NIST Специальная публикация 800-64 Пересмотр 2

Рассмотрения безопасности в жизненном цикле разработки систем

Richard Kissel
Kevin Stine
Matthew Scholl
Hart Rossman
Jim Fahlsing
Jessica Gulick

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Отдел компьютерной безопасности
Лаборатории информационных технологий
Национальный институт стандартов и технологий
Гейтерсбург, MD 20899-8930

Октябрь 2008

МИНИСТЕРСТВО ТОРГОВЛИ США
Carlos M.Gutierrez, Министр

НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И ТЕХНОЛОГИЙ
Patrick D. Gallagher, Заместитель директора

Отчёты по технологиям компьютерных систем

Лаборатория информационных технологий (ITL) в Национальном институте стандартов и технологий (NIST) продвигает американскую экономику и общее благосостояние, обеспечивая техническое лидерство для национальной инфраструктуры измерений и стандартов. ITL разрабатывает тесты, методы испытаний, справочные данные, осуществляет подтверждения концепций реализации и технический анализ, чтобы продвинуть разработку и продуктивное использование информационных технологий. Обязанности ITL включают разработку управленческих, административных, технических и физических стандартов и руководств для обеспечения рентабельной безопасности, и приватности информации, не связанной с национальной безопасностью в федеральных информационных системах. Специальные публикации 800-серии содержат информацию относительно исследований, руководств и усилий ITL, направленных на повышение безопасности информационных систем, и её совместных работ с отраслями, правительством и академическими организациями.

Полномочия

Эта публикация была разработана NIST в соответствии с его обязанностями, установленными согласно Закона об управлении безопасностью федеральной информации (FISMA), Общественный закон (P.L). 107-347.

NIST является ответственным за разработку стандартов и руководств по информационной безопасности, включая минимальные требования для федеральных информационных систем, но такие стандарты и руководства не должны применяться к системам национальной безопасности без специального санкционирования соответствующих федеральных должностных лиц, осуществляющих полномочия по таким системам. Это руководство непротиворечиво с требованиями Циркуляра A-130 Министерства управления и бюджета (OMB), Раздел 8b (3), *Обеспечение безопасности информационных систем агентств*, как указано в Циркуляре A-130, Приложение IV: Анализ ключевых разделов. Дополнительная информация предоставлена в Циркуляре A-130, Приложение III, Безопасность федеральных автоматизированных информационных ресурсов.

Это руководство было подготовлено к использованию федеральными агентствами. Оно может быть также использовано на добровольной основе неправительственными организациями и это не попадает по действие авторского права. (Однако упоминание приветствовалось бы NIST.)

Ничто в этой публикации не должно использоваться в противоречие со стандартами и руководствами, определёнными Министром торговли в соответствие с его законными полномочиями как обязательные для федеральных агентств. Также, это руководство не должно быть интерпретировано как изменение или замена существующих полномочий Министра торговли, Директора OMB или какого-либо другого федерального должностного лица.

Некоторые коммерческие сущности, оборудование или материалы могут быть указаны в этом документе, чтобы описать экспериментальную процедуру или концепцию соответственно. Такое указание не предназначено, чтобы означать рекомендацию или одобрение NIST, а также оно не предназначено, чтобы означать, что сущности, материалы или оборудование - обязательно наилучшие имеющиеся по предназначению.

Благодарность

Авторы, Richard Kissel, Kevin Stine, и Matthew Scholl от NIST, хотят поблагодарить своих коллег, Hart Rossman, Jim Fahlsing и Jessica Gulick, от Science Applications International Corporation (SAIC), которые помогли дополнить этот документ, подготовить проекты и рассматривали материалы. Кроме того, особая благодарность адресована авторам исходного документа, а также нашим рецензентам, Arnold Johnson, John Garguilo, Marianne Swanson и Elizabeth Lennonot из NIST, которые значительно способствовали разработке документа. NIST также с благодарностью признает и ценит большое содействие людей из государственного и частного секторов, вдумчивые и конструктивные комментарии которых улучшили качество и полноценность этой публикации.

Оглавление

РЕЗЮМЕ **1**
ВВЕДЕНИЕ **2**
1.1 НАЗНАЧЕНИЕ И ОБЛАСТЬ 2
1.2 АУДИТОРИЯ 2
1.3 ВАЖНОСТЬ ДЛЯ ПРЕДНАЗНАЧЕНИЯ, ПРОГРАММАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И УПРАВЛЕНИЯ ИТ АГЕНТСТВА 2
1.4 ОРГАНИЗАЦИЯ ДОКУМЕНТА 3
ОБЗОР ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЖИЗНЕННОГО ЦИКЛА РАЗРАБОТКИ СИСТЕМ **4**
2.1 УСТАНОВЛЕНИЕ ОБЩЕГО ПОНИМАНИЯ 5
2.2 РАССМОТРЕНИЯ ПО УНАСЛЕДОВАННЫМ СИСТЕМАМ 8
2.3 КЛЮЧЕВЫЕ РОЛИ И ОБЯЗАННОСТИ В SDLC 8
ВКЛЮЧЕНИЕ БЕЗОПАСНОСТИ В SDLC **11**
3.1 ФАЗА SDLC: ИНИЦИИРОВАНИЕ 13
3.2 ФАЗА SDLC: РАЗРАБОТКА/ПРИОБРЕТЕНИЕ 21
3.3 ФАЗА SDLC: РЕАЛИЗАЦИЯ/ОЦЕНКА 28
3.4 ФАЗА SDLC: ЭКСПЛУАТАЦИЯ И ПОДДЕРЖКА 32
3.5 ФАЗА SDLC: ЛИКВИДАЦИЯ 36
ДОПОЛНИТЕЛЬНЫЕ РАССМОТРЕНИЯ БЕЗОПАСНОСТИ **40**
4.1 СИСТЕМА ПОСТАВОК И ДОВЕРЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ 40
4.2 СЕРВИСНО-ОРИЕНТИРОВАННАЯ АРХИТЕКТУРА 41
4.3 СПЕЦИАЛЬНАЯЯ АТТЕСТАЦИЯ МОДУЛЕЙ БЕЗОПАСНОСТИ ДЛЯ ПОВТОРНОГО ИСПОЛЬЗОВАНИЯ 41
4.4 МЕЖ-ОРГАНИЗАЦИОННЫЕ РЕШЕНИЯ 42
4.5 ПРОДВИЖЕНИЕ ТЕХНОЛОГИЙ И ОСНОВНЫЕ МИГРАЦИИ 42
4.6 РАЗРАБОТКА ДАТА-ЦЕНТРОВ ИЛИ ИТ ОБОРУДОВАНИЯ 43
4.7 ВИРТУАЛИЗАЦИЯ 44
ПРИЛОЖЕНИЕ A - ГЛОССАРИЙ **A-1**
ПРИЛОЖЕНИЕ B - АКРОНИМЫ **B-1**
ПРИЛОЖЕНИЕ C - ССЫЛКИ **C-1**
ПРИЛОЖЕНИЕ D - МАТРИЦА ССЫЛОК И ВЕБСАЙТЫ NIST **D-1**
ПРИЛОЖЕНИЕ E - ДРУГИЕ МЕТОДОЛОГИИ SDLC **E-1**
ПРИЛОЖЕНИЕ F - ДОПОЛНИТЕЛЬНЫЕ РАССМОТРЕНИЯ ПЛАНИРОВАНИЯ ПРИОБРЕТЕНИЯ **F-1**
ПРИЛОЖЕНИЕ G - ДОПОЛНИТЕЛЬНЫЕ ГРАФИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ БЕЗОПАСНОСТИ В SDLC **G-1**

ТАБЛИЦА РИСУНКОВ

РИСУНОК 2-1. ПОЗИЦИОНИРОВАНИЕ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ 4
РИСУНОК 3-1. SDLC – КОНЦЕПТУАЛЬНОЕ ПРЕДСТАВЛЕНИЕ 11
РИСУНОК 3-2. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ ИНИЦИИРОВАНИЯ 13
РИСУНОК 3-3. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ РАЗРАБОТКИ/ПРИОБРЕТЕНИЯ 21
РИСУНОК 3-4. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ РЕАЛИЗАЦИИ/ОЦЕНКИ 28
РИСУНОК 3-5. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ ЭКСПЛУАТАЦИИ/ПОДДЕРЖКИ 32
РИСУНОК 3-6. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ ЛИКВИДАЦИИ 36

РЕЗЮМЕ

Специальная публикация (SP)Национального института стандартов и технологий (NIST) 800-64, *Рассмотрения безопасности в жизненном цикле разработки систем,* была разработана чтобы помочь агентствам федерального правительства в интеграции важных этапов обеспечения безопасности информационных технологий (ИТ) в установленный жизненный цикл разработки IT-систем (SDLC). Это руководство относится ко всем федеральным IT-системам кроме систем национальной безопасности. Документ предназначен как справочный ресурс, а не в качестве учебника и должен использоваться вместе с другими публикациями NIST как обязательный в процессе разработки системы.

Эта публикация служит федеральной аудитории профессионалов по информационным системам и информационной безопасности, включая владельцев информационных систем, владельцев информации, разработчиков информационных систем и менеджеров программ.

Чтобы быть наиболее эффективной, информационная безопасность должно быть интегрирована в SDLC с самого начала создания систем. Ранняя интеграция безопасности в SDLC даёт возможность агентствам максимизировать доход от инвестиций в их программы обеспечения безопасности через:

- Раннее определение и смягчение уязвимостей системы обеспечения безопасности и неверных конфигураций, приводящих к более низкой стоимости реализации мер безопасности и снижению уязвимостей;
- Осознание потенциальных технических проблем, вызванных обязательными мерами безопасности;
- Определение общих сервисов безопасности и повторное использование стратегий и инструментов безопасности, чтобы уменьшить затраты на разработку и календарное планирование, наряду с повышением состояния безопасности, через проверенные методы и технологии; и
- Помощь в информировании для принятия управленческих решений посредством всестороннего своевременного управления рисками.

Это руководство сосредотачивается на компонентах информационной безопасности SDLC. Во-первых, представлено описание ключевых ролей и обязанностей по безопасности, которые необходимы в большинстве разработок информационных систем. Во-вторых, представлена достаточная информация о SDLC, чтобы позволить человеку, который незнаком с процессом SDLC понять отношения между информационной безопасностью и SDLC.

Этот документ интегрирует шаги безопасности в линейный, последовательный (иначе водопад) SDLC. SDLC с пятью шагами, приведенный в этом документе, является примером одного метода разработки и не предназначен, чтобы сделать обязательной эту методологию.

Наконец, SP 800-64 обеспечивает понимание проектов и инициатив в сфере ИТ, которые не определены явно как разработки, базирующиеся на SDLC, таких как сервисно-ориентированные архитектуры, междуведомственные проекты и разработки ИТ оборудования.

ГЛАВА ОДИН

ВВЕДЕНИЕ

Рассмотрение безопасности в жизненном цикле разработки систем важно для реализации и интеграции всеобъемлющей стратегии управления риском для всех активов информационных технологий в организации. Специальная публикация (СП) 800-64 Национального института стандартов и технологий (NIST) предназначена, чтобы помочь агентствам федерального правительства интегрировать существенные работы по безопасности в свои установленные руководства по жизненному циклу разработки систем.

1.1 Назначение и область

Назначение этого руководства состоит в том, чтобы помочь агентствам во встраивании безопасности в их процессы разработки ИТ. Это должно привести к более рентабельному, соответствующему риску, определению, разработке и тестированию мер безопасности. Это руководство сосредотачивается на компонентах информационной безопасности SDLC. Всесторонне внедрение и разработка систем рассматриваются вне области этого документа. Также вне области рассматривается процесс управления информационными системами организации.

Во-первых, руководство описывает ключевые роли и обязанности по безопасности, которые необходимы при разработке большинства информационных систем. Во-вторых, предоставлена достаточная информация о SDLC, чтобы позволить человеку, который незнаком с процессом SDLC, понять отношения между информационной безопасностью и SDLC.

Область этого документа - работы безопасности, которые происходят в методологии водопада SDLC. При этом подразумевается, что это может быть перенесено на любую другую методологию SDLC, которую, возможно, приняло агентство.

1.2 Аудитория

Эта публикация предназначена, чтобы служить разнообразной федеральной аудитории профессионалов по информационным системам и информационной безопасности, включая: (i) людей с обязанностями по управлению и надзору за информационными системами и информационной безопасностью (например, директора по информации, высшие должностные лица агентства по информационной безопасности и санкционирующие должностные лица); (ii) сотрудников организаций, имеющих непосредственную заинтересованность в достижении предназначения организаций (например, владельцы сфер предназначения и деятельности, владельцы информации); (iii) людей с обязанностями по разработке информационных систем (например, менеджеры программ и проектов, разработчики информационных систем); и (iv) людей с обязанностями по реализации и эксплуатации информационной безопасности (например, владельцы информационных систем, владельцы информации, сотрудники безопасности информационных систем).

1.3 Важность для предназначения, программам обеспечения безопасности и управления ИТ агентств

Федеральные агентства в значительной степени зависят от своей информации и информационных систем, чтобы успешно выполнять критические задачи. С увеличением надёжности на и ростом сложности информационных систем, а также постоянным изменением среды риска, информационная безопасность стала существенной для предназначения функцией. Эта функция должна выполняться таким образом, который снижает риск для получения информации, предписанной агентству, его общему предназначению и его способности осуществлять деятельность и служить американскому обществу. Информационная безопасность - инструмент реализации деятельности, который применяется через надлежащее и эффективное управление рисками для конфиденциальности, целостности и доступности информации.

Агентства могут понять ценность интеграции безопасности в установленный жизненный цикл разработки систем во многих отношениях, включая:

- Раннее определение и смягчение уязвимостей системы обеспечения безопасности и неверных конфигураций, приводящих к более низкой стоимости реализации управления безопасностью и снижения уязвимостей;
- Освоение потенциальных технических проблем, вызванных обязательными мерами безопасности;
- Определение общих сервисов безопасности и повторное использование стратегий и инструментов безопасности, чтобы уменьшить затраты на разработку и календарное планирование, наряду с повышением состояния безопасности через проверенные методы и технологии;
- Помощь в информировании для принятия управленческих решений посредством всестороннего своевременного управления рисками;
- Документирование важных решений по безопасности, принимаемых во время разработки, гарантирующих такое управление, при котором безопасность будет полностью рассмотрена во время всех фаз;
- Повышение доверия организаций и потребителей для облегчения принятия и использования, а также доверия правительства, чтобы способствовать продолжению инвестиций; и
- Улучшение совместимости и интеграции систем, которые иначе препятствовали бы обеспечению безопасности систем на различных системных уровнях.

1.4 Организация документа

Остальные главы этого руководства обсуждают следующее:

- Глава 2, предоставляет обзор информационной безопасности и жизненного цикла разработки систем, суммирует отношения между SDLC и другими дисциплинами ИТ, устанавливает общее понимание SDLC и обсуждает роли и обязанности, включённые в интеграцию информационной безопасности в SDLC.
- Глава 3, рассматривает встраивание безопасности в жизненный цикл разработки информационных систем**,** описывает различные рассмотрения безопасности, которые помогают интегрировать информационную безопасность в каждую фазу SDLC.
- Глава 4, предоставляет дополнительные рассмотрения безопасности, выделяет рассмотрения безопасности для сценариев разработки, таких как сервисно-ориентированные архитектуры и виртуализация, для которых подход к интеграции безопасности несколько отличается от традиционных усилий по разработке систем.

Это руководство содержит семь приложений. Приложение A предоставляет глоссарий терминов. Приложение B представляет всесторонний список акронимов. Приложение C перечисляет ссылки, процитированные в этой публикации. Приложение D обеспечивает отображение подходящих публикаций NIST к соответствующим работам безопасности SDLC. Приложение E даёт обзор других методологий SDLC. Приложение F обсуждает дополнительные рассмотрения планирования для фаз разработки/приобретения SDLC. Приложение G обеспечивает дополнительное графическое представление интеграции безопасности в SDLC.

ГЛАВА ДВА

ОБЗОР ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЖИЗНЕННОГО ЦИКЛА РАЗРАБОТКИ СИСТЕМ

Процессы и действия по обеспечению безопасности информационных систем обеспечиваю ценный вклад в управление IT-системами и их разработку, обеспечивающий возможность выявления, планирования и смягчения риска. Подход к управлению рисками[1] включает постоянное уравновешивание защиты информации и активов агентства со стоимостью мер безопасности и стратегий смягчения всюду по полному жизненному циклу разработки информационной системы (см. **рисунок 2-1**). Самый эффективный способ реализовать управление рисками состоит в том, чтобы определить критические активы и действия, а также уязвимости систем во всём агентстве. Риски являются общими и не ограничиваются организацией, источником дохода или топологией. Определение и верификация критических активов и действий и их взаимосвязи могут быть достигнуты посредством процесса планирования безопасности системы, а также через компиляцию информации из процессов Планирования капиталовложений и управления инвестициями (Capital Planning and Investment Control (CPIC)) и Архитектуры предприятия (Enterprise Architecture (EA)), чтобы установить понимание жизненно важных операций для деятельности агентства, поддерживающих их активов и существующих взаимозависимостей и отношений. С определёнными критическими активами и действиями, организация может и должна выполнить анализ влияния на деятельность (BIA). Назначение BIA состоит в том, чтобы связать системы и активы с обеспечивающими их критическими сервисами и оценить последствия их нарушения. Определяя эти системы, агентство может эффективно управлять безопасностью, устанавливая приоритеты. Это позиционирует службу безопасности на то, чтобы облегчить рентабельное выполнение программы ИТ, а также ясно сформулировать её влияние на деятельность и значимость для агентства.

Осуществление для систем и проектов подхода, базирующегося на управлении рисками, означает интегрирование безопасности в начале и всюду по установленной агентством жизненным циклам систем и CPIC. Интеграция облегчает планирование, приобретение, встраивание и развёртывание безопасности как неотъемлемой части проекта или системы. Это играет значительную роль в определении и предписании требований безопасности по всем фазам жизненного цикла.

Управление жизненным циклом помогает документировать важные для безопасности решения, и предоставляет доверие для руководства, что безопасность полностью рассмотрена во всех фазах. Менеджеры систем могут использовать эту информацию в качестве напоминаний для самоконтроля того, почему решения были приняты так, чтобы воздействие изменений в среде могло быть с большей готовностью оценено. Группы по надзору и независимому контролю могут использовать эту информацию в их анализах чтобы проверить, что руководство системой сделало адекватную работу и выделить области, где безопасности, возможно, было уделено недостаточно внимания. Это включает

[1] Проект NIST Специальная Публикация 800-39, *Управляя Риском от Информационных систем: Организационная Перспектива,* описывает основу для строительства программы управления риском безопасности информационной системы.

исследование того, отражает ли документация ясно то, как системой на самом деле управляют и поддерживают.

Есть много методологий SDLC, которые могут использоваться организацией, чтобы эффективно разработать информационную систему. Традиционный SDLC, линейная последовательная модель (также известный как метод водопада), предполагает, что система будет поставлена в её заключительных этапах жизненного цикла разработки. Другой метод SDLC использует модель прототипирования, которая часто используется, чтобы разработать понимание системных требований, не разрабатывая на самом деле законченную автоматизированную систему. Более сложные системы могут потребовать моделей более итерационной разработки. Более сложные модели разрабатывались и успешно использовались, чтобы учесть развивающуюся сложность передовых и иногда больших проектов информационных систем. Примерами таких более сложных моделей является модель быстрой разработки приложений (RAD), модель совместной разработки приложений (JAD), модель прототипирования и спиральная модель. Ожидаемый размер и сложность системы, график разработки и длина жизни системы будут влиять на выбор того, какую модель SDLC использовать. Во многих случаях выбор модели SDLC будет определён политикой приобретения организации. Приложение E предоставляет обзор других методологий SDLC.

Это руководство включает безопасность в линейную последовательную модель SDLC, потому что эта модель является самой простой из различных моделей, и это - соответствующая платформа для этого рассмотрения. Однако рассмотренные концепции могут быть адаптированы к любой модели SDLC.

2.1 Установление общего понимания

2.1.1 Политика и руководство по SDLC агентства

У каждого агентства должны быть задокументированные и повторяемые политика и руководство по SDLC, которые поддерживают его потребности деятельности и соответствуют его уникальной специфике. Руководство по SDLC агентства может быть детализированным или более сконцентрированным по цели в зависимости от стиля агентства управления ИТ, сложности потребностей и предпочтений приобретения. Например, некоторые агентства поддерживают деятельность по разработке, которая создаёт и обслуживает системы, в то время как другие осуществляют разработку, а также потенциальную поддержку на аутсорсинге. Первым могут требоваться более подробные процедуры, в то время как для деятельности, сконцентрированной на приобретении, возможно, понадобятся только цели, уровни сервиса и подробные поставки. У деятельности, сконцентрированной на приобретении, есть специфические наборы уязвимостей вследствие потенциально неизвестной и не контролируемой по сути системы поставок. Эти уязвимости должны быть поняты и включены в любые основанные на риске решения.

Типичный SDLC включает пять фаз: инициирование, разработка/приобретение,[2] реализация/оценка, эксплуатация/поддержка и ликвидация. Каждая фаза включает минимальный набор задач по безопасности, необходимых для эффективного включения безопасности в процесс разработки системы. Обратите внимание на то, что фазы могут постоянно повторяться в течение жизни системы до ликвидации.

- Инициирование. Во время фазы инициирования выражается потребность в системе, и документируется назначение системы.

[2] Эта публикация не предоставляет исчерпывающее описание процессов приобретения. Организации должны обратиться к соответствующим Федеральным нормативным документам по поставкам (Federal Acquisition Regulations (FAR)) и конкретным для организации политикам и процедурам за подробные информации по приобретению.

- Разработка/Приобретение. Во время этой фазы система проектируется, закупается, программируется, разрабатывается или иначе создаётся.
- Реализация/Оценка. После приёмочных испытаний системы, система устанавливается или выдаётся.
- Эксплуатация/Поддержка. Во время этой фазы система выполняет свою работу. Система почти всегда изменяется добавлением аппаратного и программного обеспечения и различными другими событиями.
- Ликвидация. Работы, проведенные во время этой фазы, гарантируют организованное прекращение функционирования системы, сохранение существенной информацию системы, а переносимые данные передаются системой к новой системе, или сохраняются в соответствии с применимыми нормативными документами и политиками управления записями.

Руководство по SDLC обеспечивает полезные средства для документирования:

- понимания главных работ и вех;
- моментов принятия решений или управляющих воздействий;
- конкретных результатов, которые представляют существенную информацию для проектирования системы;
- проектных достижений; и
- рассмотрений по поддержке, безопасность и эксплуатации системы.

Руководство должно поддерживать и быть поддержано через процессы предназначения, архитектуру предприятия и финансовые процессы агентства.

2.1.2 Введение в интеграцию безопасности

Выполнение основанного на управлении рисками подхода для систем и проектов означает интегрирование безопасности в установленные в агентстве жизненные циклы разработки систем и CPIC. Интегрированный компонент безопасности (состоявший из вех, поставок, контрольных результатов и взаимозависимостей), который конкретно определяет управление рисками (обсуждаемый в следующем разделе) облегчает планирование, приобретение, встройку и развёртывание безопасности как неотъемлемой части проекта или системы. Он также играет значительную роль в определении и обеспечении соблюдения требований безопасности по всему жизненному циклу. Полная и эффективная интеграция в SDLC облегчает профессионалам по информационной безопасности, сотрудничающим с представителями CPIC, ИТ и EA продвижение эффективного управления и надзора за рассмотрениями безопасности по всему жизненному циклу.

Реализация информационной безопасности с начала проекта позволяет требованиям реализовываться по мере необходимости и интегрированным и рентабельным образом. Проектирование безопасности в фазе инициирования продукта, как правило, стоит меньше, чем приобретение технологий позже, что может потребовать повторного формирования, настройки или будет обеспечивать больше или меньше мер безопасности, чем требуется. Безопасность должна быть включена во время формирования требований любого проекта. Проектирование решения с рассмотрением безопасности может существенно уменьшить потребность в совокупных мерах безопасности (например, проектирование дома с двумя дверями вместо четырёх требует меньшего количества безопасности для пунктов входа, а прокладка электрических проводов в дом для системы безопасности и электричества одновременно исключает проделывание отверстий в стенах позже). Это также допускает планирование обеспечения безопасности на уровне предприятия, что позволяет осуществлять повторное использование, уменьшение стоимости и разработку календарного плана, и повышает надёжность безопасности.

Совет по реализации

Работы безопасности должны быть физически и логически интегрированы в политику и руководства агентства по SDLC в противовес поддержания их в отдельном, дополнительном документе или жизненном цикле безопасности. Это гарантирует более глобальную аудиторию и уменьшает потребность для читателя излишне обращаться ко множественным документам. Конечно, интеграция безопасности может и должна использовать дополнительные документы процесса, которые предоставляют более подробную информацию.

Самый эффективный способ достигнуть интеграции безопасности в жизненном цикле разработки систем состоит в том, чтобы планировать и реализовывать всестороннюю программу управления рисками (см. раздел 2.1.5). Это отражается на стоимости и требованиях к интегрированной защите, а также вложенном, повторяемом процессе санкционирования, который предоставляет информацию о рисках заинтересованным сторонам и разработчикам ИТ по всему агентству.

2.1.3 Процесс планирования капиталовложений & управления инвестициями

У каждого агентства есть установленный и зарегистрированный процесс CPIC в соответствии с Циркуляром OMB A-11. NIST SP 800-65, *Интегрирование безопасности IT в* п*роцесс планирования капиталовложений и управления инвестициями*, ясно формулирующим интеграцию и значимость безопасности. Это руководство стремится продолжить это обсуждение с концентрацией на интеграции безопасности в SDLC.

Ключевые концепции NIST SP 800-65, которые необходимо рассмотреть, читая это руководство, включают:

- Процесс CPIC определён Циркуляром OMB A-130 как “процесс управления для постоянного определения, выбора, управления и оценки инвестиций в информационные ресурсы. Процесс связывает формирование и выполнение бюджета, и сосредоточен на предназначении агентства и достижении конкретных результатов программы”. Интеграция безопасности в этот процесс гарантирует, что информационные ресурсы спланированы и обеспечены полностью, упорядоченным образом, обеспечивая повышение безопасности при инвестировании в IT.
- Интеграция безопасности в процесс CPIC определяется методологией с семью шагами, чтобы гарантировать, что предназначение и требования безопасности учтены всюду в инвестируемом жизненном цикле.
- В то время как конкретные роли и обязанности изменятся от агентства к агентству, участие в процессе на уровне производственных и эксплуатирующих подразделений позволяет агентствам гарантировать, что что цели и задачи планирования капиталовложений и информационной безопасности выполнены.
- Совместно с планированием капиталовложений OMB и руководствами NIST, агентства обязаны придерживаться методов наиболее успешной практики Управления государственной отчётности (GAO), инвестиционной модели жизненного цикла с тремя фазами для федеральных инвестиций в IT.
- Стоимость, связанная с реализацией и оценкой мер обеспечения информационной безопасности и обеспечением эффективной защиты федеральных ресурсов ИТ, должна определяться в процессе планирования капиталовложений.

2.1.4 Архитектуры безопасности

Архитектуры безопасности должны соответствовать руководствам NIST, состоящим из семей мер безопасности, определённых в NIST SP 800-53 в отношении защиты конфиденциальности, целостности и доступности федеральной информации информационных систем. Комплексная архитектура безопасности учитывает текущие сервисы, инструменты и опыт по безопасности, определяет

прогнозируемые бизнес-потребности и требования, и ясно формулирует план внедрения, согласованный со спецификой и стратегическими планами агентства. Обычно, архитектура безопасности увязана с интегрированным календарным планом задач, который определяет ожидаемые результаты (признаки и условия для дальнейшего рассмотрения/ выравнивания), устанавливает временные проектные шкалы, обеспечивает оценки требований к ресурсам и определяет ключевые проектные зависимости.

2.1.5 Роль в основах управления рисками NIST

NIST SP 800-64 дополняет Основы управления рисками, обеспечивая типовой путеводитель для интеграции функциональности безопасности и доверия в SDLC. Кроме того, эта публикация обеспечивает более подробную информацию о дополнительных работах, которые ценны для получения понимания, что отличает специфику каждой системы и агентства. Эти дополнительные работы дополняют основы управления рисками. Более подробное описание Основ управления рисками NIST представлено в Проекте NIST SP 800-39, *Управление риском информационных систем: видение организации.*

2.2 Рассмотрения по унаследованным системам

Во многих случаях организации будут применять рассмотрения жизненного цикла информационной безопасности к унаследованным информационным системам, которые были в действии в течение некоторого длительного периода времени. У некоторых унаследованных систем могут быть превосходные планы по безопасности, которые предоставляют подробную документацию по принятым решениям управления рисками, включая идентификацию того, какие меры безопасности в настоящее время используются. Другие унаследованные системы могут иметь ограниченную доступную документацию. Однако, рассмотрения безопасности относятся также и к этим унаследованным системам, и должны применяться и документироваться, чтобы гарантировать, что меры безопасности существуют и функционируют эффективно, чтобы обеспечить надлежащую защиту для информации и информационных систем.

Совет по реализации

Эффективная связь требований безопасности и ожидаемых результатов - важный и сложный шаг. Ключевым является документирование требований безопасности в конкретных и измеримых терминах так, чтобы это ясно определяло, кто является ответственным и подконтрольным. Форма (меморандум, соглашение или предполагаемый документ), а также степень детализации и сложность должны быть управляемыми и рентабельными. Эта тема обсуждается всюду в этой публикации.

2.3 Ключевые роли и обязанности в SDLC

У многих участников есть роль в разработке информационной системы. Названия для ролей и должностей различаются среди организаций. Не каждый участник работает над каждой работой в фазе. Определение того, каких участников необходимо учитывать в каждой фазе, так же уникально по отношению к организации, как и разработка. В любом проекте разработки важно включить соответствующий персонал информационной безопасности как можно раньше, предпочтительно в фазе инициирования. Перечень ключевых ролей предоставлен ниже. В некоторых организациях отдельный человек может выполнять несколько ролей.

ТАБЛИЦА 2-1. КЛЮЧЕВЫЕ РОЛИ БЕЗОПАСНОСТИ И ОБЯЗАННОСТИ В SDLC

Роль	Обязанности
Санкционирующее должностное лицо, Authorizing Official (AO)	AO - высшее должностное лицо или руководитель с полномочиями по официальному принятию на себя ответственности за эксплуатацию информационной системы на допустимом уровне риска к деятельности и активам организации, людям, другим организациям и Нации. Чтобы выполнять это, AO полагается, прежде всего, на: (i) утверждённый план обеспечения безопасности; (ii) отчёт по оценке безопасности; и (iii) план действий и вехи по снижению или устранению уязвимостей информационной системы.
Директор по информации, Chief Information Officer (CIO)	Директор по информации ответственен за планирование, составление бюджета, инвестирование, применение и приобретение информационной системы организации. В качестве такового, директор по информации предоставляет консультации и помощь

Роль	Обязанности
	высшему персоналу организации в приобретении наиболее эффективных и продуктивных информационных систем, соответствующих архитектуре предприятия организации.
Менеджер по управлению конфигурацией, Configuration Management (CM) Manager	Менеджер CM ответственен за управление результатами изменений или различий в конфигурации информационной системs или сети. Таким образом, менеджер CM помогает в оптимизации процесса управления изменениями и предотвращает изменения, которые могли бы нанести ущерб состоянию безопасности системы, прежде чем они произойдут.
Контрактный специалист, Contracting Officer	Контрактный специалист - человек, у которого есть полномочия по заключению, управлению и/или завершению контрактов и получению соответствующих решений и результатов.
Технический уполномоченный контрактного специалиста, Contracting Officer's Technical Representative	COTR - компетентный сотрудник, назначенный контрактным специалистом действовать как его техническое представитель в управлении техническими аспектами контракта.
Сотрудник безопасности информационной системы, Information System Security Officer	Сотрудник безопасности информационной системы ответственен за обеспечение безопасности информационной системы всюду в её жизненном цикле.
Совет по инвестициям в информационные технологии (или эквивалент), Information Technology Investment Board (or equivalent)	Совет по инвестициям в информационные технологии (IT) или его эквивалент, ответственен за управление процессом CPIC, определённым законом Клингер-Коэна от 1996 г. (Раздел 5).
Консультант по правовым вопросам/Контрактный юрист, Legal Advisor/Contract Attorney	Консультант по правовым вопросам ответственен за консультирование команды по юридическим вопросам во время процесса приобретения.
Специалист по приватности, Privacy Officer	Специалист по приватности ответственен за обеспечение того, чтобы сервисы или система обеспечивали учёт существующей политики по приватности в отношении защиты, распространения (совместного пользования и обмена информацией) и раскрытие информации.
Менеджер/должностное лицо программ (Владелец информации), Program Manager/Official (Information Owner)	Этот человек представляет в информационной системе во время процесс SDLC интересы, относящиеся к деятельности и программам. Менеджер программ играет основу роль в безопасности и, в идеале, глубоко знает функциональные требования к системе.
Директор по контролю качества/тестированию, QA/Test Director	Директор по контролю качества/тестированию ответственен за тестирование и оценку системы, и функционирует как ресурс во множестве программ, помогая в разработке и выполнении планов тестирования во взаимодействии с менеджерами программ и клиентами. Этот человек рассматривает системные спецификации и определяет тестовые потребности и работает с менеджерами программ, чтобы планировать продвижение работ до работ по объектовым испытаниям.
Высшее должностное лицо агентства по безопасности, Senior Agency Information Security Officer (SAISO)	SAISO, также известный как Директор по безопасности информации, ответственен за формирование политики по интеграции безопасности в SDLC и разработку стандартов предприятия по безопасности информации. Этот человек играет ведущую роль в представлении соответствующей структурированной методологии, чтобы помочь в определении, оценке и минимизации рисков информационной безопасности для организация.
Разработчик программного обеспечения, Software Developer	Разработчик ответственен за программное кодирование соответствующих приложений, программного обеспечения и Интернет/интранет-сайтов, включая "безопасное кодирование", а также координацию и работу с менеджером по управлению конфигурацией (CM) для определения, решения и реализации мер безопасности и других проблем CM.
Системный архитектор, System Architect	Как общий проектировщик и интегратор приложений, системный архитектор ответственен за создание общего замысла архитектуры и за поддержание концептуальной целостности архитектуры всюду по жизненному циклу проекта. Системный архитектор также ответственен за обеспечение качества технических результатов работы, поставляемых проектной группой, включая проекты, спецификации, процедуры и документацию.
Владелец системы, System Owner	Владелец системы ответственен за приобретение, разработку, интеграцию, модификацию, эксплуатацию и поддержку информационной системы.
Другие участники, Other Participants	Список ролей SDLC в разработке информационной системы может вырасти по мере увеличения сложности. Жизненно важно, чтобы все члены группы разработчиков сотрудничали, чтобы гарантировать успешное завершение разработки. Поскольку сотрудники информационной безопасности должны в процессе разработки принимать очень важные решения, они должны быть включены как можно раньше в процесс. Пользователи системы могут помочь в разработке, помогая менеджерам программ в определении потребностей, усовершенствовании требований и проверке и приёмке разработанной системы. Участники могут также включать персонал, который представляет ИТ, управления конфигурацией, проектирование и разработку и группы обеспечения.

ВКЛЮЧЕНИЕ БЕЗОПАСНОСТИ В SDLC

Этот раздел описывает рассмотрения безопасности, которые помогают интегрировать информационную безопасность в SDLC. Рассмотрения безопасности определены в каждой фазе SDLC, продвигая, таким образом, бизнес-приложения и требования безопасности вместе, чтобы гарантировать сбалансированный подход во время разработки. **Рисунок 3-1**, систематизирующий этап разработки, обеспечивает полное представление процесса.

РИСУНОК 3-1. SDLC – КОНЦЕПТУАЛЬНОЕ ПРЕДСТАВЛЕНИЕ

Чтобы предоставить читателю ясное, краткое руководство, каждая фаза жизненного цикла далее описана в отдельном разделе, который организован следующим образом:

- Даётся краткое описание фазы SDLC.
- Определяются общие управляющие условия или установленные точки в жизненном цикле, когда система должна быть оценена и когда руководство должно определить, должен ли проект продолжаться как есть, изменить направление, или быть прекращён. Управляющие условия должны быть гибкими и адаптированы к конкретной организации. Ценность управляющих условий в том, что они предоставляют организации возможность проверить, что рассмотрения безопасности учитываются, адекватная безопасность встраивается и определить, что риски ясно поняты перед тем, как разработка системы перейдёт к следующей фазе жизненного цикла.
- Определяются и описываются основные работы по безопасности в каждой фазе. Каждая работа при этом определяется в следующих аспектах:

- Описание. Описание предоставляет подробный обзор работы и выделяет конкретные рассмотрения, необходимые, чтобы определить задачу.
- Ожидаемые результаты. Перечисляются общие выходы и продукты задач наряду с предложениями для интеграции этих результатов работы вперёд/назад в SDLC.
- Синхронизация. Представлена обратная связь, которая обеспечивает возможность гарантировать, что SDLC реализован как гибкий подход, который допускает соответствующее и непротиворечивую взаимосвязь и адаптацию задач и поставок по мере разработки системы.
- Взаимозависимости. Эта секция определяет ключевые взаимозависимости с другими задачами чтобы гарантировать, что на работы по интеграции безопасности не влияют отрицательно другие ИТ процессы.

3.1 Фаза SDLC: инициирование

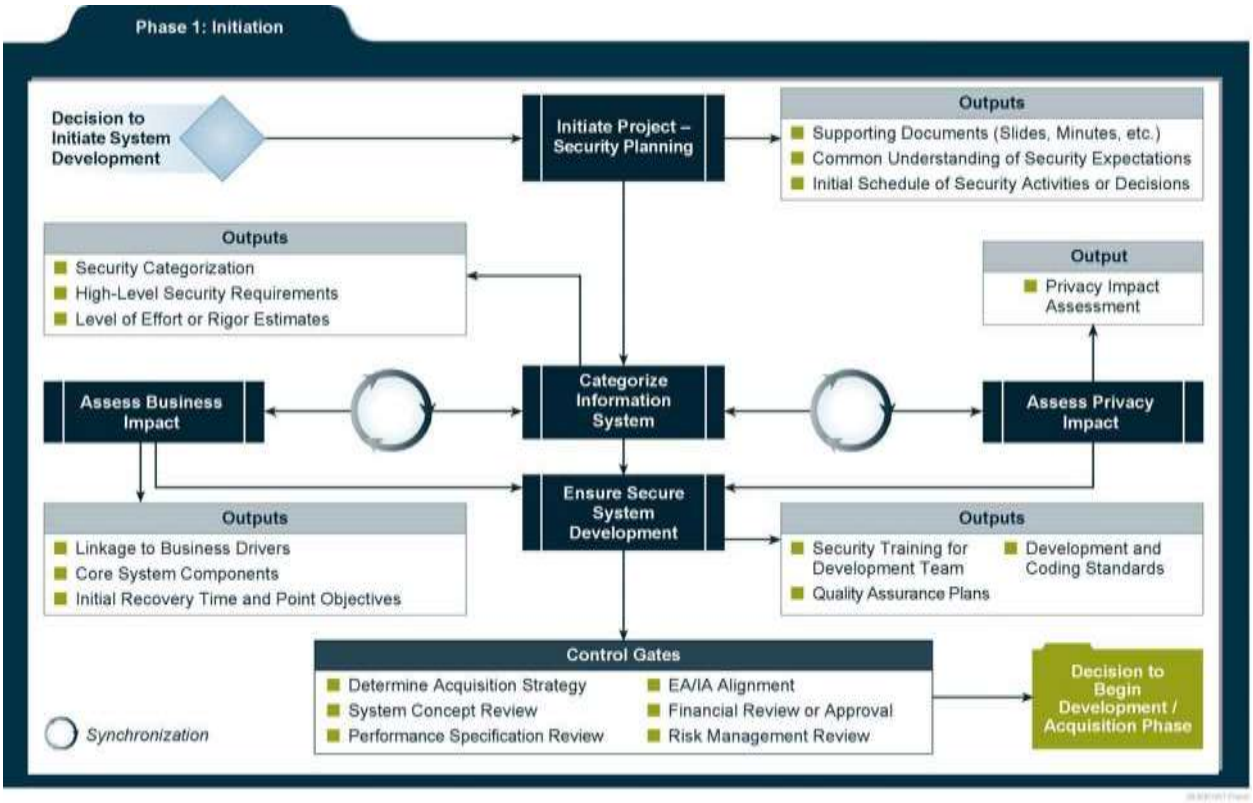

РИСУНОК 3-2. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ ИНИЦИИРОВАНИЯ

3.1.1 Описание

Во время этой первой фазы жизненного цикла разработки рассмотрения безопасности являются ключевыми для тщательной и ранней интеграции, гарантируя, таким образом, что будут рассмотрены угрозы, требования и потенциальные ограничения в функциональности и интеграции. В этот момент на безопасность смотрят больше с точки зрения рисков для деятельности с позиции службы информационной безопасности. Например, агентство может определить политический риск, проистекающий из внешнего вебсайта, изменённого или сделанного недоступным во время критического периода деятельности, приводящий к уменьшению доверия граждан. Ключевые работы безопасности для этой фазы включают:

- Начальный проект бизнес-требований с точки зрения конфиденциальности, целостности и доступности;
- Определение категорий информации и идентификация известных специальных требований к обработке по передаче, хранению или формированию информации, такой как персональная идентификационная информация; и
- Определение любых требований приватности.

Раннее планирование и освоение отразится на стоимости и экономии времени посредством надлежащего планирования управления рисками. Обсуждения безопасности должны быть выполнены как часть (а не отдельно от) проекта разработки, чтобы гарантировать единое понимание бизнес-решений среди проектного персонала и риска их последствий в отношении общего проекта разработки.

3.1.2 Управляющие условия

Общие типы управляющих условий для этой фазы могут включать:

- Определение стратегии приобретения, которая будет использоваться всюду в оставшейся части процесса разработки;
- Рассмотрение концепции системы, чтобы проверить жизнеспособность, полноту, достижимость концепции, и её соответствие целям предназначения организации и бюджетным ограничениям;
- Рассмотрение требований по производительности, чтобы гарантировать, что начальный проект системы учитывает все определённые на текущее время установленные требования безопасности;
- Согласование с архитектурой предприятия (EA), которое приводит в соответствие видение ИТ, стандарты и бизнес-требования, а также согласование безопасности с текущими и предстоящими сервисами безопасности;
- Финансовый анализ, который проверяет, что система будет согласована с образцами и руководством по CPIC, уравновешивая, в то же время, последствия для стоимости, связанные с управлением рисками; и
- Рассмотрение управления рисками, чтобы соответствовать рекомендуемым руководствам по основам управления рисками NIST, чтобы уменьшить неопределённость в управлении системным риском. В это рассмотрение управления рисками включается анализ результатов категорирования безопасности информационной системы, которые включают определение типов информации, результирующих уровней воздействия и заключительное категорирование безопасности системы.

3.1.3 Основные работы по безопасности

3.1.3.1 Начальное планирование обеспечения безопасности

Описание:	Планирование обеспечения безопасности должно начаться в фазе инициирования путём: • Определения ключевых ролей по безопасности в разработке системы; • Определения источников требований безопасности, таких как соответствующие законы, нормативные документы и стандарты; • Обеспечения у всех ключевых заинтересованных сторон общего понимания, включая последствия безопасности, рассмотрения и требования; и • Выделение начальных соображений о ключевых вехах безопасности, включая периоды времени или условия разработки, которые сигнализируют о приближающемся шаге безопасности. Такое раннее вовлечение даёт возможность разработчикам планировать в проекте требования безопасности и связанные ограничения. Это также напоминает руководителям проекта о том, что многие принимаемые решения имеют последствия для безопасности, которые должны быть соответственно взвешены по мере продолжения проекта. **Определение ролей по безопасности** Определение ISSO - важный шаг, который должен учесть количество времени, которое человек посвятит этой задаче, квалификацию, необходимую для выполнения обязанностей и возможности человека по эффективному выполнению обязанностей. Определение ISSO в начале процесса обеспечивает человеку ключевое понимание основанных на риске решений, принятых в начале процесса, и предоставляет другим членов команды доступ к ISSO для поддержки в интеграции безопасности в разработку системы. **Информирование заинтересованных сторон об интеграции безопасности** ISSO предоставляет бизнес-владельцу и разработчику раннее понимание шагов, требований и ожиданий в отношении безопасности, таким образом, безопасность может быть спланирована с начала. Темы могут включать: • Обязанности по безопасности • Метрики сообщений по безопасности • Обеспечиваемые общие меры безопасности (если применимо) • Процесс испытаний & аттестации • Технологии тестирование и оценки безопасности • Предоставляемые документы & требования по безопасности • Методы проектирования, построения архитектуры и кодирования по безопасности

	• Соображения относительно приобретений по безопасности • Основные работы по графику разработки и воздействию на ресурсы, такие как активное тестирование, аттестация и обучение **Начальное планирование проекта** Разработка начальной структуры проекта для вех безопасности, которая интегрирована в график разработки проекта работ, позволяет осуществлять надлежащее планирование по мере внесения изменений. На данном этапе, работы могут представляться более с точки зрения решений, связанных с работами по безопасности.
Ожидаемые результаты:	• Поддерживающие документы (слайды, протоколы совещаний, и т.д.) • Общее понимание ожиданий от безопасности. • Начальный календарный план работ или решений по безопасности.
Синхронизация:	Должна быть спланирована серия вех или совещаний по вопросам безопасности, чтобы обсудить каждое рассмотрение по безопасности в течение разработки системы.
Взаимозависимости:	График проектных работ должен интегрировать работы по безопасности, чтобы гарантировать надлежащее планирование любого будущего решения, связанного с календарными планами и ресурсами.
Советы по реализации	
• Планирование обеспечения безопасности в фазе инициирования должно включать приготовления ко всему жизненному циклу системы, включая определение ключевых вех безопасности и поставок, а также инструментов и технологий. Специальное внимание должно быть уделено элементам, которые, возможно, должны быть приобретены (например, инструменты тестирования/оценки). • Многие образцы инициирования проекта (протоколы совещаний, брифингов, идентификаторы ролей) могут быть стандартизированы и предоставлены разработчикам для надлежащего планирования уровня усилий. • Лично встреча даёт участникам важную возможность оценить понимание и освоение. • Если агентство определило того же самого человека ISSO для многих систем, плановый подход повысит его возможности по мульти-деятельности, такие как назначение общих систем или общих организаций с собственностью. • Консультируйтесь с должностными лицами агентств Оперативной отчётности, Приватности и Закона о свободе информации (FOIA) в начале жизненного цикла разработки, чтобы гарантировать согласие с политикой агентств и действующими законами.	

3.1.3.2 Категорирование информационной системы

Описание	Категорирование безопасности, которое соответствует шагу 1 в Основах управления рисками NIST, обеспечивает существенный шаг к интеграции безопасности в управление деятельностью и функции управления информационными технологиями правительственных агентств и устанавливает основу для стандартизации безопасности среди информационных систем. Категорирование безопасности начинается с определения того, какая информация поддерживает какие направления деятельности правительства, как определено в EA и описано в Специальной публикации NIST 800-60, *Руководство по отображению типов информации и информационных систем к категориям безопасности*. Последующие шаги сосредотачиваются на оценке безопасности с точки зрения конфиденциальности, целостности и доступности. Результат - непосредственная связь между предназначением, информацией и информационными системами, и рентабельной информационной безопасностью. Публикация 199 Федеральных стандартов обработки информации (FIPS), *Стандарты для категорирования безопасности федеральной информации и Информационных систем*, обеспечивает стандартизованный подход для установления категорий безопасности для информации и информационных систем организации. NIST SP 800-60, сопутствующее руководство к FIPS 199, обеспечивает путеводитель процесса и таксономию информации, чтобы категорировать информацию и информационные системы. Категории безопасности основаны на потенциальном воздействии на организацию в результате реализации некоторых событий, которые подвергают опасности информацию и информационные

	системы, необходимые организации, чтобы выполнять её установленное предназначение, защищать её активы, выполнять её юридическую ответственность, сопровождать её ежедневные функции и защищать людей. Категории безопасности должны использоваться в сочетании с информацией об уязвимостях и угрозах в оценке риска для организации от применения информационной системы. FIPS Публикация 199 определяет три уровня (т.е., низкий, умеренный или высокий) потенциального воздействия на организации или людей в следствие нарушения безопасности (то есть, потери конфиденциальности, целостности, или доступности). Стандарты и руководства по категорированию безопасности помогают организации в осуществлении соответствующего выбора мер безопасности для их информационных систем.
Ожидаемые результаты:	• Категорирование безопасности - Важным для процесса категорирования безопасности является документирование исследования, ключевых решений и поддерживающего обоснования по категорированию безопасности информационной системы (оно включается в План обеспечения безопасности системы). • Требования безопасности высокого уровня • Уровень оценок усилий - Начальный уровень усилий может быть получен из применения результатов категорирования безопасности к минимальным мерам безопасности из NIST SP 800-53 и процедур оценки из NIST SP 800-53A, *Руководство по оценке мер безопасности в федеральных информационных системах*.
Синхронизация:	Категорирование безопасности должно быть пересмотрено, если есть существенные изменения в информационной системе или когда обновлён анализ влияния на деятельность.
Взаимозависимости:	• Анализ влияния на деятельность: Персонал агентства должен рассмотреть перекрёстное использование категорирования безопасности и Анализа влияния на деятельность (BIA) информации в выполнении каждой работы. Так как у этих работ есть общие цели, агентства должны совместно выполнять эти работы для каждой информационной системы и использовать результаты, чтобы гарантировать точность. • CPIC и EA: Так же, как инвестиции в IT не должны быть сделаны без одобренной деятельностью архитектуры,[3] категорирование безопасности в начале жизненного цикла безопасности является работой, обеспечивающей деятельность, непосредственно подпитывающей процессы EA и CPIC, а также решения по миграции и модернизации. • Проектирование системы: Понимание и проектирование архитектуры системы с различными подразумеваемыми уровнями воздействия могут помочь в достижении экономии за счёт роста сервисов безопасности и защите через общие зоны безопасности в предприятии. Этот тип подхода требует основательного понимания информации и типов данных агентства, полученных посредством процесса категорирования безопасности. • Планирование непредвиденных обстоятельств и аварийного восстановления: Персонал планирования непредвиденных обстоятельств и аварийного восстановления должен рассмотреть информационные системы, которые имеют множественные типы данных различных уровней воздействия и сгруппировать приложения с аналогичными уровнями воздействия на системы с достаточно защищёнными инфраструктурами. Это гарантирует эффективное применение правильных мер безопасности от непредвиденных обстоятельств и восстановления защиты и позволяет избегать излишней защиты систем более низкого воздействия. • Соглашения по совместному пользованию информации и взаимодействию систем: оценивая межведомственное взаимодействие персонал агентства должен использовать обобщённую и конкретную информацию категорирования безопасности.
Советы по реализации	
• Чтобы обеспечить соответствующий уровень поддержки предназначения и надлежащею реализацию текущих и будущих требований информационной безопасности, каждое агентство должно установить формальный процесс, чтобы подтвердить категорирование уровня систем с точки зрения приоритетов агентства. Это будет не только способствовать сопоставимой оценке систем, но также и приводить к дополнительным преимуществам, которые включают усиление общих мер безопасности и установление глубокой защиты. • Персонал агентства должен рассмотреть уместность предварительных уровней воздействия в отношении организации, окружающей среды, предназначения, использования и взаимодействия, связанных с рассматриваемой информационной системой, чтобы учесть: важность предназначения агентства; результаты жизненного цикла и календарного планирования; информацию, связанную с конфигурацией и политикой безопасности; специальные требования к обработке; и т.д., и внести, при необходимости, изменения.	

[3] Документ Объединённой эталонной модели FEA, версия 2.1, декабрь 2006.

- Даже при том, что категорирование безопасности информационной системы может привести к определению системы как умеренного или высокого воздействия, отдельные меры безопасности SP 800-53, предписанные для конфиденциальности, целостности и/или доступности, могут быть установлены в наивысшем значении, определённом для отдельной цели безопасности, если меры безопасности действительно независимы и, если стоимость или другие соображения являются существенными. В этом случае, необходимо следовать подходу управления рисками к выбору мер безопасности, и любые допустимые различия должны документироваться в план обеспечения безопасности информационной системы.
- Персонал агентства должен знать, что есть несколько факторов, которые нужно рассмотреть во время агрегирования типов информации системы. При рассмотрении этих факторов, могут появиться ранее непредвиденные соображения, затрагивающие категорирование воздействия конфиденциальности, целостности и/или доступности на уровень системы. Эти факторы включают агрегирование данных, критическую функциональность системы, смягчающие обстоятельства и другие системные факторы.

3.1.3.3 Оценка влияния на деятельность

Описание:	Оценка воздействия системы на направления деятельности агентства соотносит конкретные компоненты системы с обеспечиваемыми критическими сервисами деятельности. Эта информация затем используется для характеристики последствий для деятельности и предназначения от нарушения компонентов системы. Начальный проект этого, разрабатываемый в начале жизненного цикла, подготавливает заинтересованные стороны системы к принятию решений по ИТ и безопасности. Эта задача должна также учитывать уровень воздействия, определённый во время категорирования безопасности. Используйте NIST SP 800-34, *Руководство по планированию на случай непредвиденных ситуаций для систем информационных технологий*, как шаблон для оценки влияния на деятельность.
Ожидаемые результаты:	• Определение направлений деятельности, поддержанных этой системой, и какое влияние будет оказываться на эти направления деятельности; • Определение основных компонентов системы, необходимых для сопровождения минимальной функциональности; • Определение отрезка времени, в течение которого может снизиться работоспособность системы, прежде чем это повлияет на деятельность (начальное назначение необходимого Времени восстановления); и • Определение допустимости для деятельности потери данных (начальное назначение необходимой Точки восстановления).
Синхронизация:	• Это должно периодически пересматриваться и обновляться по мере принятия основных решений по разработке (таких, как новая функциональность), или значительного изменения назначения и области системы. • По мере развития системы, BIA должен расширяться большей детальностью по основным ИТ компонентам.
Взаимозависимости:	• BIA - ключевой шаг в процессе планирования на случай непредвиденных ситуаций. BIA облегчает улучшение характеристик требований, процессов и взаимозависимостей системы и использует эту информацию, чтобы определить требования на случай непредвиденных ситуаций и решения по их смягчению. • Действия по категорированию безопасности в соответствии с FIPS 199 с точки зрения входов и назначения определяет его как дополнительную работу, которая обеспечивает сдержки и противовесы, чтобы гарантировать что все факторы деятельности соответственно учтены.

Советы по реализации

- Часть этой информации может быть получена из исходной оригинальной экономической модели.
- Для больших и более сложных разработок, рассмотрите проведение встречи заинтересованных сторон, чтобы провести мозговой штурм взаимосвязей и воздействий.
- Когда применимо, используйте повторно данные и информацию для различного назначения. Решения по категорированию могут быть снова использованы для решений по оценкам влияния на деятельность (BIA), аварийному восстановлению (DR), планированию на случай непредвиденных ситуаций (CP) и непрерывности деятельности (COOP). Категорирование должно отражать приоритеты DR. В противном случае существует возможность, что категорирование не будет проведено на соответствующем уровне, или приоритеты DR неправильные.
- Результаты BIA могут использоваться, чтобы разработать требования или цели для соглашений об уровне обслуживания (SLAs) с поставщиками вспомогательных сервисов.

3.1.3.4 Оценка воздействия на приватность

Описание:	При разработке новой системы важно предметно рассмотреть, будет ли система передавать, хранить или создавать информацию, которая может быть рассмотрена как приватная информация. Это, как правило, определяется во время процесса категорирования безопасности, когда определяются типы информации. После того как определено, что разрабатываемая система будет, вероятно, иметь дело с приватной информацией, владелец системы должен работать над

	определением и реализацией надлежащих мер защиты и безопасности, включая процессы по учёту требований к обработке и документированию инцидентов с приватной информацией. Многие агентства используют или одно или двухступенчатую модель для учёта рассмотрений по приватности. Модель с одним шагом требует для всех систем в реестре систем агентства разработать оценку воздействия на приватность, которая устанавливает критерии определения информации приватности и документирует использование мер безопасности, для правильной защиты информации. Напротив, двухступенчатая модель осуществляет разделение путём обработки всех систем посредством порогового анализа, который фокусируется на том, должна ли выполняться оценка воздействия на приватность. При положительном ответе должна выполняться более подробная оценки данных о приватности и надлежащих мер обеспечения безопасности в форме оценки воздействия на приватность. Результирующий документ любого процесса должен быть включён в план обеспечения безопасности системы и соответственно сопровождён.
Ожидаемые результаты:	Подробная информация Оценки воздействия на приватность о том, где и до какой степени приватная информация собирается, хранится или создаётся в системе.
Синхронизация:	По мере принятия важных решений или значительного изменения назначения и области системы должны постоянно осуществляться пересмотр и обновление.
Взаимозависимости:	• Категорирование безопасности по FIPS 199 - начальный шаг в определении типов информации таких, как приватная информация. • Определение и оценка мер безопасности должны отражать являются ли необходимыми дополнительные меры безопасности для защиты приватной информации. • Это оказывает влияние на План обеспечения безопасности системы, План действий в непредвиденных ситуациях и Оценку воздействия на деятельность, что, возможно, должно быть отражено в этих документах.
Советы по реализации	
• Управление приватной информацией: Закон о неприкосновенности частной жизни 1974 г., 5 U.S.C. § 552A • Закон об электронном Правительстве 2002 усилил требования по защите приватности Закона о неприкосновенности частной жизни 1974 г. В соответствии с этими публичными законами, у агентств федерального правительства есть конкретные обязанности относительно сбора, распространения или разглашения информации относительно людей. • Меморандум OMB, “Руководство OMB для реализации положений по приватности закона об электронном Правительстве 2002” от 29 сентября 2003, приводит положения приватности закона об электронном Правительстве 2002 г. в действие. Руководство относится к информации, которая идентифицирует людей в распознаваемой форме, включая имя, адрес, номер телефона, номер социального страхования и адреса электронной почты. • OMB M-06-16 и OMB M-07-17.	

3.1.3.5 Обеспечение использования процессов разработки безопасных информационной систем

Описание:	Основная ответственность за безопасность приложений, во время ранних фаз, лежит в руках группы разработчиков, у которой есть самое всестороннее понимание подробностей работы приложений и возможность определить дефекты безопасности в функциональном поведении и логике процессов деятельности. Они являются первым уровнем обороны и возможностью построить безопасно. Важно, чтобы их роль не была присвоенной или уменьшенной. Взаимодействие и обеспечение ожиданий являются ключевыми для планирования и предоставления среды, которая защищает далее до уровня кода. Рассмотрения для планирования включают: ***Концепция безопасности деятельности (CONOPS) для разработки.*** Документ по концепции деятельности для безопасной разработки должен быть установлен для окружающей среды, и должен существовать план действий в непредвиденных ситуациях в месте нахождения репозитория кода, так как исходный код - преобладающий продукт разработки программного обеспечения и системы и должен быть сохранен в случае нарушений в среде разработки. ***Стандарты и процессы.*** Разработка системы должна происходить по стандартным процессам, которые учитывают безопасные методы, являются задокументированными и повторяемыми. Чтобы достигнуть этого, должны быть определены и задокументированы соответствующие процессы обеспечения безопасности для уровня доверия, требуемого для систем. Таким образом, системам с высокими требованиями доверия, возможно, понадобятся дополнительные меры безопасности, встроенные в процесс разработки.

	Обучение безопасности для команды разработчиков. Для ключевых разработчиков может потребоваться дополнительное обучение по безопасности, чтобы понять текущие угрозы и потенциальную эксплуатацию их продуктов, а также обучение по технологиям безопасного проектирования и кодирования. Это облегчает разработчикам создание более безопасных проектов и позволяет им решать ключевые проблемы с начала процессов разработки. ***Управление качеством.*** Управление качеством, которое включает планирование, обеспечение и контроль, является ключевым для обеспечения минимальных дефектов в и надлежащего создания информационной системы. Это сокращает лазейки или дыры, которые иногда остаются открытыми для эксплуатации или неправильного использования (намеренно или нет), порождая уязвимости в системе. ***Безопасная среда.*** Среда разработки системы должна соответствовать минимальным критериям соответствия FISMA, как определено в SP 800-53. Она должна включать рабочие станции, серверы, сетевые устройства и репозитории кода. Среды разработки должны быть аттестованы, как любая другая автоматизированная система или окружающая среда. Безопасная среда разработки является залогом разработки безопасного программного обеспечения и систем. ***Методы безопасного кодирования и репозитории.*** Особое внимание должно быть обращено на репозитории кода с акцентом на системы, которые поддерживают поставку дистрибутивного кода с функциональностью входного/выходного контроля. Для организации доступа к репозиторию кода должен применяться ролевой доступ, и должны регулярно рассматриваться журналы регистрации, как часть безопасного процесса разработки. Код должен разрабатываться в соответствии со стандартными методами. Необходимая часть вышеупомянутого CONOPS - установление и поддержание образцов и компонентов безопасного кодирования. Образцы безопасного кодирования воплощают примеры уровня кодирования и сопроводительную документацию, которые иллюстрируют, как удовлетворять конкретным функциональным требованиям, одновременно достигая эталонов безопасности. Эти образцы могут затем снова быть использованы разработчиками, чтобы гарантировать, что все компоненты программного обеспечения разработаны доверенным способом, могут быть приняты и одобрены организацией. Когда возможно, законченные компоненты программного обеспечения, которые прошли сертификацию безопасности должна быть сохранены как компоненты многократного использования для будущей разработки программного обеспечения и системной интеграции. Как команда, разработчики системы и представители безопасности должны договориться о том, какие шаги могут и должны быть сделаны, чтобы гарантировать полезное и рентабельное содействие безопасной среде разработки.
Ожидаемые результаты:	• Планы обучения безопасности этапа разработки. • Запланированные технологии, поставки и вехи обеспечения качества. • Стандарты разработки и кодирования, включая среду разработки.
Синхронизация:	Уроки, извлечённые из завершённых продуктов и тестирования безопасности, должны быть оценены для применимости в настройке процессов и стандартов разработки, чтобы предотвратить неэффективные вложения.
Взаимозависимости:	• Стандарты разработки ИТ должны содержать соответствующие методологии, которые добавляют значимость к процессам и не ухудшают безопасность. • Обучение и ориентация на разработку систем должны включать основное и специализированное (по среде) осведомление, обучение и образование по безопасности.

Советы по реализации

- Понимание современных дефектов безопасности приложений и методов нападения важно для защиты против них систем. Обеспечение обучения безопасности приложений для команд по разработке и тестированию увеличит понимание проблем и технологий и должно способствовать разработке более защищённых систем. Если разработчики знают, что искать и что проверять во время этапа разработки, количество дефектов безопасности, выделенных и исключённых при обеспечении качества (QA), должно быть сокращено. Кроме того, если испытательная команда QA хорошо обучена в области применения безопасности, она более вероятно определит проблемы безопасности, прежде чем продукт перейдёт в следующую фазу тестирования. Такое обучение должно привести к большей уверенности в общей безопасности реализованной системы. Обеспечение обучения безопасности приложений будет также подчёркивать для команды важность безопасности приложений.
- Любой недостаток, ставший известным команде разработчиков, должен учитываться как можно скорее. Неблагоразумно предполагать, что сложные нападения, требующие существенного знания внутренних работ системы, маловероятны для

злонамеренных нападающих. Есть много случаев, когда владельцы систем были удивлены обнаружив, что нападавшие смогли «обнаружить» информацию, которую владельцы систем считали скрытой.

- Чтобы уменьшить возможность дефектов безопасности в системе, должны быть рассмотрены и включены в существующие стандарты кодирования или руководящие документ разработки дополнения, сосредоточенные на безопасности. Эти стандарты должны учитывать все типы используемых языков разработки программного обеспечения, такие как C++, Java, HTML, JavaScript и SQL.

3.2 Фаза SDLC: Разработка/приобретение

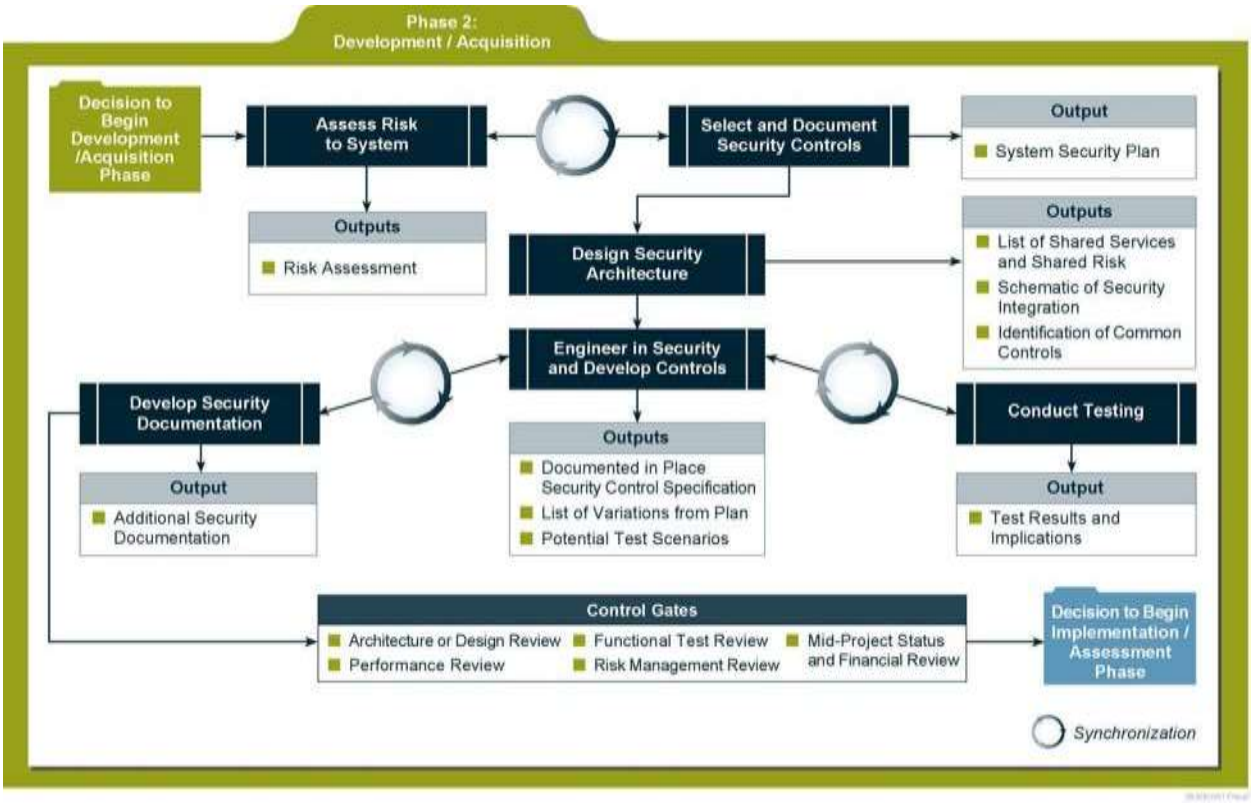

РИСУНОК 3-3. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ РАЗРАБОТКИ/ПРИОБРЕТЕНИЯ

3.2.1 Описание

Этот раздел определяет рассмотрения безопасности, относящиеся ко второй фазе SDLC. Ключевые работы безопасности для этой фазы включают:

- Проведение оценки риска и использование результатов для дополнения базового набора мер обеспечения безопасности;
- Анализ требований безопасности;
- Проведение функционального тестирования и тестирования безопасности;
- Подготовку исходных документов к сертификации и аттестации системы; и
- Проектирование архитектуры безопасности.

Хотя этот раздел представляет компоненты информационной безопасности последовательным нисходящим образом, порядок завершения не обязательно установлен. Анализ безопасности сложных систем должен повторяться до достижения согласованности и полноты.

3.2.2 Управляющие результаты

Общие типы управляющих результатов для этой фазы могут включать:

- Анализ архитектуры/проекта, который оценивает проект планируемой системы и потенциальную интеграцию с другими системами, а также включение общих сервисов и общих мер обеспечения безопасности, таких как аутентификация, аварийное восстановление, обнаружение вторжений или отчётность об инцидентах.
- Анализ исполнения системы, который оценивает, предоставляет ли система, или способна ли предоставить задокументированные ожидания владельца и ведёт ли себя система

предсказуемым образом если её подвергнуть неправильному использованию. (Например, способность системы поддержать доступность и целостность данных при ожидаемых чрезвычайных нагрузках ресурсов.)

- Функциональный анализ системы, который гарантирует, что определённые функциональные требования являются достаточно детализированными и тестируемыми.
- Промежуточный проектный & Финансовый анализ важен для обнаружения основных изменений в запланированном уровне усилий, чтобы гарантировать, что отношения эффективности-стоимости контролируются и принимаются эффективные решения.
- Последующий анализ решений по управлению рисками может быть необходим, если вследствие вышеупомянутых анализов изменяются система и/или её меры безопасности и/или её требования.

3.2.3 Основные работы по безопасности

3.2.3.1 Оценка риска для системы

Описание:	Агентства должны обращаться к NIST SP 800-30, *Руководство по управлению рисками для систем информационных технологий*, для руководства при проведении оценок риска. Назначение оценки риска состоит в том, чтобы оценить текущее понимание проекта системы, заявленные требования и минимальные требования безопасности, следующие из процесса категорирования безопасности, чтобы определить их эффективность для снижения ожидаемых рисков. Результаты должны показать, что установленные меры безопасности обеспечивают соответствующую защиту или выделить области, где необходимо дальнейшее планирование. Чтобы быть успешным, необходимо участие людей, которые хорошо осведомлены в дисциплинах в системной области (например, пользователи, специалисты по технологиям, эксперты по эксплуатации). Оценка риска безопасности должна быть проведена перед санкционированием спецификаций проекта, так как это может привести к дополнительным спецификациям или привести к дальнейшему обоснованию спецификаций. В дополнение к рассмотрению перспективы безопасности разрабатываемой/приобретаемой системы, организации должны также рассмотреть, как система могла бы затронуть другие системы, с которыми она будет прямо или косвенно связана. Это может означать, что есть унаследованные общие меры безопасности, которые необходимо усилить, или дополнительные риски, которые должны быть снижены. В этих случаях может быть необходим анализ предприятия, чтобы обеспечить более полное представление об угрозах и уязвимостях.
Ожидаемые результаты:	Усовершенствованная оценка риска на основе более зрелого проекта системы, которая более точно отражает потенциальный риск для системы, известные слабые места в проекте, установленные проектные ограничения и известные угрозы для деятельности и компонент ИТ. Кроме того, предыдущие требования теперь трансформируются в конкретные меры безопасности системы.
Синхронизация:	Так как эта оценка риска закончена в более зрелой стадии разработки системы, это может потребовать пересмотреть ранее законченные шаги по безопасности, такие как BIA или категорирование безопасности. Разработка редко идёт как запланировано и у требований есть путь измениться.
Взаимозависимости:	• Категорирование безопасности предоставляет начальную информацию для оценки риска на основе типов информации. • На основе оценки риска могут быть спланированы или изменены дополнительные меры безопасности или компенсирующие меры безопасности, чтобы обеспечить требуемую защиту для информации и информационных систем.
Советы по реализации	
• В любой организации угроза из внутренних источников остаётся самой вероятной для возникновения. Нелояльные сотрудники [разработчики системы], которые являются также привилегированными пользователями системы, являются реальной угрозой, тем более, что у таких сотрудников могут быть активные учётные записи в системе. Методы должны включать независимые проверки системы и процессов её поддержки. Могут использоваться постоянный контроль внутренних источников и инструменты контроля целостности, чтобы гарантировать аудит и управление конфигурацией, посредством автоматизированного централизованного сбора, корреляции и аналитических инструментов для журналов. • Хорошим средством является мониторинг Национальной базы данных уязвимостей (http://nvd.nist.gov) для известных уязвимостей компонентов и модификация мер безопасности, чтобы смягчить их. Затем они должны быть проверены.	

- Имея дело с системой, имеющей многих владельцев (иногда в различных областях), важно определить и учесть разделённые и унаследованные риски.
- В зависимости от необходимой точности и сложности системы, может быть важным следить за потоком данных/ совместным пользованием информации за пределами первого интерфейса. Отказ делать так может привести к наследованию неизвестных рисков.
- Другие унаследованные риски могут быть оценены посредством поставки материалов для системы. Риск системы поставок должен быть понят и оценён, чтобы смягчить потенциальное использование мошеннического, пиратского, нелицензированного или намеренно ставящего под угрозу материала.

3.2.3.2 Выбор и документирование мер обеспечения безопасности

Описание:	Выбор и документирование мер безопасности соответствуют шагу 2 в Основах управления рисками NIST. Выбор мер безопасности включает три действия: выбор базового набора мер обеспечения безопасности (включая общие меры обеспечения безопасности); приложение руководства по адаптации мер безопасности, чтобы приспособить начальный базовый набор мер безопасности; и дополнение адаптированного базового набора дополнительными мерами безопасности, базируясь на оценке риска и местных условиях. В процессе выбора мер безопасности важно рассмотрение всей организации, чтобы гарантировать, что адекватное смягчение риска достигнуто для всех процессов предназначения/деятельности, информационных систем и инфраструктуры организации, поддерживающей эти процессы. Процесс выбора мер безопасности должен включать анализ законов и нормативных документов, таких как FISMA, циркуляры OMB, законы, определяющие деятельность агентства, конкретное для агентства регулирование, FIPS и Специальные публикации NIST, и другое законодательство и нормы федерального права, которые определяют применимую специфику к выбору мер безопасности. Как и с другими аспектами безопасности, целью должна быть рентабельная реализация, которая учитывает требования для защиты информационных активов организации. В каждой ситуации, должен существовать балансе между эффектом от безопасности системы для исполнения предназначения и рисками, связанными с применением системы. Меры безопасности, связанные с отдельными информационными системами, документируются в план обеспечения безопасности систем, как описано в Специальной публикации NIST 800-18. Планы обеспечения безопасности предоставляют обзор требований безопасности для информационных систем в организации и описывают существующие или планируемые меры безопасности для соответствия этим требованиям. Планы также содержат обоснование для категорирования безопасности, действий по адаптации и дополнению, реализации отдельных мер безопасности в конкретных средах эксплуатации и любых ограничений использования, применяемых в информационных системах при ситуациях, связанных с высоким риском. Планы обеспечения безопасности важны потому, что они документируют решения, принятые во время процесса выбора мер безопасности и обоснования для этих решений. Они одобряются соответствующими санкционирующими должностными лицами в организации и представляют один из ключевых документов в пакетах аттестации безопасности, которые способствуют решениям по санкционированию.
Ожидаемые результаты:	• План безопасности системы - спецификация мер безопасности, которая определяет какие, где и как меры безопасности будут применятся.
Синхронизация:	• Меры безопасности и связанные спецификации должны отражать применённые уровни защиты системы в соответствии с критериями выбора мер безопасности. • Существенные решения должны рассматривать любые возможные вторичные риски, которые могут в итоге оказать влияние на предыдущие соображения в отношении мер безопасности и защитных мер, определённых во время оценка риска.
Взаимозависимости:	• После того, как они сформулированы, требования к мерам безопасности должны быть включены в план обеспечения безопасности системы. • Оценка степени риска - основной инструмент для определения, эффективны ли адаптированные меры безопасности в отношении учёта допустимого риска организации.
Советы по реализации	
• Учёт требований безопасности в матричном формате позволяет разработчикам и инженерам по безопасности рассматривать реализацию в отношении основных компонентов системы и может облегчить гэп-анализ, гарантируя надлежащий анализ рисков и контроль реализации.	

- Требования информационной безопасности должны быть выражены в конкретных терминах. Для сложных систем может быть необходим итерационный анализ требований. При этом, плановые пересмотры должны происходить в основных вехах SDLC.
- Любое новое функциональное требование может иметь последствия относительно безопасности. Появление дополнительного риска или ослабление существующих мер безопасности более вероятны, если конкретный анализ безопасности не выполнен для каждого добавленного функционального требования. При этом возможно попадание в систему недокументированного риска.
- Более подробные требования «предотвращения вторжения» также помогут гарантировать, что меры и методы безопасности проверены до реализации. Если существует документированное требование, то предполагается, что должен будет быть разработан и выполнен тестовый сценарий.
- Меры безопасности не одномерны и должны учитываться соответствующим образом на многих компонентах по всей системе. Например, если ваша система состоит из SQL-серверов, Веб-Сферы и универсальной ЭВМ, то оценки, возможно, должны быть запланированы, в зависимости от системы, для всех, некоторых или ни для одного компонента. Документирование этого во время этой стадии уменьшает уровень усилий во время тестирования.
- Агентства должны начать планирование ликвидации во время этой фазы и планировать ликвидацию/передачу на всех фазах жизненного цикла. Эту работу лучше всего сделать как часть фазы формирования требований так, чтобы полные требования к ресурсам для ликвидации были поняты и планированы. Процедуры ликвидации могут добавлять стоимость всюду по жизненному циклу, поскольку аппаратное и программное обеспечение становятся устаревшими или повреждаться в других фазах.

3.2.3.3 Проектирование архитектуры безопасности

Описание:	С увеличением поставщиков общих услуг и централизации некоторых ключевых сервисов безопасности в агентствах становится более важно планировать эти сервисы и понимать, как они будут интегрированы в систему. Архитектура предприятия системы должно гарантировать, что инициатива соответствует будущим планам агентства и не находится в противоречии или не предоставляет без необходимости избыточные услуги. Кроме того, по мере продвижения системы и большего принятия решений относительно используемых сервисов, EA должна пересматриваться для оптимальной интеграции. На системном уровне, должна быть создана архитектура безопасности и затем внедрена в проект системы. Это может быть достигнуто путём зонирования или кластеризации сервисов, сосредоточения или распределения для избыточности или для дополнительных уровней защиты. Проектирование безопасности на системном уровне должен учесть сервисы, получаемые извне, планируемое взаимодействие систем и различные ориентации пользователей системы (например, пользователи сервисов или системные администраторы). Другим примером была бы стратегия аудита системы, которая должна быть разработана, чтобы дать возможность точного отслеживания или реконструкции всех приоритетных и высоко-рискованных потоков операций. Стратегия аудита должна включать различные записи аудита от нескольких различных компонентов, включая (но не ограничиваясь) Веб-приложения, базы данных, универсальные ЭВМ и веб-серверы. Цель должна состоять не в том, чтобы получить как можно больше информации об аудите, а получить только то, что необходимо, чтобы обеспечить достаточно информации для исследования потенциальных нарушений защиты и системных отказов. Эти действия могут выполняться, когда анализ разработки ИТ показывает известные узкие места и отдельные точки отказов. Минимальные требования безопасности, а также требования и ограничения, определённые в начале процесса, должны предоставить архитекторам ряд предположений и ограничений для создания окружения. Эта работа может иметь большое значение для системы в понижении общей стоимости владения путём планирования компонентов ядра систем безопасным способом.
Ожидаемые результаты:	• Схематичное представление интеграции безопасности предоставляет детали того, где в системе безопасность реализована и распределена. Архитектуры безопасности должны быть графически изображены и детализированы до такой степени, чтобы читатель мог увидеть, где основные меры безопасности применены и как. • Список общих сервисов и результирующего общего риска. • Идентификация общих мер безопасности, используемых системой.
Синхронизация:	• Архитектура безопасности становится ключевым компонентом документации по системе, которая должна пересматриваться и сопровождаться при наступлении значительных изменений или существенных управляющих условий (вех). • Значительные следствия оценок, тестирования безопасности и пересмотров должны быть исследованы на потенциальную обратную связь с эффективностью.
Взаимозависимости:	• Архитектура предприятия должна обеспечить понимание от других подобных систем или сервисов, где интеграция оптимальна.

	• Планы безопасности системы должны обобщённо документировать подход или стратегию архитектуры безопасности. • Анализ требований безопасности предоставляет большинство информации на подробном уровне. Это даёт возможность архитектору рассмотреть информацию, применить её теоретически на системном уровне и определить, будут ли меры безопасности работать как предназначено или если есть бреши или ненужная избыточность.
Советы по реализации	
• Архитектура безопасности может предоставить эффективные компенсационные меры безопасности, когда есть проблемы с реализацией минимальных требований безопасности в специфике проекта системы. Архитектуры безопасности также определят общие меры безопасности, которые наследует система, а также кто несёт ответственность за эти общие меры безопасности. • Демонстрация логики последствий безопасности этой системы поможет в определении потребности в дополнительных мерах безопасности. • Риски, принятые для системы, которые могут иметь неблагоприятное влияние на предприятие, могут быть определены и подняты как проблемы во время пересмотра архитектуры. Риск предприятия, наивысший из всех рисков отдельных систем, должен быть выражен и отслежен через процесс Архитектуры предприятия агентства.	

3.2.3.4 Проектирование безопасности и разработка мер обеспечения безопасности

Описание:	Во время этой стадии меры безопасности реализуются и становятся частью системы, что лучше, чем их применение, когда она создана. Применение мер безопасности при разработке необходимо тщательно рассматривать и последовательно планировать. Намерение состоит в том, чтобы интегрировать меры безопасности так, чтобы проблемы с работой системы стали известны как можно раньше. Кроме того, некоторые меры безопасности могут ограничивать или препятствовать нормальным действиям по разработке. Для новых информационных систем требования безопасности, определённые и описанные в соответствующих планах безопасности систем, теперь спроектированы, разработаны и реализованы. Планы безопасности систем для эксплуатируемых информационных систем могут потребовать разработки дополнительных мер безопасности для дополнения существующих мер безопасности или модификации мер безопасности, которые, возможно, являются недостаточно эффективными. Во время этой задачи, решения принимаются на основе проблем интеграции и компромиссов. Является важным документировать основные решения и их причины, связанные с деятельностью/технологиями. В случаях, когда применение запланированной меры безопасности невозможно или нежелательно, должны быть рассмотрены и задокументированы компенсирующие меры безопасности.
Ожидаемые результаты:	• Реализованные меры безопасности с задокументированной спецификацией для включения в план обеспечения безопасности. • Список изменений мер безопасности, следующих из решений по разработке и компромиссов. • Потенциальные сценарии оценки для проверки известных уязвимостей или ограничений.
Синхронизация:	• Применение мер безопасности может претерпеть изменение в результате функционального и пользовательского тестирования. Изменения должны быть задокументированы.
Взаимозависимости:	• Анализ требований безопасности должен быть пересмотрен и обновлён, если необходимы изменения. • Стратегия архитектуры безопасности должна быть пересмотрена и обновлена, если необходимы изменения. • Конкретные конфигурации должны быть задокументированы или упомянуты в плане обеспечения безопасности системы.
Советы по реализации	
Документирование отклонений безопасности от начальных требований безопасности на данном этапе будет способствовать целостному планированию рисков и уменьшит в дальнейшем время на возврат к обоснованию деятельности. Кроме того, это представляет свидетельство планирования риска.	

3.2.3.5 Разработка документации по безопасности

Описание:	При том, что самым значимым документом является План обеспечения безопасности системы, поддерживающая его документация может включать: • План управления конфигурацией • План действий в непредвиденных ситуациях (включая Оценку влияния на деятельность) • План постоянного мониторинга

	• План освоения, обучения и образования по безопасности (SATE) • План реагирования на инциденты • Оценка воздействия на приватность (PIA) Разработка этих документов должна свидетельствовать о зрелости документирования сервисов безопасности. В некоторых случаях, эти документы могут содержать только известные требования, общие меры безопасности и шаблоны. Заполнение этих документов должно начаться как можно раньше в проекте. На данном этапе, важно закрепить подход к безопасности, область приложения и понимание обязанностей. Например, план DR может быть закрыт соединением с Системой общей поддержки, а SATE может быть на субподряде у поставщика общих услуг. В этом случае, планы могут сосредоточиться на специфических особенностях системы и могут ссылаться на ключевые пункты имеющегося соглашения об уровне обслуживания. Документирование, как прогресс разработки системы может обеспечить снижение издержек и улучшить возможности принятия решений через комплексный подход, который обеспечивает раннее обнаружение брешей.
Ожидаемые результаты	• Дополнительная документация по безопасности, поддерживающая план обеспечения безопасности системы.
Синхронизация	Эти документы необходимо обновить к завершению приёмочного тестирования пользователями, чтобы гарантировать, что они корректны.
Взаимозависимости	• Документация по безопасности систем должна быть согласована с: o Анализом требований безопасности o Архитектурой безопасности o Оценкой влияния на деятельность, и o Категорированием безопасности.
Советы по реализации	
• Деятельность по безопасности не должна направляться документацией по соответствию, а основываться на системе, требуемой и описанной в соответствии с руководством по безопасности. • Для основных систем, которые являются большими по размеру, комплексными по проекту или политически чувствительными, лучше назначать точки контакта (POC) для каждого документа и начинать разработку с ознакомления с областью, ожиданиями и уровнем детализации документа.	

3.2.3.6 Проведение тестирования (Связанного с разработкой, функциональностью и безопасностью)

Описание:	Разрабатываемые системы или подвергающееся модификации (ям) в части программного обеспечения, аппаратных средств и/или коммуникационного оборудования должны быть протестированы и оценены до того, как они будут реализованы. Цель процесса тестирования и оценки состоит в том, чтобы проверить то, что разработанная система выполняет требования по функциональности и безопасности. Тестирование мер безопасности основано на технических спецификациях безопасности для этих мер безопасности, с дополнением процедурами оценки, детализированными в SP 800-53A NIST, *Руководство по оценке мер безопасности в Федеральных информационных системах*. Процесс фокусируется на конкретности, воспроизводимости и повторяемости. Для конкретности, тестирование должно определяться контекстом, чтобы протестировать соответствующее требование безопасности, как оно определено для использования в его среде. Для воспроизводимости процесс тестирования должен быть способным к выполнению серии тестов для информационной системы неоднократно (или параллельно на подобных системах) и приводить каждый раз к подобным результатам. Для повторяемости, для каждой системы требуется выполнять функциональные тесты полностью или частично последовательно несколько раз, чтобы достигнуть допустимого уровня согласия с требованиями системы. Чтобы достигнуть этого, функциональное тестирование должно быть до возможной степени автоматизировано, и тестовые варианты должны быть подробны описаны, чтобы гарантировать, что процесс тестирования является воспроизводимым и повторяемым. Включение инструментов автоматизированного тестирования и интеграция с Автоматизированным протоколом контента безопасности NIST (SCAP) должны быть завершено до начала тестирования мер безопасности и работ по оценке. Любая функциональность безопасности, не протестированная во время функционального или автоматизированного тестирования, должна быть тщательно исследована, чтобы гарантировать соответствие требованиям во время комплексного тестирования и оценки мер безопасности. При разработке систем должны использоваться только тестовые данные или "заглушки". Абсолютно ни какая эксплуатационная, относящаяся к безопасности или персональная идентификационная информация (PII) не должна находиться ни в какой системе или программном обеспечении во время разработки.

Ожидаемые результаты	Документация с результатами испытаний, включая любые непредвиденные отклонения, обнаруженные при тестировании.
Синхронизация	Все результаты испытаний возвращаются разработчикам для управления конфигурацией обновлений. Непредвиденные результаты могут потребовать, чтобы потребитель разъяснил сущность требования.
Взаимозависимости	• Может быть оказано воздействие на Анализ требований безопасности и потребуется его обновление. • Изменения могут оказать воздействие на архитектуру безопасности и потребовать её обновления. • Оценке риска для системы, возможно, потребуется обновление, чтобы точно отразить текущие послабления.

Советы по реализации

- Чтобы уменьшить усилия по избыточным работам тестирования функционала и безопасности, рекомендуется, чтобы планы функционального тестирования включали общее тестирование средств защиты (до максимально возможной степени).
- Предварительное тестирование основных мер безопасности во время функционального тестирования может уменьшить или устранить проблемы в начале цикла разработки (например, мер мандатного доступа, разработки безопасного кода и межсетевых экранов). Предварительным тестированием считается тестирование на уровне разработки, а не тестирование для оценки и аттестации (C&A), но если не происходит изменений, то результаты испытаний повторно до максимальной степени используются при C&A.
- Для систем высокой открытости и чувствительности, может быть рекомендовано независимое тестирование разработки.
- Предварительное тестирование сокращает стоимость и направлено на уменьшение риска.
- Предварительное тестирование, может быть сделано на уровне компонентов или зон безопасности, чтобы гарантировать, что каждый компонент или зона безопасности безопасны как сущность.
- Фиксируйте процессы и результаты всего тестирования безопасности, которое проводится по жизненному циклу для оценки, идентификации проблем и потенциального повторного использования.
- Должен периодически пересматриваться исходный код, как часть процесса QA разработки программного обеспечения, используя автоматизированные инструменты или ручную выборочную проверку для общих ошибок программирования, которые оказывают вредное влияние на безопасность системы, включая: уязвимости между объектовых сценариев, буферные переполнения, условия состязательности, нарушения объектной модели, плохая проверка ввода данных пользователей, плохая обработка ошибок, незащищённость параметров безопасности, очевидность паролей и нарушения заявленной политики, моделей или архитектуры безопасности.

3.3 Фаза SDLC: Реализация/Оценка

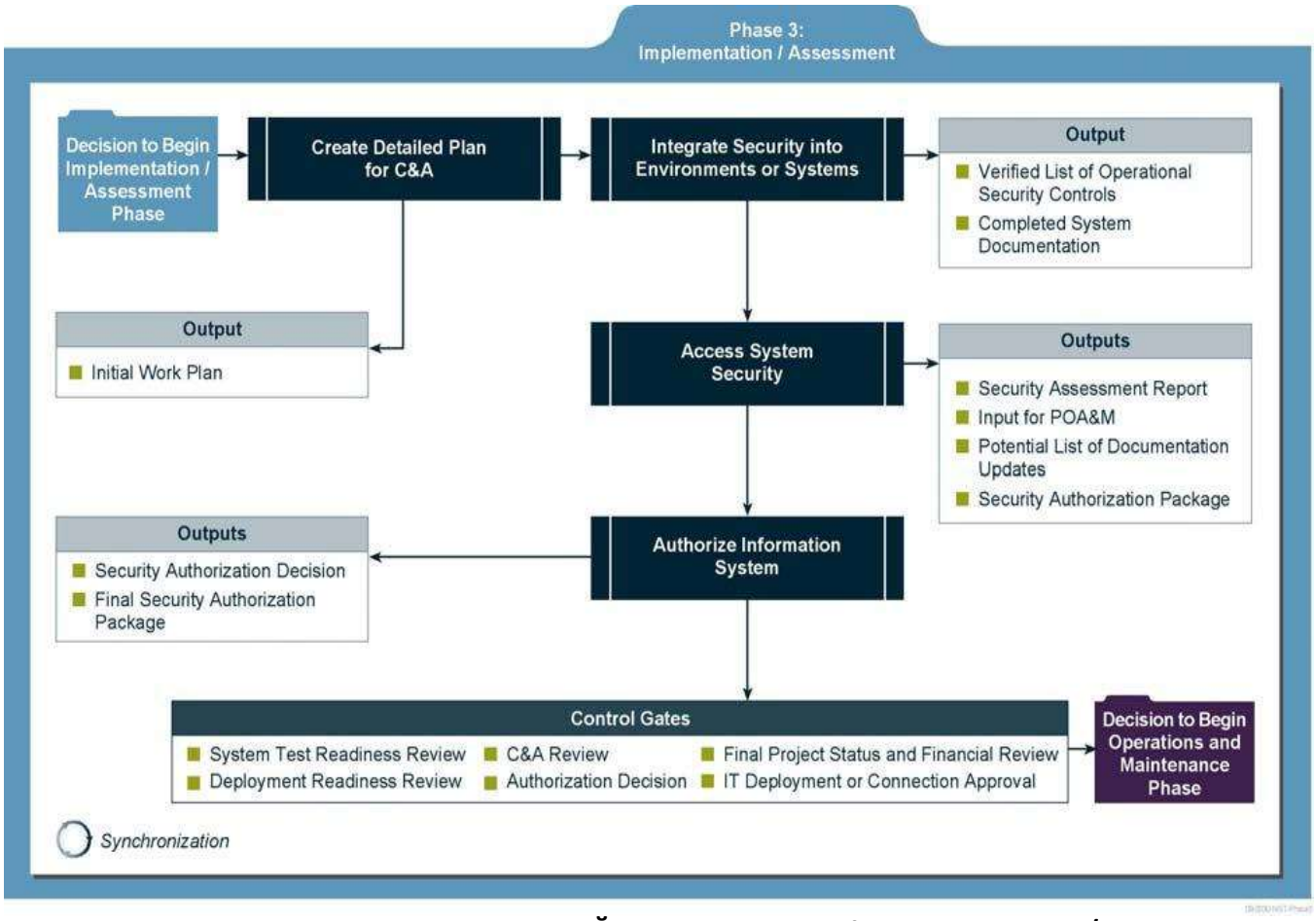

РИСУНОК 3-4. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ РЕАЛИЗАЦИИ/ОЦЕНКИ

3.3.1 Описание

Реализация/Оценка - третья фаза SDLC. Во время этой фазы система должна быть установлена и оценена в эксплуатационной среде организации.

Ключевые работы по безопасности для этой фазы включают:

- Интеграцию информационной системы в её среду;
- Планирование и проведение работ по аттестационным испытаниям системы в синхронизации с тестированием мер безопасности; и
- Работы по комплексной аттестации системы.

3.3.2 Управляющие условия

Общие типы управляющих условий для этой фазы включают:

- Анализ тестовой готовности системы
- Анализ C&A
- Заключительный обзор статуса проекта и финансов
- Анализ готовности развёртывания

- Решение Санкционирующего должностного лица (АО)
- Одобрение развёртывания или подключения ИТ.

3.3.3 Основные работы по безопасности

3.3.3.1 Создание подробного плана C&A

Описание:	Поскольку Санкционирующее должностное лицо (АО) ответственно за принятие риска применения систем, АО может советоваться с группой разработчиков, если риски, связанные с возможным применением системы, кажутся недопустимыми. Если приемлемые остаточные риски не известны, то спецификации могут наложить чрезмерное бремя и стоимость. Для определения приемлемых остаточных рисков требуется участие АО. Легче осуществить изменение требований во время стадии планирования приобретения системы, чем во время стадий предложения, начального выбора или контроля за исполнением контракта. Группа разработчиков и АО должны также обсудить формирование свидетельства, по которому АО должно принять решение. Это свидетельство может включать результаты испытаний системы и другие данные. Кроме того, инициатор приобретения и санкционирующее должностное лицо должны обсудить, как учитывать изменения в системе и её среде. Должна быть обсуждена возможность создания рабочей группы по безопасности. Такая группа может состоять из такого персонала, как пользователи, руководители программ и заказчики приложений; администраторы системы, безопасности или баз данных; сотрудники или специалисты по безопасности, включая представителей C&A; и аналитики систем или приложений. Чтобы гарантировать надлежащее тестирование и уменьшить вероятность расползания границ проекта во время тестирования, должно быть точно определено завершение аттестации безопасности. Это должно сформировать основание для плана тестирования, который должен быть создан и одобрен до работ по реализации. В этой точке должен быть близок к завершению пакет оценки и начаться определённый агентством начальный обзор соответствия.
Ожидаемые результаты	• Начальный план работ: документ планирования, который определяет ключевых игроков, проектные ограничения, базовые компоненты, область тестирования и уровень ожидаемой конкретности. Пакет оценки должен быть близок к завершению, и инициированы любые начальные, определённые агентством, обзоры соответствия.
Синхронизация	ISSO предоставляет владельцу системы завершённую документацию, требуемую, чтобы инициировать и провести C&A. АО уведомляется.
Взаимозависимости	План Оценки мер безопасности должен получить основополагающую информацию из этого планирующего документа/мероприятия.
Советы по реализации	
• Проведение мероприятия по планированию или завершение предварительного проектного планирования за четыре - шесть недель до тестирования должны предоставить достаточное количество времени для получения соответствующих ресурсов и плана. • Быстрое проведение начального анализа пакета оценки поможет обнаружить потенциальные проблемы. • Активное тестирование будет влиять на разработку и должно быть хорошо спланировано перед его выполнением. • Включение АО как можно раньше в процесс планирования (даже в фазе 1) должно определить предполагаемые результаты от C&A и исключить неожиданности до получения контрольных результатов C&A.	

3.3.3.2 Интеграция безопасности в установленные среды или системы

Описание:	Интеграция системы происходит на объекте эксплуатации, где информационная система разворачивается для применения. Интеграция и приёмочное тестирование происходят после поставки и установки информационной системы. Установка мер безопасности осуществляется в соответствии с инструкциями производителей, имеющимся руководством по реализации безопасности и задокументированными параметрами безопасности.

Ожидаемые результаты	• Подтверждённый список эксплуатационных мер безопасности. • Завершённая документация на систему.
Синхронизация	• Проблемы, с которыми встречаются во время внедрения, должны быть оценены для включения в план действий при непредвиденных обстоятельствах, основываясь на возможности их повторения. • ISSO должен проанализировать внедрённую систему, чтобы гарантировать, что меры безопасности реализованы и должным образом сконфигурированы и предоставить подтверждённый список владельцу системы и АО.
Взаимозависимости	В базовые документы по безопасности должны быть внесены изменения.
Советы по реализации	
• Очистите тестовую среду и среду разработки, чтобы гарантировать, что все данные тестирования удалены. • Должна быть проявлена чрезвычайная забота о том, чтобы при интеграции информационных систем в эксплуатационные среды или системы не была нарушена критическая деятельность.	

3.3.3.3 Оценка безопасности системы

Описание:	Разрабатываемые системы или подвергающиеся модификации программное обеспечение, аппаратные средства и/или коммуникационное оборудование должны быть формально оценены до предоставления на формальную аттестацию. Цель процесса оценки безопасности состоит в том, чтобы проверить, что система выполняет функциональность и требования безопасности и будет работать в пределах допустимого уровня остаточного риска по безопасности. Тестирование мер безопасности основано на процедурах оценки, детализированных в NIST SP 800 - 53A, *Руководство по оценке мер безопасности в Федеральных информационных системах.* До начала эксплуатации должна быть проведена оценка безопасности, чтобы оценить степень, до которой меры безопасности реализованы, работают как предназначено и производят желаемый результат относительно соответствия требованиям безопасности для системы. Кроме того, должны проводиться периодическое тестирование и оценка мер безопасности в информационной системе, чтобы гарантировать поддержание эффективности. В дополнение к проверке эффективности мер безопасности оценка безопасности может вскрыть и описать фактические уязвимости в информационной системе. Определение эффективности мер безопасности и уязвимостей информационной системы обеспечивает важную информацию для санкционирующих должностных лиц чтобы принять правильные, основанные на риске решения по аттестации безопасности.
Ожидаемые результаты	• Пакет Аттестации безопасности, который включает Отчёт об оценке безопасности, POA&M и обновлённый План безопасности системы.
Синхронизация	• Оценщик предоставляет зафиксированные результаты Пакета Оценки владельцу системы, ISSO и системному администратору. • Результаты оценки совместно используются владельцем системы, ISSO, системным администратором и разработчиками.
Взаимозависимости	Все предыдущие шаги.
Советы по реализации	
• Все документы должны быть в завершённом состоянии для анализа, чтобы гарантировать текущее состояние системы во время анализа. • Копирование Пакета оценки на CD / DVD или другие электронные носители также помогает гарантировать управление конфигурацией и текущее архивирование. • Поручение рабочей группе представителей главных заинтересованных сторон встретиться в течение тестирования поможет во взаимодействии и уменьшит неожиданности. • Точное формулирование C&A процесса всем сторонам и достижение соглашения об уровне строгости и области тестирования очень важны в обеспечении ровных усилий по оценке. • Отдавайте предпочтение непрерывному мониторингу риска и рентабельности. • Насколько возможно используйте повторно большинство предшествующих и соответствующих результатов оценки.	

3.3.3.4 Санкционирование информационной системы

Описание:	Циркуляр OMB A-130 требует санкционирования безопасности информационной системы для обработки, хранения или передачи информации. Это санкционирование (также известное как аттестация безопасности), предоставляемое высшим должностным лицом агентства, основано на

	проверке эффективности мер безопасности на некотором согласованном уровне доверия и идентификации остаточного риска активам или деятельности агентства (включая предназначение, функцию, имидж или репутацию). Решение о санкционировании безопасности - основанное на риске решение, которое зависит в значительной степени, но не исключительно, на результатах тестирования и оценки безопасности, проведенных во время процесса проверки мер безопасности. Официальное санкционирование полагается прежде всего на: (i) окончательный план обеспечения безопасности системы; (ii) результаты тестирования и оценки безопасности; и (iii) POA&M для уменьшения или устранения уязвимостей информационной системы, в получении решения о санкционировании безопасности, чтобы разрешить эксплуатацию информационной системы и явно принять остаточный риск активам или деятельности агентства.
Ожидаемые результаты	• Решение о санкционировании безопасности, задокументированное и переданное от Санкционирующего должностного лица Владельцу системы и ISSO • Заключительный Пакет санкционирования безопасности
Синхронизация	• Инвентаризационные описи и учётные данные по системе должны быть обновлены, чтобы отразить аттестованное состояние. • Действия CPIC также должны отразить аттестацию системы.
Взаимозависимости	• Обновление документации по безопасности и бюджету по результирующему статусу. • Сообщение об оценке информационной системы.
Советы по реализации	
Санкционирующие должностные лица должны принять решения не только о риске для информационной системы, но и для риска, расширенного на организацию в целом, при принятии системы в эксплуатацию.	

3.4 Фаза SDLC: Эксплуатация и сопровождение

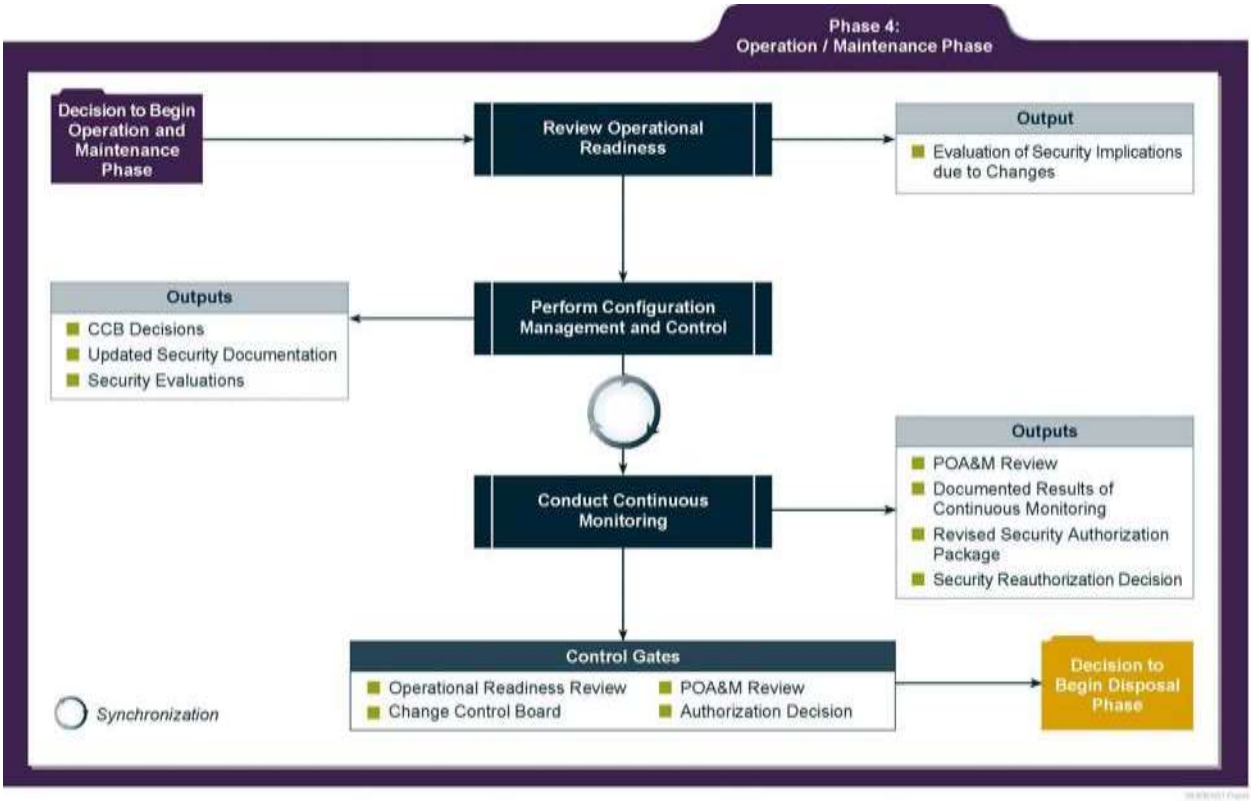

РИСУНОК 3-5. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ ЭКСПЛУАТАЦИИ/СОПРОВОЖДЕНИЯ

3.4.1 Описание

Эксплуатация и сопровождение - четвертая фаза SDLC. В этой фазе системы развёрнуты и эксплуатируются, улучшения и/или модификации для систем разработаны и протестированы, и аппаратные средства и/или программное обеспечение добавлены или заменены. Система контролируется для длительной работы в соответствии с требованиями безопасности и необходимые модификации системы внедрены. Эксплуатируемая система периодически оценивается, чтобы определить, как система может быть сделана более эффективной, безопасной и результативной. Эксплуатация продолжается до тех пор, пока система может быть эффективно изменена, чтобы ответить на потребности организации, будучи поддержанной на установленном уровне риска. Когда определена необходимость модификации или изменений, система может повторно прейти в предыдущую фазу SDLC.

Ключевые работы по безопасности для этой фазы включают:

- Проведение анализа эксплуатационной готовности;
- Управление конфигурацией системы;
- Установление процессов и процедур для надёжной эксплуатации и непрерывного мониторинга мер безопасности информационной системы; и
- Выполнение пересанкционирования при необходимости.

3.4.2 Управляющие условия

Общие типы управляющих условий для этой фазы включают:

- Обзор эксплуатационной готовности
- Обзор Совета по контролю за изменениями по предложенным изменениям
- Обзор POA&Ms
- Решения по аттестации (Каждые три года или после значимого изменения системы).

3.4.3 Основные работы по безопасности

3.4.3.1 Рассмотрение эксплуатационной готовности

Описание:	Когда система переходит в производственное окружение, часто происходят незапланированные модификации в системе. Если изменения являются существенными, может потребоваться проверка изменения мер безопасности, такая как конфигурирование, чтобы гарантировать целостность мер безопасности. Этот шаг не всегда необходим; однако это, как полагают, помогает смягчить риск и эффективно учесть сиюминутные неожиданности.
Ожидаемые результаты	Оценка последствий для безопасности вследствие любых системных изменений.
Синхронизация	• Системный администратор и ISSO подтверждают Владельцу системы, что система работает штатно и соответствует требованиям безопасности. • Если происходят текущие изменения, которые существенно изменяют уровень риска для системы, владелец системы должен рассмотреть переоценку - это редко.
Взаимозависимости	• Обзор эксплуатационной готовности дополняет процесс C&A, чтобы гарантировать, что пересмотрены изменения для значения риска. • Любое изменение мер безопасности должно быть учтено в документации по безопасности.
Советы по реализации	
• Когда улучшается или изменяется приложение, регрессионное тестирование помогает гарантировать, что не были внесены дополнительные уязвимости. Например, добавление исходного кода может часто вносить ошибки в других областях, и может негативно воздействовать на существующие и не изменяемые функции. • Нужно обратить внимание и проанализировать изменения, которые включают дополнительные поля данных, чтобы определить, ухудшилось ли состояние безопасности системы или возникла ли потребность в дополнительных мерах безопасности. • Гарантируйте, что пользователи соответственно обучены пониманию и практикам по безопасности для новой системы IT до развёртывания системы в производственной среде.	

3.4.3.2 Выполнение управления и контроля конфигурации

Описание:	Эффективное политика агентства по управлению и контролю конфигурации и связанные процедуры важны, чтобы гарантировать адекватное рассмотрение потенциальных воздействий на безопасность, обусловленных конкретными изменениями в информационной системе или её среде. Процедуры управления и контроля конфигурации являются критическими по отношению к установлению начального базового набора компонентов аппаратных средств, программного обеспечения и встроенного микропрограммного обеспечения для информационной системы и впоследствии для контроля и поддержания точного реестра любых изменений в системе. Изменения в аппаратных средствах, программном обеспечении или встроенном микропрограммном обеспечении системы могут оказать существенное влияние на безопасность. Документирование изменений в информационной системе и оценка потенциального воздействия на безопасность системы на непрерывной основе является существенным аспектом поддержания аттестации безопасности. Эти шаги, если реализованы эффективно, вносят важный вклад в возможность непрерывного мониторинга системы. Это также облегчает агентству возможность идентифицировать существенные изменения, которые изменяют состояние безопасности системы, и контролировать эффективность, для гарантии надлежащего проведения оценки и тестирования. Примечание: Протокол автоматизации контента безопасности (SCAP) является методом использования конкретные стандартов, чтобы обеспечить автоматизированное управление

	уязвимостями, измерение и оценку соответствия политике (например, соответствие FISMA). Процедуры управления конфигурацией агентства должны интегрировать эту деятельность, чтобы гарантировать воспроизводимость и согласованность. Это - итеративный процесс, который требует периодического анализа профильных изменений.
Ожидаемые результаты	• Решения Совета по контролю за изменениями (CCB) • Обновлённая документация по безопасности (План обеспечения безопасности системы, POA&M) • Оценки безопасности задокументированных изменений системы
Синхронизация	• Обновления системы должны быть включены в документацию по безопасности системы, по крайней мере, ежегодно или при существенных изменениях. • Документы УК системы должны обеспечить вход в План непрерывного мониторинга системы.
Взаимозависимости	• Архитектура безопасности должна содержать ключевые детали о сервисе безопасности на компонентном уровне, которые направляют проведение сравнительных проверок, чтобы оценить воздействие планируемого изменения. Например, если Вы обновляете программное обеспечение базы данных до новой версии, у которой есть меньшая возможность по аудиту, архитектура безопасности или документация мер безопасности должны обеспечить понимание, нуждается ли этот компонент в том уровне возможностей аудита. Результирующий анализ должен определить, необходимо ли дальнейшее рассмотрение перед реализацией.
Советы по реализации	
• Значение безопасности не всегда легко определить, глядя на результаты УК. Эксперт должен иметь в виду любые изменения, которые будут прямо или косвенно влиять на конфиденциальность, целостность и доступность. • Некоторые улучшения системы, которые добавляют новые данные, могут потребовать рассмотрения воздействия на категорирование безопасности системы и связанные меры безопасности. • Для непредвиденных ситуаций должны быть определены сокращённые процессы УК, которые учитывают чрезвычайные ситуации. Когда позволит время, эти ситуации должны всегда быть отслежены полностью.	

3.4.3.3 Проведение непрерывного мониторинга

Описание:	Конечная цель непрерывного мониторинга состоит в том, чтобы определить, продолжают ли меры безопасности в информационной системе быть эффективными в течение долгого времени в свете неизбежных изменений, которые происходят в системе, а также в среде, в которой работает система. Хорошо разработанный и хорошо управляемый непрерывный процесс мониторинга может эффективно преобразовать статическую оценку мер безопасности и процесс определения риска в динамический процесс, который обеспечивает соответствующим должностным лицам организации важную, близкую к реальному времени, информацию о состоянии безопасности. Эта информация может использоваться, чтобы предпринять соответствующие меры уменьшения риска и сделать правильные, основанные на риске решения о санкционировании в отношении продолжения эксплуатации информационной системы и явного принятия риска, который следует из этих решений. Постоянный мониторинг эффективности мер безопасности может быть выполнен различными путями, включая анализ безопасности, самооценку, управление конфигурацией, антивирусное управление, управление изменениями, тестирование и оценку безопасности или аудиты. Везде где только возможно должна использоваться автоматизация, чтобы уменьшить уровень усилий и гарантировать воспроизводимость. Переаттестация включается как часть непрерывного мониторинга, которая используется, когда есть существенные изменения в информационной системе, влияющие на безопасность системы или, когда в соответствии с федеральной политикой или политикой агентства истёк требуемый период времени.
Ожидаемые результаты	• Задокументированные результаты непрерывного мониторинга • Обзор POA&M • Обзор безопасности, анализ метрик, мер и тенденций • Обновлённая документация по безопасности и решения по переаттестации безопасности, по мере необходимости
Синхронизация	• Непрерывный мониторинг должен быть скорректирован при значительном изменении уровней риска и изменении, добавлении и устранении мер безопасности.

Взаимозависимости	• Непрерывный мониторинг предоставляет системным владельцам эффективный инструмент для проведения текущих обновлений планов обеспечения безопасности информационной системы, отчётов об оценке безопасности и планов действий и вех.

Советы по реализации

- Агентства должны стремиться реализовать рентабельную непрерывную программу мониторинга. Где возможно, программа непрерывного мониторинга должна использовать общие сервисы для более частого мониторинга, а также специфический для системы мониторинг для критических мер безопасности.
- Понимая, что это невозможно и не рентабельно контролировать все меры безопасности в каждой информационной системе на непрерывной основе, агентства должны рассмотреть установление календарного плана для мониторинга мер безопасности, чтобы гарантировать, что все меры безопасности, требующие более частого мониторинга, соответственно охвачены и что все меры безопасности, по крайней мере, однажды охвачены между каждым решением по аттестации.
- Процессы непрерывного мониторинга должны периодически оцениваться, чтобы анализировать изменения в угрозах и их влиянии на возможности мер безопасности по защите системы. Уточнения угроз могут иметь результат в обновлённых решениях по рискам и изменениях в существующих мерах безопасности.
- Относитесь с вниманием к уже выполняемым работам, которые имеют значение для непрерывного мониторинга. Обновления файла DAT AV, стандартная поддержка, пожарные учения по физической безопасности, анализ регистрационных записей, и т.д., должны все быть идентифицированы и охвачены в фазе непрерывного мониторинга.
- Соотнесите непрерывный мониторинг с важностью мер безопасности для смягчения риска, подтверждением соответствия POA&M элементов, которые должны быть охвачены, и отдельными точками контроля отказов.
- Рассмотрите цикл мониторинга, который совпадает со сроком действия оценки системы и фиксируйте процедуры и результаты тестирования для повторного использования при периодической аттестации.
- Работы непрерывного мониторинга могут обеспечить полезные данные для поддержки планов работ по безопасности и мер по возврату инвестиций в безопасность (ROI).
- Определение специфичных для агентства критериев для инициирования переаттестации помогает гарантировать информирование принимающих решения лиц и взаимопонимание всех заинтересованных сторон. Критерии должны иметь некоторые допуска с тем, чтобы учесть уникальные ситуации.

3.5 Фаза SDLC: ликвидация

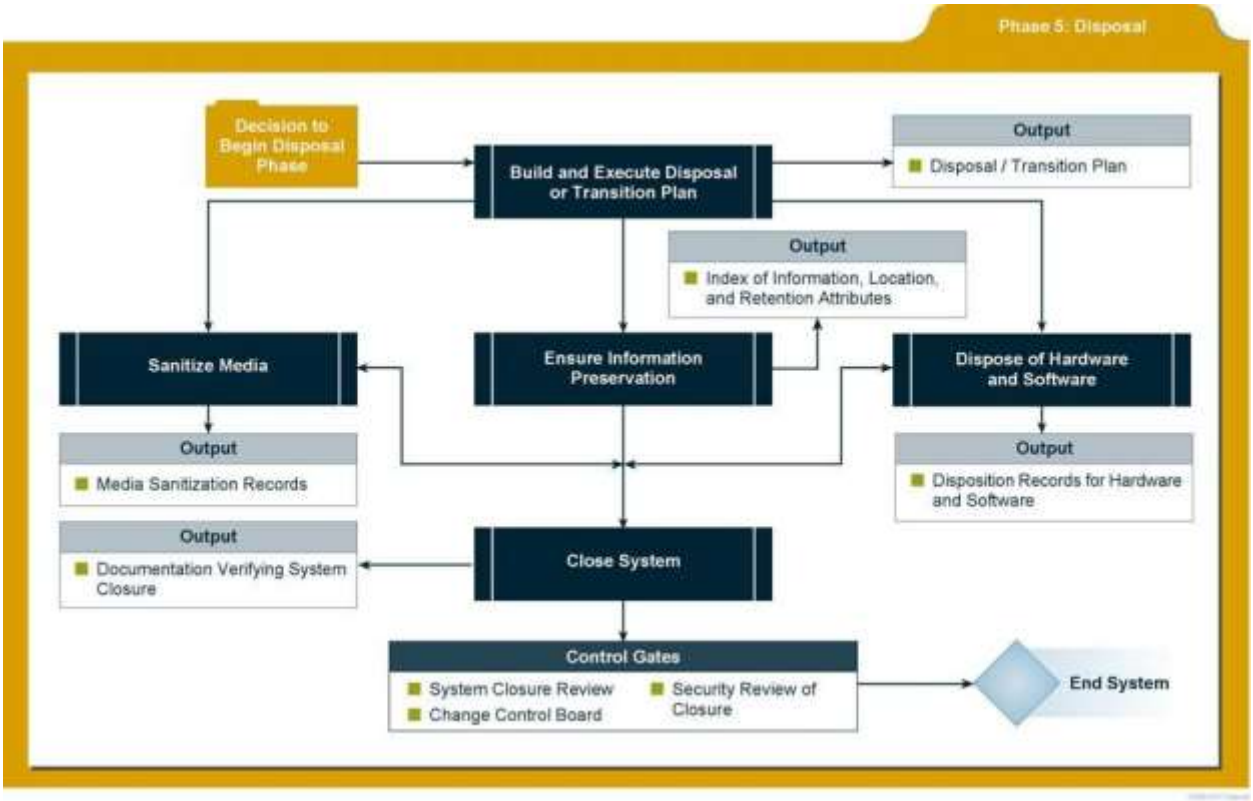

РИСУНОК 3-6. СВЯЗЬ РАССМОТРЕНИЙ БЕЗОПАСНОСТИ В ФАЗЕ ЛИКВИДАЦИИ

3.5.1 Описание

Ликвидация, заключительная фаза в SDLC, предусматривающая ликвидацию системы и закрытие любых контрактов объекта. Проблемы информационной безопасности, связанные с ликвидацией информации и системы, должны быть полностью решены. Когда информационные системы передаются, становятся устаревшими или больше не применимы, важно гарантировать, что правительственные ресурсы и активы защищены.

Обычно, это не окончательный конец системы. Системы обычно развиваются или переходят к следующему поколению из-за изменяющихся требований или улучшений технологии. Планы обеспечения безопасности системы должны непрерывно развиваться с системой. Кроме того, большая часть информации об окружении, управлении и эксплуатации должна быть подходящей и полезной в разработке плана обеспечения безопасности для последующей системы.

Работы по ликвидации гарантируют аккуратное завершение использования системы и сохраняют важную информацию о системе так, чтобы некоторая или вся информация могла бы быть, в случае необходимости, восстановлена в будущем. Особый акцент делается на надлежащее сохранение данных, обрабатываемых системой с тем, чтобы данные были эффективно перемещены в другую систему или заархивированы в соответствии с применимыми нормативными актами и политиками по управлению записями для потенциального будущего доступа.

Ключевые работы по безопасности для этой фазы включают:

- Создание и выполнение плана Ликвидации/Передачи;

- Архивирование критичной информации;
- Очистка носителей информации; и
- Избавление от аппаратного и программного обеспечения.

3.5.2 Управляющие условия

Общие типы управляющих условий для этой фазы включают:

- Анализ закрытия системы
- Совет по контролю изменений
- Анализ безопасности закрытия.

3.5.3 Основные работы по безопасности

3.5.3.1 Создание и выполнение плана Ликвидации/Передачи

Описание:	Создание плана Ликвидации/Передачи гарантирует, что все заинтересованные стороны знают о планируемом будущем системы и её информации. Этот план должен учесть статус Ликвидации/ Передачи для всех критических компонентов, сервисов и информации. Прежде всего, как план работ, этот план определяет шаги, решения и вехи необходимые, чтобы должным образом закрыть, передать или переместить систему или её информацию. Во многих случаях, ликвидируемые системы или компоненты систем остаются бездействующими, но вместе с тем соединёнными с инфраструктурой. В результате эти компоненты часто забываются, снимаются с учёта или сопровождаются в неоптимальных уровнях обеспечения безопасности, представляя, таким образом, дополнительный и ненужный риск для инфраструктуры и всех взаимодействующих систем. План перехода помогает в смягчении этих возможных исходов.
Ожидаемые результаты	Задокументированный план Ликвидации/Передачи по закрытию или передаче системы и/или её информации.
Синхронизация	Документация безопасности должна отразить ожидаемые планы, если решения по безопасности и финансирование перераспределяются или иначе изменяются из-за решения по ликвидации.
Взаимозависимости	Документация по безопасности, такая как план обеспечения безопасности и требования к мерам безопасности, возможно, потребует обновления.
Советы по реализации	
• Консультируйтесь с должностными лицами агентства по управлению Записями, Приватности и Законом о свободе информации (FOIA) до ликвидации, чтобы гарантировать согласие с этими законами и применимой политикой агентства. • Не дожидайтесь фазы ликвидации, чтобы сделать план Ликвидации/Передачи. Планируйте Ликвидацию/Передачу на всех фазах жизненного цикла. Это лучше всего сделать как часть фазы требований, таким образом, полные требования по ресурсам для Ликвидации/Передачи будут поняты и спланированы. Это может быть сделано всюду по жизненному циклу, как только аппаратное и программное обеспечение становятся устаревшими или повреждёнными; в других фазах это потребует задач, указанных в этой фазе.	

3.5.3.2 Гарантирование сохранения информации

Описание:	Сохраняя информацию, организации должны рассмотреть методы, которые требуются для того, чтобы получить информацию в будущем. Технология, используемая чтобы получить записи, может не быть легко доступной в будущем (особенно если используется шифрование). Избавляясь от систем необходимо рассмотреть законодательные требования по сохранению записей.
Ожидаемые результаты	Каталог сохранённой информации, и атрибуты её расположения и сохранения.
Синхронизация	Необходимо рассмотреть требования Управления записями, Закона о неприкосновенности частной жизни и FOIA.
Взаимозависимости	Рассмотрения или работы в части приватности, могут быть важны с точки зрения FOIA.
Советы по реализации	
• В планировании этой работы поможет тесная координация с организацией Управление Закона о свободе информации (FOIA). • Организации могут также получить практические советы от Офиса надзора за безопасностью информационных систем Национального управления архивов и документации.	

3.5.3.3 Очистка носителей информации

Описание:	Основываясь на результатах категорирования безопасности, владелец системы должен обратиться к Специальной публикации (SP) NIST 800-53, *Рекомендуемые меры безопасности для Федеральных информационных систем*, которая определяет, что "организация очищает цифровые данные информационной системы, используя одобренное оборудование, технологии и процедуры. Организации отслеживают, документируют и проверяют очистку носителей информации и действия по разрушению и периодически тестируют оборудование/процедуры очистки, чтобы гарантировать корректную работу. Организация очищает или уничтожает цифровые данные информационной системы перед её ликвидацией или реализацией для повторного использования вне организации, чтобы препятствовать тому, что неправомочные люди получат доступ к и используют информацию, содержащуюся на носителях информации." NIST SP 800-88, *Руководство по очистке носителей информации*, делит очистку носителей информации на четыре категории: удаление, стирание, уничтожение и разрушение. Это предлагает далее, чтобы владелец системы категорирует информацию, оценит тип носителя, на котором сделана запись, оценит риск к конфиденциальности и определит будущие планы по носителю информации. Затем, выберет соответствующий процесс очистки. Выбранный процесс должен быть оценён относительно стоимости, воздействия на окружающую среду, и т.д., и принято решение, которое лучше всего смягчит риск к конфиденциальности и лучше всего удовлетворит другие ограничения, наложенные на процесс. Принимая решения по очистке нужно рассмотреть несколько факторов, наряду с категорированием безопасности конфиденциальности системы. Соотношение стоимости и выгоды от процесса очистки носителя информации должно быть понято до окончательного решения. Например, это может быть не рентабельно, размагничивать недорогие носители информации, такие как дискеты.
Ожидаемые результаты	Записи по очистке носителей информации
Синхронизация	Нет
Взаимозависимости	Категорирование безопасности обеспечивает идентификацию и соответствующий уровень риска информации системы.
Советы по реализации	
• Даже при том, что стирание или уничтожение могут быть рекомендуемыми решениями, может быть более рентабельным (рассматривая обучение, прослеживание, подтверждение и т.д.) разрушить носитель информации, а не использовать одну из других альтернатив. • Организации могут всегда увеличить степень применяемой очистки, если это разумно и определено оценкой существующего риска так, чтобы были применены надлежащие технологии очистки.	

3.5.3.4 Ликвидация аппаратного и программного обеспечения

Описание:	Аппаратное и программное обеспечение может быть продано, отдано или списано в соответствии с действующим законом или нормативным актом. При избавлении от программного обеспечения необходимо соблюсти лицензию или другие соглашения с разработчиком и с правительственными постановлениями. Редко когда требуется уничтожить аппаратные средства, за исключением некоторых носителей, которые содержат чувствительную информацию и не могут быть очищены без разрушения. В ситуациях, когда носители не могут быть соответственно очищены, может быть возможно удаление и физическое разрушение носителей информации так, чтобы остающиеся аппаратные средства могли быть проданы или отданы. Некоторые системы могут содержать чувствительную информацию после того, как носители удалены. Если есть сомнение в том, остаётся ли чувствительная информация в системе, перед избавлением от системы нужно консультироваться с ISSO. Кроме того, поставщик может быть проконсультирован по дополнительным параметрам ликвидации или подтверждения риска.
Ожидаемые результаты	• Записи по ликвидации аппаратного и программного обеспечения. Эти записи могут включать списки аппаратных средств и реализованного программного обеспечения (проданного, списанного или пожертвованного), и списки аппаратного и программного обеспечения, переданного в другие проекты или задачи в пределах организации.
Синхронизация	Уточнение материальных запасов систем и компонентов.
Взаимозависимости	Должен быть соответственно обновлён реестр аппаратного и программного обеспечения системы.
Советы по реализации	
• Ликвидируя систему не забудьте про требования материальной ответственности. Когда возможно, рассмотрите пожертвование используемого ИТ и/или повторное использование опасных частей. • Раздел 40 USC информирует владельцев и кураторов систем, что избыточное оборудование - " Полезно для образования " и "Федеральное оборудование, является существенным национальным ресурсом." Везде, где возможно, избыточное оборудование и носители информации должны быть сделаны доступными для подготовки в школах и некоммерческих организациях до степени, разрешённой законом. • Для снижения издержек некоторые агентства разумно поддерживают старые части для деятельности по непредвиденным обстоятельствам. Например, используют ликвидированные ноутбуки для сценария взаимодействия, который требует только частичной обработки для важного взаимодействия по Интернету или электронной почте.	

3.5.3.5 Закрытие системы

Описание:	Информационная система формально прекратила работу и демонтирована на этом объекте.
Ожидаемые результаты	• Документация, подтверждающая закрытие системы, включает заключительное уведомление о закрытии для санкционирующих и аттестующих должностных лиц, управления конфигурацией, владельцев системы, ISSO и руководителей программ.
Синхронизация	Нет
Взаимозависимости	• Архивация документации безопасности если применимо. • Если предоставлены услуги непрерывного мониторинга, необходимо уведомление о закрытии их поставщикам (может включать УК, AV, IR, и ССВ). • Обновление реестров отчётов по FISMA и архитектуре предприятия.
Советы по реализации	
• Меморандум, ясно формулирующий формальное закрытие системы и предпринятые надлежащие меры, который включается в доставку всем ключевым заинтересованным сторонам, обеспечивает самый простой подход для формального закрытия.	

ГЛАВА ЧЕТЫРЕ

ДОПОЛНИТЕЛЬНЫЕ РАССМОТРЕНИЯ БЕЗОПАСНОСТИ

"Создание безопасности в" является технологией управления безопасностью, которая реализует конкретные рассмотрения безопасности во время фаз SDLC. Однако, проекты и инициативы в сфере ИТ не всегда так ясно определены как разработки систем или приложений. Некоторые инициативы являются сервис-ориентированными и кросс-платформенными ИТ (и, в некоторых случаях, организационными) или ориентированы на возможности, подобно созданию информационного центра или резервного объекта информатизации. Эти проекты должны в максимально возможной степени следовать обзорам, подготовленным советами, и учитывать и применять необходимые рассмотрения безопасности. Этот раздел выделяет типичные примеры и представляет некоторые ориентированные на безопасность рассмотрения. Базовые элементы интегрирования безопасности в SDLC остаются теми же самыми для этих областей. Взаимодействие и документация заинтересованных сторон в отношении решений по обеспечения безопасности будут ключевым фактором успеха.

4.1 Система поставок и доверие к программному обеспечению

Гарантирование системы поставок[4] и доверие к программному обеспечению требуют частно-государственных усилий по распространению лучших методов и методологий, которые способствуют целостности, безопасности и надёжности в разработке аппаратуры и программного кода, включая процессы и процедуры, которые снижают возможность ошибочного кода, вредоносного кода или лазеек, которые могли быть внедрены во время разработки. Эта область находится в становлении и будущие руководства, вероятно, обеспечат более конкретные особенности. Вообще, эти процессы и процедуры должны быть объектом трёх следующих целей:

Доверенность - Отсутствуют годные для использования уязвимости, злонамеренно или неумышленно внедрённые, и материалы содержат всё, что требуется, чтобы быть без подделки, пиратства или нарушения интеллектуальных прав.

Предсказуемое выполнение - Обоснованная уверенность, что аппаратное и программное обеспечение, при применении, функционируют как предназначено.

Соответствие - Спланированный и систематизированный набор мультидисциплинарных работ, которые гарантируют, что аппаратные и программные процессы и продукты соответствует требованиям, стандартам и процедурам.

По отношению к этим целям менеджеры по приобретению и менеджеры по информационной безопасности должны распределить угрозы, представляемые системой поставок, как часть их усилий по уменьшению риска, включая:

- Информацию относительно возможностей процессов поставщиков (практики деловых отношений), которая должна использоваться, чтобы определить риски безопасности, предоставляемые продуктами и услугами поставщиков в отношении проекта приобретения и деятельности, допускаемой системой.
- Информацию об оценённых продуктах, которая должна быть доступной и проанализированной, с учётом изменения условий, для того, чтобы обнаружить годные для использования уязвимости, и чтобы продукты были безопасно сконфигурированы при использовании.

[4] Система поставок имеет отношение к каналу распределения продукта от его возникновения до его поставки до конечного потребителя.

4.2 Сервис-ориентированная архитектура

Сервис-ориентированная архитектура (SOA) является стилем архитектуры информационных систем, в которых существующая или новая функциональность объединяется по сервисам. Эти сервисы взаимодействуют друг с другом, передавая данные от одного к другому, или координируя действия между одним или более сервисами. NIST SP 800-95, *Руководство по защищённым веб-сервисам*, даёт больше информации относительно рассмотрений безопасности SOA.

Основные проблемы управления безопасностью при SOA включают рассмотрение границ безопасности, назначение соответствующего уровня риска и управление ожиданиями и обязанностями по безопасности через множественные заинтересованные стороны и соглашения. Проектирование стратегии аттестации может также составить проблему с точки зрения календарного плана и ресурсов. Несмотря на то, что традиционный процесс SDLC не будет, вероятно, соответствующим, рассмотрения безопасности, по большей части, остаются применимыми. Агентства должны планировать свой подход так, чтобы аттестация, так же как и непрерывный мониторинг и переаттестация, были экономически выгодны и управляемы.

Так как многие традиционные аналитические инструменты (сканеры, системы обнаружения вторжений [IDSs], инструменты обработки/анализа пакетов и т.д.) не в состоянии эффективно оценить совокупное состояние безопасности сервис-ориентированной архитектуры, это заставляет аналитика безопасности использовать аналитические инструменты, применять уникальные прецеденты SOA и экстраполировать синтетическую модель среды безопасности для анализа уязвимостей и рисков.

В дополнение к автоматизированному тестированию, которое может быть доступным, могут быть предложены следующие обзоры, которые сосредотачиваются на специфических аспектах SOA:

- Контрольный журнал по Оценке & Сопоставлению;
- Интерактивное описание сервис-ориентированной архитектуры (Portlets, Security Assertions Markup Language (SAML), Simple Object Access Protocol (SOAP), Universal Description, Discovery, and Integration (UDDI), Web Services Description Language (WSDL), Extensible Access Control Markup Language (XACML), так же как многие из WS-* стандартов, появляющихся на арене веб-сервисов включая WS-безопасность, WS-политику, и WS - функциональную совместимость; выделение средств защиты и преимуществ в каждом);
- Контроль доступа (такие как дискреционный и ролевой);
- Формирование и использование базовых сервисов предприятия; и
- Создание, защита и ликвидация робастных метаданных.

4.3 Специфика аттестации модулей безопасности для повторного использования

Поскольку приложения и информационные системы становятся более объектно-ориентированными и компонентно-ориентированными, появляется необходимость рассматривать значение для безопасности, а также стоимости многократного использования программных модулей для многих проектов и, возможно, для многих организаций. Рекомендуется, чтобы компоненты и программные модули были созданы с учётом повторного использования, особенно для кода, на котором нужно основываться, чтобы обеспечить функциональность безопасности для широкого диапазона проектов. Оценка & аттестация этих модулей очень похожие на поблочное тестирование для оценки функциональности, предоставляют разработчикам, архитекторам и инженерам готовый инструментарий доверенного кода, который может быть реализован при необходимости, по уменьшенной стоимости, чтобы гарантировать согласие безопасности и управление рисками во время разработки информационной системы по уменьшенной стоимости.

Аттестованные модули должны быть хорошо задокументированы относительно их особенностей и функций; документация по аттестации должна храниться вместе с модулем; и документация для разработчиков, отражающая варианты использования и методы реализации, которые не аннулируют аттестацию, также должна быть доступной. Модуль и документация должны быть подписаны разработчиком (или группой разработчиков) в цифровой форме, чтобы сохранить целостность и аутентичность аттестации. Достаточно сложные модули (вероятно, должны рассматриваться как самостоятельные приложения) могут подтверждаться по тому же самому процессу, как описано в NIST SP 800-37.

4.4 Меж-организационные решения

Меж-организационные решения направлены на обеспечение доступа к информационным приложениям в соответствии с меморандумом о соглашении или соглашением об уровне обслуживания, которые представляют ценность и выгоду для обоих (или многих) организаций. Приложения, делаемые доступными между организациями, могут быть категорированы на две группы, основываясь на предполагаемых потребителях. В первом случае, предполагаемая группа потребителей - "Предприятие", рассматривается как организация вообще и включает взаимозависимые ресурсы (то есть, людей, организации и технологии), которые должны координировать функции и делиться информацией в поддержку общего предназначения (или ряда связанных предназначений). Во втором случае предполагаемая группа потребителей – Сообщество по интересам (COI). COI это группа людей, которые обмениваются информацией, используя общий словарь, в поддержку совместно используемых предназначений, бизнес-процессов и целей. Сообщество состоит из пользователей/операторов, которые участвуют в информационном обмене, разработчиках сервисов, приложений, возможностей и систем для этих пользователей, и функциональных сторонников, которые определяют требования и получают ресурсы для приобретения от имени пользователей.

При разработке кросс-организационных решений должна быть проявлена забота, чтобы подготовить проекты руководящих документов (меморандум о соглашении или соглашение об уровне обслуживания), которые чётко описывают средства защиты, требования и ожидаемые уровни исполнения, чтобы гарантировать, что все стороны соответственно защищены. Далее, необходимо согласовать обязанности по испытаниям и подтверждению соответствия, процедуры реагирования на инциденты, и политики мониторинга и эксплуатации, которые обеспечат достаточное продвижение по управлению риском. Особое внимание должно быть направлено на аутентификацию и авторизацию пользователей и кода/приложений, которые включают планирование роста пользовательской базы, взаимозависимости систем аутентификации и авторизации между организациями, общие среды доступа и процедуры регистрации/исключения.

4.5 Продвижение технологий и основные миграции

В виду быстрого темпа инноваций и соответственно выборочного устаревания на арене информационных технологий, внимание должно быть уделено не только интегрированию безопасности в SDLC для новых систем и интеграции систем, но также и к перестройке, обновлению или миграции систем, чтобы учесть продвижение технологий. Продвижение технологий создаёт новые проблемы в безопасности предприятия, а также в рисках нового внедрения известных уязвимостей через дефектные методы реализации/интеграции. Совместное использование технологии создаёт совместную подверженность воздействиям, объединяющую существующие проблемы.

Борясь с последствиями безопасности технологического продвижения или планируя миграцию главной системы, организации, вероятно, выработают следующие виды поведения относительно безопасности информационной системы:

- Поскольку технология внедряется, прежде всего, чтобы обеспечить предназначение организации (или изменение в предназначении) или решить острую проблему деятельности, организация будет часто стремиться ослабить или исключить требования базового уровня безопасности, чтобы ускорить процесс продвижения.
- Во время возможной C&A наследуемой информационной системы, будет оценено соответствие существующих мер безопасности информационной системы. Безопасность, как правило, определяется через меры безопасности на наследуемой инфраструктуре, которые были оценены и аттестованы, обоснованием будет то, что они обеспечивают адекватное смягчение.
- В конечном счёте, развитие, освоение расширения или понимание уязвимостей, рисков и стратегий смягчения для технологий информационных систем или их среды совершенствуются до такой степени, что руководство становится, по крайней мере, столь же довольно планом управления рисками новой технологии, как и унаследованной системы, и, возможно, более уверенно предоставляет демонстрируемые передовые возможности системы.

Однако, продвижение технологий, вместе с ожидаемым поведением организации, предоставляет организации возможности, чтобы извлечь выгоду из потребности в передовой технологии, планируя безопасную миграцию от наследуемых технологий безопасным способом.

Далее, этот образец поведения не ограничен технологией, которая действительно продвинута или нова. Это не является редким для технологий, разработанных десять или более лет назад, чтобы попасть в центр внимания. Такая технология, однако, возможно, испытывала недостаток в исследованиях в течение долгого времени, чтобы гарантировать, что были выполнены выявление уязвимостей и активное исправление уязвимостей, обнаруженных в подобных/эквивалентных технологиях.

4.6 Разработки оборудования информационных центров или ИТ

Для безопасности, связанной с разработкой оборудования информационных центров или ИТ, особое внимание акцентируется на решениях для физической безопасности, и это справедливо. Тем не менее, важно помнить, что информационные центры - это хранилища для большого количества вычислительной мощности и хранения, на которых строятся приложения, и особое внимание требуется чтобы гарантировать, что все клиенты, использующие средства информационного центра, соответственно защищены.

Типичная крупная организация может иметь много информационных центров, каждый направленный на поддержании конкретного набора клиентов и предназначений, но находящихся во взаимосвязи, чтобы предоставить высокую доступность и обеспечить непрерывность деятельности и требований по аварийному восстановлению (часто требующие возможности хранить сторонние данные или предусмотреть альтернативные объекты информатизации для обработки данных) рентабельным способом. Информационные центры должны иметь общую нагрузку и обеспечивать матрицу избыточности. При этих условиях, крайне важно, чтобы разделение данных поддерживалось как для данных на места, так и при передаче, и что, в частности, разделение режимов работы и проверяемость административных функций для персонала информационного центра были строго определены. Во многих случаях, это будет оправдывать потребность в отдельных локальных сетях (LAN) или виртуальных LAN (VLANs) для административного трафика и приложений.

Эта интеграция безопасности, как технической, так и эксплуатационной, становится даже более важной с повышением виртуализации в информационном центре и возможности перемещать все виртуальные среды операционной системы между независимыми и различными аппаратными платформами в информационном центре.

Одно специфическое рассмотрение для информационного центра - это безопасность контекстных данных среды. Эти данные будут следовать из мониторинга систем физической безопасности (камеры, датчики движения, и т.д.), а также как систем среды, необходимых, чтобы сохранить вычислительные аппаратные средства в умеренных производственных условиях. Эти данные все в большей степени хранятся на цифровых носителях, которые доступны для сети и с которыми надо обращаться с заботой, поскольку они чувствительны по своей сущности и могут предоставить доступ атакующему к базовым информационным системам. Эти системы должны быть соответственно защищены, и результирующие данные должны храниться во вне или раздельно (то есть, не в тех же самых сетях/информационных системах как пользовательские информационные системы, находящиеся в информационном центре).

4.7 Виртуализация

Виртуализация, использование виртуальных машин и приложений, является растущей тенденцией, которая обеспечивает возможность для снижения издержек. Несмотря на то, что это может обеспечить дополнительную безопасность с точки зрения изоляции и восстановления, это требует дополнительного планирования обеспечения безопасности для уникальных рисков безопасности, наследуемых в реализациях виртуализации, таких как перехват данных через совместно используемый буфер обмена, регистрация нажатия клавиш в пределах виртуальной машины и отказ в обслуживании для ресурсов узла.

Меры безопасности, связанные с традиционными физическими платформами, обычно игнорируемыми при реализации виртуализации, включают:

- Антивредоносное программное обеспечение в пределах виртуальной машины и узла;
- Сегрегация административных режимов работы для узлов и версий;
- Аудит журналов, а также экспорт и хранение журналов регистрации вне виртуальной среды;
- Конфигурация и управление обновлениями виртуальных машин и узлов;
- Шифрование сетевого трафика между виртуальной машиной и узлом; и
- Мониторинг систем обнаружения вторжений (IDS) и систем предотвращения вторжений (IPS).

Вследствие распределённости и сложности сети, привлечение виртуализации может в дальнейшем усилить проблемы общей безопасности, такие как вредоносное программное обеспечение, утечки данных, управление обновлениями и слабость контроля доступа.

Для лучших результатов агентства должны планировать безопасность в свои критерии отбора и, как минимум, до реализации виртуального решения создать и задокументировать план безопасности развёртывания и поддержки.

ПРИЛОЖЕНИЕ А - ГЛОССАРИЙ

ТЕРМИН	ОПРЕДЕЛЕНИЕ
Acceptance Принятие	Акт уполномоченного представителя правительства, которым правительство, само или как представитель другого, берет на себя управление или владение существующими идентифицированными предложенными поставками или одобряет конкретные услуги, оказанные как частичное или полное исполнение контракта. Это - заключительное определение, выполняют ли средство или система конкретные технические и производственные стандарты.
Acquisition Приобретение	Включает все стадии процесса получения свойства или сервисов, начинание с процесса определения потребности в свойстве или сервисах и заканчивая окончанием контракта и закрытие.
Business Impact Analysis (BIA) Анализ влияния на деятельность	Анализ требований, процессов и взаимозависимостей систем информационных технологий (ИТ), используемый, чтобы характеризовать требования и приоритеты для непредвиденных обстоятельств систем в случае существенного разрушения. *ИСТОЧНИК: SP 800-34*
Оценка и Аттестация - (C&A)	Всесторонняя оценка управленческих, эксплуатационных и технических мер безопасности в информационной системе, производимая в поддержку аттестации безопасности, чтобы определить степень, до которой меры безопасности реализованы правильно, работают как предназначено и производят желаемый результат относительно соответствия требованиям безопасности для системы. *Аттестация* - официальное управленческое решение, принимаемое высшим должностным лицом агентства, чтобы санкционировать деятельность информационной системы и явно принять риск для деятельности агентства (включая предназначение, функции, имидж или репутацию), активов агентства или людей, основанное на реализации согласованного набор мер безопасности. *ИСТОЧНИК: SP 800-37*
Закон Клингер-Коэна от 1996 г.	Также известный как Парламентская реформа управления информационными технологиями. Законодательный акт, который существенно пересмотрел способ, которым ресурсы ИТ управляются и обеспечиваются, включая требование, чтобы каждая разработка и реализация агентства являлись способом максимизировать полезность и оценить и управлять рисками инвестиций в IT.
Closeout Закрытие	Включает все заключительные действия по контракту (например, обеспечение выполнения всех требований, произведение окончательного расчета).
Commercial off-the-shelf (COTS) Коммерческий готовый к использованию, «коробочный»	Программное и аппаратное обеспечение, которое уже существует и доступно из коммерческих источников. Это также упоминается как готовый к использованию, «коробочный».
Contract administration	Правительственное управление контрактами, осуществляемое чтобы гарантировать, что правительство получит соответствующее

Контроль за исполнением контрактов	качество продуктов и услуг, определенных в контракте, в пределах установленной стоимости и календарных планов.
Contracting Officer (CO) Контрактный специалист	Человек с полномочиями по заключению, администрированию и/или завершению контрактов и принятию соответствующих решений и заключений.
Contracting Officer's Technical Representative Технический уполномоченный Контрактного специалиста	Человек, которому CO делегирует некоторые обязанности контроля за исполнением контракта, обычно связанные с техническим направлением и проблемами приёмки.
Control Gate Ожидаемые результаты	Момент времени, когда усилие по разработке системы должно быть оценено и когда руководство будет определять, должен ли проект продолжаться как есть, изменить направление или быть прекращён.
Deliverable Поставка	Продукт или услуга, которые подготовлены для и поставлены правительству в соответствии с контрактом.
Среда	Совокупность внешних процедур, условий и объектов, влияющих на разработку, эксплуатацию и поддержку информационной системы. *ИСТОЧНИК: FIPS 200; CNSSI-4009*
Federal Acquisition Regulation (FAR) Федеральный нормативный акт по закупкам	Нормативный акт, который кодифицирует универсальные политики и процедуры закупок для исполнительных агентств.
Federal Information Processing Standards Стандарты обработки федеральной информации	Стандарт для принятия и использования федеральными агентствами, который разработан в Лаборатории информационных технологий и опубликован Национальным институтом стандартов и технологий, частью американского Министерства торговли. FIPS затрагивает определённую тему по информационным технологиям, в целях достижения общего уровня качества или некоторого уровня функциональной совместимости.
Federal Information Processing Standards Publications Публикации стандартов обработки федеральной информации	Публикации FIPS, выпущенные NIST после санкционирования Министром торговли. Некоторые публикации FIPS обязательны для использования при федеральных закупках.
Federal Information Security Management Act (FISMA) Закон об управлении безопасностью федеральной информации	Требует, чтобы агентства интегрировали безопасность IT-систем в свое планирование капиталовложений и процессы архитектуры предприятия в агентстве, проводили ежегодный анализ IT-безопасности всех программ и систем, и отчитывались по результатам этого анализа Министерству управления и бюджета (OMB). *ИСТОЧНИК: SP 800-65*
Information Resources Информационные ресурсы	Информация и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии. *ИСТОЧНИК: 44 U.S.C., Раздел 3502*
Information Security Информационная безопасность	Защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, разрушения, модификации или разрушение для обеспечения

	конфиденциальности, целостности и доступности. *ИСТОЧНИК: 44 U.S.C., Раздел 3542*
Information System Информационная система	Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, распределения, распространения или избавление от информации. *ИСТОЧНИК: 44 U.S.C., Раздел 3502; Циркуляр OMB A-130, Приложение. III*
Information System Owner	Официальное должностное лицо ответственное в целом за приобретение, разработку, интеграцию, модификацию или эксплуатацию и поддержку информационной системы. *ИСТОЧНИК: FIPS 200; Уточненный CNSSI-4009*
Information System Security Officer (ISSO) Сотрудник безопасности информационной системы (ISSO)	Человек, на которого высшим должностным лицом агентства по информационной безопасности, санкционирующим должностным лицом, должностным лицом руководства или владельцем информационной системы возложена ответственность чтобы гарантировать, что для информационной системы или программы поддерживается соответствующее эксплуатационное состояние безопасности. *ИСТОЧНИК: SP 800-53; Уточненный CNSSI-4009*
Information Technology (IT) Информационная технология	Любое оборудование или взаимодействующая система, которые используются в автоматизированном получении, хранении, манипулировании, управлении, перемещении, управлении, представлении, коммутации, обмене, передаче или приеме данных или информации. Оно обычно включает компьютеры, вспомогательное оборудование, программное обеспечение, встроенное микропрограммное обеспечение, соответствующие процедуры, сервисы и связанные ресурсы.
Plan of Action and Milestones (POA&M) План действий и вех (POA&M)	Документ, который определяет задачи, требующие выполнения. Он детализирует ресурсы, требуемые чтобы выполнить элементы плана, любые вехи, относящиеся к задачам и намеченные даты завершения для вех. Назначение POA&M состоит в том, чтобы помочь агентствам в определении, оценке, приоритезации и мониторинге прогресса корректирующих усилий для слабых мест безопасности, найденных в программах и системах. *ИСТОЧНИК: Меморандум 02-01 OMB.*
Privacy Impact Assessment (PIA) Оценка воздействия на приватность	Анализ того, как информация обрабатывается, чтобы: 1) гарантировать обработку в соответствии с применимым, законодательством, нормативными документами и требованиями политики в отношение приватности; 2) определить риски и результаты сбора, поддержания и распространения информации в соответствующей форме в электронной информационной системе; и 3) исследовать и оценить защиту и альтернативные процедуры для обработки информации, чтобы смягчить потенциальные риски в отношение приватности. *ИСТОЧНИК: Меморандум 03-22 OMB*.
Residual Risk Остаточный риск	Остающийся потенциальный риск после применения всех мер по IT безопасности. Есть остаточный риск, связанный с каждой угрозой. *ИСТОЧНИК: SP 800-33.*

ПРИЛОЖЕНИЕ B - АКРОНИМЫ

AO	Санкционирующее должностное лицо
AV	Антивирус
BIA	Оценка влияния на деятельность
C&A	Оценка и аттестация
CCB	Совет по контролю за изменениями
CIO	Директор по информации
CISO	Директор по информационной безопасности
CM	Управление конфигурацией
COI	Сообщество по интересам
CONOPS	Концепция эксплуатации
COOP	Непрерывность деятельности
COTR	Технический уполномоченный Представителя заказчика
COTS	Коммерческий готовый к использованию, «коробочный»
CP	План действий при непредвиденных обстоятельствах
CPIC	Планирование капиталовложений и управление инвестициями
DR	Аварийное восстановление
EA	Архитектура предприятия
FAR	Федеральный регистр закупок
FIPS	Стандарт обработки федеральной информации
FISMA	Закон об управлении безопасностью федеральной информации
FOIA	Закон о свободе информации
GAO	Управление государственной подотчётности
IDS	Система обнаружения вторжений
IPS	Система предотвращения вторжений
IR	Реакция на инциденты
ISSO	Сотрудник безопасности информационной системы
IT	Информационная технология
ITL	Лаборатория информационных технологий
JAD	Совместная разработка приложений
LAN	Локальная сеть
NIST	Национальный институт стандартов и технологий
OMB	Министерство управления и бюджета
PIA	Оценка воздействия на приватность
PII	Персональная идентификационная информация
POA&M	План действий и вех
QA	Оценка качества
RAD	Быстрая разработка приложений
RFP	Запрос предложения
SAISO	Высший сотрудник агентства по информационной безопасности
SAML	Язык разметки утверждений безопасности
SATE	Освоение, обучение и образование по безопасности
SCAP	Протокол автоматизации контента безопасности
SDLC	Жизненный цикл разработки систем
SLA	Соглашение об уровне обслуживания
SOA	Сервис-ориентированная архитектура
SOAP	Простой объектный протокол доступа
SOW	Техническое задание
SP	Специальная публикация

SSP	План обеспечения безопасности системы
ST&E	Тестирование и оценка безопасности
UDDI	Универсальное описание, получение и интеграция
USC	Свод законов Соединённых Штатов
VLAN	Виртуальная локальная сеть
WSDL	Язык описания веб-сервисов
XACML	Язык разметки расширенного контроля доступа

ПРИЛОЖЕНИЕ С - ССЫЛКИ

Закон Клингера-Коэна, 40 Свод законов Соединенных Штатов (U.S.C). 1401 и следующие, 1996.

Закон о компьютерной безопасности 1987, Публичный закон (P.L). 100-235.

Закон о передаче и продвижении национальных технологий 1995 (P.L. 104-113).

Закон о неприкосновенности частной жизни 1974, 5 U.S.C. 552a.

Закон об электронном правительстве, P.L. 107-347, декабрь 2002.

Закон об управлении безопасностью федеральной информации (FISMA) 2002, 44 U.S.C. Глава 35, Подглава III, 2002.

Циркуляр OMB A-130, *Управление Федеральными информационными ресурсами*, ноябрь 2000.

Публикация GSA, *Руководство по Планированию, получению и управлению системами информационных технологи*й, Версия 1, декабрь 1998.

Стандарт обработки федеральной информации (FIPS) 140-2, *Требования безопасности для криптографических модулей*, июнь 2001.

FIPS 199, *Стандарты по категорированию безопасности федеральной информации и информационных систем*, февраль 2004.

FIPS 200, *Минимальные требования безопасности для федеральной информации и информационных систем*, март 2006.

NIST SP 800-18 Версия 1, *Руководство по разработке планов обеспечения безопасности для систем информационных технологий*, февраль 2006.

NIST SP 800-30,[5] *Руководства по управлению рисками для систем информационных технологий*, январь 2002.

NIST SP 800-33, *Основополагающие технические модели безопасности информационных технологий*, декабрь 2001.

NIST SP 800-37 Версия 1, Проект, *Руководство по санкционированию безопасности федеральных информационных систем: Подход жизненного цикла безопасности*, август 2008.

NIST SP 800-39, Проект*, Управление риском информационных систем: Организационная перспектива*, апрель 2008

NIST SP 800-53, *Рекомендуемые меры безопасности для федеральных информационных систем*, декабрь 2007.

[5] NIST SP 800-30 пересматривается, чтобы фокусироваться исключительно на оценках степени риска с приложением к различным шагам в основах управления рисками, представленных в SP 800-39.

NIST SP 800-53A, *Руководство по оценке мер безопасности в федеральных информационных системах*, июнь 2008.

NIST SP 800-60 Версия 1, *Руководство по отображения типов информации и информационных систем к уровням категорирования безопасности*, август 2008.

NIST SP 800-65, *Интегрирование безопасности в процесс планирования капиталовложений и управления инвестициями*, январь 2005.

Межведомственный отчёт NIST (NISTIR) 7298, *Глоссарий ключевых терминов по информационной безопасности*, апрель 2006.

ПРИЛОЖЕНИЕ D - МАТРИЦА ССЫЛОК И ВЕБСАЙТЫ NIST

Чтобы помочь в дальнейшем исследовании, приведенная ниже матрица отображает соответствующие публикации NIST к соответствующим действиям по безопасности SDLC. Дополнительная информация доступна на следующих вебсайтах NIST: http://csrc.nist.gov и http://nvd.nist.gov/scap.

Действия по безопасности	Поддерживающие публикации NIST
Фаза 1 - Инициирование	
1. Начальное планирование обеспечения безопасности	SP 800-64, -100, -37, -53
2. Категорирование информационной системы	SP 800-60, FIPS 199
3. Оценка влияния на деятельность	SP 800-34
4. Оценка воздействия на приватность	SP 800-37
5. Гарантирование разработки безопасных информационных систем	SP 800-64, -16
Фаза 2 - Разработка/Приобретение	
1. Оценка риска для системы	SP 800-30
2. Выбор и документирование мер безопасности	SP 800-53
3. Проектирование архитектуры безопасности	SP 800-30
4. Конструирование безопасности и разработка мер безопасности	SP 800-53, FIPS 200
5. Разработка документации по безопасности	SP 800-18
6. Проведение тестирования, связанного с разработкой,	FIPS 140-2; SCAP website (see
Фаза 3 - Реализация/Оценка	
1. Создание подробного плана по C&A	SP 800-37
2. Интеграция безопасности в установленные среды или системы	SP 800-64
3. Оценка безопасности системы	SP 800-37, -53A
4. Санкционирование информационной системы	SP 800-37
Фаза 4 - Эксплуатация /Сопровождение	
1. Рассмотрение эксплуатационной готовности	SP 800-70, -53A
2. Выполнение управления конфигурацией	SP 800-53A, -100
3. Проведение непрерывного мониторинга	SP 800-53A, -100
Фаза 5 - Ликвидация	
1. Создание и выполнение плана ликвидации или передачи	None
2. Гарантирование сохранения информации	SP 800-12, -14
3. Очистка носителей информации	SP 800-88
4. Ликвидация аппаратного и программного обеспечения	SP 800-35
5. Закрытие системы	None

ПРИЛОЖЕНИЕ E - ДРУГИЕ МЕТОДОЛОГИИ SDLC

Есть много методологий SDLC, в дополнение к методологии водопада, обсуждённой в этой публикации, которые могут использоваться организацией, чтобы эффективно разработать информационную систему. Ожидаемый размер и сложность системы, график разработки и ожидаемая продолжительность жизни системы могут влиять на выбор какую модель SDLC использовать. Во многих случаях, выбор модели SDLC будет определён политикой приобретения организации. Независимо от используемой методологии, формализации или продолжительности процесса разработки, является критичным, чтобы требования безопасности и рассмотрения, включая ключевую документацию по безопасности, были спланированы и соответственно учитывались на всём жизненном цикле.

Совместная разработка приложений

В традиционной методологии водопада, группа разработчиков собирает требования, многократно через серию интервью с клиентом, и затем приступает к разработке приложения. При использовании методологии Совместной разработки приложений (JAD), клиент или конечный пользователь сотрудничают с разработчиками через сеансы JAD, чтобы спроектировать и разработать приложение. Поскольку процесс разработки включает большее участие клиента, эта методология может привести к более быстрой разработке и к большему удовлетворению клиента.

Модель прототипирования

Модель прототипирования - методология разработки, подобная водопадной модели, в которой, прототипная разработка начинается, как только выполнен анализ требований и разработан прототип. После создания, прототип оценивается клиентом, который, тем самым, предоставляет обратную связь разработчику. Разработчик, в свою очередь, совершенствует продукт согласно ожиданий клиента. После многих итераций этого процесса конечный продукт предоставляется клиенту.

Быстрая разработка приложений

Быстрая разработка приложений (RAD) является методологией разработки, которая создаёт приложение более быстро путём использования технологий, нацеленных на ускоренную разработку приложений, таких как использование менее формальных методологий и повторное использование компонентов программного обеспечения. В обмен на более быструю разработку, могут быть реализованы некоторые компромиссы в функциональности и эффективности. Важно, однако, гарантировать, что этот обмен для более быстрой поставки продукта, не имел результат в компромиссах, сделанных в выборе и спецификации мер безопасности необходимых, чтобы обеспечить адекватную безопасность для информации и информационной системы и функций предназначения, которые они поддерживают.

Спиральная модель

Спиральная модель - методология разработки, которая сочетает особенности прототипной и водопадной моделей, и часто применяется для больших, дорогих и сложных проектов. Процесс спиральной модели в общем включает определение требований и создание начального проекта, конструирование и оценку первого прототипа. Этот же самый процесс повторяется для последующих прототипов, пока усовершенствованный прототип не представляет требуемый продукт. Заключительная система строится, основываясь на финальном прототипе, и он оценивается и сопровождается в среде применения.

ПРИЛОЖЕНИЕ F - ДОПОЛНИТЕЛЬНЫЕ РАССМОТРЕНИЯ ПЛАНИРОВАНИЯ ПРИОБРЕТЕНИЯ

Эта публикация была разработана, чтобы помочь агентствам в интегрировании важных шагов ПО безопасности информации в установленный жизненный цикл разработки системы ИТ (SDLC). Это приложение обсуждает дополнительные рассмотрения планирования приобретения, которые способствуют информационной безопасности во время фазы Разработка/Приобретение SDLC.

- **Тип Контракта**

  Тип контракта (например, твёрдая фиксированная цена, время и материалы, издержки плюс фиксированная плата), может иметь существенные последствия в безопасности. Технический уполномоченный по информационной безопасности, разрабатывающий спецификации, и контрактный специалист должны сотрудничать, чтобы выбрать тип контракта, который будет самым выгодным для организации.

- **Анализ другой функциональной группой**

  В зависимости от размера и области системы, может быть полезным анализ системы участниками от различных функциональных групп (например, юристы, кадровые ресурсы, физическая безопасность, управление записями). У этих функциональных групп должно быть понимание требований конфиденциальности, целостности и доступности. Включение этих групп важно в начале процесса планирования, потому что это может иметь результат в уменьшении стоимости жизненного цикла, и это позволяет легче изменить требования на ранних стадиях.

- **Анализ агентом оценки и санкционирующим должностным лицом**

  Циркуляра OMB-130, Приложение III, требует, чтобы системы были одобрены или санкционированы для обработки данных в конкретных средах. Чтобы соответственно защитить информационную систему должны быть использованы управленческие, эксплуатационные и технические меры безопасности. Управленческие и эксплуатационные меры безопасности могут иногда выходить за рамки контракта, поскольку разработчик, в большинстве случаев, не может быть ответственным за реализацию организацией этих мер безопасности. Функционал технических мер безопасности и спецификации доверия должна содержаться в контракте с разработчиком. Эти меры безопасности должны быть включены в разработку технических спецификаций. Санкционирующее должностное лицо (АО) может принять эти предположения во внимание, когда определяет соответствие полного набора мер безопасности для уменьшения остаточных рисков до допустимого уровня.

  Испытания при C&A также включают проверку управленческих и эксплуатационных мер безопасности, реализованных организацией. Определение эффективности этих реализованных организацией мер безопасности - часть оценки мер безопасности. Процессы оценки должны подтвердить, что предположения в плане безопасности системы были реализованы, и что полный набор мер безопасности соответствует тому, чтобы уменьшить остаточные риски до допустимого уровня. Приёмочное тестирование свойств безопасности разработанной подрядчиком системы является необходимым условием к испытаниям безопасности, как части процесса C&A.

  Поскольку АО ответственны за принятие риска применения системы, они могут делать предложения группе разработчиков, если риски, связанные с возможной деятельностью системы, кажутся недопустимы. Спецификации могут накладывать чрезмерные нагрузку и стоимость, если не известны приемлемые остаточные риски. Для определения приемлемых остаточных рисков требуется участие АО. Легче включить изменения требований во время стадии планирования приобретения системы, чем во время стадий запроса предложений, начального выбора или контроля за исполнением контракта.

- **Циклический характер процессов**

  Шаги безопасности в фазе Разработка/Приобретение, возможно, должны выполняться циклически. Эти шаги безопасности находятся во взаимосвязи и основываются друг на друге. В зависимости от размера и сложности системы, эти шаги могут выполняться так часто, как уточняются замыслы.

- **Оценка и принятие**

  План оценки системы и соответствующие критерии приёмки разрабатываются в фазе Разработка/Приобретение. Для оценки должен быть разработаны спецификации, которые должны включать испытания и анализ. Спецификации должны быть написаны таким образом, чтобы облегчить точное определение того, выполняет ли реализованная система спецификацию. Вообще, два отдельных действия требуют тестирования безопасности - приёмка контракта и C&A.

  Приёмка контракта обычно учитывает только функциональность и спецификации доверия безопасности, содержащиеся в контракте с разработчиком. Испытания при C&A включают также управленческие и эксплуатационные меры безопасности, реализованные организацией. Наличие и корректное применение мер безопасности, которые могли предполагаться разработчиком, возможно, были включены как предположения в требованиях безопасности системы. Адекватное определение реализации организацией мер безопасности - часть испытаний при C&A. Приёмочные испытания свойств безопасности разработанной системы – необходимое условие испытания безопасности в процессе C&A.

- **Запрос предложения (RFP) на разработку**

  RFP облегчает организации принятие наилучшего решения, основанного на предложениях конкурсантов. Сильная сторона процесса RFP - гибкость, которая даёт возможность правительству и конкурсанту согласовать контракт, который лучше всего удовлетворяет потребности правительства. Организация может определить необходимые возможности, процедуры и доверие по информационной безопасности разными способами. RFP может быть гибким документом. Руководство по альтернативному приобретению должно быть представлено офисом приобретения организации или контрактным специалистом.

- **Разработка спецификаций безопасности и технического задания**

  Спецификации безопасности и техническое задание (SOW) основываются на анализе требований. Спецификации обеспечивают детали того, что система, как предполагается, делает. Спецификации должны также быть написаны независимыми от механизмов реализации, стратегии и проекта. Другими словами, спецификации должны заявить то, что система должна сделать, а не как. Реализация разработчиком системы в соответствии со спецификациями может и должна быть проверена. Это подразумевает, что правильно написанные спецификации - те, которые могут быть проверены.

  SOW детализирует то, что разработчик должен сделать во исполнение контракта. Например, в SOW определяется документация, разрабатываемая в соответствии с контрактом. Требования доверия безопасности, которые детализируют много аспектов процессов, которым следует разработчик, и то, какие свидетельства должны быть представлены, чтобы уверить организацию, что процессы были проведены правильно и полностью, могут также быть определены в SOW.

  Есть исключение к общему правилу, как функциональные требования по безопасности отражаются в спецификации безопасности. Выбор механизмов для реализации функций безопасности может произойти во время жизненного цикла применения системы, а не во время подготовки к предложению. Такие решения могут быть подчинены жизненному циклу применения системы, чтобы ответить на изменения в технологии или среде безопасности. Например, во время жизненного цикла механизм аутентификации может измениться от запоминания, допускающего повторное

использование пароля, до токена для биометрической технологии. Заказывающая организация может иметь дело с выбором механизмов, чтобы реализовать функции безопасности во время жизненного цикла работы системы, определяя задачу для разработчика в SOW, чтобы провести исследования и рекомендовать механизм или комбинацию механизмов. Выбор механизма или комбинации механизмов являются обеспечивающей функцией организации.

Опыт показал, что, если спецификации и SOW полностью и однозначно не очерчивают свойства безопасности системы, то система может не достигнуть требуемого уровня безопасности.

Следующие разделы описывают два источника для спецификаций информационной безопасности: общие спецификации и федеральные установленные спецификации. Инициатор приобретения должен сосредоточиться на том, что требуется, и работать с контрактным специалистом, чтобы определить лучший способ запросить это.

- Общие спецификации

  Для спецификаций безопасности являются доступными много источников общей информации, которые могут включать руководства NIST, коммерческие источники и отраслевые организации.

  Общая информация для спецификаций безопасности должна быть рассмотрена на применимость для получаемой системы. Эти спецификации могут предоставить информацию об не учтённых областях. Они могут также сэкономить время, потому что они обеспечивают язык, который может использоваться непосредственно. Однако, необходимо проявлять осторожность при выборе возможностей, процедур и доверия из этих источников. Отдельные элементы в этих документах могут быть сгруппированы, основываясь на взаимозависимостях между элементами. Необходимо понять возможности, процедуры, доверие и их группировки, прежде чем определить их отдельно.

  Каждая спецификация должна быть обоснована исходя из анализа требований, особенно из оценки степени риска. Меры защиты, рекомендуемые общим источником, необходимо рассмотреть, но они не должны быть включены в RFP, если их не поддерживает оценка степени риска.

- Федеральные установленные спецификации

  Агентства должны также включать дополнительные спецификации в RFP, как требуется согласно закону. Они часто упоминаются как предписанные спецификации. Все федеральные агентства должны гарантировать, что системы выполняют применимые федеральные политики и публикации FIPS. Агентствам могут требоваться предписанные спецификации, которые являются официальными политиками, выпущенными с согласия правомочной организации и должностных лиц приобретения.

  Предписанные спецификации должны быть включены в RFP или другой применимый документ приобретения если система, получается в соответствии с критериями в предписанной спецификации. Очень важно знать о предписанных спецификациях.

  Обязанностью приобретающего агентства является включение в RFP действующих законов, нормативных актов и политик. В дополнение к предписаниям, распространяющимся на всю Исполнительную власть, у каждого департамента и независимого ведомства есть свой собственный набор директив, политик и стандартов.

  Простое цитирование требований, взятых из технических спецификаций, может оказаться недостаточным. Предъявление этого подрядчиком разработки, чтобы объяснить политику, не работает. Скорее соответствующая политика и руководство должны быть объяснены или, по крайней мере, упомянуты в технических спецификациях по безопасности.

Публикации Федеральных стандартов обработки информации (FIPS), могут быть найдены в Ресурсном центре компьютерной безопасности NIST (http://csrc.nist.gov). Применимые документы циркуляров, меморандумов и политик OMB могут быть найдены в http://www.whitehouse.gov/omb.

Национальный закон о передаче и продвижении технологий 1995 (Общественный закон [P.L]. 104-113), предписывает департаментам и агентствам федерального правительства использовать, когда целесообразно, технические промышленные стандарты, которые разработаны в добровольных, основанных на согласии, организациях по стандартизации.

На инициатора приобретения возложено знать, какие федеральные установленные спецификации, применимые к системе (ам), должны быть обеспечены. Многие люди ошибочно полагают, что за это усилие ответственен контрактный специалист. Поскольку это технические проблемы, ответственен за это инициатор приобретения.

- **Оценка предложения**

Процесс оценки предложения определяет, выполняет ли предложение минимальные требования, описанные в RFP, и оценивает возможность предлагающего успешно выполнить предполагаемый контракт. Это усилие включает технический анализ достоинств предложения. Как часть фазы Разработка/Приобретение, инициатор приобретения, работающий с контрактным специалистом, разрабатывает план оценки, чтобы определить основание для оценки и как она будет проведена. Сама оценка выполняется во время исходного выбора фазы приобретения. Информационная безопасность должна учитываться в критериях оценки, чтобы привлечь внимание к важности безопасности для правительства. Предлагающие изучают RFP, чтобы понять то, что правительство считает самым важным.

- **Разработка плана оценки**

Оценивая возможности информационной безопасности, может быть трудно оценить, выполняет ли предложение минимальные требования или может ли успешно выполнить предполагаемый контракт. Поэтому, предлагающие должны предоставить гарантии правительству, что связанные с аппаратным и программным обеспечением утверждения относительно возможностей по информационной безопасности - истинны, и что предлагающий может предоставить предложенные услуги. Поскольку информационная безопасность, как и другие аспекты компьютерных систем, является сложным и важным предметом, утверждения предлагающего могут не обеспечить достаточное доверие. То, как доверие обеспечено, может определить возможность правительства соответственно оценить их. SOW определяет требования правительства к разработке системы, включая требования доверия. Спецификации доверия, как правило, включают документацию, которая будет исследована правительством. После принятия решения, если правительство решает, что требуется большее доверие, может потребоваться дополнительное финансирование, чтобы полностью разработать систему.

Разрабатывая план оценки нужно рассмотреть определение того, как предлагающие будут обязаны обеспечивать доверие. Этот план будет использоваться, чтобы помочь разработать разделы RFP, которые предоставляют инструкции предлагающим и информации о том, как предложения будут оценены и как будет выполнен исходный выбор.

Как часть этого процесса, должно быть сделано определение приёмочной проверки безопасности. Это может быть важным, чтобы скоординировать работы проверки и оценки безопасности (ST&E), как часть приёмки, а также C&A, чтобы эффективно управлять усилиями правительства.

Определённое количество проверки и оценки может быть сделано, как часть оценки предложения. Могут использоваться сравнительные проверки и демонстрации функциональности. Сравнительные проверки включают стресс-тестирование (например, время отклика, пропускная способность),

которое подобно некоторой проверке безопасности. Выбор охвата и глубины таких сравнительных проверок является бизнес-решением. И правительство, как покупатель, и предлагающий несут затраты. Любая сторона может решить, что стоимость является препятствием. Является возможным структурировать оценку предложения, чтобы ограничить число предложений, которые включают интенсивные ST&E. Например, демонстрация функциональности безопасности, может требоваться от всех предлагающих, тогда как проверка доверия и возможности проникновения может быть применена только к очевидно подходящим.

Есть существенные различия среди ST&E существующих продуктов, систем, которые должны быть разработаны, и сервисов. Организации имеют некоторую неопределённость относительно сервисов и систем, которые должны быть разработаны. Один подход состоит в том, чтобы рассмотреть возможность отказа поставить предложенные функции безопасности, доверие и сервисы как нарушение условий контракта, для которого существуют различные законные средства. Правительство может так структурировать функциональные демонстрации до принятия решения, чтобы они обеспечили значимые и непротиворечивые результаты для целей оценки.

Важно, чтобы угрозы безопасности и приверженности политике безопасности организации были ясно сформулированы и что предложенные меры безопасности быть очевидно достаточными для их намеченного назначения. Доверие должно быть основано на оценке (активное исследование) продукта или информационной системы, которые должны быть доверенными. Обоснованность документации и результирующего продукта или системы ИТ должна быть определена опытными оценщиками с усиленным акцентом на область, глубину и строгость.

Архитектура и проект оказывают большое влияние на уязвимости и испытания. Хороший проект включает испытания как критерий. Стоимость ST&E может быть минимизирована архитектурой и проектом, которые уменьшают воздействие на безопасность от используемых систем и сервисов с неизвестными свойствами безопасности. Архитектура и проект безопасности должны использовать технологии (например, инкапсуляция и изоляция) и механизмы (например, демилитаризированные зоны и межсетевые экраны), чтобы смягчить уязвимости, риски и стоимость ST&E.

Должна быть рассмотрена архитектура безопасности, которая интегрирует контрмеры. Эти контрмеры включают точечные решения для отдельных сетей (например, межсетевые экраны и системы обнаружения вторжений [IDSs]), управление безопасностью информации (SIM) систем, и интеграция SIM с системой управления безопасностью сети.

- **Элементы для рассмотрения в плане оценки**

Оставшаяся часть от этого раздела представляет соображения для помощи в разработке частей плана оценки, касающихся информационной безопасности.

Когда план оценки разработан, альтернативы по функциональности и безопасности могут конфликтовать друг с другом. Например, возможности, которые обеспечивают информационную безопасность, могут конфликтовать с теми, которые обеспечивают простоту использования. Правительство должно разъяснить, как предлагающие делают предложения различных конфигураций и представляют конфликтные параметры и компромиссы. Однако, должна быть проявлена осторожность по сохранению размера предложения управляемым, чтобы облегчить анализ и минимизировать стоимость подготовки предложения.

Испытания - один метод определения, выполняют ли предложенные система или продукт требования информационной безопасности. В зависимости от сущности системы, испытания могут быть частью оценки предложения, в форме натурных демонстрационных испытаний или сравнительных испытаний, или они могут быть частью предварительного приёмочного тестирования. Во время процесса оценки испытания могут использоваться в разное время, в зависимости от стоимости, технических аспектов и рассмотрений целостности приобретения. Дорогие испытания должны быть сведены к минимуму, чтобы помочь предлагающему контролировать стоимость

подготовки предложения. Дорогие предложения не только ограничивают соревновательность, но их стоимость также, в конечном счёте, передаётся правительству в более высокой стоимости контракта.

Испытания информационной системы, особенно испытания на применимость, должны быть выполнены с активированными опциями информационной безопасности.

Чем больше инициатор приобретения знает о рынке, тем более легко он должен разработать план оценки. Однако, предложения не могут использоваться для исследования рынка. План оценки не может быть изменён после получения предложений. Дополнительная информация из других предложений не может использоваться, чтобы изменить план оценки. Стоит исследовать альтернативы, которые могли быть предложены, чтобы гарантировать разработку системы оценки, которая отражает истинные приоритеты правительства.

- **Специальные требования контракта**

  Некоторые элементы в RFP связаны с информационной безопасностью, но не содержатся в SOW или критериях оценки. Эти элементы обычно адресуют права, обязанности и средства, назначенные на стороны контракта. Часто такие обязательства сохраняются за фактическим периодом исполнения контракта. Поэтому, такие элементы лучше всего учитывать через специальные пункты или требования контракта. Одним примером являются требования по неразглашению информации, полученной в течение контракта.

G ПРИЛОЖЕНИЯ - ДОПОЛНИТЕЛЬНЫЕ ГРАФИЧЕСКИЕ ПРЕДСТАВЛЕНИЯ БЕЗОПАСНОСТИ В SDLC