9 2.3 Примечания

Примерный сценарий оценки: оценивают стандартный процесс системного проектирования организации с помощью модели SE-CMM® и связанного с ней метода оценки. Используют результаты оценки для установления или обновления целей функционирования процесса.

Если при выполнении существующего процесса системного проектирования имеют место задержки и очереди, то при сокращении оперативного времени организация может сосредоточиться на них как на отправных точках. Еще раз проверяют такие свойства процесса, как критерии готовности, входные данные и механизмы верификации.

B.9.3 BP.18.02 – Планирует усовершенствования процесса

Планирование усовершенствований процессов организации на основе анализа воздействия этих потенциальных усовершенствований на достижение целей процессов.

B.9.3.1 Описание

Оценка процесса задает импульс к внесению изменений. Этот импульс должен использоваться при планировании усовершенствований, которые обеспечивают большую часть окупаемости для организации в отношении ее бизнес-целей. Планы усовершенствований представляют собой основу для использования преимущества импульса, полученного при оценке. Планирование должно включать в себя цели введения усовершенствований, которые приведут к приносящим большую выгоду улучшениям процесса.

Организации должны использовать эту благоприятную возможность для защиты процесса от ошибок и сокращения лишних усилий. Важно сделать процесс стабильным (то есть, выполняемым любым лицом аналогичным образом). Обычно проблемой является внедрение усовершенствований. При внесении усовершенствований стараются избегать локальной оптимизации, которая может создать проблемы в других частях процесса.

B.9.3.2 Примеры результатов деятельности:

- план усовершенствований процесса.

B.9.3.3 Примечания

Принимается компромиссное решение по предложенным усовершенствованиям процесса в сравнении с предполагаемыми возвратами в отношении оперативного времени, производительности и качества. Используются методы PA09.

B.9.4 BP.18.03 – Изменяет стандартный процесс

Изменение стандартного процесса системного проектирования организации с целью отражения заданных усовершенствований.

B.9.4.1 Описание

Усовершенствования стандартного процесса системного проектирования организации наряду с необходимыми изменениями в рекомендациях по адаптации в библиотеке активов процесса защитят усовершенствованный процесс и будут способствовать внедрению усовершенствований в новую продукцию.

B.9.4.2 Примеры результатов деятельности:

- стандартный процесс системного проектирования организации;
- рекомендации по адаптации стандартного процесса системного проектирования организации.

B.9.4.3 Примечания

После внедрения и оценивания усовершенствований организация должна принять успешные усовершенствования как постоянные изменения в стандартном процессе системного проектирования.

B.9.5 BP.18.04 – Передает сообщения об усовершенствованиях процесса

Передача сообщений об усовершенствованиях процесса существующим проектам и другим задействованным группам.

B.9.5.1 Описание

Некоторые усовершенствования процесса могут быть полезными для существующих проектов, и организации могут внедрять эти полезные усовершенствования в свой текущий процесс в зависимости от состояния проекта. Другие лица, ответственные за подготовку, доверие к качеству, измерения и т.д., должны быть проинформированы об усовершенствованиях процесса.

B.9.5.2 Примеры результатов деятельности:

- инструкции по применению библиотеки активов процесса;
- рекомендации по адаптации стандартного процесса системного проектирования организации;
- перечень и логическое обоснование изменений, внесенных в процесс системного проектирования;
- график внедрения изменений процесса.

B.9.5.3 Примечания

Усовершенствования процесса, а также логическое обоснование и ожидаемые преимущества внесения изменений должны быть сообщены всем задействованным проектам и группам. Организация должна разработать план ввода в действие обновленных процессов и проводить мониторинг выполнения этого плана.

B.10 PA19 – Управление процессом изменения производственной линии

B.10.1 Область процесса

B.10.1.1 Соображения безопасности

Производственная линия (номенклатура изделий), состоящая из изделий защиты (security products), предъявляет специфические требования, которые включают в себя: жёсткие практические приемы управления конфигурацией; требования по допуску персонала к разработке засекреченного кода, сертификацию и аттестацию защищенных изделий. Все эти требования удлиняют цикл проектирования изделия и издержки за срок службы.

PA06 также можно применять для обеспечения соответствия новых или модифицированных изделий потребностям заказчика в безопасности.

B.10.1.2 Краткое описание

Назначением области процесса «Управление процессом изменения номенклатуры изделий» является введение услуг, оборудования и новых технологий для получения оптимальных преимуществ от процесса изменения изделий, стоимости, графика и функционирования со временем по мере изменения производственной линии.

Прежде всего организация должна определить процесс изменения изделия. Затем она должна принять решение о методе проектирования и производства изделий, включая критические компоненты, экономичный инструментарий, а также эффективность и результативность процессов.

B.10.1.3 Цели:

- процесс изменения производственных линий в направлении выполнения их конечных целей.

B.10.1.4 Перечень базовых практик

Приведенный ниже перечень содержит базовые практики, необходимые для качественного системного проектирования:

BP.19.01 определяет предлагаемые типы изделий.

BP.19.02 определяет новые технологии или вводит в действие инфраструктуру, которая будет способствовать организации в приобретении, разработке и применении этой технологии для получения конкурентного преимущества.

BP.19.03 вносит необходимые изменения в цикл проектирования изделия для поддержки разработки новых изделий.

BP.19.04 обеспечивает критические компоненты для поддержки запланированного процесса изменения изделия.

BP.19.05 интегрирует новые технологии с проектированием, маркетингом и производством.

B.10.1.5 Примечания к области процесса

Область процесса Управление процессом изменения номенклатуры изделий» необходима «для обеспечения объединения усилий по проектированию изделий для достижения стратегических бизнес-целей, а также для создания и улучшения потенциальных возможностей, необходимых для превращения перспективных разработок и проектирования изделий в конкурентное преимущество на долгосрочный период».

Данная часть проекта охватывает практические приемы, связанные с управлением производственными линиями, но не с проектированием самих изделий.

При отслеживании выполнения этой области процесса анализ тенденций между различными базовыми практиками указывает на удовлетворение аргументу доверия. См. PA06.

Тема и содержание области процесса 19 рассматриваются в двух процессах ИСО/МЭК 15288:2002, а именно в «Управлении средой» и «Функционировании».

B.10.2 BP.19.01 – Определяет процесс изменения изделий

Определение предлагаемых типов изделий.

B.10.2.1 Описание

Определяют производственные линии (номенклатуры изделий), поддерживающие стратегическую концепцию организации.

Рассматривают сильные и слабые стороны организации, условия конкурентной борьбы, объем потенциального рынка и имеющиеся технические возможности.

B.10.2.2 Примеры результатов деятельности

Определение номенклатуры изделий.

B.10.2.2 Примечания

Определенные производственные линии делают возможным применение более эффективного метода повторного использования и позволяют делать капиталовложения с высокой потенциальной отдачей.

B.10.3 BP.19.02 – Определяет новые технологии для изделий

Определение новых технологий или введение в действие инфраструктуры, которая будет способствовать организации в приобретении, разработке и применении этой технологии для получения конкурентного преимущества.

B.10.3.1 Описание

Определяют новые технологии для их потенциального внедрения в производственную линию (номенклатуру изделий). Формируют и поддерживают источники и методы определения новых технологий и усовершенствований инфраструктуры, такие как оборудование и техническое обслуживание.

B.10.3.2 Примеры результатов деятельности:

- анализы технологий производственных линий;
- усовершенствования, рекомендованные технологической группой.

B.10.3.3 Примечания

Данная практика включает в себя идентификацию, выбор, оценку и контрольное испытание новых технологий. Поддерживая осведомленность об инновациях в области технологий, постоянно оценивая их и экспериментируя с ними, организация выбирает подходящие технологии для повышения качества своей производственной линии, эффективности своих действий по проектированию и производству. Для оценки новых и непроверенных технологий проводят контрольные испытания перед внедрением этих технологий в производственную линию. Усовершенствования инфраструктуры, такие как модернизация оборудования или улучшения в обслуживании в сфере обращения, могут также обеспечить благоприятные возможности для развития производственной линии.

B.10.4 BP.19.02 – Адаптирует процессы разработки

Для поддержки разработки новых изделий внесят необходимые изменения в цикл их разработки.

B.10.4.1 Описание

Адаптируют процессы разработки изделия организации для использования преимуществ компонентов, предназначенных для применения в будущем.

B.10.4.2 Примеры результатов деятельности

Адаптированные процессы разработки.

B.10.4.3 Примечания

Данная практика может включать в себя создание библиотеки повторно используемых компонентов, которая включает в себя механизмы идентификации и восстановления компонентов.

B.10.5 BP.19.04 – Обеспечивает наличие критических компонентов

Обеспечение наличия критических компонентов для поддержки запланированного развития изделия.

B.10.5.1 Описание

Организация должна определять критические компоненты производственной линии и планировать их доступность.

B.10.5.2 Примеры результатов деятельности

Компоненты производственной линии.

B.10.5.3 Примечания

Доступность критических компонентов можно обеспечить путем включения соображений о будущем применении этих компонентов в требования производственной линии. Организация должна распределить ресурсы для постоянного поддержания компонентов.

B.10.6 BP.19.05 – Внедряет технологию продукции

Внедрение новой технологии в процессы разработки изделий, маркетинг и производство.

B.10.6.1 Описание

Внедряют новую технологию в производственные линии, включая как модификации имеющихся компонентов производственной линии, так и новые компоненты. Идентифицируют риски, связанные с изменениями в конструкции изделий, и управляют ими.

B.10.6.2 Примеры результатов деятельности

Определение новой производственной линии.

B.10.6.3 Примечания

Целью выполнения данной практики является повышение качества изделий и производительности, уменьшение издержек в течение жизненного цикла и сокращение периода разработки изделия.

B.11 PA20 – Управляет средой поддержки системного проектирования

B.11.1 Область процесса

B.11.1.1 Соображения безопасности

Разработка продуктов в средах выверенного программного обеспечения и коммуникационной безопасности предъявляет уникальные требования к основным практическим приемам BP.20.02, BP.20.03 и BP.20.04, например, таким как требования доверия к допуску персонала и заботе о сохранности информации.

Среда поддержки системного проектирования должна быть включена в действия области процесса PA03. Область процесса PA06 должна быть усилена надлежащим образом управляемой средой поддержки системного проектирования.

B.11.1.2 Краткое описание

Назначением части изделия «Управление средой поддержки системного проектирования» является обеспечение технологической среды, необходимой для разработки изделий и выполнения процесса. Технология разработки и обработки внедряется в среду с целью минимизации прерывания действий по разработке во время модернизации с тем, чтобы сделать новую технологию доступной.

Потребности организации в технологиях со временем изменяются и изложенные в этой области процесса работы должны выполняться повторно по мере развития потребностей.

B.11.1.3 Цели:

Доведение эффективности процесса до максимума при помощи среды поддержки системного проектирования.

B.11.1.4 Перечень базовых практик

Приведенный ниже перечень содержит базовые практики, являющиеся неотъемлемыми элементами качественного системного проектирования:

BP.20.01 обеспечивает осведомленность о технологиях, поддерживающих выполнение целей организации.

BP.20.02 определяет требования к среде поддержки системного проектирования организации, основанные на потребностях организации.

BP.20.03 определяет, разрабатывает и формирует среду поддержки системного проектирования, соответствующую требованиям, установленным в области процесса «Определение требований поддержки», путем использования практических приемов из области процесса «Анализ вариантов решения».

BP.20.04 адаптирует среду поддержки системного проектирования для потребностей отдельного проекта.

BP.20.05 внедряет новые технологии в среду поддержки системного проектирования на основании бизнес-целей организации и потребностей проектов.

BP.20.06 сохраняет среду поддержки системного проектирования для постоянной поддержки зависящих от нее проектов.

BP.20.07 осуществляет мониторинг среды поддержки системного проектирования в отношении возможностей ее усовершенствования.

B.11.1.5 Примечания к области процесса

В данной области процесса рассматриваются вопросы, связанные со средой поддержки системного проектирования, как на уровне проекта, так и на уровне организации. Элементы среды поддержки состоят из всех средств выполнения действий по системному проектированию, включая в себя:

- вычислительные ресурсы;
- каналы связи;
- методы анализа;
- структуры, политики и методики организации;
- механические мастерские;
- оборудование для химического процесса;
- оборудование для определения нагрузки на окружающую среду;
- средства моделирования системного проектирования;
- утилиты для повышения производительности программного обеспечения;
- специализированные средства системного проектирования;
- рабочее пространство.

При отслеживании функционирования этой области процесса анализ тенденций, существующих среди различных базовых практик, может указать на удовлетворение аргументу доверия (см. PA06) .

Тема и содержание области процесса PA20 рассматриваются в оставшихся действиях «Процесса управления средой» ИСО/МЭК 15288:2002.

B.11.2 BP20.01 – Поддерживает техническую осведомленность

Поддержание осведомленности о технологиях, способствующих выполнению целей организации.

B.11.2.1 Описание

Осведомленность о современном техническом уровне или состоянии практических приемов является необходимым элементом оценки вариантов усовершенствований. Следовательно, для внедрения новой технологии организация должна быть в достаточной степени осведомлена о ней. Подобная осведомленность может обеспечиваться в рамках организации или извне.

B.11.2.2 Примеры результатов деятельности

Анализ технологии среды поддержки.

B.11.2.3 Примечания

Осведомленность можно поддерживать чтением технических журналов, участием в профессиональных обществах и созданием технической библиотеки.

B.11.3 BP.20.02 – Определяет требования поддержки

Определение требований к среде поддержки системного проектирования организации, основанных на потребностях организации.

B.11.3.1 Описание

Потребности организации определяются в первую очередь оценкой вопросов. Например, ухудшает ли среда поддержки организации ее конкурентноспособность. Позволяет ли каждый основной элемент среды поддержки организации выполнять системное проектирование с достаточной скоростью и точностью.

B.11.3.2 Примеры результатов деятельности

Требования к среде поддержки системного проектирования.

B.11.3.3 Примечания

Определяют потребности организации в повышении производительности компьютерной сети, улучшенных методах анализа, компьютерном программном обеспечении и реконструировании процесса.

B.11.4 BP.20.03 – Формирует среду поддержки системного проектирования

Определение, разработка или создание среды поддержки системного проектирования, отвечающей требованиям, установленным в практическом приеме «Определение требований поддержки», при помощи практических приемов из области процесса «Анализ вариантов решений».

B.11.4.1 Описание

Определение критериев оценки и потенциальных вариантов решений для требуемой среды поддержки системного проектирования. Затем выбор решения с помощью практик из области процесса PA09. Наконец, внедрение выбранной среды поддержки системного проектирования.

B.11.4.2 Примеры результатов деятельности

Среда поддержки системного проектирования.

B.11.4.3 Примечания

Среда поддержки системного проектирования может включать в себя многое из перечисленного: утилиты для повышения производительности программного обеспечения, средства моделирования сис-

темного проектирования, собственные специализированные инструментальные средства, заказные и серийно выпускаемые инструментальные средства, специальное испытательное оборудование и новую аппаратуру.

B.11.5 BP.20.04 - Адаптирует среду поддержки системного проектирования

Адаптация среды поддержки системного проектирования для потребностей отдельного проекта.

B.11.5.1 Описание

Общая среда поддержки представляет потребности организации в целом. Однако у отдельного проекта могут быть уникальные потребности в выборочных элементах этой среды. В этом случае адаптация элементов среды поддержки системного проектирования может способствовать более эффективному функционированию проекта.

B.11.5.2 Примеры результатов деятельности

Адаптированная среда поддержки системного проектирования.

B.11.5.3 Примечания

Адаптация позволяет отдельному проекту делать среду поддержки системного проектирования на заказ. Например, в проекте А не задействуется обработка сигналов, поэтому автоматические средства обработки сигналов изготавливаются (то есть, не предоставляются) из набора автоматических средств данного проекта. Напротив, проект В является единственным проектом организации, нуждающийся в автоматическом отслеживании требований, так что соответствующие средства добавляются (то есть, предоставляются в дополнение) к набору автоматических средств этого проекта.

B.11.6 BP.20.05 – Внедряет новую технологию

Внедрение новых технологий в среду поддержки системного проектирования на основе бизнес-целей организации и потребностей проекта.

B.11.6.1 Описание

Среда поддержки системного проектирования должна модернизироваться с помощью новых технологий по мере их появления и подтверждения их способности быть полезными бизнес-целям организации и потребностям проекта.

Следует обязательно обеспечить обучение по использованию новой технологии в среде поддержки системного проектирования.

B.11.6.2 Примеры результатов деятельности

Новая среда поддержки системного проектирования.

B.11.6.3 Примечания

Внедрение новых технологий в среду поддержки системного проектирования представляет определенные трудности. Для минимизации этих трудностей выполняют следующие шаги:

- тщательно тестируют новую технологию;
- принимают решение по внедрению усовершенствования в рамках всей организации или только в ее избранных подразделениях;
- уведомляют заранее о предстоящих изменениях всех, кого они затронут;
- обеспечивают необходимое обучение по применению новой технологии;
- проводят мониторинг принятия новой технологии.

B.11.7 BP.20.06 – Сохраняет среду

Сохранение среды поддержки системного проектирования для оказания постоянной поддержки зависящих от нее проектов.

B.11.7.1 Описание

Сохраняют среду поддержки системного проектирования на уровне функционирования, соответствующем ожидаемому. Действия по сохранению могут включать в себя администрирование компьютерной системы, обучение, поддержка по «горячей линии», наличие специалистов, расширение технической библиотеки и т.д.

B.11.7.2 Примеры результатов деятельности

Отчет о функционировании среды поддержки системного проектирования.

B.11.7.3 Примечания

Поддержание среды поддержки системного проектирования может осуществляться несколькими путями:

- наем или обучение администраторов компьютерных систем;
- подготовка квалифицированных пользователей для работы с выбранными автоматизированными инструментальными средствами;
- подготовка специалистов по методологии, которых можно использовать в разнообразных проектах;
- подготовка специалистов по технологическому процессу, которых можно использовать в разнообразных проектах.

B.11.8 BP.20.07 – Осуществляет мониторинг среды поддержки системного проектирования

Мониторинг среды поддержки системного проектирования с целью получения благоприятных возможностей для усовершенствования.

B.11.8.1 Описание

Определяет факторы, влияющие на применимость среды поддержки системного проектирования, включая любую вновь внедренную технологию. Проводит мониторинг принятия новой технологии и всей среды поддержки системного проектирования.

B.11.8.2 Примеры результатов деятельности

Проверки технологии, применяемой в среде поддержки системного проектирования.

B.11.8.3 Примечания

Проектирует большую часть мониторинга в виде автоматизированной вспомогательной деятельности для того, чтобы пользователям среды поддержки не надо было специально представлять данные. Также предоставляет пользователям среды поддержки системного проектирования возможность сознательно предоставлять входные данные о применимости среды поддержки системного проектирования и предлагать усовершенствования.

B.12 PA21 – Обеспечивает действующие навыки и знания

B.12.1 Область процесса

B.12.1.1 Соображения безопасности

Необходимо обеспечить обучение в области применения процесса проектирования безопасности организации.

B.12.1.2 Краткое описание

Назначением области процесса «Обеспечение совершенствующихся навыков и знаний» является обеспечение проектов и организаций необходимыми знаниями и навыками для достижения их целей. С целью эффективного применения этих критических ресурсов, которые в основном имеются только у людей, необходимо идентифицировать требования к навыкам и знаниям в рамках организации наряду с потребностями конкретного проекта или организации (подобные тем, которые связаны с возникающими программами или технологиями, новыми изделиями, технологическими процессами и политиками).

Требуемые навыки и знания можно получить в рамках организации и из источников, сторонних для организации. Знания приобретаются из таких сторонних источников, как ресурсы заказчика, работники, нанятые на временную работу, новые работники, консультанты и субподрядчики.

B.12.1.3 Цели:

Наличие у организации практического опыта, необходимого для достижения целей проекта и организации.

B.12.1.4 Перечень базовых практик

В приведенном ниже перечне содержатся базовые практики, являющиеся неотъемлемыми элементами качественного системного проектирования:

BP.21.01 идентифицирует необходимые улучшения навыков и знаний по всей организации, используя в качестве руководства потребности проекта, стратегический план организации и имеющиеся навыки работников.

BP.21.02 оценивает и выбирает соответствующую методику получения знаний в ходе обучения или из других источников.

BP.21.03 обеспечивает соответствующие навыки и знания для выполнения работ по системному проектированию.

BP.21.04 подготавливает учебный материал на основе идентифицированных потребностей обучения.

BP.21.05 проводит обучение персонала для получения навыков и знаний, необходимых для выполнения его должностных обязанностей.

BP.21.06 оценивает эффективность обучения в отношении соответствия его идентифицированным потребностям.

BP.21.07 ведет учет процесса обучения и передачи опыта.

BP.21.08 сохраняет учебный материал в общедоступном архиве.

B.12.1.5 Примечания к области процесса

Выбор внутреннего или стороннего источника обучения с целью приобретения необходимых знаний и навыков часто определяется наличием компетенции в области обучения, графиком выполнения проекта и бизнес-целями. Реализация программ успешного обучения в рамках организации обусловлена возможностями организации. Кроме того, они управляются способом, оптимизирующим процесс обучения, который является повторяемым, оцениваемым и легко изменяемым с целью удовлетворения новых потребностей организации. Обучение не ограничивается занятиями в «классах»: оно включает многие средства, способствующие повышению навыков и приобретению знаний. В случае неадекватности обучения в пределах организации, связанной с расписанием или наличием учебных ресурсов, рассматривается вопрос привлечения сторонних источников.

При отслеживании функционирования этой области процесса анализ тенденций, существующих среди различных основных практических приемах, может указать на удовлетворение аргументу доверия (см. PA06).

Тема и содержание области процесса PA21 рассматриваются в действиях «Процесса Управления Ресурсами» ИСО/МЭК 15288:2002.

B.12.2 BP.21.01 – Выявляет потребности в обучении

Идентификация необходимых улучшений навыков и знаний по всей организации, используя в качестве руководства потребности проекта, стратегический план организации и имеющиеся навыки работников.

B.12.2.1 Описание

Данная базовая практика определяет усовершенствования, требуемые для получения навыков и знаний в рамках организации. Потребности определяются с помощью имеющихся программ, стратегического плана организации и совокупности имеющихся навыков сотрудников. Входные данные помогают идентифицировать имеющиеся недостатки, которые могут быть устранены посредством обучения или приобретения навыков и знаний иными средствами. Стратегический план организации используется для содействия идентификации новых технологий, а имеющиеся навыки применяются для оценки текущих возможностей.

Идентификация потребностей в навыках и знаниях также определяет обучение, которое можно обобщить для достижения эффективности функционирования организации и улучшения обмена информацией внутри организации посредством применения общих инструментальных средств. Обучение следует предлагать во время процесса системного проектирования организации и адаптации процесса для конкретных проектов.

B.12.2.2 Примеры результатов деятельности:

- потребности организации в обучении;
- навыки и знания в области проектов.

B.12.2.3 Примечания

Организация должна выявлять дополнительные потребности в обучении, определяемые из результатов оценок и идентифицируемые процессом предупреждения дефектов. План обучения организации должен разрабатываться и корректироваться в соответствии с документированной процедурой. Каждый проект должен разрабатывать план обучения, в котором подробно изложены его потребности в обучении, и придерживаться его.

B.12.3 BP.21.02 – Выбирает методику приобретения знаний и навыков

Оценивает и выбирает соответствующую методику приобретения знаний и навыков относительно обучения или других источников знаний.

B.12.3.1 Описание

Целью этой практики является обеспечение выбора наиболее эффективного метода своевременного предоставления навыков и знаний проектам. Потребности проектов и организаций подвергаются анализу и для осуществления выбора из таких вариантов, как консультанты, субподрядчики, приобретение знаний у специалистов по предмету изучения или обучение, применяются методы из PA09.

B.12.3.2 Примеры результатов деятельности:

- обзор необходимых навыков или знаний;
- результаты изучения коммерческой деятельности, указывающие на наиболее эффективную методику приобретения знаний и навыков.

B.12.3.3 Примечания

Примерные критерии, которые могут использоваться для определения наиболее эффективной методики приобретения знаний и навыков, включают в себя:
- время, имеющееся для подготовки выполнения проекта;
- бизнес-цели;
- наличие собственных специалистов;
- доступность обучения.

B.12.4 BP.21.03 Обеспечивает наличие навыков и знаний

Обеспечивает наличие имеющихся навыков и знаний для выполнения работ по системному проектированию.

B.12.4.1 Описание

Данная практика касается приобретения всей совокупности навыков и знаний, которые должны быть в наличии для проведения работ по системному проектированию проекта. Посредством взвешенной оценки и подготовки можно разработать и выполнить планы по предоставлению совокупности требуемых знаний и навыков, включающей в себя навыки по функциональному проектированию, знания в проблемной области приложений, навыки в области межличностных отношений и навыки, связанные с различными дисциплинами и технологическими процессами. После идентификации требуемых навыков соответствующие методы приобретения знаний и навыков могут использоваться для выбора наиболее эффективного метода.

B.12.4.2 Примеры результатов деятельности:

- оценка видов навыков, требуемых в соответствии с категорией навыков;
- план приобретения знаний для проекта;
- план обучения;
- перечень идентифицированных и доступных специалистов по предмету изучения.

B.12.4.3 Примечания

Соответствующий охват всей совокупности знаний и навыков можно исследовать с помощью перечня видов знаний (например, о функциональном проектировании, проблемной области и т.д.) в сопоставлении с каждым элементом декомпозиции проекта.

Примером определения наличия соответствующих знаний в проблемной области приложений (например, обработка спутниковых метеорологических данных) может быть план опроса специалистов по предмету изучения в связи с интерпретацией требований или системным проектированием. Такой метод принимают при отсутствии в организации требуемых специалистов (как в случае с первой программой в новой отрасли производства).

B.12.5 BP.21.04 – Подготавливает учебный материал

Подготовка учебного материала на основе идентифицированных потребностей в обучении.

B.12.5.1 Описание

Разработка учебного материала для каждого урока, который готовится и проводится сотрудниками организации, или получение пособий для каждого урока, который проводится посторонними людьми.

B.12.5.2 Примеры результатов деятельности

Описание курсов обучения и требования к ним.
Учебный материал.

B.12.5.3 Примечания

Описание курса должно включать в себя:
- предполагаемую аудиторию;
- подготовку участия;
- цель обучения;
- срок обучения;
- планы уроков;
- критерии определения успешности завершения обучения.

Подготавливают:
- методики периодической оценки эффективности обучения и специальные соображения по таким пунктам, как проверка курса обучения в реальных условиях;
- обоснование потребностей в повышении квалификации и благоприятных возможностей для дальнейшей подготовки кадров;
- пособия для обучения конкретной практике, которые будет применяться как область процесса (например, технические приемы метода);
- пособия для обучения процессу;
- пособия для получения таких навыков в области технологического процесса, как применение статистических методов, статистическое управление процессом, применение инструментов и методов оп-

ределения качества, описательное моделирование процесса, определение процесса и измерение процесса;

- анализ учебного материала специалистами по обучению, предмету изучения и учащимися по экспериментальной программе.

B.12.6 BP.21.05 –Обучает персонал

Обучение персонала с целью приобретения навыков и знаний, требуемых для выполнения своих должностных обязанностей.

B.12.6.1 Описание

Персонал проходит обучение в соответствии с планом обучения и разработанным материалом.

B.12.6.2 Примеры результатов деятельности

Список обученного персонала.

B.12.6.3 Примечания

Для оптимального запоминания и получения самых высоких уровней навыков проводят обучение своевременно (обучение «точно в срок»), для чего:

- должна существовать методика определения уровня квалификации работника перед прохождением обучения с целью установления необходимости его обучения (т.е., следует ли исключить работника из курса обучения);
- должен существовать процесс побуждения работников к участию в обучении;
- модули онлайнового обучения/заказного обучения объединяют различные стили и культуры обучения в дополнение к передаче меньших объемов знаний.

B.12.7 BP.21.06 – Оценивает эффективность обучения

Оценивание эффективности обучения для удовлетворения идентифицированных требований к работникам.

B.12.7.1 Описание

Ключевым аспектом обучения является определение его эффективности. Методы оценки эффективности следует рассматривать параллельно с разработкой плана обучения и учебного материала; в некоторых случаях эти методы должны быть неотъемлемой частью учебного материала. С целью внесения корректировок в процесс обучения результаты оценки эффективности должны сообщаться своевременно.

B.12.7.2 Примеры результатов деятельности:

- анализ эффективности обучения;
- внесение изменений в обучение.

B.12.7.3 Примечания

Должна существовать методика определения уровня квалификации работника после прохождения обучения с целью установления успешности обучения. Она может реализовываться посредством формального тестирования, демонстрации навыков на рабочем месте и механизмов оценки, внедренных в программное обеспечение обучения.

B.12.8 BP.21.07 – Ведет учебную документацию

Ведение документации по обучению и повышению квалификации.

B.12.8.1 Описание

Документация ведется с целью отслеживания процесса обучения каждого работника, а также состояния его навыков и возможностей.

B.12.8.2 Примеры результатов деятельности:

- учебные документы и документы о квалификации.

B.12.8.3 Примечания

Документы сохраняются обо всех учащихся, успешно завершивших каждый курс обучения или какой-либо иной вид обучающей деятельности. При назначении персонала и руководителей для рассмотрения также предоставляются документы об успешном прохождении обучения.

B.12.9 BP.21.08 – Сохраняет учебные материалы

Сохранение учебных материалов в общедоступном архиве.

B.12.9.1 Описание

Материал программного обеспечения обучения сохраняется в архиве для будущего доступа работникам и для поддержания отслеживаемости изменений в материале программного обеспечения обучения.

B.12.9.2 Примеры результатов деятельности:

- основные учебные материалы;
- пересмотренные версии учебных материалов.

B.12.9.3 Примечания

Поддерживает архив учебных материалов и предоставляет доступ к нему всем работникам (например, библиотека организации может предоставлять книги, журналы, видеозаписи и т.д.; учебные материалы могут сохраняться в общественных файловых серверах). Включает в себя извлеченные из опыта уроки в учебные материалы и обучающие программы. Обновляет учебные материалы по процессу с учетом всех изменений и усовершенствований процесса.

B.13 PA22 – Координирует действия с поставщиками

B.13.1 Область процесса

B.13.1.1 Соображения безопасности

Если поставщик выполняет область процесса PA10, оцениваемая организация выступает в роли заказчика.

B.13.1.2 Краткое описание

Назначением области процесса «Согласованность с поставщиками» является исследование потребностей организации в эффективном управлении частями производственного процесса, которые выполняются другими организациями. Решения, принимаемые в этой области процесса, должны приниматься в соответствии с установленным процессом. Общий термин «поставщик» применяется для определения организации, которая разрабатывает, производит, испытывает, поддерживает компонент системы. Поставщиками могут быть продавцы, субподрядчики, партнеры и т.д. в качестве гаранта деловой деятельности организации.

В дополнение к согласованию графиков, процессов и поставок рабочей продукции задействованные организации должны обладать общим видением рабочих взаимоотношений. Взаимоотношения могут быть как между объединенными группами разработчиков изделия, так и между генеральными подрядчиками/субподрядчиками, продавцами и т.д. Успешные взаимоотношения между организацией и поставщиком зависят от возможностей обеих организаций и их взаимопонимания.

B.13.1.3 Цели:

- выбор и использование эффективных поставщиков.

B.13.1.4 Перечень базовых практик

В приведенном ниже перечне содержатся базовые практики, являющиеся существенными элементами качественного системного проектирования:

BP.22.01 идентифицирует необходимые компоненты или услуги, которые должны предоставляться другими/сторонними организациями.

BP.22.02 определяет поставщиков, продемонстрировавших достаточную компетенцию в заданных областях

BP.22.03 выбирает поставщиков в соответствии с установленным процессом.

BP.22.04 предоставляет поставщикам информацию о требованиях, ожидаемых результатах и мерах эффективности, предъявляемых организацией в отношении системных компонентов или услуг, предназначенных для поставки.

BP.22.05 поддерживает своевременную двустороннюю связь с поставщиками.

B.13.1.5 Примечания к области процесса

При поставке поставщиками продукции, которая не соответствует требованиям организации, она имеет возможность сделать выбор между сменой поставщика, понижением своих стандартов и приемкой поставленной продукции и оказанием помощи поставщику или продавцу в удовлетворении требований организации.

При выполнении поставщиком области процесса PA10 организация выступает в роли поставщика. Организации следует оказать помощь поставщику в обеспечении полного понимания им ее целей. Если у поставщика отсутствуют процессы для выполнения этой части, организация должна подсказать поставщику, где получить необходимую информацию.

При отслеживании функционирования этой области процесса анализ тенденций, существующих среди различных основных практических приемах, может указать на удовлетворение аргументу доверия (см. PA06).

Тема и содержание области процесса PA22 распределены между тремя процессами ИСО/МЭК 15288:2002, в частности, «Процессом Приобретения», некоторыми действиями «Процесса Поставки» и некоторыми действиями «Процесса Планирования Проекта».

B.13.2 BP.22.01 – Определяет системные компоненты или услуги

Определение требуемых компонентов или услуг, которые должны предоставляться другими/сторонними организациями.

B.13.2.1 Описание

Организация редко производит каждый компонент системы. Анализы и решения в отношении альтернативы «произвести/купить» определяют, какие элементы следует приобрести. Требования системы, которым удовлетворяют сторонние организации, обычно представлены требованиями, в отношении которых организация недостаточно компетентна или заинтересована.

B.13.2.2 Примеры результатов деятельности:

- изучение компромиссного решения между альтернативами «произвести/купить»;
- перечень системных компонентов;
- подгруппа системных компонентов, представленных сторонним организациям для исследования;
- список потенциальных поставщиков;
- источники критериев завершения требуемых работ.

B.13.2.3 Примечания

Примеры практических приемов включают в себя:
- изучение коммерческой деятельности;

- проверку своей организации с целью определения недостатка компетенции для удовлетворения требованиям системы.

B.13.3 BP.22.02 - Определяет поставщиков или продавцов компонентов

Определение поставщиков, продемонстрировавших достаточную компетенцию в заданных областях.

B.13.3.1 Описание

Потенциальные возможности поставщика должны быть дополняющими и совместимыми с возможностями организации. Проблемные области включают в себя надлежащие процессы разработки и производства, ответственность за верификацию, своевременную поставку, процессы поддержки жизненных циклов и способность эффективного обмена информацией на больших расстояниях (видеоконференции, электронная передача файлов, электронная почта и т.п.).

B.13.3.2 Примеры результатов деятельности:

- список поставщиков;
- преимущества и недостатки каждого поставщика;
- потенциальные способы работы с поставщиками на физических расстояниях.

B.13.3.3 Примечания

Примеры практических приемов включают в себя:
- чтение отраслевых журналов;
- пользование услугами библиотеки;
- использование базы знаний организации (это может быть система, работающая в режиме онлайн).

B.13.4 BP.22.03 – Выбирает поставщика или продавцов

Выбор поставщиков в соответствии с заданным процессом.

B.13.4.1 Описание

Поставщики выбираются на логической и объективной основе, с учетом их соответствия целям товарной политики организации. Определяют характеристики поставщика, которые лучше всего дополняют возможности организации, и идентифицируют достаточно компетентных кандидатов.

B.13.4.2 Примеры результатов деятельности:

- слабые места организации, которые могут быть смягчены поставщиком;
- характеристики желательных рабочих отношений с поставщиком;
- требования поставщика;
- требования заказчика, предъявляемые поставщику;
- выбранный поставщик;
- зафиксированное обоснование выбора поставщика.

B.13.4.3 Примечания

Важным фактором при выборе поставщика являются предполагаемые рабочие отношения. Они могут быть представлены как комплексной группой разработки продукта, так и классическими отношениями типа «удовлетворение требованиям». Вероятно, критерии выбора отличаются в зависимости от желательных отношений.

B.13.5 BP.22.04 – Обеспечивает ожидаемые результаты

Предоставление поставщикам информации о требованиях, ожидаемых результатов и мерах эффективности, предъявляемых организацией в отношении системных компонентов или услуг, предназначенных для поставки.

B.13.5.1 Описание

Организация-подрядчик должна четко определять свои требования и ожидаемые результаты и обозначать их приоритеты, а также любые ограничения со стороны поставщиков. Организация работает в тесном сотрудничестве с поставщиками с целью установления взаимопонимания по требованиям к продукции, обязанностям и процессам, которые будут применяться для достижения программных целей.

B.13.5.2 Примеры результатов деятельности:

- формулировка требований;
- технические эксплуатационные параметры;
- спецификации проверки.

B.13.5.3 Примечания

Примеры технических приемов и совещаний, связанных с информированием поставщиков и продавцов о требованиях, ожидаемых результатах и мерах эффективности, включают в себя:
- изучение рынка товаров;
- формальные договоры;
- проверки в процессе эксплуатации;
- общие собрания;
- промежуточные этапы платежей.

B.13.6 BP.22.05 – Поддерживает обмен информацией

Регулярная поддержка двустороннего обмена информацией с поставщиками.

B.13.6.1 Описание

Организация и поставщик устанавливают взаимопонимание по ожидаемому и необходимому обмену информацией.

Характеристики заданного обмена информацией включают в себя типы информации, считающейся открытой и не подлежащей ограничениям, типы информации, подлежащей ограничениям (например, политика или договорные отношения), ожидаемую своевременность запросов и ответов, инструментарий и методы, предполагаемые для применения в обмене информацией, обеспечение безопасности и ожидаемые результаты распределения. Учитывают потребность в обмене информацией «лицом к лицу» и «на расстоянии», а также потребность и механизм архивирования обмена информацией.

B.13.6.2 Примеры результатов деятельности:

- обусловленная договором передача информации;
- инструментарий обмена информацией;
- планы по обмену информацией;
- список распределения (групповых сообщений) при обмене информацией.

B.13.6.3 Примечания

Крайне важны эффективные условия обмена информацией между организацией и поставщиком. При отсутствии необходимости в двустороннем общении достаточно обмена информацией посредством электронной почты и передачи речевых сообщений в почтовый ящик.

Обмен информацией, влияющий на стоимость выполнения работ или область применения, следует ограничить сторонами, имеющими разрешение на этот обмен.

Приложение С
(справочное)

Концепции модели зрелости возможностей

С.1 Общая часть

Назначением настоящего раздела является обзор концепций и положений, используемых в модели SSE-CMM®. В нем представлена информация о требованиях, которыми руководствовались при проектировании SSE-CMM®, описание архитектуры и подраздел, содержащий ключевые понятия и термины, способствующие пониманию модели. Он служит вводной частью к детальному обсуждению модели в разделе 6.

Модель SSE-CMM® обеспечивает в государственном (правительство и промышленность) масштабе стандартную метрику для формирования и продвижения безопасного проектирования как развитой измеримой дисциплины. Модель и методы ее оценки исходят из неотъемлемости обеспечения безопасности от действий по проектированию, в ходе которых возникают проблемы, связанные с безопасностью аппаратных средств, программного обеспечения, систем и предприятий. Модель определяет характеристики процесса обеспечения безопасности проектирования, детальное определение которого приводитсяи который управляется, контролируется и является эффективным во всех видах проектно-конструкторских разработок.

С.2 Усовершенствование процесса

Процесс является последовательностью шагов, выполняемых с определенной целью и представляет собой систему из заданий, вспомогательных инструментальных средств и людей, участвующих в получении и развитии какого-то конечного результата (например, изделия, системы или услуги). Понимая, что процесс является одним из определяющих элементов стоимости продукта, графика выполнения и качества (другими определяющими элементами являются люди и технологии), различные организации, связанные с проектированием, начали сосредоточивать усилия на путях усовершенствования своих процессов производства продукции и услуг.

Возможности процесса относят к потенциалу организации. Это рамки, в которых предполагается функционирование организации. Функционирование процесса является мерой фактических результатов выполнения определенного проекта, который может или не может вмещаться в эти рамки.

«На производственном предприятии руководитель наблюдает за проблемами, связанными с какой-либо производственной линией. Ему известно, только то, что рабочие на этой линии производят большое число бракованных изделий. Его первым намерением может быть обращение к рабочим с просьбой работать усерднее и быстрее. Но вместо этого он собирает данные и составляет диаграмму процентного содержания дефектных изделий. Диаграмма показала, что число этих изделий и их ежедневное варьирование были предсказуемы».

Приведенный выше пример иллюстрирует систему со статистическим управлением технологическим процессом, то есть возможности определяются конкретным диапазоном и пределы варьирования являются предсказуемыми, но при этом не исключается повторяемость производства дефектных изделий. Этот пример показывает, что наличие системы статистического управления технологическим процессом не подразумевает отсутствия дефектных изделий.

Однако это действительно означает, что примерно одинаковое повторение работы дает примерно одинаковые результаты. Важно сформировать статистическое управление потребностями процесса с целью идентификации мест, где можно внести эффективные усовершенствования. Многие организации использовали модель SSE-CMM® в качестве руководства для организации статистического управления технологическим процессом.

Другая концепция «развитости процесса» демонстрирует, в какой степени конкретный процесс однозначно определяется, управляется, контролируется и является эффективным. Развитость процесса подразумевает потенциал расширения возможностей и указывает на полноту процесса организации и последовательность, с которой он применяется во всей организации.

Деминг совместно с японскими разработчиками применил концепции статистического управления технологическим процессом в промышленности. В работе «Снятие характеристик программного процесса: Основа развитости» Хамфри описывает структуру развитости программного процесса, которая интерпретирует работу Деминга для процесса разработки программного обеспечения. Хамфри утверждал, что «несмотря на значительные различия, эти концепции так же применимы к программному обеспечению, как и к автомобилям, фотокамерам, наручным часам и производству стали. Процесс разработки программного обеспечения, находящийся под статистическим управлением, принесет желаемые резуль-

таты в предвидимых пределах стоимости, графика и качества». Применяя концепции статистического управления технологическим процессом к программному процессу, Хамфри описывает уровни развитости (зрелости) процесса, которые управляют улучшением возможностей процессов организации небольшими шагами. Описанные им уровни образуют основу модели зрелости возможностей CMM® for Software программного обеспечения, разработанной Институтом программной инженерии.

Модель CMM® является основой развития от узко специализированной, менее систематизированной, менее эффективной проектной организации высокоэффективной организации со сложной структурой. Применение подобной модели является средством подчинения организацией своих практических приемов статистическому управлению с целью улучшения возможностей своих технологических процессов. В результате применения модели CMM® for Software многие организации, занимающиеся программным обеспечением, продемонстрировали положительные результаты в отношении стоимости, производительности, графика выполнения и качества. Модель SSE-CMM® была разработана исходя из предположения, что применение концепций статистического управления процессом к безопасному проектированию будет способствовать разработке защищенных систем и надежных продуктов с предвиденными пределами стоимости, графика выполнения и качества.

С.3 Предполагаемые результаты

Основываясь на аналогиях в организациях, занимающихся программным обеспечением, и других организациях можно предсказать некоторые результаты улучшений процесса и продуктов, которые приводятся в данном разделе.

С.3.1 Улучшение предсказуемости

Первое улучшение, ожидаемое в ходе совершенствования организации, связано с предсказуемостью. По мере возрастания возможностей различия между намеченными и фактическими результатами по всем проектам уменьшаются. Например, организации на уровне 1 часто в значительной степени не соблюдают запланированные сроки поставок, тогда как организации на более высоком уровне возможностей смогут предсказать результаты, связанные с аспектами стоимости и выполнения графика, с более высокой точностью.

С.3.2 Улучшение контроля

Второе улучшение, ожидаемое в ходе совершенствования организации, связано с контролем. По мере возрастания возможностей процесса для более точного формирования пересмотренных целей могут применяться пошаговые результаты. Для выбора наилучшего применения мер контроля альтернативные корректирующие действия можно оценивать на основе опыта работы с процессом и результатов процесса других проектов. В результате в организации с более высоким уровнем возможностей будут более эффективно контролироваться эксплуатационные характеристики в диапазоне допустимых значений.

С.3.3 Повышение эффективности процесса

Третье улучшение, ожидаемое в ходе совершенствования организации, связано с эффективностью процесса. С увеличением развитости организации намеченные результаты улучшаются. По мере совершенствования организации издержки уменьшаются, сокращается период разработки, а производительность и качество повышаются. В организации на уровне 1 период разработки может быть довольно длительным вследствие большого объема доработок, выполняемых для исправления допущенных ошибок. Напротив, организации на более высоком уровне развития могут добиться сокращения общей продолжительности разработки посредством повышения эффективности процесса и уменьшения числа дорогостоящих доработок.

С.4 Общие неверные толкования

В приведенных ниже характеристиках модели представлены некоторые общие возражения против использования моделей CMM®. Данный подраздел предназначен для разъяснения некоторых общих неверных толкований модели.

С.4.1 Модели CMM® дают определение процессу проектирования

Распространенным неправильным представлением является то, модели CMM® определяют какой-то конкретный процесс. Они предоставляют организациям руководство по определению своих процессов и со временем улучшению эти процессов. Руководство применяется независимо от типа выполняемых процессов. Модель CMM® описывает, какие действия должны выполняться для оказания помощи в определении, управлении, мониторинге и улучшении процесса организации, а не как в точности должны выполняться конкретные действия.

Модели CMM® для определенных дисциплин, такие как SSE-CMM®, требуют обязательного выполнения определенных основных конструкторских работ как области процесса проектирования для этой дисциплины, но они не определяют точно, как должны выполняться эти действия.

Основным принципом применения модели CMM® является оказание поддержки проектным организациям в разработке и улучшению наиболее подходящего для них процесса проектирования. Основанием для этого является способность определять, документировать процесс проектирования и управлять им, а также стандартизировать его во всей организации. Этот принцип не фокусируется на каком-то конкретном жизненном цикле разработки, структуре организации или проектных технологиях.

С.4.2 Модели CMM® являются справочниками или руководствами для обучения

CMM® предназначены для руководства организациями при увеличении их возможностей по выполнению заданного процесса (например, безопасного проектирования). Модели CMM® не предназначены для применения в качестве справочников или учебных руководств с целью оказания помощи отдельным лицам в усовершенствовании их конкретных навыков в области проектирования. Целью является принятие организацией принципа, изложенного в CMM®, и использование методов, определенных в CMM®, как руководства для определения и усовершенствования ее процессов проектирования.

С.4.3 Модель SSE-CMM® заменяет оценку товара

Замена оценки продукта или сертификации системы моделью CMM® маловероятна. Но модель безусловно может направить проведение анализа третьей стороной на участки, указанные в оценке моделью CMM® как слабые места. Статистическое управление процессом не означает отсутствие дефектов. Скорее оно делает дефекты более предсказуемыми, поэтому выборочный контроль в виде анализа все еще необходим.

Все преимущества, ожидаемые от использования SSE-CMM®,основаны на интерпретациях практического опыта, полученного при использовании модели SEI CMM® for Software. Для предъявления претензий в отношении использования SSE-CMM® в оценках и сертификации организациям, занимающимся безопасным проектированием, следует прийти к соглашению о том, что развитость означает для безопасного проектирования. Как и в случае с моделью SEI CMM® for Software, претензии подлежат изучению, поскольку SSE-CMM® продолжает использоваться организациями.

С.4.4 Требуется слишком много документации

При прочтении CMM® можно поразиться изобилию подразумеваемых процессов и планов. CMM® включает в себя требования к документированию процессов и процедур и обеспечению их выполнения в соответствии с документацией. Несмотря на то, что в CMM® требуется некоторое число процессов, планов и других типов документации, число или тип документов, предназначенных для разработки, не указывается. Один план обеспечения безопасности может удовлетворять требованиям многих областей процесса. Модель CMM® просто указывает на типы информации, которые должны документироваться.

С.5 Ключевые понятия

С.5.1 Введение

В данный документ введены термины и понятия, имеющие определенное значение в контексте SEE CMM®. В этом разделе конкретизируются понятия, являющиеся критическими для эффективного понимания, интерпретации и использования модели SEE CMM®. Некоторым понятиям, таким как «общая практика» и «базовая практика», дается определение в посвященных им разделах описания модели. Понятиями, обсуждаемыми в этом разделе, являются:

- организация;

- проект;
- система;
- рабочий продукт;
- заказчик;
- процесс;
- область процесса;
- независимость должности;
- возможности процесса;
- институционализация;
- управление процессом;
- модель зрелости (зрелости) возможностей.

С.5.2 Организации и проекты

Двумя терминами, применяемыми в рамках модели SEE CMM® для обозначения различий между аспектами организационной структуры, являются организация и проект. Другие компоненты структуры, такие как группы, существуют в рамках хозяйственных единиц, но общепринятая терминология, охватывающая все бизнес-контексты, отсутствует. Эти два термина выбраны, поскольку они используются/понимаются большинством предполагаемых пользователей SEE CMM®.

С.5.2.1 Организация

В модели SEE CMM® организация определяется как подразделение компании, вся компания или другой экономический объект (например, правительственное учреждение или отрасль обслуживания), ответственные за наблюдение за различными проектами. Все проекты в рамках организации обычно используют общие политики на высшей ступени структуры отчетности. Организация может состоять из локализованных или географически распределенных проектов и вспомогательных инфраструктур.

Термин «организация» используется для обозначения инфраструктуры поддержки общих стратегических, бизнес- и связанных с процессом функций. Инфраструктура существует и должна сохраняться для обеспечения эффективности деловой деятельности в отношении производства, поставки, поддержки и маркетинга своей продукции.

С.5.2.2 Проект

Проектом является совокупность усилий и других ресурсов, сосредоточенной на разработке и/или поддержании конкретного продукта или предоставления услуги. Продукт может представлять собой аппаратные средства, программное обеспечение и другие компоненты. Обычно проект имеет собственное финансирование, смету и график поставок. Проект может учреждать собственный организационный объект, в его рамках может быть структуирована бригада сотрудников, целенаправленная рабочая группа или другая группа, используемая организацией для производства продукции или предоставления услуг.

Области процесса в доменной области модели SEE CMM® были разделены на три категории - инжиниринг, проект и организация. Категории проекта и организации различаются на основе типичного права собственности. Модель SEE CMM® различает категории проект и организация, отмечая фокусирование проекта на определенном продукте, в то время как организация объединяет один или более проектов.

С.5.3 Система

В модели SEE CMM® система определяется как:

- интегрированная комбинация из людей, продукции, услуг и процессов, обеспечивающих возможность удовлетворять потребность или достигать цели;
- монтаж предметов или деталей, формирующих комплекс или одно целое (то есть, набор компонентов, организованный для выполнения определенной функции или многих функций);
- взаимодействующая комбинация элементов, рассматриваемая в отношении к функции.

Системой может быть продукт, являющийся только аппаратными средствами, аппаратными средствами/программным обеспечением, только программным обеспечением или услугой. Термин «система» применяют по всей модели для указания на общее число продуктов, доставленных заказчику(ам) или пользователю(ам). Определение продукта как системы является признанием потребности рассмотрения

всех элементов продукта и их средств сопряжения систематическим и дисциплинированным образом, чтобы, в конечном счете, достичь общих целей в области издержек, графика выполнения и функционирования (включая безопасность) фирмы, производящей продукт.

С.5.4 Рабочая документация

Рабочей документацией являются все документы, отчеты, файлы и т.д., собранные в ходе выполнения любого процесса. Вместо перечисления отдельных рабочих документов для каждой области процесса модель SEE CMM® составляет список «Примеры результатов деятельности» определенной базовой практики с целью дальнейшего развития его предполагаемой области действия. Эти списки являются чисто иллюстративными и отражают диапазон контекста организации и продукта. Их нельзя считать «обязательными» рабочими документами.

С.5.5 Заказчик

Заказчиком является отдельное лицо(а) или экономический объект, для которого разрабатывается продукт или предоставляется услуга и/или отдельное лицо(а) или экономический объект, которые используют продукт или услугу.

В контексте модели SEE CMM® заказчик может быть договорным или не договорным. Договорным заказчиком является отдельное лицо или экономический объект, который заключает договор с другим объектом по производству определенного продукта или партии продуктов по спецификациям, представленным заказчиком. Не договорным или заказчиком, руководствующимся рынком, является одно из многих отдельных лиц или фирм, у которых есть реальная или воспринимаемая потребность в каком-либо продукте. Заказчика может также представлять его доверенное лицо, например, фокус-группы по маркетингу или продукции.

В большинстве случаев модель SEE CMM® для удобства в грамматическом плане применяет термин «заказчик» в единственном числе. Однако вполне допустимо участие многочисленных заказчиков.

Следует отметить, что в контексте SEE CMM® отдельное лицо или объект, пользующиеся продуктом или услугой, также включены в понятие «заказчик». Это справедливо для случая с договорным заказчиком, поскольку объект, которому поставляется продукт или предоставляется услуга, не всегда является лицом или объектом, который будет фактически пользоваться этим продуктом или услугой.

Понятие и применение термина "заказчик" в отношении проектирования безопасности в настоящем стандарте применяется расширенно, включая в себя и последующих пользователей.

С.5.6 Процесс

Процессом называется совокупность действий, осуществляемых для достижения заданной цели. Действия могут осуществляться итеративно, последовательно или параллельно. Некоторые действия могут трансформировать входные рабочие продукты в выходные, необходимые для других действий. Допустимая последовательность выполнения действий ограничивается наличием входных рабочих продуктов и ресурсов и административным управлением. Четко заданный процесс включает в себя действия, входные и выходные артефакты каждого действия и механизмы контроля за осуществлением действий.

В модели SEE CMM® упоминаются несколько типов процессов, включая «заданные» и «выполняемые» процессы. Заданный процесс описывается для организации или организацией для применения ее специалистами по безопасности. Это описание может содержаться, например, в документе или библиотеке активов процесса. Заданным процессом является то, что должны делать специалисты по безопасности организации. Выполняемым процессом является то, что фактически делают специалисты по безопасности.

С.5.7 Область процесса

Областью процессов (PA) является заданная совокупность связанных с безопасностью характеристик процесса проектирования, которые при совместном выполнении могут содействовать достижению заданной цели.

Область процесса состоит из базовых практик, являющихся обязательными характеристиками, которые должны присутствовать в рамках внедренного процесса безопасности до того, как организация сможет заявить об удовлетворении процесса в данной области. Содержание базовых практик разрабатываются далее в подразделе, в котором приведена архитектура модели.

С.5.8 Ролевая независимость

Областями процессов в модели SEE CMM® являются группы практических приемов, которые вместе служат достижению общей цели. Но группирование не означает, что все базовые практики процесса обязательно выполняются одним должностным лицом. Все базовые практики записаны в формате «действие-объект» (то есть без определенного субъекта) с целью минимизации ощущения, что определенная базовая практика «принадлежит» определенной должности. Это один способ, которым синтаксис модели обеспечивает ее применение в широком спектре организационных контекстов.

С.5.9 Возможности процесса

Возможности процесса формулируются как поддающаяся количественному определению совокупность ожидаемых результатов, которые можно получить, следуя заданному процессу. Метод оценки модели SEE CMM® (SSAM) основан на концепциях статистического управления процессом, которые определяют использование возможностей процесса. SSAM может применяться для определения уровней возможностей процесса для каждой области процесса в рамках проекта или организации. Эти концепции находят свое отражение в аспекте возможностей модели SEE CMM®, которые обеспечивают руководство по улучшению возможностей практики проектирования безопасности, на которые делается ссылка в домене модели SEE CMM®.

Возможности процесса организации помогают предсказать способность проекта к выполнению каких-либо целей. Проекты в организациях с низкими возможностями имеют большое количество вариантов достижения целей, связанных с издержками, графиком, функциональными возможностями и качеством.

С.5.10 Институционализация

Институционализацией является создание инфраструктуры предприятия и корпоративной культуры, определяющие методы, практические приемы и процедуры деятельности, даже когда лица, которые их установили, уже с ними не связаны. Часть модели SEE CMM®, связанная с возможностями процессов, поддерживает институционализацию посредством предоставления практических приемов и определения путей реализации деятельности и непрерывного ее улучшения.

Таким образом, модель SEE CMM® утверждает, что организациям следует однозначно поддерживать определение и улучшение процесса, а также управление им. Институционализация предоставляет собой путь к получению максимального преимущества от процесса, демонстрирующего стабильные характеристики проектирования безопасности.

С.5.11 Управление процессом

Управление процессом является совокупностью действий и инфраструктур, используемых для предсказания, оценки и контроля за выполнением процесса. Управление процессом подразумевает определенность процесса (поскольку невозможно контролировать и прогнозировать нечто неопределенное). Фокусирование на менеджмент процесса подразумевает, что проект или организация учитывает связанные как с продуктом, так и с процессом факторы при планировании, эксплуатации, оценивании, мониторинге и корректировании.

С.5.12 Модель зрелости возможностей®

Модель зрелости возможностей®, подобная SEE-CMM®, описывает этапы, по которым процессы совершенствуются по мере их определения, реализации и усовершенствования. Модель предоставляет руководство по выбору стратегий усовершенствования процессов путем определения текущих возможностей конкретных процессов и выявления проблем, наиболее критичных для улучшения качества и процесса в пределах определенного домена (области). CMM® может принимать вид эталонной модели с целью использования ее в качестве руководства для разработки и улучшения развитого и заданного процесса.

Модель CMM® может также применяться для оценивания наличия и институционализации заданного процесса, который выполняет упомянутые в ссылках практические приемы. Модель зрелости возможностей охватывает процессы, применяемые для выполнения задач указанного домена (например, проектирования безопасности). Модель CMM® может также охватывать процессы, используемые для эффективного развития и применения людских ресурсов, а также внедрения соответствующей технологии в продукцию и инструменты, применявшиеся для ее производства. В отношении проектирования безопасности последние аспекты еще не были разработаны детально.

Приложение D
(справочное)

Общие практики

D.1 Общая часть

Настоящее приложение содержит общие практики (то есть практические приемы, применимые ко всем процессам). Они применяются в оценке процесса для определения его возможностей. Общие практики группируются по общему признаку и уровню возможностей. Данные приемы делятся на следующие уровни возможностей, каждый из которых обладает общими признаками:

- уровень возможностей 1 – выполняется неформально;
- уровень возможностей 2 – планируется и отслеживается;
- уровень возможностей 3 – четко определяется;
- уровень возможностей 4 – контролируется в количественном отношении;
- уровень возможностей 5 – постоянно совершенствуется.

Примечание - Данное приложение содержит материал, который находился в Приложении А предыдущей версии настоящего стандарта. Оно сохраняется в качестве справочного приложения для обеспечения полной совместимости с предыдущими версиями.

Общий формат уровней возможностей показан на рисунке D.1. В кратком описании содержится обзор каждого уровня возможностей. Каждый уровень разлагается на набор общих признаков, который состоит из группы общих практик. Каждая общая практика описана детально, следуя краткому изложению общих признаков.

Уровень возможностей 1 – Наименование уровня возможностей
Краткое описание – Обзор уровня возможностей
Перечень общих признаков – Перечень, показывающий номер и наименование каждого общего признака
Общий признак 1.1 – Наименование общего признака
Краткое описание – Обзор уровня возможностей
Перечень общих практик - Перечень, показывающий номер и наименование каждой общей практики
GP 1.1.1 – Наименование общей практики
Описание - Обзор данной общей практики
Примечания - Любые примечания о данном общем практическом приеме
Взаимосвязи - Все взаимосвязи с другими частями модели
GP 1.1.2…

Рисунок D.1 - Формат уровней возможностей

D.2 Уровень возможностей 1 – Выполняется неформально

D.2.1 Общие признаки уровня возможностей

D.2.1.1 Общие практики с общим признаком

D.2.1.1.1 Краткое описание

Базовые практики области процесса в целом выполняются. Выполнение этих базовых практик не может строго планироваться и отслеживаться. Выполнение вообще зависит от знаний и усилий отдельных лиц. Выполнение этих практик подтверждается рабочей продукцией. Лица внутри организации признают необходимость выполнения какого-либо действия и приходят к общему соглашению о выполнении этого действия так, каким образом и когда это требуется. Для процесса имеются идентифицируемые рабочие документы.

D.2.1.1.2 Перечень общих признаков

Этот уровень возможностей имеет следующие общие признаки:

Общий признак 1.1 – Базовые практики выполнены.

D.2.2 Общий признак 1.1 – Базовые практики выполнены

D.2.2.1 Общие практики общего признака

D.2.2.1.1 Краткое описание

Общие практики этого общего признака просто обеспечивают выполнение тем или иным образом базовых практик области процесса. Однако, по - видимому, согласованность функционирования и качество произведенной рабочей продукции в значительной степени являются непостоянными непостоянны вследствие нехватки (малочисленности) имеющихся средств управления.

D.2.2.1.2 Перечень общих практик

Этот общий признак объединяет следующие общие практики:

- GP 1.1.1 – Выполняет процесс.

D.2.2.2 GP 1.1.1 – Выполняет процесс

D.2.2.2.1 Описание

Выполнениепроцесса, который реализует базовые практики процесса для предоставления рабочей продукции и/или услуг заказчику.

D.2.2.2.2 Примечания

Этот процесс можно назвать «неформальным процессом». Заказчик этой области процесса может принадлежать организации или быть посторонним.

D.3 Уровень возможностей 2 – Запланирован и отслежен

D.3.1 Общие признаки уровня возможностей

D.3.1.1 Общие практики общего признака

D.3.1.1.1 Краткое описание

Выполнение базовых практик в области процесса планируется и отслеживается. Соответствие выполнения заданным процедурам верифицируется. Рабочая продукция соответствует установленным стандартам и требованиям. В целях отслеживания выполнение области процесса измеряется, таким образом позволяя организации управлять своими действиями на основе фактических показателей. Основное отличие от «Уровень 1 – Выполняется неформально» заключается в том, что выполнение процесса планируется и управляется.

D.3.1.1.2 Перечень общих признаков

Этот уровень возможностей имеет следующие общие признаки:

- общий признак 2.1 Планирование выполнения;
- общий признак 2.2 Упорядоченное выполнение;
- общий признак 2.3 Проверка выполнения;
- общий признак 2.4 Отслеживание выполнения.

D.3.2 Общий признак 2.1 – Планирование выполнения

D.3.2.1 Общие практики общего признака

D.3.2.1.1 Краткое описание

Общие практики этого общего признака сосредоточены на аспектах планирования выполнения этой области процесса и связанных с ней базовых практик. Таким образом рассматривается все: документация по процессу, обеспечение соответствующего инструментария для выполнения процесса, планирование выполнения процесса, обучение выполнению процесса; распределение ресурсов для процесса и распределение обязанностей по выполнению процесса. Эти общие практики формируют важную основу для упорядоченного выполнения процесса.

D.3.2.1.2 Перечень общих практик

Этот общий признак объединяет следующие общие практики:

- GP 2.1.1 - Распределяет ресурсы;

- GP 2.1.2 - Распределяет обязанности;
- GP 2.1.3 - Документирует процесс;
- GP 2.1.4 - Обеспечивает инструментарий;
- GP 2.1.5 - Обеспечивает обучение;
- GP 2.1.6 - Планирует процесс.

D.3.2.2 GP 2.1.1 - Распределяет ресурсы

D.3.2.2.1 Описание
Распределяет адекватные ресурсы (включая людей) для выполнения области процесса.
D.3.2.2.2 Примечания
Отсутствуют.
D.3.2.2.3 Взаимосвязи
Идентификация критически важных ресурсов осуществляется в области процесса PA16.

D.3.2.3 GP 2.1.2 - Распределяет обязанности

D.3.2.3.1 Описание
Распределяет обязанности по разработке изделий и/или предоставлению услуг области процесса.
D.3.2.3.2 Примечания
Отсутствуют.
D.3.2.3.3 Взаимосвязи
Эта практика связана конкретно с областью процессов PA16.

D.3.2.4 GP 2.1.3 - Документирует процесс

D.3.2.4.1 Описание
Документирует подход к выполнению области процесса в стандартах и/или процедурах.
D.3.2.4.2 Примечания
Участие людей, выполняющих процесс (его владельцев), имеет большое значение при создании описания процесса. Процессы в организации или процессы проекта не обязательно должны полностью соответствовать частям процесса данной модели. Следовательно, область процесса может быть представлена несколькими путями (например, политиками, стандартами и/или процедурами) и описание процесса может распространяться более чем на одну область процесса.
D.3.2.4.3 Взаимосвязи
Это описание процесса уровня 2. Описания процесса совершенствуются с увеличением возможностей процесса (см. описания этого процесса в GP 3.1.1, GP 3.1.2, GP 5.1.2, GP 5.2.3).
Стандарты и процедуры, описывающие процесс на этом уровне, вероятно, должны включать в себя измерения, так что выполнение можно отследить с помощью оценки результатов измерения (см. общий признак 2.4).

D.3.2.5 GP 2.1.4 - Обеспечивает инструментарий

D.3.2.5.1 Описание
Обеспечивает соответствующий инструментарий для поддержки выполнения области процесса.
D.3.2.5.2 Примечания
Требуемый инструментарий меняется в зависимости от выполняемого процесса. Лица, выполняющие процесс, должны хорошо знать инструментарий, требуемый для выполнения процесса.
D.3.2.5.3 Взаимосвязи
Изменения в инструментарии могут быть частью усовершенствований процесса (см. практические приемы по усовершенствованиям процесса в GP 5.1.2, GP 5.2.3).
Инструментарий рассматривается в PA20.

D.3.2.6 GP 2.1.5 - Обеспечивает обучение

D.3.2.6.1 Описание
Обеспечивает должное обучение лиц, выполняющих область процесса.
D.3.2.6.2 Примечания
Обучение и метод его проведения изменяют возможности процесса вследствие изменений в методе его выполнения и управления.

D.3.2.6.3 Взаимосвязи
Обучение и руководство обучением изложены в PA21.

D.3.2.7 GP 2.1.6 - Планирует процесс

D.3.2.7.1 Описание
Планирование выполнения области процесса.
D.3.2.7.2 Примечания
Планы по выполнению областей процесса по категориям проектирования и проекта могут быть представлены в виде плана проекта, тогда как планы для категории организации могут быть на организационном уровне.
D.3.2.7.3 Взаимосвязи
Планирование проекта изложено в части проекта PA16.

D.3.3 Общий признак 2.2 – Упорядоченное выполнение

D.3.3.1 Общие практики общего признака

D.3.3.1.1 Краткое описание
Общие практики этого общего признака сосредоточены на объеме контроля, осуществляемого над процессом. Следовательно, учитываются использование планов выполнения процесса в соответствии со стандартами и процедурами и передача рабочей продукции, полученной в ходе выполнения процесса, под управление конфигурациями. Эти общие практики образуют важную основу для возможности проверять выполнение процесса.

D.3.3.1.2 Перечень общих практик
Этот общий признак объединяет следующие общие практики:

- GP 2.2.1 - Применяет планы, стандарты и процедуры;
- GP 2.2.2 - Осуществляет управление конфигурациями.

D.3.3.2 GP 2.2.1 - Применяет планы, стандарты и процедуры

D.3.3.2.1 Описание
Применяет документированные планы, стандарты и процедуры при выполнении области процесса.
D.3.3.2.2 Примечания
Процесс, выполняемый в соответствии с его описаниями, называется «описанный процесс». Меры измерения процесса должны быть определены в стандартах, процедурах и планах.
D.3.3.2.3 Взаимосвязи
Используемые стандарты и процедуры были документированы в GP 2.1.3, а планы - в GP 2.1.6. Эта практика является развитием GP 1.1.1 и эволюционирует далее в GP 3.2.1.

D.3.3.3 GP 2.2.2 - Осуществляет управление конфигурациями

D.3.3.3.1 Описание
Передает рабочую продукцию области процесса под управление версиями или конфигурациями.
D.3.3.3.2 Примечания
Отсутствуют.
D.3.3.3.3 Взаимосвязи
Типичные процессы, требуемые для поддержки системного проектирования в дисциплине управления конфигурациями, описаны в области процесса.
Там, где область процесса PA13 фокусируется на общих практических приемах управления конфигурациями, эта общая практика сосредоточена на применении этих практических приемов относительно рабочей продукции отдельной исследуемой области процесса.

D.3.4 Общий признак 2.3 – Проверяет выполнение процесса

D.3.4.1 Общие практики общего признака

D.3.4.1.1 Краткое описание

Общие практики этого общего признака сосредоточены на подтверждении выполнения процесса, как это было намечено. Учитываются проверка выполнения процесса на соответствие применяемым стандартам и процедурами и аудит результатов деятельности. Эти общие практики образуют важную основу для возможности отслеживания выполнения процесса.

D.3.4.1.2 Перечень общих практик

Этот общий признак объединяет следующие общие практики:

- GP 2.3.1 - Проверяет соответствие процесса;
- GP 2.3.2 - Проводит проверку рабочей продукции.

D.3.4.2 GP 2.3.1 - Проверяет соответствие процесса

D.3.4.2.1 Описание

Проверяет соответствие процесса применимым стандартами/или процедурам.

D.3.4.2.2 Примечания

Отсутствуют.

D.3.4.2.3 Взаимосвязи

Применимые стандарты и процедуры документированы в GP 2.1.3 и применяются в GP 2.2.1.

Процесс менеджмента качества и/или гарантирования изложен в PA12.

D.3.4.3 GP 2.3.2 - Проводит проверку рабочей продукции

D.3.4.3.1 Описание

Проверяет соответствие рабочей продукции применимым стандартами/или процедурам.

D.3.4.3.2 Примечания

Отсутствуют.

D.3.4.3.3 Взаимосвязи

Применимые стандарты и процедуры документированы в GP 2.1.3 и применяются в GP 2.2.1.

Требования к продукции разработаны и представлены в области процесса PA10. Далее верификация и проверка достоверности рассматриваются в PA11.

D.3.5 Общий признак 2.4 - Отслеживает выполнение процесса

D.3.5.1 D.3.4.1 Общие практики общего признака

D.3.5.1.1 Краткое описание

Общие практики этого общего признака сосредоточены на возможности контролировать прогресс выполнения процесса. Таким образом, учитываются отслеживание выполнения процесса в сопоставлении с измеримым планом и принятие корректирующих мер в случае значительного отклонения выполнения процесса от плана. Эти общие практики образуют важную основу для возможности получения четко определенных процессов.

D.3.5.1.2 Перечень общих практик

Этот общий признак объединяет следующие общие практики:

- GP 2.4.1 - Отслеживает с измерением;
- GP 2.4.2 - Принимает корректирующие меры.

D.3.5.2 GP 2.4.1 - Отслеживает с измерением

D.3.5.2.1 Описание

Отслеживает состояние области процесса, сопоставляя его с планом и используя измерения графика, стоимости и эффективности выполнения проекта.

D.3.5.2.2 Примечания

Создание статистики измерений является основой управления данными и начинается здесь. Отслеживание посредством измерений обеспечивает основу создания четко определенных данных, которые будут применяться в рамках четко определенных процессов на уровне возможностей 3. Общие про-

екты могут использовать меры измерения улучшения процессов и меры измерения безопасности информации. Данные, необходимые для вычисления мер, должны быть надежными, а рассматриваемый процесс должен быть измеримым. Для измерения должны приниматься во внимание только те процессы, которые могут быть последовательными и повторяемыми.

D.3.5.2.3 Взаимосвязи

Использование измерения подразумевает, что в GP 2.1.3 и GP 2.1.6 были определены и выбраны меры измерения, а в GP 2.2.1 собраны данные.

Меры измерения безопасности информации изложены в области процесса PA06.

Отслеживание проекта описано в области процесса PA15.

D.3.5.3 GP 2.4.2 - Принимает корректирующие меры

D.3.5.3.1 Описание

Принимает корректирующие меры в случае значительного отклонения прогресса процесса от запланированного.

D.3.5.3.2 Примечания

Прогресс может изменяться из-за того, что были неточными оценки, посторонние факторы влияли на выполнение процесса или были изменены требования, на которых был основан план. Корректирующие меры могут включать в себя изменение процесса, плана или их обоих.

D.3.5.3.3 Взаимосвязи

Использование измерения подразумевает, что в GP 2.1.3 и GP 2.1.6 были определены и выбраны меры измерения, а в GP 2.2.1 — были собраны данные.

Управление процессом описано в области процесса PA15.

D.4 Уровень возможностей 3 – Четко заданный процесс

D.4.1 Общие признаки уровня возможностей

D.4.1.1 Общие практики общего признака

D.4.1.1.1 Краткое описание

Базовые практики выполняются в соответствии с четко заданным процессом, используя утвержденные специализированные версии стандартных документированных процессов. Основное отличие от Уровня возможностей 2 «Запланированный и отслеженный» заключается в том, что процесс планируется и управляется с помощью стандартного процесса, применяемого во всей организации.

D.4.1.1.2 Перечень общих признаков

Данный уровень возможностей объединяет следующие общие признаки:

- общий признак 3.1 - Определение стандартного процесса;
- общий признак 3.2 - Выполняет заданный процесс;
- общий признак 3.3 - Координирует практические процессы.

D.4.2.1 Общие практики общего признака

D.4.2.1.1 Краткое описание

Общие практики этого общего признака сосредоточены на институционализации стандартного процесса организации. Источником или основой процесса институционализации может быть один или более аналогичных процессов, успешно применявшихся в специфических проектах. Видимо, стандартный процесс организации надо адаптировать для применения в конкретной ситуации, чтобы учитывались также потребности адаптации. Таким образом, учитываются документация стандартного процесса организации и адаптация этого процесса для конкретных использований. Эти общие практики образуют важную основу для выполнения определенных процессов.

D.4.2.1.2 Перечень общих практик

Данный общий признак объединяет следующие общие практики:

- GP 3.1.1 - Стандартизирует процесс;
- GP 3.1.2 - Адаптирует стандартный процесс.

D.4.2.2. GP 3.1.1 - Стандартизирует процесс

D.4.2.2.1 Описание

Документирует стандартный процесс или семейство процессов организации, которое описывает путь реализации базовых практик области процесса.

D.4.2.2.2 Примечания

Основным различием между общими практиками 2.1.3 и 3.1.1 и описаниями процессов Уровней 2 и 3 является область применения политик, стандартов и процедур. В GP 2.1.3 стандарты и процедуры могут использоваться только в случае конкретного процесса (например, в определенном процессе). В ПЗ 3.1.1 политики, стандарты и процедуры разрабатываются на организационном уровне для общего пользования и называются «определение стандартного процесса».

Для охвата области процесса могут быть определены несколько процессов, так как в данной модели зрелости возможностей процессы в организации необязательно должны соответствовать частям процесса по принципу «один к одному». Заданный процесс может охватывать многочисленные области процесса. Модель SSE-CMM® не навязывает организациям структуру описаний процессов. Следовательно, для изучения различий между областями применения, ограничениями заказчика и т.д. можно определить несколько стандартных процессов. Они называются «семейством стандартных процессов».

D.4.2.2.3 Взаимосвязи

Описание процесса Уровня 2 документировано в GP 2.1.3. Описание процесса Уровня 3 адаптировано в GP 3.1.2.

Процесс разработки описания процесса изложен в области процесса PA17.

D.4.2.3 GP 3.1.2 - Адаптирует стандартный процесс

D.4.2.3.1 Описание

Адаптирует семейство стандартных процессов для создания заданного процесса, учитывающего определенные потребности специфического применения.

D.4.2.3.2 Применения

Адаптация стандартного процесса организации создает определение процесса Уровня 3. Для определенных процессов на уровне проекта при адаптации учитываются конкретные потребности проекта.

D.4.2.3.3 Взаимосвязи

Стандартный процесс организации (семейство) документируется в GP 3.1.1. Определение адаптированного процесса используется в GP 3.2.1.

Рекомендации по адаптации приведены в области процесса PA17.

D.4.3 Общий признак 3.2 – Выполнение заданного процесса

D.4.3.1 Общие практики общего признака

D.4.3.1.1 Краткое определение

Общие практики этого общего признака сосредоточены на повторяемом выполнении четко заданного процесса. Таким образом, учитываются использование процесса институционализации, проверка результатов процесса (т.е. рабочей продукции) на наличие дефектов и использование данных о выполнении и результатах процесса. Эти общие практики создают важную основу координации практик, связанных с безопасностью.

D.4.3.1.2 Перечень общих практик

Данный общий признак объединяет следующие общие практики:

- GP 3.2.1 - Использует четко заданный процесс;
- GP 3.2.2 - Проводит проверку на наличие дефектов;
- GP 3.2.3 - Использует четко определенные данные.

D.4.3.2 GP 3.2.1 - Использует четко заданный процесс

D.4.3.2.1 Описание

Использует четко заданный процесс при реализации области процесса

D.4.3.2.2 Примечания

Определение «заданный процесс» обычно является специально измененным вариантом определения стандартного процесса организации. Четко заданный процесс состоит из политик, стандартов, входных данных, критериев входа, действий, процедур, специфических ролей, измерений, проверки дос-

товерности, шаблонов, выходных данных и критериев выхода, которые документированы, последовательны и завершены.

D.4.3.2.3 Взаимосвязи

Определение стандартного процесса организации приведены в GP 3.1.1. Заданный процесс создан посредством адаптации в GP 3.1.2.

D.4.3.3 GP 3.2.2 - Проводит проверку на наличие дефектов

D.4.3.3.1 Описание

Проводит проверку соответствующей рабочей продукции области процесса на наличие дефектов.

D.4.3.3.2 Примечания

Отсутствуют.

D.4.3.3.3 Взаимосвязи

Отсутствуют.

D.4.3.4 GP 3.2.3 - Использует четко определенные данные

D.4.3.4.1 Описание

Использует данные по выполнению заданного процесса для его управления.

D.4.3.4.2 Примечания

Данные измерений, впервые собранные на Уровне 2, в этой точке используются более активно, закладывая основу количественного управления на следующем уровне.

Чтобы быть полезными для отслеживания выполнения и управления процессом, меры измерения должны представить соответствующие тенденции выполнения по прошествии длительного времени и указывать действия по улучшению, которые можно применить в проблемных областях. В измерениях должны применяться четко определенные данные. Анализ мер измерения многочисленных проектов мог бы идентифицировать тенденции и предоставить организациям дополнительную информацию по воздействиям на деловую деятельность.

D.4.3.4.2 Взаимосвязи

Эта практика является развитием GP 2.4.2; принятые здесь корректирующие действия основаны на четко определенном процессе, имеющем объективные критерии для определения прогресса (см. GP 3.2.1.).

D.4.4 Общий признак 3.3 – Координирует практические приемы

D.4.4 1 Общие практики общего признака

D.4.4.1.1 Краткое определение

Действия общих практик этого общего признака сосредоточены на координации действий по всему проекту и всей организации. Многие значимые действия выполняются совершенно разными группами в рамках проекта и группами технического обслуживания организации от имени проекта. Отсутствие координации может привести к задержкам или получению несравнимых результатов. Следовательно, изучается координация действий внутри групп, между группами и сторонних действий. Эти общие практики образуют важную основу для получения способности количественного управления процессами.

D.4.4.1.2 Перечень общих практик

Данный общий признак объединяет следующие общие практики:

- GP 3.3.1 - Выполняет координацию внутри групп;
- GP 3.3.2 - Выполняет координацию между группами;
- GP 3.3.3 - Выполняет внешнюю координацию.

D.4.4.2 GP 3.3.1 - Выполняет координацию внутри групп

D.4.4.2.1 Описание

Координирует обмен информацией в рамках инженерной дисциплины.

D.4.4.2.2 Примечания

Этот вид координации рассматривает потребность в инженерной дисциплине для согласованного принятия решений по техническим вопросам (например, средства управления доступом, проверка состояния безопасности). Обязательства, ожидаемые результаты и ответственность соответствующих

технических специалистов согласовываются всеми участниками и документируются. Технические проблемы отслеживаются и решаются.

D.4.4.2.3 Взаимосвязи

Эта общая практика тесно связана с GP 3.2.1 в том плане, что для обеспечения эффективной координации между процессами взаимосвязи должны быть четко определены.

Цели и методы координации рассматриваются в PA07.

D.4.4.3 GP 3.3.2 - Выполняет координацию между группами

D.4.4.3.1 Описание

Координирует обмен информацией между различными группами организации.

D.4.4.3.2 Примечания

Этот вид координации требует от технических специалистов учета взаимосвязей между техническими областями (например, оценка риска, входные данные проектирования, проверка состояния безопасности) среди задействованных зон обслуживания. Целью является проверка координации данных, собранных в качестве части GP 3.3.1, с другими инженерными областями.

Взаимосвязь между инженерными группами устанавливается посредством общей договоренности по обязательствам, ожидаемым результатам и обязанностям каждой конструкторской работы в рамках организации. Эти работы и договоренности согласуются и документируются по всей организации и учитывают взаимодействие между различными группами в рамках проекта/организации. Технические проблемы отслеживаются и решаются задействованными инженерными группами в рамках проекта/организации.

D.4.4.3.3 Взаимосвязи

Эта общая практика тесно связана с GP 3.2.1 в том плане, что для обеспечения между процессами эффективной координации они должны быть четко определены.

Цели и методы координации рассматриваются в PA07. Специфические практические приемы проектирования безопасности для других инженерных групп предоставляются своевременно, а точные входные данные рассматриваются в PA09.

D.4.4.4 GP 3.3.3 - Выполняет внешнюю координацию

D.4.4.4.1 Описание

Координирует обмен информацией со сторонними группами.

D.4.4.4.2 Примечания

Данный вид координации учитывает потребности сторонних объектов и субъектов, запрашивающих или требующих технических результатов (например, заказчиков, сертификационных действий, оценщиков).

Взаимосвязь между сторонними группами (например, заказчиком, органом сертификации безопасности систем, пользователем) устанавливается посредством общей договоренности по обязательствам, ожиданиям и обязанностям каждой конструкторской работы в рамках организации. Инженерные группы выявляют, отслеживают и решают сторонние технические проблемы.

D.4.4.4.3 Взаимосвязи

Эта общая практика тесно связана с GP 3.2.1 в том плане, что для обеспечения эффективной координации между процессами взаимосвязи должны быть четко определены.

Цели и методы координации рассматриваются в PA07. Потребности заказчика в обеспечении безопасности идентифицируются в PA10. Потребности заказчика в доверия рассматриваются в PA06.

D.5 Уровень возможностей 4 – Количественно управляемый

D.5.1 Общие признаки уровня возможностей

D.5.1.1 Общие практики общего признака

D.5.1.1.1 Краткое описание

Собираются и анализируются детальные меры измерения выполнения. Результатом этих действий является понимание возможностей процесса в количественном отношении и улучшению способности прогнозирования выполнения. Выполнение управляется эффективным образом и качество рабочей продукции известно в количественном отношении. Основным отличием от Четко Определенного Уровня является понимание заданного процесса в количественном отношении и его контролирование.

D.5.1.1.2 Перечень общих признаков

Данный уровень возможностей объединяет следующие общие признаки:

- общий признак 4.1 - Установление измеримых целей получения качества;
- общий признак 4.2 - Объективное управление выполнением.

D.5.1.2 Общий признак 4.1 - Установление измеримых целей получения качества

D.5.2.1 Общие практики общего признака

D.5.2.1.1 Краткое описание

Действия общих практик этого общего признака сосредоточены на установлении измеримых целей для рабочей продукции, разработанных в ходе технологических процессов организации. Таким образом, рассматривается установление целей получения качества. Эти общие практики образуют важную основу для объективного управления выполнением процесса.

D.5.2.1.2 Перечень общих практик

Этот общий признак объединяет следующие общие практики:

- GP 4.4.1 - Устанавливает цели получения качества.

D.5.2.2 GP 4.4.1 - Устанавливает цели получения высокого качества

D.5.2.2.1 Описание

Устанавливает измеримые цели получения высокого качества рабочей продукции семейства стандартных процессов организации.

D.5.2.2.2 Примечания

Эти цели получения высокого качества могут быть привязаны к стратегическим целям получения высокого рейтинга организации, определенным потребностями и приоритетами заказчика или тактическими потребностями проекта. Указанные здесь меры измерения выходят за пределы традиционных мер измерения конечного продукта. Они предназначены для обеспечения достаточного понимания процессов, используемых для установления и применения промежуточных целей для получения качества высокого рабочей продукции.

D.5.2.2.3 Взаимосвязи

Для установления целей получения высокого качества рабочей продукции особенно важны данные, собранные при проверках дефектов (GP 3.2.2).

D.5.3 Общий признак 4.2 – Объективное управление выполнением процесса

D.5.3.1 Общие практики общего признака

D.5.3.1.1 Краткое описание

Общие практики этого общего признака сосредоточены на определении количественной меры измерения возможностей процесса и применение этих мер для управления процессом. Следовательно, рассматриваются количественное определение возможностей процесса и применение этих мер в качестве основы для проведения корректирующих действий. Эти общие практики создают важную основу для владения способностью обеспечения непрерывного усовершенствования.

D.5.3.1.2 Перечень общих практик

Общим признаком объединяющим следующие общие практики являются:

- GP 4.2.1 - Определение возможности процесса;
- GP 4.2.2 - Использование возможности процесса.

D.5.3.2 GP 4.2.1 - Определяет возможности процесса

D.5.3.2.1 Описание

Определяет в количественном отношении возможности заданного процесса.

D.5.3.2.2 Примечания

Это возможность количественного определения, основанная на четко определенном (см. GP 3.1.1 и GP 3.2.3) и измеряемом процессе (см. GP 2.4.1). Измерения присущи определению процесса и их результаты собираются в ходе выполнения процесса.

D.5.3.2.3 Взаимосвязи

Этот заданный процесс устанавливается посредством адаптации в GP 3.1.2 и выполняется в GP 3.2.1.

D.5.3.3 GP 4.2.2 - Использует возможности процесса

D.5.3.3.1 Описание

Корректирующие меры применяются в случае невыполнения процесса в рамках его возможностей.

D.5.3.3.2 Примечания

Для понимания, когда и какие корректирующие меры следует применять, используются специальные причины изменения, идентифицированные на основе знания возможностей процесса.

D.5.3.3.3 Взаимосвязи

Эта практика является развитием GP 3.2.3 с добавлением возможности количественной оценки к заданному процессу.

D.6 Уровень возможностей 5 – Постоянное усовершенствование

D.6.1 Общие признаки уровня возможностей

D.6.1.1 Общие практики общего признака

D.6.1.1.1 Краткое описание

Количественные цели (задачи) выполнения процесса в отношении эффективности и результативности устанавливаются на основе бизнес-целей организации. Постоянное усовершенствование процесса в сопоставлении с этими целями осуществляется при помощи количественной обратной связи от выполнения определенных процессов и тестирования новых идей и технологий. Основное отличие от контролируемого в количественном отношении уровня заключается в том, что определенный и стандартный процессы подвергаются постоянной модернизации и усовершенствованию, основываясь на количественном понимании воздействия изменений на эти процессы.

D.6.1.1.2 Перечень общих признаков

Данный уровень возможностей объединяет следующие общие признаки:

- общий признак 5.1 - Улучшение организационных возможностей;
- общий признак 5.2 - Повышение эффективности процесса.

D.6.2 Общий признак 5.1 - Улучшение организационных возможностей

D.6.2.1 Общие практики общего признака

D.6.2.1.1 Краткое описание

Действия общих практик этого общего признака сосредоточены на сравнении использования стандартного процесса во всей организации и сравнениях этих различных применений процесса. В ходе использования процесса осуществляется поиск благоприятных возможностей улучшения стандартного процесса, а произведенные дефекты анализируются с целью идентификации других потенциальных улучшений этого процесса. Таким образом, устанавливаются цели повышения эффективности процесса, идентифицируются усовершенствования стандартного процесса и анализируются его потенциальные изменения. Эти общие практики создают важную основу для повышения эффективности процесса.

D.6.2.1.2 Перечень общих практик

Этот общий признак объединяет следующие общие практики:

- GP 5.1.1 - Устанавливает цели получения эффективности.
- GP 5.1.2 - Постоянно улучшает стандартный процесс.

D.6.2.2 GP 5.1.1 - Устанавливает цели получения эффективности

D.6.2.2.1 Описание

Устанавливает количественные цели повышения эффективности семейства стандартных процессов на основе бизнес-целей организации и текущих возможностей процесса.

D.6.2.2.2 Примечания

Отсутствуют.

D.6.2.2.3 Взаимосвязи

Отсутствуют.

D.6.2.3 GP 5.1.2 - Постоянно улучшает стандартный процесс

D.6.2.3.1 Описание

Постоянно улучшает процесс путем изменения семейства стандартных процессов организации для повышения ее эффективности.

D.6.2.3.2 Примечания

Информация, полученная от управления индивидуальными проектами, передается обратно организации для анализа и использования в других областях применения. Изменения семейства стандартных процессов организации могут быть результатом нововведений в технологии и постепенных улучшений. Новаторские усовершенствования привносятся извне новыми технологиями. Постепенные улучшения обычно обусловлены усовершенствованиями, полученными при адаптации заданного процесса. Улучшение стандартного процесса устраняет причины отклонения от номинальной величины.

D.6.2.2.3 Взаимосвязи

Специальные причины изменений контролируются в GP 4.2.2.

Улучшение процесса организации управляется в области процесса PA18.

D.6.3 Общий признак 5.2 - Повышение эффективности процесса

D.6.3.1 Общие практики общего признака

D.6.3.1.1 Краткое описание

Действия общих практик этого общего признака сосредоточены на создании постоянного состояния управляемого улучшения стандартного процесса. Таким образом, рассматривается возможность устранения причины дефектов, производимых стандартным процессом, и улучшения этого процесса.

D.6.3.1.2 Перечень общих практик

Этот общий признак объединяет следующие общие практики:

- GP 5.2.1 - Выполняет внеплановый анализ;
- GP 5.2.2 - Устраняет причины дефектов;
- GP 5.2.3 - Постоянно улучшает заданный процесс.

D.6.3.2 GP 5.2.1 - Выполняет внеплановый анализ

D.6.3.2.1 Описание

Выполняет внеплановый анализ дефектов.

D.6.3.2.2 Примечания

Лица, выполняющие процесс, обычно участвуют в его анализе. Этот анализ является профилактическим и внеплановым, а также реактивным. Для выявления областей улучшения могут использоваться дефекты из предыдущих проектов с аналогичными атрибутами.

D.6.3.2.3 Взаимосвязи

Результаты этих анализов применяются в GP 5.2.2 и/или GP 5.2.3.

D.6.3.3 GP 5.2.2 - Устраняет причины дефектов

D.6.3.3.1 Описание

Выборочно устраняет причины дефектов в заданных процессах.

D.6.3.3.2 Примечания

В этом общем практическом приеме предполагаются как общие, так и специальные причины изменений, и каждый тип дефекта может давать в результате различное действие.

D.6.3.3.3 Взаимосвязи

Причины идентифицированы в GP 5.2.1.

D.6.3.4 GP 5.2.3 - Постоянно улучшает заданный процесс

D.6.3.4.1 Описание

Постоянно улучшает выполнение процесса посредством изменения заданного процесса с целью повышения его эффективности.

D.6.3.4.2 Примечания

Улучшения могут быть постепенными (GP 5.1.2) или радикальными, такими как появление новых технологий (например, как часть контрольного испытания). Обычно улучшения инициируются целями, установленными в GP 5.1.1.

D.6.3.4.3 Взаимосвязи

Источником улучшений может быть GP 5.1.2. Цели были установлены в GP 5.1.1.

Управление внедрением производственной технологии осуществляется в PA19.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 7498-2:1989	IDT	ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации»
ИСО 9000:2005	IDT	ГОСТ Р ИСО 9000-2001 «Системы менеджмента качества. Основные положения и словарь»
ИСО/МЭК12207:1995	IDT	ГОСТ Р ИСО/МЭК 12207:1995-99 «Информационная технология. Процессы жизненного цикла программных средств»
ИСО/МЭК ТО 13335-1:1996	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 15288:2002	IDT	ГОСТ Р ИСО/МЭК 15288-2005 «Информационная технология. Системная инженерия. Процессы жизненного цикла систем»
ИСО/МЭК 15408-1:2005	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 ТО 15443-1:2005	-	*
ИСО/МЭК 15504-1:2004	-	*
ИСО/МЭК 15504-2:2003	-	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта.

Примечание – В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT – идентичные стандарты.

Библиография

[1] CCEB96 Common Criteria Editorial Board, «Общие критерии оценки безопасности информационных технологий», версия 1.0, 31 января 1996

[2] NIST94a National Institute of Standards and Technology, «Преимущество по доверию: Протоколы пригласительного семинара по доверию к ИТ и их надежности», внутренние/межведомственные отчеты НИСТ, 5472, 21-23 марта 1994

УДК 351.864.1:004:006.354 ОКС 35.040

Ключевые слова: проектирование систем безопасности, модель SSE-CMM®, модель зрелости процесса, область процесса, базовая практика, общая практика

Электронное издание

Тираж 14 экз. Зак. 1.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»

123995 Москва, Гранатный пер., 4.

www.gostinfo.ru gost.e-ecolog.ru

gost.e-ecolog.ru