NIST Специальная Публикация 800-18

Версия 1

Руководство по разработке планов обеспечения безопасности для федеральных информационных систем

Marianne Swanson
Joan Hash
Pauline Bowen

National Institute of Standards and Technology
U.S. Department of Commerce

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

Февраль 2006

МИНИСТЕРСТВО ТОРГОВЛИ США
Carlos M.Gutierrez, Министр

НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И ТЕХНОЛОГИЙ
William Jeffrey, Директор

Отчеты 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 ITL, руководств и усилий, направленных на повышение безопасности информационных систем, и ее совместных работ с отраслями, правительством и академическими организациями.

Полномочия

Этот документ был разработан NIST в соответствии с его обязанностями, установленными согласно Закона об управлении безопасностью федеральной информации от 2002г., Общественный закон (P.L). 107-347.

NIST ответственен за разработку стандартов информационной безопасности и руководств, включая минимальные требования для обеспечения соответствующей информационной безопасности для деятельности и активов всех агентств, но такие стандарты и руководства не должны применяться к системам национальной безопасности. Это руководство непротиворечиво с требованиями Циркуляра А-130 Министерства управления и бюджета (OMB), Раздел 8b (3), Обеспечение безопасности информационных систем агентств, как указано в А-130, Приложение IV: Анализ ключевых разделов. Дополнительная информация предоставлена в А-130, Приложение III.

Это руководство было подготовлено для использования федеральными агентствами и может быть использовано на добровольной основе неправительственными организациями и это не попадает по действие авторского права. (Упоминание приветствовалось бы NIST).

Ничто в этой публикации не должно использоваться в противоречие со стандартами и руководствами, определенными 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 идентифицированы в этом документе, чтобы описать экспериментальную процедуру или концепцию соответственно. Такая идентификация не предназначена, чтобы означать рекомендацию или одобрение Национального института стандартов и технологий, а также это не предназначено, чтобы означать, что сущности, материалы или оборудование - обязательно наилучшее имеющееся по предназначению.

Благодарности

Национальный институт стандартов и технологий хотел бы поблагодарить авторов исходной NIST Специальной Публикации 800-18, *Руководство по разработке планов обеспечения безопасности для систем информационных технологий.* Оригинал документа использовался в качестве основы для этой версии. Дополнительно, спасибо всему персоналу NIST, который просмотрел и прокомментировал документ.

Оглавление

Резюме

Цель планирования обеспечения безопасности системы состоит в том, чтобы улучшить защиту ресурсов информационной системы. Все федеральные системы имеют некоторый уровень чувствительности и требуют защиты, как часть хорошей практики управления. Защита системы должна быть задокументирована в план обеспечения безопасности системы. Наличие планов безопасности системы - требование Циркуляра A-130 Министерства управления и бюджета (OMB), "Управление ресурсами федеральной информации," Приложение III, "Безопасность федеральных автоматизированных информационных ресурсов," и Раздела III закона об Электронном правительстве, названного Закон об управлении безопасностью Федеральной информации (FISMA).

Назначение плана обеспечения безопасности системы состоит в том, чтобы обеспечить обзор требований безопасности системы и описать существующие меры безопасности или планируемые для удовлетворения предъявленным требованиям. План обеспечения безопасности системы также очерчивает обязанности и ожидаемое поведение всех людей кто имеет доступ к системе. План обеспечения безопасности системы должен рассматриваться как документирование структурированного процесса планирования адекватного, рентабельного обеспечения безопасности системы. Он должен отражать участие различных менеджеров с обязанностями в отношении системы, включая владельцев информации, владельца системы и высшего сотрудника по информационной безопасности агентства (SAISO). Дополнительная информация может быть включена в основной план в структуре и формате, соответствующим потребностям агентства, когда основные разделы, описанные в этом документе, соответственно охвачены и подготовлены.

В соответствии с планами, адекватно отражающими защиту ресурсов, высшее руководящее должностное лицо должно санкционировать применение системы. Санкционирование системы на обработку информации, предоставляемое руководящим должностным лицом, является важный для управления качеством. Санкционируя обработку в системе, руководитель принимает связанный с этим риск.

Санкционирование руководством должно быть основано на оценке управленческих, эксплуатационных и технических мер безопасности. Так как план обеспечения безопасности системы устанавливает и документирует меры безопасности, он должен сформировать основание для санкционирования, дополненное отчётом об оценке и планом действий и вех. Кроме того, будущему санкционированию должен также способствовать периодическое рассмотрение мер безопасности. Пересанкционирование должно происходить всякий раз, когда есть существенные изменения в процессе обработки, но, по крайней мере, каждые три года.

1. Введение

Сегодняшняя быстро изменяющаяся техническая среда требует, чтобы федеральные агентства приняли минимальный набор мер безопасности, чтобы защитить их информацию и информационные системы. Федеральный стандарт обработки информации (FIPS) 200, *Минимальные требования безопасности для федеральной информации и информационных систем*, определяет минимальные требования безопасности для федеральной информации и информационных систем в семнадцати связанных с безопасностью областях. Федеральные агентства должны выполнить минимальные требования безопасности, определенные в FIPS 200 с помощью мер безопасности в Специальной Публикации NIST 800-53, *Рекомендуемые меры безопасности для федеральных информационных систем*. NIST SP 800-53 содержит управленческие, эксплуатационные и технические меры защиты или контрмеры, предписанные для информационных систем. Выбранные или планируемые меры безопасности должны быть задокументированы в план обеспечения безопасности системы. Настоящий документ дает представление федеральным агентствам о том, как разрабатывать планы обеспечения безопасности для федеральных информационных систем.

1.1 Фон

Раздел III закона об Электронном правительстве, названный Законом об управлении безопасностью Федеральной информации (FISMA), требует, чтобы каждое федеральное агентство разработало, задокументировало и реализовало общую для агентства программу информационной безопасности по обеспечению информационной безопасности информации и информационных систем, которые поддерживают деятельность и активы агентства, включая обеспечиваемые или управляемые другим агентством, подрядчиком или другим источником. Планирование обеспечения безопасности систем является важной работой, которая поддерживает жизненный цикл разработки систем (SDLC) и должно корректироваться, по мере того, как события в системе инициируют потребность в новой редакции, чтобы точно отразить актуальное состояние системы. План обеспечения безопасности системы предоставляет сводку требований безопасности для информационной системы и описывает существующие или планируемые меры безопасности для удовлетворения этим требованиям. План может также ссылаться на другие ключевые, связанные с безопасностью документы для информационной системы, такие как оценка степени риска, план действий и вех, документ с решением по аттестации, оценка воздействия на приватность, план действий при непредвиденных обстоятельствах, план управления конфигурацией, контрольные списки конфигурации безопасности и соглашения о взаимосвязи систем, как соответствующе.

1.2 Целевая аудитория

Руководители программ, владельцы систем и персонал службы безопасности в организации должны понимать процесс планирования обеспечения безопасности системы. Кроме того, пользователи информационной системы и ответственные за определение требований к системе должны быть знакомы с процессом планирования обеспечения безопасности системы. Ответственные за реализацию и управление информационными системами должны участвовать в определении мер безопасности, которые будут применены к их системам. Это руководство предоставляет основную информацию о том, как подготовить план обеспечения безопасности системы и разработано, чтобы быть применимым во множестве организационных структур и использоваться в качестве справочной информации теми, которые несут ответственность за деятельность, связанную с планированием обеспечения безопасности.

1.3 Организация документа

Эта публикация представляет ряд действий и концепций, чтобы разработать план обеспечения безопасности информационной системы. Краткое описание содержания публикации:

- ***Глава 1*** содержит вводную информацию, относящуюся к процессу планирования обеспечения безопасности системы, целевую аудитория, информацию относительно FIPS 199, *Стандарты по категорированию безопасности федеральной информации и информационных систем*, обсуждение различных категорий информационных систем, идентификацию связанных публикаций NIST и описание ролей и обязанностей, имеющих отношение к разработке планов обеспечения безопасности системы.
- ***В Главе 2*** обсуждается, как агентства должны проанализировать оборудование своей информационной системы в процессе установления границ системы. В ней также обсуждается идентификация общих мер обеспечения безопасности и руководство по учёту границ.
- ***Глава 3*** проводит читателя по шагам разработки плана обеспечения безопасности системы.
- ***Приложение А*** содержит шаблон плана обеспечения безопасности системы.
- ***Приложение В*** содержит глоссарий терминов и определения.
- ***Приложени*е ***С*** содержит ссылки, которые поддерживают эту публикацию.

1.4 Реестр систем и стандарты обработки федеральной информации (FIPS 199)

FISMA требует, чтобы у агентств был реестр информационных систем. Все информационные системы в реестре должны быть прокатегорированы, используя FIPS 199, как первый шаг в деятельности по планированию обеспечения безопасности систем.

FIPS 199 является обязательным стандартом, который используется всеми федеральными агентствами, чтобы категорировать всю информацию и информационные системы, принадлежащие или сопровождаемые непосредственно, или от имени каждого агентства, основываясь на целях обеспечения соответствующих уровней информационной безопасности согласно воздействиям. Стандарты категорирования безопасности для информации и информационных систем обеспечивают общие основы и понимание для определения безопасности, которые, для федерального правительства, способствуют: (I) эффективному управлению и надзору за программами информационной безопасности, включая координацию усилий по информационной безопасности в сообществах гражданского сектора, национальной безопасности, подготовленности к чрезвычайным ситуациям, безопасности отечества и обеспечения правопорядка; и (II) созданию непротиворечивых отчетов Министерству управления и бюджета (OMB) и Конгрессу по соответствию и эффективности политик, процедур и методов обеспечения информационной безопасности.

1.5 Главные приложения, системы общей поддержки и второстепенные приложения

Все информационные системы должны быть охвачены планами обеспечения безопасности систем и определены, как главные приложения[1] или системы общей поддержки.[2] Конкретные планы

[1] Циркуляра OMB A-130, Приложение III, определяет главное приложение как приложение, которое требует особого внимания к безопасности вследствие величины риска и вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации в приложении.

[2] Циркуляра OMB A-130, Приложение III, определяет систему общей поддержки, как объединенный набор информационных ресурсов под общим управлением, которые совместно предоставляют общую функциональность. Это обычно включает аппаратные средства, программное обеспечение, информацию, данные, приложения, коммуникации и людей.

обеспечения безопасности систем второстепенных приложений[3] не требуются, потому что меры безопасности для этих приложений, как правило, обеспечиваются системой общей поддержки или главным приложением, в котором они работают. В тех случаях, когда второстепенное приложение не соединено с главным приложением или системой общей поддержки, второстепенное приложение должно быть кратко описано в плане системы общей поддержки, которая имеет или общее физическое расположение или поддерживается той же самой организацией. Дополнительная информация приведена в Главе 2.

1.6 Другие связанные публикации NIST

Чтобы разработать план обеспечения безопасности системы, необходимо быть знакомым со стандартами обеспечения безопасности и руководствами NIST. Важно, чтобы пользователи этой публикации понимали требования и методологию категорирования информационных систем, которые описаны в NIST FIPS 199, также, как и требования по минимальным мерам безопасности для конкретной системы, которые описаны в NIST SP 800-53, *Рекомендуемые меры обеспечения безопасности для федеральных информационных систем,* и FIPS 200*, Минимальные требования по безопасности для федеральной информации и информационных систем.*

Другими ключевыми публикациями NIST, непосредственно поддерживающими подготовку плана обеспечения безопасности, являются NIST SP 800-30, *Руководство по управлению рисками для систем информационных технологий* и NIST SP 800-37, *Руководство, по оценке безопасности и аттестации федеральных информационных систем.* Все документы могут быть получены на вебсайте Ресурсного центра компьютерной безопасности NIST в: http://csrc.nist.gov/.

1.7 Обязанности по плану обеспечения безопасности системы

Агентства должны разработать политику по процессу планирования безопасности системы. Планы обеспечения безопасности систем являются живыми документами, которые требуют периодического пересмотра, модификации и планирования действий и вех для того, чтобы реализовать меры обеспечения безопасности. Процедуры должны конкретно определять, кто рассматривает планы, поддерживает планы актуальными и развивает запланированные меры безопасности. Кроме того, процедуры должны требовать, чтобы планы обеспечения безопасности систем были разработаны и рассмотрены до начала процесса оценки безопасности и аттестации систем.

Во время процесса оценки безопасности и аттестации план безопасности системы анализируется, уточняется и принимается. Исполнитель оценки подтверждает, что меры безопасности, описанные в плане безопасности системы, непротиворечивы с категорией безопасности FIPS 199, определенной для информационной системы, и что угрозы и уязвимости идентифицированы и определение начального риска проведено и задокументировано в план обеспечения безопасности системы, оценку степени риска или эквивалентный документ. Результаты оценки безопасности используются, чтобы переоценить риски, разработать план действий и вех (POA&Ms), которые обязаны отслеживать восстановительные действия и обновлять план обеспечения безопасности системы, обеспечивая, таким образом, фактическое основание для официального санкционирования, чтобы представить решение по аттестации безопасности. Для дополнительной информации о процессе оценки безопасности и аттестации см. NIST SP 800-37. Рисунок 1

[3] Специальная Публикация NIST 800-37 определяет второстепенное приложение как приложение, отличное от главного приложения, которое требует внимания к безопасности вследствие риска и величина вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации в приложении. Второстепенные приложения, как правило, включаются как часть системы общей поддержки.

изображает ключевые исходные положения/результаты процесса планирования обеспечения безопасности.

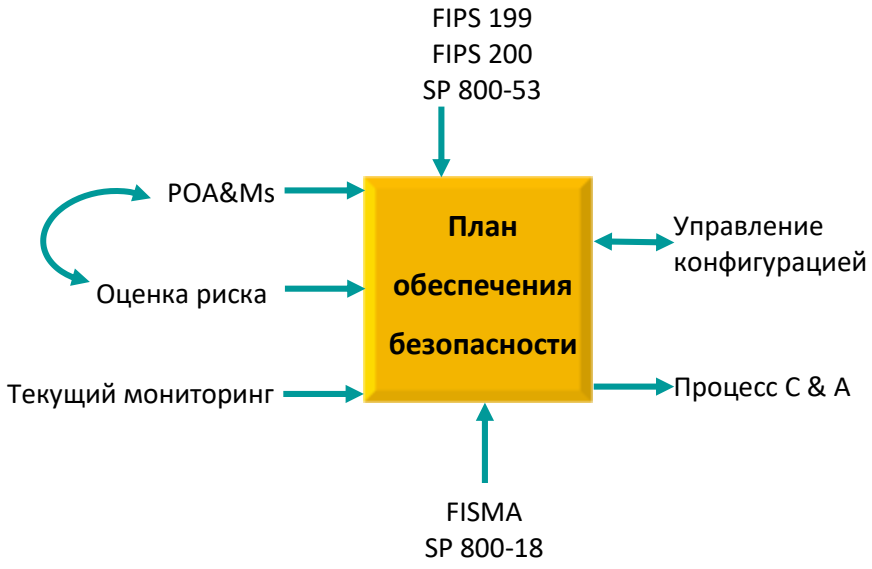

Рисунок 1: Исходные положения/результаты процесса планирования обеспечения безопасности

Роли и обязанности в этом разделе специфичны для планирования обеспечения безопасности информационных систем. Учёт того, что у агентств есть значительно различающиеся предназначения и организационные структуры, может отражаться в различиях в наименовании ролей, связанных с планированием обеспечения безопасности, и в распределении связанных обязанности среди персонала агентства (например, несколько людей, выполняющих одну роль, или один человек, выполняющий несколько ролей[4]).

1.7.1 *Директор по информации*

Директор по информации (CIO)[5] является официальным должностным лицом агентства, ответственным за разработку и поддержание общеагентсткой программы информационной безопасности, и имеет следующие обязанности по планированию обеспечения безопасности систем:

- Назначает старшего сотрудника информационной безопасности агентства (SAISO), который должен выполнять обязанности CIO по планированию обеспечения безопасности систем,

[4] Необходимо проявлять осторожность, когда один человек исполняет множественные роли в процессе планирования обеспечения безопасности, чтобы гарантировать, что человек сохраняет соответствующий уровень независимости и остается избавленным от конфликтов интересов.

[5] Когда агентство не определяет формальную позицию CIO, FISMA требует, чтобы соответствующие обязанности выполнялись сопоставимым официальным должностным лицом агентства.

- Разрабатывает и сопровождает политики информационной безопасности, процедуры и методы управления, предназначенные для планирования обеспечения безопасность системы,
- Управляет идентификацией, реализацией и оценкой общих мер обеспечения безопасности,
- Гарантирует, что персонал с существенными обязанностями по планированию обеспечения безопасности систем является подготовленным,
- Помогает высшим должностным лицам агентства по их обязанностям по планированию обеспечения безопасности систем, и
- Определяет и координирует общие меры обеспечения безопасности для агентства.

1.7.2 *Владелец Информационной системы*

Владелец[6] информационная система является официальным лицом агентства, ответственным в целом за приобретение, разработку, интеграцию, модификацию, или применение и поддержку информационной системы. Владелец информационной системы имеет следующие обязанности, связанные с планированием обеспечения безопасности системы:

- Разрабатывает план обеспечения безопасности системы в координации с владельцами информации, системным администратором, сотрудником безопасности информационной системы, высшим сотрудником информационной безопасности агентства и функциональными "конечными пользователями,"
- Сопровождает план обеспечения безопасности системы и гарантирует, что система развернута и применяется согласно согласованным требованиям безопасности,
- Гарантирует, что пользователи системы и персонал поддержки получают необходимое обучение по безопасности (например, инструктаж по правилам действий),
- Обновляет план обеспечения безопасности системы всякий раз, когда происходят существенные изменения, и
- Помогает в определении, реализации и оценке общих мер обеспечения безопасности.

1.7.3 *Владелец информации*

Владелец информации является должностным лицом агентства с установленными законом или должностными полномочиями по конкретной информации и ответственностью за установление мер обеспечения безопасности по её формированию, сбору, обработке, распространению и ликвидации. Владелец информации имеет следующие обязанности, связанные с планированием обеспечения безопасности систем:

[6] Роль владельца информационной системы может быть интерпретирована во множестве путей в зависимости от определенное агентство и фаза жизненного цикла разработки систем информационной системы. Некоторые агентства могут именовать владельцев информационной системы как владельцев деятельности/актива/предназначения или диспетчеры программ.

- Устанавливает правила для соответствующего использования и защиты данных/информации субъектов (правила поведения),[7]
- Предоставляет владельцам информационной системы исходные данные относительно требований безопасности и мер безопасности для информационной системы (систем), где находится информация,
- Решает, кто имеет доступ к информационной системе и с какими типами полномочий или правами доступа, и
- Помогает в идентификации и оценке общих мер обеспечения безопасности там, где находится информация.

1.7.4 *Высший сотрудник информационной безопасности агентства (SAISO)*

Высший сотрудник информационной безопасности агентства является, официальным должностным лицом агентства, ответственным за то, чтобы являться основной связью CIO с владельцами информационных систем агентства и с сотрудниками безопасности информационных систем. SAISO имеет следующие обязанности в отношение планов обеспечения безопасности систем:

- Выполняет обязанности CIO по планированию обеспечения безопасности систем,
- Координирует разработку, рассмотрение и принятие планов обеспечения безопасности систем с владельцами информационных систем, сотрудниками безопасности информационных систем и санкционирующими должностными лицами,
- Координирует определение, реализацию и оценку общих меры обеспечения безопасности, и
- Обладает профессиональной квалификацией, включая обучение и опыт, требуемой для разработки и рассмотрения планов обеспечения безопасности систем.

1.7.5 *Сотрудник безопасности информационной системы*

Сотрудник безопасности информационной системы - официальное должностное лицо агентства с обязанностями, возложенными SAISO, санкционирующим должностным лицом, должностным лицом руководства или владельцем информационной системы для гарантии того, что поддерживается соответствующее состояние безопасности для информационной системы или программы. Сотрудник безопасности информационной системы имеет следующие обязанности отношение планов обеспечения безопасности системы:

- Помогает высшему сотруднику информационной безопасности агентства в определении, реализация и оценке общих мер обеспечения безопасности, и

[7] Владелец информации сохраняет эту ответственность даже когда данные/информация используются совместно с другим организации.

- Играет активную роль в разработке и обновлении плана безопасности системы, а также координирует с владельцем информационной системы любые изменения к системе и оценивает воздействие этих изменений на безопасность.

1.7.6 *Санкционирующее должностное лицо*

Санкционирующее должностное лицо (или назначенный одобряющий/аттестовывающий орган, как упомянуто некоторыми агентствами) является высшим должностным лицом руководства или исполнительным органом с полномочиями по формальному принятию на себя ответственности за эксплуатацию информационной системы на допустимом уровне риска к деятельности агентства, активам агентства или людям.[8] Санкционирующее должностное лицо имеет следующие обязанности отношение планов обеспечения безопасности системы:

- Одобряет планы безопасности системы,
- Санкционирует эксплуатацию информационной системы,
- Даёт временную санкцию на эксплуатацию информационной системы с учётом конкретных положений и условий, или
- Отказывает в санкционировании эксплуатации информационной системы (или останавливает эксплуатацию, если система уже эксплуатируется), если существуют недопустимые риски безопасности.

1.8 Правила Поведения

Правила поведения, которые определены в Циркуляре OMB A-130, Приложение III, и являются мерой безопасности, содержащейся в NIST SP 800-53, должны ясно очерчивать обязанности и ожидаемое поведение всех людей с доступом к системе. Правила должны описывать последствия несообразного поведения или несоблюдения и быть доведены до каждого пользователя до получения санкционирования для доступа к системе. Требуется, что правила содержали страницу подписи каждого пользователя для письменного подтверждения, что они читали, понимают и соглашаются соблюдать правила поведения. Для подтверждения правил поведения приемлемы электронные подписи.

Рисунок 2 содержит примеры из Приложения III Циркуляра OMB A-130 того, что должно содержаться в типичных правилах поведения. Это только примеры, и у агентств имеется гибкость в их деталях и содержании. Разрабатывая правила поведения имейте в виду, что намерение состоит в том, чтобы сделать всех пользователей ответственными за их действия с подтверждением, что они читали, понимают и соглашаются соблюдать правила поведения. Правила не должны быть полной копией политики безопасности или руководства по процедурам, а скорее охватом, на высоком уровне, некоторых из мер безопасности, описанных на следующем рисунке.

[8] В некоторых агентствах, высшее должностное лицо и Директор по информации, могут быть со-уполномочивающими должностными лицами. В эта ситуация, высшее должностное лицо одобряет эксплуатацию информационной системы до Директора по информации.

Примеры мер безопасности, содержавшихся в правилах поведения

- Очертите обязанности, ожидаемое использование системы, и поведение всех пользователей.
- Опишите соответствующие ограничения по взаимодействию.
- Определите приоритеты предоставления и восстановления услуг.
- Опишите последствия поведения не сообразного с правилами.
- Затроньте следующие темы:
  - Работа дома
  - Коммутируемый доступ
  - Соединение с Интернетом
  - Использование произведений, охраняемых авторским правом
  - Неофициальное использование правительственного оборудования
  - Присвоение и ограничение системных полномочий и индивидуальной подконтрольности
  - Использование Пароля
  - Поиск в базах данных и разглашение информации.

Рисунок 2: Правила Примеров Поведения

1.9 Утверждение плана безопасности системы

Политика организации должна ясно определять, кто ответственен за утверждение плана безопасности системы и процедуры, разрабатываемые для доведения плана, включая любой специальный меморандума или другую документацию, требуемую агентством. Назначенное санкционирующее должностное лицо, независимое от системного владельца, одобряет план, как правило, до проведения процесса аттестации.

2. Анализ границ системы и мер безопасности

Прежде, чем план обеспечения безопасности системы может быть разработан, информационная система и резидентная информация в этой системе должны быть категорированы, основываясь на анализе воздействий по FIPS 199. Затем может быть сделано определение того, какие системы могут быть логически отнесены в реестре в главные приложения, а какие в системы общей поддержки. Когда определяются границы системы и выбирается начальный набор мер безопасности (то есть, базовый набор мер безопасности) необходимо рассматривать уровни воздействия по FIPS 199. Меры базового уровня безопасности могут быть тогда адаптированы, основываясь на оценке риска и локальных условиях, включая специфичные для организации требования безопасности, конкретную информацию угроз, анализ эффективности – стоимости, доступность компенсационных мер безопасности или особые обстоятельства. Общие меры безопасности, которые являются одними из рассматриваемых при адаптации, должны быть идентифицированы до подготовки плана обеспечения безопасности системы, чтобы идентифицировать те меры безопасности, которые не специфичны для системы и закрываются на уровне агентства. Эти общие меры безопасности могут тогда быть включены в план обеспечения безопасности системы ссылкой.

2.1 Границы системы

Процесс назначения уникальных информационных ресурсов[9] для информационной системы определяет границы безопасности для этой системы. У агентств есть большая гибкость в определении того, что представляет собой информационная система (то есть, главное приложение или система общей поддержки). Если набор информационных ресурсов идентифицирован как информационная система, ресурсы должны обычно находиться под одним и тем же прямым административным управлением. Прямое административное управление[10] не обязательно подразумевает, что там отсутствует промежуточное управление. Информационная система может также содержать множественные *подсистемы*.

Подсистема - главная составная часть или компонент информационной системы, состоящий из информации, информационной технологии и персонала, которые выполняют одну или больше конкретных функций. Подсистемы, как правило, находятся под тем же самым должностным лицом управления и включаются в один плана обеспечения безопасности системы. Рисунок 3 изображает систему общей поддержки с тремя подсистемами.

Если информационные ресурсы идентифицированы как информационная система, может быть полезно для агентств, чтобы рассмотреть, в дополнение к рассмотрению прямого административного управления:

- Имеют ли ту же самую функцию или цель деятельности и, по существу, те же самые рабочие характеристики и потребности безопасности, и

[9] Информационные ресурсы состоят из информации и связанных ресурсов, таких как персонал, оборудование, фонды и информационная технология.

[10] Прямое административное управление включает, как правило, бюджетные, программные или эксплуатационные полномочия и связанную ответственность. Для новых информационных систем административное управление может быть интерпретировано как наличие бюджетных/программных полномочий и ответственности за разработку и развертывание информационных систем. Для информационных систем, находящихся в федеральном реестре, административное управление может быть интерпретировано как наличие бюджетных/эксплуатационных полномочий для повседневной деятельности и поддержки информационных систем.

- Находятся ли в той же самой общей операционной среде (или в случае распределенной информационной системы, находятся ли в различных расположениях с подобными операционными средами).

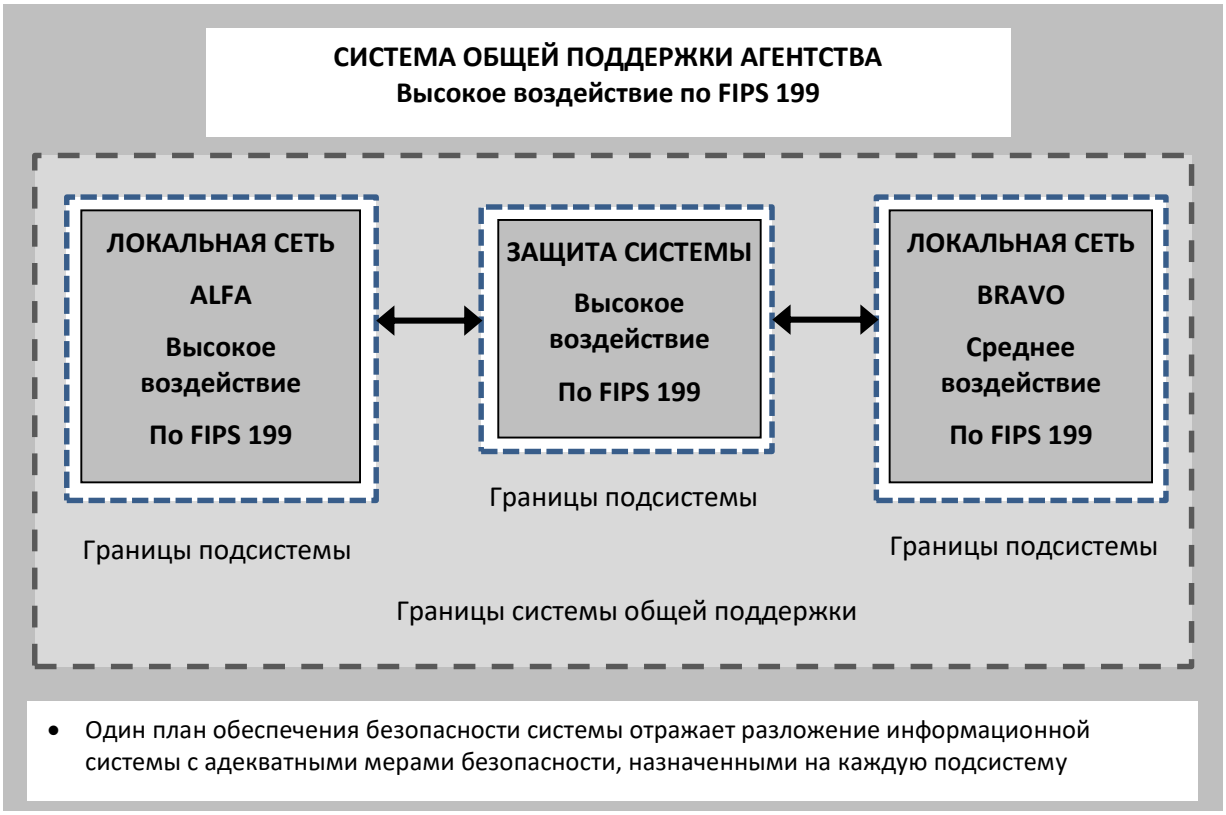

Рисунок 3: Разложение больших и сложных информационных систем

В то время как вышеупомянутые рассмотрения, могут быть полезны для агентств в определении границ информационной системы с целью аттестации безопасности, они не должны рассматриваться как ограничение гибкости агентства в установлении границ, которые способствуют эффективной информационной безопасности в рамках доступных ресурсов агентства. Санкционирующие должностные лица и высшие сотрудники информационной безопасности агентства, устанавливая границы информационной системы, должны консультироваться с возможными владельцами информационной системы. Процесс установления границ для информационных систем агентства и связанных последствий безопасности, это деятельность на уровне агентства, которая должна включать тщательное согласование среди всех ключевых участников - принятия во внимание требований предназначение/деятельности агентства, технических рассмотрений относительно информационной безопасности и программной стоимости для агентства.

FIPS 199 определяет категории безопасности для информационных систем, основанные на потенциальном воздействии на организации, активы или людей, которое должно иметь следствием нарушение безопасности - то есть, потерю конфиденциальности, целостности или доступности. Категории безопасности FIPS 199 могут играть важную роль в определении границ информационной системы, деля информационные системы агентства согласно критичности или чувствительности информации и информационных систем и значимости этих систем в выполнении предназначения агентства. Это особенно важно, когда имеются различные уровней воздействия по FIPS 199, относящиеся к одной информационной системе. FIPS 199 требует, чтобы обеспечивалась безопасность информационной системы по отношению к самому высокому

применимому уровню воздействия, группируя незначительные приложения/подсистемы различных уровней воздействия по FIPS 199 в отдельную систему общей поддержки или главное приложение, если это дает адекватную защиту границ, например, межсетевое экранирование и шифрование, вокруг тех подсистем или приложений с самым высоким уровнем воздействия. Дополнительно, должно быть доверие к тому, что совместно используемые ресурсы, то есть, сети, коммуникации и физический доступ в целом в системе общей поддержки или главном приложении, защищены соответственно для самого высокого уровня воздействия. Наличие возможности изолировать системы высокого воздействия будет иметь результат не только в более безопасных системах, но также уменьшит количество ресурсов, требуемых чтобы обеспечить безопасность много приложений/систем, которые не требуют этого уровня безопасности. NIST SP 800-53 обеспечивает три набора базовых мер безопасности, то есть низкий, умеренный и высокий, которые связаны с тремя уровнями воздействия по FIPS 199; поэтому сделайте минимальные требования доверия в соответствии с увеличением уровня воздействия. При сообщении о назначениях, то есть, в годовом отчет по FISMA, в случае, когда у информационной системы есть различные уровни воздействия по FIPS 199, такая система категорируется по самому высокому уровню воздействия из относящихся к информационной системе.

2.2 Главные Приложения

Все федеральные приложения имеют значение и требуют некоторого уровня защиты. Некоторые приложения, из-за информации, которую они содержат, обрабатывают, хранят или передают, или из-за их критичности к предназначению агентства, требуют специального надзора руководства. Эти приложения являются главными приложениями. Главное приложение, как ожидается, будет иметь умеренный или высокий уровень воздействия по FIPS 199. Циркуляра OMB-130 определяет "главную информационную систему" как информационную систему, которая требует специального внимания руководства из-за его важности для предназначения агентства; высоких затраты на его разработку, эксплуатацию или обслуживание; или его существенной роли в администрировании программ агентства, финансов, имущества или других ресурсов. Главные приложения - по определению главные информационные системы.

Главные приложения - системы, которые выполняют ясно определенные функции, для которых есть легко определимые рассмотрения безопасности и потребности (например, система электронного перевода средств). Главное приложение может включать много отдельных программ и компонентов аппаратных средств, программного обеспечения и телекоммуникационных средств. Эти компоненты могут быть отдельным программным приложением или комбинацией аппаратных средств/программного обеспечения, сосредоточенном на том, чтобы поддерживать конкретную, связанную с предназначением функцию. Главное приложение может также состоять из множества отдельных приложений, если они все связаны с одной функцией предназначения (например, заработная плата или персонал). Если система определена как главное приложение и приложение запущено на системе общей поддержки другой организации, владелец главного приложения ответственен за принятие риска и кроме того:

- Уведомляет владельца системы общей поддержки, что приложение является критическим и обеспечивает конкретные требования безопасности;
- Предоставляет копию плана обеспечения безопасности главного приложения оператору системы общей поддержки;

- Запрашивает копию плана обеспечения безопасности системы общей поддержки и гарантирует, что он обеспечивает надлежащую защиту для приложения и информации; и
- Включает ссылку на план обеспечения безопасности системы общей поддержки в план обеспечения безопасности главного приложения.

2.3 Системы общей поддержки

Система общей поддержки является объединенным набором информационных ресурсов под одним прямым административным управлением, который совместно использует общую функциональность. Система общей поддержки обычно включает аппаратные средства, программное обеспечение, информацию, данные, приложения, коммуникации, средства и людей и оказывает поддержку для множества пользователей и/или приложений. Системой общей поддержки, например[11], могут быть:

- LAN, включая умные терминалы, которые поддерживают филиал;
- опорная сеть (например, общеагентсткая);
- система коммуникаций;
- центр обработки данных агентства, включая его операционную систему и утилиты,
- тактическая радиосеть; или
- совместно используемые возможности сервиса обработки информации.

У системы общей поддержки может быть низкий, умеренный или высокий уровень воздействия по FIPS 199 при его категорировании безопасности в зависимости от критичности или чувствительности системы и любых главных приложений, которые поддерживает система общей поддержки. Систему общей поддержки считают главной информационной системой, когда требуется специальное внимание управления, имеются высокие затраты на разработку, эксплуатацию или на обслуживание; и у системы/информации есть существенная роль в администрировании программ агентства. Когда система общей поддержки является главной информационной системой, уровень воздействия для системы по FIPS 199 устанавливается или умеренным, или высоким.

Главное приложение может быть размещено на системе общей поддержки. План системы общей поддержки должен ссылаться на план обеспечения безопасности главного приложения.

2.4 Незначительные приложения

Агентства, как ожидается, используют управленческие решения в определении какие из приложений, являются второстепенными приложениями и гарантируют, что требования безопасности для второстепенных приложений представляются как часть плана обеспечения безопасности системы для применимых систем общей поддержки или, в некоторых случаях, применимого главного приложения. В большинстве случаев большинство мер безопасности для второстепенного приложения может быть обеспечено системой общей поддержки или главным приложением, с которым они используются. Если это верно, то владелец информационной системы общей поддержки или главного приложения является владельцем информационной системы для второстепенного приложения и ответственен за разработку плана обеспечения

[11] Пример представляет маленькую выборку систем общей поддержки; это не исчерпывающий список.

безопасности системы. Дополнительные меры безопасности, специфичные для второстепенного приложения, должны быть задокументированы в план обеспечения безопасности системы как приложение или раздел. Владелец второстепенного приложения (часто это тот же самый владелец информации) может разработать приложение или раздел, описывающий дополнительные меры безопасности. Полный план обеспечения безопасности системы общей поддержки или главного приложения должен быть общим совместно с владельцем информации.

Второстепенное приложение может иметь низкую или умеренную категорию безопасности по FIPS 199. Однако, если второстепенное приложение базируется на систему, у которой нет адекватной защиты границ, второстепенное приложение должно реализовывать минимальные базовые меры безопасности, требуемые узлом или взаимодействующей системой.

2.5 Меры безопасности

FIPS 200 определяет семнадцать минимальных требований безопасности для федеральной информации и информационных систем. Требования представляют всеобъемлющую, сбалансированную программу информационной безопасности, которая определяет организационные, эксплуатационные и технические аспекты защиты конфиденциальности, целостности и доступности федеральной информации и информационных систем. Агентство должно выполнить минимальные требования безопасности в этом стандарте, применяя меры безопасности, выбранные в соответствии с NIST SP 800-53 и определяемые уровнями воздействия на информационные системы. У агентства есть гибкость, чтобы адаптировать базовые меры безопасности в соответствии с положениями и условиями, сформулированными в стандарте. Работы по адаптации включают: (I) применение руководства по учёту объектовых особенностей; (II) определение компенсирующих мер безопасности; и (III) определение установленных агентством параметров в мерах безопасности, где это позволено. В плане обеспечения безопасности системы должны быть задокументированы все работы по адаптации.

2.5.1 Руководство по учёту объектовых особенностей

Руководство по учёту объектовых особенностей предоставляет агентству конкретные положения и условия по применимости и реализации отдельных мер безопасности в базовых наборах мер безопасности, определенных в NIST SP 800-53. Несколько рассмотрений, описанных ниже, могут потенциально воздействовать на то, как меры обеспечения базового уровня безопасности применяются агентством. Планы обеспечения безопасности систем должны ясно определять, какие меры безопасности используют руководство по учёту объектовых особенностей, и включать описание видов рассмотрений, которые были сделаны. Применение руководства по учёту объектовых особенностей должно быть рассмотрено и одобрено санкционирующим должностным лицом информационной системы.

Рассмотрения, связанные с технологией -

- Меры безопасности, которые обращаются к конкретным технологиям (например, беспроводная связь, криптография, инфраструктура публичных ключей) должны применяться только если эти технологии используются или требуются для использования в информационной системе.
- Меры безопасности должны применяться только к тем компонентам информационной системы, которые, как правило, обеспечивают возможности безопасности, определяемые минимальными требованиями безопасности.

- Меры безопасности, которые могут быть или явно, или неявно поддержаны автоматизированными механизмы не должны требовать разработки таких механизмов, если механизмы уже существуют или доступны в коммерческих или правительственных стандартных продуктах. Чтобы удовлетворить минимальные требования безопасности в ситуациях, когда автоматизированные механизмы не доступны или технически не выполнимы, должны использоваться компенсирующие меры безопасности, реализуемые через неавтоматизированные механизмы или процедуры.

Рассмотрения, связанные с общими мерами безопасности -

- Меры безопасности, определяемые агентством как общие меры безопасности, должны, в большинстве случаев, управляться кем-то в организации помимо владельца информационной системы. Каждая мера безопасности в базовом наборе мер безопасности должна определяться или агентством через общие меры безопасности или владельцем информационной системы. Решения о назначении общих мер безопасности не должны, однако, влиять на ответственность агентства по обеспечению необходимых мер безопасности, требуемых, чтобы выполнить минимальные требования безопасности для информационной системы. (Дополнительная информация об общих мерах безопасности представлена в разделе 2.5.3.).

Рассмотрения, связанные с информационными системами открытого доступа -

- Меры безопасности, связанные с информационными системами открытого доступа, должны быть тщательно рассмотрены и примененный с осторожностью, так как некоторые из мер безопасности из указанных базовых наборов мер безопасности (например, меры безопасности персонала, меры идентификации и аутентификации) могут быть не применимы к пользователям, получающим доступ к информационным системам через общие интерфейсы.[12]

Рассмотрения, связанные с инфраструктурой -

- Меры безопасности, которые обращаются к службам агентства (например, контроль физического доступа, такой как блокировки и охрана, контроль за состоянием окружающей среды по температуре, влажности, освещению, огню и энергии), будут применимы только к тем аспектам служб, которые непосредственно обеспечивают защиту, поддержку или связаны с информационной системой (включая активы информационных технологий такие, как электронная почта или веб-серверы, фермы серверов, информационные центры, сетевые узлы, оборудование контроля интерфейсов и оборудование связи).

[12] Например, в то время как меры базового уровня безопасности требуют идентификации и аутентификации персонала организации, который сопровождает и поддерживает информационные системы, которые предоставляют услуги открытого доступа, те же самые меры безопасности, могут не требоваться для пользователей, получающих доступ к этим системам через открытые интерфейсы, чтобы получать публично доступную информацию. С другой стороны, идентификация и аутентификация должны требоваться для пользователей, получающих доступ к информационным системам через открытые интерфейсы доступа к их приватным/персональным данным.

Рассмотрения, связанные с расширяемостью -

- Меры безопасности должны быть масштабируемы в зависимости от размера и комплексности конкретного агентства, реализующего меры безопасности, и уровня воздействия на информационные системы. Расширяемость определяет ширину и глубину реализации мер безопасности. Масштабирование мер безопасности к определенной среде использования требует осмотрительности, чтобы гарантировать рентабельный, основанный на риске подход к реализации мер безопасности.[13]

Рассмотрения, связанные с риском -

- Меры безопасности, которые поддерживают исключительно цели безопасности конфиденциальность, целостность или доступность могут быть понижены до соответствующих мер безопасности в более низком базовом наборе(или соответственно изменены или устранены если не определены в более низком базовом наборе), если, и только если, действие понижения: (I) непротиворечиво с категорированием безопасности по FIPS 199 для соответствующих целей безопасности конфиденциальности, целостности или доступности до перехода к наивысшей оценке.[14] (II) поддержано оценкой риска агентством; и (III) действительно не влияет на информацию, относящуюся к безопасности, в информационной системе.[15]

2.5.2 Компенсирующие меры безопасности

Компенсирующие меры безопасности это управленческие, эксплуатационные или технические меры безопасности, используемые агентством вместо предписанных мер безопасности в низком, умеренном или высоком базовых наборах мер безопасности, которые обеспечивают эквивалентную или сопоставимую защиту для информационной системы. Компенсирующие меры безопасности для информационной системы должны использоваться агентством только при следующих условиях: (I) агентство выбирает компенсирующие меры безопасности из каталога мер безопасности NIST SP 800-53; (II) агентство представляет полное и убедительное обоснование и мотивировку того, что компенсирующие меры обеспечивают эквивалентные возможности безопасности или уровень защиты для информационной системы; и (III) агентство оценивает и формально принимает риск, связанный с использованием компенсирующих мер безопасности в информационной системе. Использование компенсирующих мер безопасности должно быть

[13] Например, план действий при непредвиденных обстоятельствах для крупной и комплексной организации с информационными системами умеренного или высокого воздействия может быть довольно большим и содержать существенное количество деталей реализации. Напротив, план действий при непредвиденных обстоятельствах для небольшой организации с информационной системой низкого воздействия может быть значительно меньше и содержать намного меньше деталей реализации.

[14] Когда используется концепция "наивысшего значения", некоторые из целей безопасности (то есть, конфиденциальность, целостность или доступность) могут быть увеличены до более высокого уровня воздействия. Кроме того, меры безопасности, которые поддерживают исключительно эти цели безопасности должны быть также повышены. Следовательно, организации должны учитывать, что соответствующие и допустимые действия понижения должны гарантировать рентабельное, базируемое на риске применение мер безопасности.

[15] Информацию в информационной системе, относящуюся к безопасности системного уровня (например, файлы пароля, сетевые таблицы маршрутизации, информация управления криптографическими ключами) необходимо отличить от информации пользовательского уровня. Некоторые меры безопасности в информационной системе используются, чтобы поддержать цели безопасности конфиденциальность и целостность как для информации системного уровня, так и для информации пользовательского уровня. Организации должны относиться с осторожностью к понижению мер безопасности, связанных с конфиденциальностью или целостностью, чтобы гарантировать, что действие понижения нет влияет на информацию, важную для безопасности в информационной системе.

рассмотрено, задокументировано в план обеспечения безопасности системы и одобрен санкционирующим должностным лицом для информационной системы.

2.5.3 Общие меры обеспечения безопасности

Общее для агентства представление программы обеспечения информационной безопасности облегчает идентификацию общих мер обеспечения безопасности, которые могут быть применены к одной или более информационным системам агентства. Общие меры обеспечения безопасности могут примениться: (I) ко всем информационным системам агентства; (II) группе информационных систем на конкретном объекте информатизации (иногда ассоциируется с понятием объектовая сертификация/аттестация); или (III) к общим информационным системам, подсистемам или приложениям (то есть, общим аппаратным средствам, программному обеспечению и/или встроенному микропрограммному обеспечению), развертываемым на многих объектах эксплуатации (иногда ассоциируется с понятием типовая сертификация/аттестация). Общие меры обеспечения безопасности, идентифицируемые, как правило, во время общего для агентства процесса с участием CIO, SAISO, санкционирующих должностных лиц, владельцев информационных систем и сотрудников безопасности информационных систем (и менеджеров программ разработки в случае общих мер обеспечения безопасности для общих аппаратных средств, программного обеспечения и/или встроенного микропрограммного обеспечения), имеют следующие свойства:

- Разработка, реализация и оценка общих мер обеспечения безопасности может быть поручена ответственным должностным лицам агентства или структурных единиц (кроме владельцев информационных систем, чьи системы будут реализовать или использовать эти общие меры обеспечения безопасности); и
- Результаты оценки общих мер обеспечения безопасности могут использоваться для поддержки процессов сертификации и аттестации безопасности информационных систем агентства, где эти меры безопасности применяются.

Многие из управленческих и эксплуатационных мер безопасности (например, мер планирования обеспечения безопасности на случай непредвиденных ситуаций, мер обеспечения реакции на инциденты безопасности, мер обучения и освоения безопасности, мер безопасности персонала и мер обеспечения физической безопасности), необходимых для защиты информационных систем могут быть превосходными кандидатами на статус общих мер обеспечения безопасности. Цель состоит в том, чтобы уменьшить стоимость обеспечения безопасности, централизованно управляя разработкой, реализацией и оценкой общих мер обеспечения безопасности, определяемых агентством – и, впоследствии, совместно используя результаты оценки с владельцами информационных систем, где эти общие меры обеспечения безопасности применяются. Меры безопасности, не определяемые как общие меры безопасности, считают *мерами безопасности специфичными для системы* и являются ответственностью владельца информационной системы. Планы обеспечения безопасности систем должны ясно идентифицировать, какие меры безопасности определялись как общие меры обеспечения безопасности и какие меры безопасности определялись как меры безопасности, специфичные для системы.

Для эффективности использования в разрабатываемых планах обеспечения безопасности систем, общие меры обеспечения безопасности должны быть единожды задокументированы и затем вставляться или импортироваться в каждый план обеспечения безопасности информационных систем в агентстве. Человек, ответственный за реализацию общих мер безопасности, должен быть указан в плане обеспечения безопасности. Максимальная эффективность применения общих мер обеспечения безопасности в процессе планирования безопасности систем зависит от следующих факторов:

- Агентство имеет разработанное, задокументированное и распространенное специальное руководство по идентификации общих мер обеспечения безопасности;
- Агентство возложило ответственность за координацию идентификации и рассмотрения общих мер обеспечения безопасности и согласование обозначения общих мер безопасности на официальных должностных лиц руководства с обязанностями по программам обеспечения безопасности, такими как CIO или SAISO;
- Владельцы систем должны быть информированы о процессе планирования обеспечения безопасности систем, включая использование общих мер безопасности; и
- Как часть процесса должно осуществляться консультирование с экспертами агентства в установленных областях общих мер обеспечения безопасности.

Агентство может также назначить гибридный статус на меры безопасности в ситуациях, где одна часть меры безопасности, как полагают, является общей, в то время как другая часть меры безопасности, как полагают, специфична для системы. Например, агентство может рассматривать меру безопасности IR-1 (Политика и процедуры реакции на инциденты), как гибридную меру безопасности, принимаемую как общую в части политики меры безопасности, и принимаемую как специфическую для систем в части процедур обеспечения безопасности. Гибридные меры безопасности могут также служить шаблонами для дальнейшего усовершенствования мер безопасности. Агентство может хотеть, например, реализовать меру безопасности CP 2 (План действий при непредвиденных обстоятельствах) как основной шаблон для обобщенного плана действий при непредвиденных обстоятельствах для всех информационных систем агентства с конкретной адаптацией планов владельцами информационных систем, где требуется, для специфичных для системы проблем.

Владельцы информационных систем ответственны за любые специфичные для систем проблемы, связанные с реализацией общих мер обеспечения безопасности агентства. Эти проблемы идентифицируются и описываются в планах обеспечения безопасности конкретных информационных систем. SAISO, действующий от имени CIO, должен координировать с должностными лицами агентства (например, менеджерами по средствам, начальниками отделов, руководителями отделов кадров), ответственными за разработку и реализацию установленных общих мер обеспечения безопасности, чтобы гарантировать, что требуемые меры безопасности используются, меры безопасности оценены, и результаты оценки используются совместно с соответствующими владельцами информационных систем.

Разделение мер безопасности на общие меры обеспечения безопасности и специфичных для систем меры безопасности может иметь результат в существенной экономии для агентства в стоимости разработки и реализации мер безопасности. Это может также иметь результат в более непротиворечивом применении мер безопасности для агентства в целом. Кроме того, такая-же экономия может иметь место в процессе сертификации и аттестации безопасности. Вместо того, чтобы оценивать общие меры обеспечения безопасности в каждой информационной системе, аттестация использует любые применимые результаты актуальнейшей оценки общих мер обеспечения безопасности, выполненные на уровне агентства. Общий для агентства подход к повторному и совместному использованию результатов оценки может значительно улучшить действенность сертификаций и аттестаций безопасности, проводимых агентством, и значительно уменьшить стоимость программы обеспечения безопасности.

Несмотря на то, что концепция разделения мер безопасности на общие меры безопасности и специфичные для системы меры безопасности проста и интуитивна, применение этого принципа в агентстве требует планирования, координация и настойчивости. Если агентство только начинает реализовывать этот подход или только частично реализовало этот подход, это может потребовать времени, чтобы извлечь максимальную пользу из разделения мер безопасности и связанного повторного использования свидетельств оценки. Из-за потенциальной зависимости от общих мер безопасности многих из информационных систем агентства, нарушение общих мер безопасности может иметь результат в существенном увеличении риска на уровне агентства - риска, являющегося результатом деятельности систем, которые зависят от этих мер безопасности.

3. Разработка плана

Остаток от этого документа руководит читателем в написании плана безопасности системы, включая логические шаги, которым необходимо следовать в подходящей разработке плана, рекомендованную структуру и содержание, и то, как максимально использовать текущие публикации NIST в эффективной поддержке работы по планированию обеспечения безопасности системы. До инициирования работ должна быть установлена политика агентства в отношении того, как должен осуществляться контроль и доступ к планам обеспечения безопасности информационных систем.

3.1 Название и идентификатор системы

Первым элементом, указываемым в плане обеспечения безопасности системы, является название и идентификатор системы. Как требуется в Циркуляре OMB A-11, каждой системе нужно назначить название и уникальный идентификатор. Присвоение уникального идентификатора поддерживает возможность агентства легко собирать информацию по агентству и специфические для системы метрики безопасности, а также облегчает полную отслеживаемость по всем требованиям, связанным с реализацией и применением системы. Идентификатор должен остаться одним и тем же в течение жизни системы и сохраняться в журналах регистрации, связанных с использованием системы.

3.2 Категорирование системы

Каждая система, идентифицированная в реестре систем агентства, должно категорироваться, с использованием FIPS 199. NIST Специальная Публикация 800-60, *Руководство для отображения типов информации и информационных систем к категориям безопасности,* обеспечивает руководство реализации по выполнению этой работы. См. Таблицу 1 для сводки категорий FIPS 199.

3.3 Владелец системы

В плане безопасности каждой систем**ы** должен быть определён назначенный владелец системы. Этот человек - ключевая точка контакта (POC) для системы и ответственен за координацию работ жизненного цикла разработки систем (SDLC), применительно к системе. Важно, чтобы этот человек имел соответствующие знания возможностей и функциональности системы. Назначение владельца системы должно быть задокументировано в письменной форме, и план должен включать следующую контактную информацию:

- Имя
- Должность
- Агентство
- Адрес
- Номер телефона
- Адрес электронной почты

	ПОТЕНЦИАЛЬНОЕ ВОЗДЕЙСТВИЕ		
Цель безопасности	**НИЗКО**	**УМЕРЕННО**	**ВЫСОКО**
Конфиденциальность **“Сохранение авторизованных ограничений на доступ и раскрытие информации, включая средства по защите неприкосновенности частной жизни и конфиденциальной информации …”** **[44 U.S.C. США, Секция 3542]**	Несанкционированное разглашение информации, как ожидается, будет иметь **ограниченное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированное разглашение информации, как ожидается, будет иметь **серьезное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированное разглашение информации, как ожидается, будет иметь **тяжелое или катастрофическое** отрицательное воздействие на деятельность организации, активы организации или людей.
Целостность **“Принятие мер против несанкционированной модификации или разрушения информации, включая гарантирование неотказуемости от информации и её аутентичности …”** **[44 U.S.C. США, Секция 3542]**	Несанкционированная модификация или разрушение информации, как ожидается, будет иметь **ограниченное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированная модификация или разрушение информации, как ожидается, будет иметь **серьезное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированная модификация или разрушение информации, как ожидается, будет иметь **тяжелое или катастрофическое** отрицательное воздействие на деятельность организации, активы организации или людей.
Доступность **“Гарантирование своевременного и надежного доступа к и использования информации …”** **[44 U.S.C. США, Секция 3542]**	Прекращение доступа к или использования информации или информационной системы, как ожидается, будет иметь **ограниченное** отрицательное воздействие на деятельность организации, активы организации или людей.	Прекращение доступа к или использования информации или информационной системы, как ожидается, будет иметь **серьезное** отрицательное воздействие на деятельность организации, активы организации или людей.	Прекращение доступа к или использования информации или информационной системы, как ожидается, будет иметь **тяжелое или катастрофическое** отрицательное воздействие на деятельность организации, активы организации или людей.

Таблица 1: Категорирование по FIPS 199

3.4 Санкционирующее должностное лицо

В плане обеспечения безопасности системы каждой системы должно быть определено санкционирующее должностное лицо. Этот человек - высшее должностное лицо руководства у кого есть полномочия по санкционированию деятельности (аттестации) информационной системы (главного приложения или системы общей поддержки) и принятию остаточного риска, связанного с системой. Назначение санкционирующего должностного лица должно быть в письменной форме, и план должен содержать контактную информацию, которая указана в разделе 3.3.

3.5 Другие контакты

Этот раздел должен содержать имя другого ключевого контактного персонала, которому могут адресоваться запросы относительно характеристик и эксплуатации системы. Для каждого человека, указанного в этом разделе должна быть указана та же самая информация, которая перечислена в Разделе 3.3.

3.6 Назначение ответственности за обеспечения безопасности

В агентстве должна быть определена персональная ответственность за каждую систему. Это может быть выполнено разными способами. В некоторых агентствах, общая ответственность может быть делегированная SAISO. Часто, SAISO поддерживается структурой сотрудников безопасности, назначенных на каждый главный компонент. Эти сотрудники безопасности могут иметь санкции по определению требований безопасности для всех систем в пределах их домена полномочий. Другие модели могут сегментировать эту ответственность другими способами, основанными на структуре и ответственности агентства. По этим людям должна быть предоставлена та же самая контактная информация, которая указана в разделе 3.3. Очень важно то, чтобы эта ответственность была формализована в письменной форме или в описании должности сотрудника или делегирована меморандумом.

3.7 Эксплуатационный статус системы

Указывает один или более из следующих для эксплуатационных статусов системы. Если выбран более чем один статус, указывается, какая часть системы находится в каждом статусе.

- *Эксплуатация* - система действует.
- *Разрабатывается* - система проектируется, разрабатывается или реализуется.
- *Подвергается значительной модификации* - система подвергается значительному преобразованию или развитию.

Если система разрабатывается или подвергается значительной модификации, предоставляется информацию о методах, используемых чтобы гарантировать, что включены соответствующие требования безопасности. В соответствующие разделы плана включаются соответствующие меры безопасности в зависимости от того, где система находится в жизненном цикле безопасности.

3.8 Тип информационной системы

Этот раздел плана указывает, является ли система главным приложением или системой общей поддержки. Если система содержит второстепенные приложения, опишите их в разделе плана Общее описание/Назначение. Если у агентства есть дополнительные категории типов информационных систем, измените шаблон, чтобы включать другие категории.

3.9 Общее описание/Назначение

Составьте краткое описание (один - три абзаца) функций и назначения системы (например, экономические показатели, сетевая поддержка для агентства, коммерческий анализ данных переписи, поддержка создания отчетов).

Если система является системой общей поддержки, перечислите все приложения, поддерживаемые системой общей поддержки. Определите, является ли или нет приложение главным приложением, и включите уникальное имя / идентификатор, где применимо. Опишите функцию каждого приложения и обрабатываемую информацию. Включите список организаций пользователей, определите, являются ли они внутренними или внешними к агентству владельцу системы.

3.10 Среда системы

Обеспечивает резюме (один - три абзаца) общего описания технической системы. Включает любые факторы среды или технические факторы, которые повышают специальные проблемы безопасности, такие, как использование персональных цифровых секретарей, беспроводных технологий, и т.п. Обычно, среды эксплуатации являются следующими:

- **Автономный или малый офис / домашний офис (SOHO)** описывает небольшие, неформальные компьютерные установки, которые используются для домашних или бизнес-целей. Автономный офис охватывает множество небольших сред и устройств, от ноутбуков, мобильных устройств или домашних компьютеров до систем, работающих дистанционно, до предприятий малого бизнеса и небольших филиалов компаний.

- **Управление или Предприятие**, как правило, большие системы агентства с определенными, организованными комплектами аппаратных и программных конфигураций, обычно состоящие из централизованно управляемых рабочих станций и серверов, защищенных от Интернета межсетевыми экранами и другими устройствами сетевой безопасности.

- **Пользовательские** среды включают системы, в который функциональность и степень безопасности не соответствуют другим средам. Две типичных пользовательских среды это **Специализированная, ограниченная безопасностью функциональность и Наследство**:

  - **Специализированная, ограниченная безопасностью функциональность**. Среда Специализированной, ограниченной безопасностью функциональности включает системы и сети с высоким риском атак или воздействий на данные, с безопасностью, имеющей приоритет над функциональностью. Она предполагает системы ограниченной или специализированной (рабочие станции или системы не общего назначения) функциональности в среде, подверженной значительным угрозам, такие как внешний межсетевой экран или публичный Web сервер, или чей контент данных или предназначение имеют такое значение, что значительные компромиссы в пользу безопасности перевешивают потенциальные отрицательные последствия для других полезных системных атрибутов, таких как унаследованные приложения или функциональная совместимость с другими системами. Среда Специализированной, ограниченной безопасностью функциональности может быть подмножеством другой среды.

  - **Наследство**. Среда Наследства содержит более старые системы или приложения, которые могут использовать более старые, менее - безопасные коммуникационные механизмы. Другим машинам, работающим в среде Наследства, возможно, необходимы менее ограниченные установки безопасности для того, чтобы они могли взаимодействовать с унаследованными системами и приложениями. Среда Наследства может быть подмножеством автономной или управляемой среды.[16]

[16] Для подробного объяснения системных сред, см. NIST Специальная Публикация 800-70, *Программа контрольных списков конфигурации безопасности для продуктов ИТ - Руководство по контрольным спискам для пользователей и разработчиков*.

3.11 Взаимосвязь систем/ Совместное использование информации

Взаимосвязь систем представляет собой прямую связь двух или больше IT-систем для совместного использования информационных ресурсов. Взаимосвязь систем, если она не защищена соответствующим образом, может иметь результат в компрометации всех соединенных систем и данных, которые они хранят, обрабатывают или передают. Важно, чтобы владельцы систем, владельцы информации и руководство получили как можно больше информации относительно уязвимостей, связанных с взаимосвязями систем и совместным использованием информации. Это важно для выбора соответствующих мер безопасности, требуемых чтобы смягчить эти уязвимости. Соглашение о безопасности взаимосвязи (ISA), Меморандум о взаимопонимании (MOU) или Меморандум о соглашении (MOA) необходимы между системами (не относится к взаимосвязи между рабочими станциями/рабочими столами или системами, к которым получают публичный доступ) где имеются общие данные, которые принадлежат или управляются различными организациями. IS не требуется для внутренних систем агентства, если агентство руководствуется и проводит в жизнь твердый жизненный цикл разработки систем, который требует санкционирования и одобрения обеспечения согласия с требованиями безопасности. Для дополнительной информации о взаимосвязях, см. NIST SP 800-47, *Руководство по обеспечению безопасности для взаимодействующих систем информационных технологий.*

В этом разделе, для ***каждой взаимосвязи*** между системами, которые принадлежат или управляются различными организациями, предоставляется следующая информация относительно санкционирования для соединения с другими системами или обмена информацией:

Название системы;

Организация;

Тип взаимосвязи (Интернет, Коммутируемый доступ, и т.д.);

Санкционирование для взаимосвязи (MOU/MOA, ISA);

Дата соглашения;

Категории по FIPS 199;

Статус сертификации и аттестации систем; и

Имя и должность санкционирующего должностного лица (лиц).

Для агентств с многочисленными взаимосвязями, хорошим способом представить информацию может быть формат таблицы, содержащей вышеупомянутую информацию.

3.12 Законы, нормативные акты и политики, влияющие на системы

Перечень любых законов, нормативных актов или политик, которые устанавливают конкретные требования для конфиденциальности, целостности или доступности системы и информации, хранимой, передаваемой или обрабатываемой системой. Общие требования безопасности агентства не нуждаются в перечислении, так как они определяют указания по безопасности для

всех систем. Каждое агентство должно установить уровень законов, нормативных актов и политик для включения в план обеспечения безопасности систем. Примерами могут служить Закон о

неприкосновенности частной жизни от 1974 года или конкретный законодательный, или нормативный акт, касающийся обрабатываемой информации (например, налоговой информации или информация переписи). Если обрабатываемые системой сведения подчинены Закону о неприкосновенности частной жизни, включайте сведения о количестве и названиях системы(м), подчиненных Закону о неприкосновенности частной жизни, и использовании системы(м) для соответствующих вычислительных работ.

3.13 Выбор мер безопасности

При подготовке к документированию того, как меры безопасности NIST SP 800-53 для применимых базовых наборов мер безопасности (низких - умеренных - или высоких воздействий на информационные системы) реализованы или планируются быть реализованными, меры безопасности, содержавшиеся в базовых наборах, должны быть пересмотрены и возможно адаптированы. Для определения применимости или адаптации отдельных мер безопасности, должно использоваться руководства по учёту объектовых особенностей, изложенное в Разделе 2.5.1. Дополнительно, должны быть определены и затем задокументированы в план меры безопасности, которые являются общими для многих систем или для всего агентства. Смотрите Раздел 2.5.3 для руководства о том, как общие меры безопасности должны быть определены, задокументированы и координироваться. Процесс выбора соответствующих мер безопасности и применения руководств по учёту объектовых особенностей, чтобы достигнуть *адекватной безопасности*[17], является многоаспектным, базируемые на риске работы, использующие управленческий и эксплуатационный персонал агентства, должны быть проведены прежде, чем часть мер безопасности включена в план.

- Для информационных систем *низкого воздействия* агентство, как минимум, должно использовать меры безопасности низкого базового набора мер безопасности, определенного в NIST SP 800-53, и должно гарантировать, что минимальные требования доверия, связанные с низким базовым набором мер, удовлетворены.
- Для информационных систем *умеренного воздействия* агентство, как минимум, должно использовать меры безопасности умеренного базового набора мер безопасности, определенного в NIST SP 800-53, и должно гарантировать, что минимальные требования доверия, связанные с умеренным базовым набором мер, удовлетворены.
- Для информационных систем *высокого воздействия* агентство, как минимум, должно использовать меры безопасности высокого базового набора мер безопасности, определенного в NIST SP 800-53, и должно гарантировать, что минимальные требования доверия, связанные с высоким базовым набором мер, удовлетворены.

3.14 Минимальные меры безопасности

После того, как меры безопасности выбраны, адаптированы и определены общие меры безопасности, описывается каждая мера безопасности. Описание должно содержать: 1) заголовок меры безопасности; 2) как мера безопасности реализуется или как планируется быть реализованной; 3) руководства по учёту объектовых особенностей, которое было применено и

[17]) Циркуляр А-130, Приложение III Министерства управления и бюджета (OMB), определяет адекватную безопасность как безопасность, соразмерную с риском и величиной вреда, следующего из потери, неправильного употребления, или несанкционированного доступа к или модификации информации.

какой вид рассмотрения; и 4) указание, является ли мера безопасности общей мерой безопасности, и кто ответственен за ее реализацию.

У мер безопасности в каталоге мер безопасности (NIST SP 800-53, Приложение F) есть четко определенная организация и структура. Для простоты использования в процессе выбора и спецификации мер безопасности, меры безопасности организованы в классы и семейства. Есть три общих класса мер безопасности (то есть, управленческие, эксплуатационные, и технические[18]). Каждое семейство содержит меры безопасности, связанные с функцией безопасности семейства. Стандартизированный, двух-символьный идентификатор предназначен для однозначного определения каждого семейства мер безопасности. Таблица 2 суммирует классы и семейства в каталоге меры безопасности и соответствующие идентификаторы семейств.

КЛАСС	СЕМЕЙСТВО	ИДЕНТИФИКАТОР
Управленческие	Оценка риска	RA
Управленческие	Планирование	PL
Управленческие	Закупки систем и сервисов	SA
Управленческие	Аттестационные испытания, аттестация и оценка безопасности	CA
Эксплуатационные	Безопасность персонала	PS
Эксплуатационные	Физическая защита и защита окружения	PE
Эксплуатационные	Планирование действий в чрезвычайных ситуациях	CP
Эксплуатационные	Управление конфигурацией	CM
Эксплуатационные	Поддержка	MA
Эксплуатационные	Целостность систем и информации	SI
Эксплуатационные	Защита носителей	MP
Эксплуатационные	Реагирование на инциденты	IR
Эксплуатационные	Освоение и подготовка	AT
Технические	Идентификация и аутентификация	IA
Технические	Контроль доступа	AC
Технические	Аудит и подконтрольность	AU
Технические	Защита систем и коммуникаций	SC

Таблица 2: Классы, семейства и идентификаторы мер безопасности

Названия классов мер безопасности (то есть, управленческие, эксплуатационные и технические), определены ниже для разъяснения при подготовке планов обеспечения безопасности систем. ***Управленческие меры безопасности*** сосредотачиваются на управлении информационной системой и управлении риском для системы. Это технологии и интересы, которые обычно относятся к управлению. ***Эксплуатационные меры безопасности*** относятся к методам безопасности, сосредоточенным на механизмах, реализуемых и выполняемых, прежде всего, людьми (в противоположность системам). Эти меры безопасности применяются для того, чтобы

[18] Семейства меры безопасности в NIST SP 800-53 связаны с одним из трех классов мер безопасности (то есть, управленческие, эксплуатационные, технические). Семейства связывают с соответствующими классами основываясь на доминирующих характеристиках мер безопасности в этих семействах. Многие меры безопасности, однако, могут быть логически связаны с более чем одним классом. Например, мера CP 1, политика и процедуры контроля из семейства Планирование действий в чрезвычайных ситуациях (Contingency Planning), указана как эксплуатационная мера безопасности, но кроме того имеет характеристики, которые также непротиворечивы с управлением безопасностью.

улучшить безопасность определенной системы (или группы систем). Они часто требуют технической или специализированной компетентности и часто полагаются на управленческие действия, а также на технические меры безопасности. ***Технические меры безопасности*** сосредотачиваются на мерах безопасности, которые выполняет компьютерная система. Меры безопасности могут обеспечить автоматизированную защиту от несанкционированного доступа или неправильного использования, облегчить обнаружение нарушений защиты и поддержать требования безопасности для приложений и данных.

3.15 Даты завершения и санкционирования

Должна быть определена дата окончания плана обеспечения безопасности системы. Дата окончания должна уточняться всякий раз, когда план периодически пересматривается и обновляется. Когда система обновляется, должен быть добавлен номер версии. План обеспечения безопасности системы должен также содержать дату официального санкционирования или одобрения плана назначенным органом одобрения. Документация одобрения, то есть, документ по аттестации, меморандум одобрения, должна находиться в деле или быть присоединена как часть плана.

3.16 Текущая поддержка плана обеспечения безопасности системы

План обеспечения безопасности информационной системы разрабатывается однажды, важно периодически оценивать план, рассматривая любые изменения в статусе, функциональности, проекте и т.д. системы, и гарантировать, что план продолжает содержать корректную информацию о системе. Эта документация и ее корректность являются критическими для действий по аттестационным испытаниям системы. Все планы должны быть пересматриваться и обновляться, как соответствующе, по крайней мере, ежегодно. Некоторыми событиями, которые включаются в пересмотр, являются:

- Изменение владельца информационной системы;
- Изменение представителя по информационной безопасности;
- Изменение в архитектуре системы;
- Изменение в статусе системы;
- Дополнения/удаления взаимосвязей системы;
- Изменение в расположении системы;
- Изменение санкционирующего должностного лица; и
- Изменение статуса аттестационных испытаний и аттестации.

Приложение А: Типовой шаблон плана обеспечения безопасности информационной системы

Следующий образец приведен ТОЛЬКО как пример. Агентства могут быть использовать другие форматы и выбирать их для модификации, чтобы устранить любые имеющиеся недостатки, основываясь на этом руководстве. Он не является обязательным форматом; есть понимание того, что многие агентства и поставщики услуг информационной безопасности, могут разрабатывать и реализовывать различные подходы для разработки и представления плана обеспечения безопасности информационной системы, чтобы удовлетворить их собственным потребностям в гибкости.

Шаблон плана обеспечения безопасности информационной системы

1. Название/наименование информационной системы:

- Уникальный идентификатор и название, данные системе.

2. Категория информационной системы:

- Определите соответствующую категорию из FIPS 199.

	НИЗКО		УМЕРЕННО		ВЫСОКО

3. Владелец Информационной системы:

- Имя, должность, агентство, адрес, адрес электронной почты и номер телефона человека, который является владельцем системы.

4. Санкционирующее должностное лицо:

- Имя, должность, агентство, адрес, адрес электронной почты и номер телефона лица из высшего руководства, официально определённого как санкционирующее должностное лицо.

5. Другие контакты:

- Перечислите других ведущих специалистов, если имеются; включая их имя, адрес, адрес электронной почты и номер телефона.

6. Назначенный ответственный за обеспечение безопасности:

- Имя, должность, адрес, адрес электронной почты и номер телефона человека, который является ответственным за безопасность системы.

7. Эксплуатационный статус информационной системы:

- Укажите на эксплуатационный статус системы. Если выбран более чем один статус, опишите какая часть системы находится под каждым статусом.

	Эксплуатация		В разработке		Значительная модификация

8. Тип информационной системы:

- Укажите, является ли система главным приложением или системой общей поддержки. Если система содержит незначительные приложения, перечислите их в Разделе 9. Общее Системное Описание/Назначение.

	Главное приложение		Система общей поддержки

9. Общее описание /назначение системы

- Опишите функцию или назначение системы и информационных процессов.

10. Среда системы

- Приведите общее описание технической системы. Включайте основные аппаратные средства, программное обеспечение и оборудование связи.

11. Взаимосвязи системы /Совместное использование информации

- • Перечислите взаимодействующие системы и идентификаторы систем (если применимо), приведите имя системы, организации, тип системы (главное приложение или система общей поддержки), укажите, содержатся ли в перечне ISA/MOU/MOA, дату соглашения о взаимодействии, категорию FIPS 199, статус C&A и имя санкционирующего должностного лица.

Название системы	Организация	Тип	Соглашение (ISA/MOU/MOA)	Дата	Категория FIPS 199	Статус C&A	Санкционирующее должностное лицо

12. Применимые Законы/Нормативные документы/Политики

- Перечислите любые законы или нормативные документы, которые устанавливают конкретные требования для конфиденциальности, целостности или доступности данных в системе.

13. Минимальные меры безопасности

Выберите соответствующий минимальный базовый набор мер безопасности (низкое - умеренное - высокое воздействие) из NIST SP 800-53, затем обеспечьте полное описание того, как все минимальные меры безопасности в применимом базовом наборе реализуются или планируются быть реализованными. Описание должно содержать: 1) заголовок меры безопасности; 2) как мера безопасности реализуется или планируется быть реализованной; 3) любое Руководство по учёту объектовых особенностей, которое было применено и для какого типа рассмотрения; и 4) укажите, является ли мера безопасности общей мерой безопасности, и кто ответственен за её реализацию.

14. Дата завершения плана обеспечения безопасности информационной системы: _____

- Введите дату завершения плана.

15. Дата санкционирования плана обеспечения безопасности информационной системы: _____

- Введите дату, когда план обеспечения безопасности системы был одобрен, и укажите, если документация по санкционированию приложена к плану или находится в деле.

Приложение B: Глоссарий

ОБЩИЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Accreditation Аттестация [NIST SP 800-37]	Официальное управленческое решение, принимаемое высшим должностным лицом агентства для того, чтобы разрешить эксплуатацию информационной системы и явно принять риск в отношении деятельности агентства (включая предназначение, функции, имидж или репутацию), активов агентства, людей, других организаций и Нации, основанное на реализации согласованного набор мер безопасности.
Accreditation Boundary Граница аттестации [NIST SP 800-37]	Все компоненты информационной системы, которая аттестована санкционирующим должностным лицом, исключая отдельно санкционированные системы, с которыми соединена информационная система. Синоним с термином периметр безопасности, определенным в Инструкции CNSS 4009 и DCID 6/3.
Accrediting Authority Орган аттестации	См. *Санкционирующее должностное лицо*
Adequate Security Адекватная Безопасность [Циркуляр OMB A-130, Приложение III]	Безопасность, соразмерная с риском и величиной вреда, следующим из потери, неправильного употребления или несанкционированного доступа к или модификации информации.
Agency Агентство	См. *Исполнительное агентство.*
Authentication Аутентификация	Проверка идентификационных данных пользователя, процесса или устройства, обычно как предпосылка к предоставлению доступа к ресурсам в информационной системе.
Authenticity Аутентичность	Свойство, определяющее подлинность и возможность проверять и доверять; уверенность в законности передачи, сообщения или автора сообщения. См. *Аутентификация*.
Authorize Processing Санкционирование обработки	См. *Аттестация*.
Authorizing Official Санкционирующее должностное лицо [NIST SP 800-37]	Должностное лицо с полномочием по формальному принятию на себя ответственности за эксплуатацию информационной системы на допустимом уровне риска в отношении деятельности агентства (включая предназначение, функции, имидж или репутацию), активов агентства или людей.
Availability Доступность [44 U.S.C., Sec. 3542]	Обеспечение своевременного и надежного доступа к и использования информации.
Certification	Всесторонняя оценка организационных, эксплуатационных и

Аттестационные испытания [NIST SP 800-37]	технических мер безопасности в информационной системе, делаемая в поддержку аттестации безопасности, чтобы определить степень, до которой меры обеспечения реализованы правильно, эксплуатируются как предназначено и производят желаемый результат относительно выполнения требований безопасности для системы.
Certification Agent Агент по аттестационным испытаниям [NIST SP 800-37]	Человек, группа или организация, уполномоченные на проведение аттестационных испытаний безопасности.
Chief Information Officer Директор по информации [PL 104-106, Раздел 5125 (b)]	Должностное лицо агентства, ответственное за: (I) предоставление консультаций и другой помощи руководителю исполнительного агентства и другому персоналу высшего руководства агентства, чтобы гарантировать, что информационные технологии приобретаются и информационные ресурсы управляются в способе, который непротиворечив с законами, Правительственными распоряжениями, директивами, политиками, нормативными актами и приоритетами, установленными руководителем агентства; (II) разработку, поддержание и облегчение реализации осмысленной и интегрированной архитектуры информационных технологий для агентства; и (III) продвижение эффективного и рационального конструирования и использования всех основных информационных ресурсов процессов управления для агентства, включая улучшение процессов работы агентства.
Common Security Control Общая мера безопасности [NIST SP 800-37]	Мера безопасности, которая может быть применена к одной или более информационных систем агентства и имеет следующие свойства: (I) разработка, реализация и оценка меры безопасности может быть поручена ответственному должностному лицу или организационному элементу (другому, чем владелец информационной системы); и (II) результат оценки меры безопасности может быть использован для поддержки процессов аттестационных испытаний безопасности и аттестации информационных систем агентства, где эта мера безопасности может быть применена.
Compensating Security Controls Компенсирующие меры безопасности	Управленческие, эксплуатационные и технические меры безопасности (т.е., меры защиты или контрмеры), применяемые организациями вместо рекомендуемых мер в низком, умеренном или высоком базовых наборах мер безопасности, описанных в NIST Специальной Публикации 800-53, которые обеспечивают эквивалентную или сопоставимую защиту для информационной системы.
Confidentiality Конфиденциальность [44 U.S.C., Sec. 3542]	Сохранение установленных ограничений на доступ к и раскрытие информации, включая средства для защиты неприкосновенности частной жизни и конфиденциальной информации.

Configuration Control Контроль конфигурации [CNSSI 4009]	Процесс контроля модификации аппаратных средств, встроенного микропрограммного обеспечения, программного обеспечения и документации, чтобы защитить информационную систему от ненадлежащих модификаций до, вовремя и после реализации системы.
Countermeasures Контрмеры [CNSSI 4009]	Действия, устройства, процедуры, технологии или другие меры, которые уменьшают уязвимость информационной системы. Синоним с мерами безопасности и мерами защиты.
Executive Agency Исполнительное агентство [41 U.S.C., Sec. 403]	Исполнительный департамент, определенный в 5 U.S.C., Раздел 101; военный департамент, определённый в 5 U.S.C., Раздел 102; независимое учреждение, как определено в 5 U.S.C., Раздел 104 (1); и полностью находящаяся в собственности Правительства корпорация, полностью попадающая под действие 31 U.S.C., Глава 91.
Federal Enterprise Architecture Архитектура федерального предприятия [Офис управления Программой FEA]	Базирующаяся на деятельности основа для общеправительственного усовершенствования, разработанная Министерством управления и бюджета, которая предназначена, чтобы облегчить усилия по преобразованию федерального правительства к тому, которое ориентируется на гражданина, ориентируется на результат и основывается на рынке.
Federal Information System Федеральная информационная система [40 U.S.C., Sec. 11331]	Информационная система, которая используется или управляется исполнительным агентством, подрядчиком исполнительного агентства или другой организацией от имени исполнительного агентства.
General Support System Система общей поддержки [OMB Circular A-130, Appendix III]	Взаимосвязанный набор информационных ресурсов под некоторым прямым административным управлением, которые предоставляют общую функциональность. Система обычно включает аппаратные средства, программное обеспечение, информацию, данные, приложения, связь и людей.
High-Impact System Система высокого воздействия [FIPS 200]	Информационная система, в которой, по крайней мере, одной цели безопасности (то есть, конфиденциальности, целостности или доступности) назначено, в соответствии с FIPS Публикацией 199, значение потенциала воздействия «высокий».
Information Owner Владелец информации [CNSSI 4009]	Должностное лицо с установленными законом или исполнительными полномочиями для указанной информации и ответственностью за установление мер безопасности по ее генерации, сбору, обработке, распространению и ликвидации.
Information Resources Информационные ресурсы [44 U.S.C., Sec. 3502]	Информация и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии.
Information Security	Защита информации и информационных систем от

Информационная безопасность [44 U.S.C., Sec. 3542]	несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения, с целью обеспечения конфиденциальности, целостности и доступности.
Information Security Policy Политика информационной безопасности [CNSSI 4009]	Совокупность директив, нормативных актов, правил и методов, которые предписывают, как организации управлять, защищать и распределять информацию.
Information System Информационная система [44 U.S.C., Sec. 3502]	Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или ликвидации информации.
Information System Owner (or Program Manager) Владелец информационной системы (или менеджер программы) [CNSS Inst. 4009, Уточнённая]	Должностное лицо, ответственное в целом за приобретение, разработку, интеграцию, модификацию или эксплуатацию и поддержку информационной системы.
Information System Security Officer Сотрудник безопасности информационной системы [CNSSI Inst. 4009,Уточнённая]	Человек с возложенной ответственностью высшим должностным лицом агентства по информационной безопасности, санкционирующим должностным лицом, должностным лицом руководства или владельцем информационной системы за поддержание соответствующего эксплуатационного состояния безопасности для информационной системы или программы.
Information Technology Информационная технология [40 U.S.C., Sec. 1401]	Любое оборудование или взаимосвязанная система, или подсистема оборудования, которое используется в автоматизированном получении, хранении, манипулировании, управлении, перемещении, контроле, показе, переключении, обмене, передаче или приеме данных, или информации исполнительным агентством. Для целей предыдущего предложения, оборудование используется исполнительным агентством, если оборудование используется исполнительным агентством непосредственно или используется подрядчиком в соответствии с контрактом, с исполнительным агентством который: (I) требует использования такого оборудования; или (II) требует использования, до существенной степени, такого оборудования в исполнении сервиса или оснащении продукта. Термин информационная технология включает компьютеры, вспомогательное оборудование, программное обеспечение, встроенное микропрограммное обеспечение, и подобные процедуры, сервисы (включая службу поддержки) и связанные ресурсы.
Information Type Тип информации	Конкретная категория информации (например, приватная, медицинская, имущественная, финансовая, следственная,

[FIPS 199]	чувствительная для подрядчика, управления безопасностью) определенная организацией или, в некоторых случаях, согласно конкретному закону, Правительственному распоряжению, директиве, политике или нормативному документу.
Integrity Целостность [44 U.S.C., Sec. 3542]	Защита против неправомерной модификации или уничтожения информации, включающая обеспечение неотказуемости и аутентичности информации.
Label Метка	См. *Метка безопасности.*
Low-Impact System Система низкого воздействия [FIPS 200]	Информационная система, в который всем трём целям безопасности (то есть, конфиденциальности, целостности и доступности) назначено, в соответствии с FIPS Публикацией 199, значение потенциала воздействия низкий.
Major Application Главное приложение [OMB Circular A-130, Appendix III]	Приложение, которое требует особого внимания к безопасности вследствие риска и величина вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации в приложении. Примечание: Все федеральные приложения требуют некоторого уровня защиты. Однако некоторые приложения, из-за информации в них, требуют специального надзора руководства и должны быть рассмотрены как главные. Адекватная безопасность для других приложений должна быть обеспечена безопасностью систем, в которых они работают.
Major Information System Главная информационная система [OMB Circular A-130]	Информационная система, которая требует специального внимания руководства из-за её важности для предназначения агентства; высоких затрат на её разработку, эксплуатацию или поддержку; или её существенной роли в администрировании программ, финансов, собственности или других ресурсов агентства.
Management Controls Управленческие меры безопасности [NIST SP 800-18]	Меры безопасности (т.е. меры защиты или контрмеры) для информационной системы, которые фокусируются на управлении риском и управлении безопасностью информационной системы.
Media Access Control Address Адрес контроля доступа сети связи	Аппаратный адрес, который однозначно идентифицирует каждый компонент сети на основе IEEE 802. На сетях, которые не соответствуют Стандарту IEEE 802, но соответствуют эталонной модели OSI, узловой адрес вызывают адресом Контроля канала передачи данных (DLC).
Minor Application Второстепенное приложение	Приложение, другое чем главное приложение, которое требует внимания к безопасности вследствие риска и величина вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации в приложении. Второстепенные приложения, как правило, включаются как часть системы общей поддержки.
Mobile Code Мобильный код	Программы или части программ, полученных из удаленных информационных систем, передающиеся через сеть, и выполняемые на локальной информационной системе без явной установки или выполнения получателем.
Mobile Code Technologies Технологии мобильного кода	Разработки программного обеспечения, которые предоставляют механизмы для разработки и использования мобильного кода

	(например, Java, JavaScript, ActiveX, VBScript).
Moderate-Impact System Система умеренного воздействия	Информационная система, в которой, по крайней мере, одной цели безопасности (то есть, конфиденциальности, целостности или доступности) назначено в соответствии с FIPS Публикацией 199 значение потенциала воздействия умеренный и нет цели безопасности, которой назначено в соответствии с FIPS Публикацией 199 значение потенциала воздействия высокий.
*National Security Emergency Preparedness Telecommunications Service*s Телекоммуникационные Сервисы подготовленности к чрезвычайным ситуациям национальной безопасности	Телекоммуникационные сервисы, которые используются, чтобы поддерживать состояние готовности или отвечать на и управлять любым событием или кризисом (локальным, национальным или международным), который вызывает или может вызвать повреждение или ущерб населению, ущерб или потерю собственности, или ухудшить или угрожать национальной безопасности или подготовленности Соединенных Штатов к чрезвычайным ситуациям.
National Security Information Информация национальной безопасности	Информация, которая была определена в соответствии с Правительственным распоряжением 12958 и уточнено Правительственным распоряжением 13292, или любым предшествующим порядком, или законом об Атомной энергии 1954, с уточнениями, как требующая защиты против несанкционированного раскрытия и маркирована, чтобы указать на её классифицированный статус.
National Security System Система национальной безопасности [44 U.S.C., Sec. 3542]	Любая информационная система (включая любую телекоммуникационную систему) используемая или управляемая агентством или подрядчиком агентства, или другой организацией от имени агентства - (I) функция, деятельность или использование которой включает разведывательную деятельность; включает криптологические работы, связанные с национальной безопасностью; включает руководство и управление вооруженными силами; включает оборудование, которое является неотъемлемой частью оружия или системы оружия; или являются критическими по отношению к прямому выполнению военных задач или задач разведки (исключая систему, которая должна использоваться для стандартных административных и бизнес-приложений, например, платежей, финансов, логистики и приложений управления персоналом); или, (II) постоянно защищена процедурами, установленными для информации, которая была специально определена критериями, установленными Правительственным распоряжением или законом конгресса, быть классифицированной в интересах национальной обороны или внешней политики.
Non-repudiation Неотказуемость [CNSS Inst. 4009]	Доверие, что отправитель информации предоставляет доказатель-ство поставки и получатель предоставляет доказательство идентификационных данных отправителя, таким образом, ни один не может позже отрицать обработку информации.
Operational Controls Эксплуатационные меры безопасности [NIST SP 800-18]	Меры безопасности (то есть, меры защиты или контрмеры) для информационной системы, которые реализуются и выполняются, прежде всего, людьми (в противоположность системам).
Plan of Action and Milestones	Документ, который идентифицирует задачи, которые должны быть выполнены. Он детализирует ресурсы, требуемые для выполнения

План действий и вехи [Меморандум OMB 02-01]	элементов плана, любые вехи, связанные с задачами и намеченные даты завершения для вех.
Potential Impact Потенциал воздействия [FIPS 199]	Потеря конфиденциальности, целостности или доступности, как ожидается, может иметь: (I) *ограниченное* отрицательное воздействие (FIPS Публикация 199 низкое); (II) *серьезное* отрицательное воздействие (FIPS Публикация 199 умеренное); или (III) *тяжелое* или *катастрофическое* отрицательное воздействие (FIPS Публикация 199 высокое) на деятельность организации, активы организации или людей.
Privacy Impact Assessment Оценка воздействия на приватность [Меморандум OMB 03-22]	Анализ того, как информация обрабатывается: (I), чтобы гарантировать обработку, соответствующую применимым законодательным, нормативным требованиям и требованиям политик относительно приватности; (II), чтобы определить риски и результаты сбора, поддержания и распространения информации в соответствующей форме в электронной информационной системе; и (III), чтобы исследовать и оценить соответствие защиты и альтернативных процессов обработки информации для смягчения потенциальных рисков приватности.
Protective Distribution System Система защищенного распространения	Проводная или оптоволоконная система, которая включает адекватные меры защиты и/или контрмеры (например, акустические, электрические, электромагнитные и физические), чтобы разрешить её использование для передачи незашифрованной информации.
Records Записи	Записи (автоматизированные и/или ручные) свидетельств Выполняемых действий или достигнутых результатов (например, формы, отчеты, результаты испытаний), которые служат основанием для того, чтобы проверить, что организация и информационная система используются как предназначено. Также используются, чтобы обратиться к элементам связанных полей данных (то есть, группы полей данных, к которым может получить доступ программа и которые содержат полный набор информации относительно определенных элементов).
Remote Access Удаленный доступ	Доступ пользователями (или информационными системами) взаимодействующими извне к периметру безопасности информационной системы.
Remote Maintenance Удаленная поддержка	Действия поддержки, проводимые людьми, взаимодействующими извне к периметру безопасности информационной системы.
Risk Риск [FIPS 200, уточненный]	Уровень воздействия на деятельность агентства (включая предназначение, функции, имидж, или репутацию), активы агентства, или людей, следующий из функционирования информационной системы, обусловленный потенциальным воздействием угрозы и вероятностью появления этой угрозы.
Risk Assessment Оценка риска	Процесс идентификации рисков к деятельности организации (включая предназначение, функции, имидж или репутацию), активам

[NIST SP 800-30]	организации или людям, путём определения вероятности случая, результирующего воздействия и дополнительных мер безопасности, которые смягчили бы это воздействие. Часть управления риском, синоним с анализом риска, и включает анализ уязвимостей и угроз.
Risk Management Управление рисками [NIST SP 800-30]	Процесс управления рисками к деятельности агентства (включая предназначение, функции, имидж или репутацию), активам агентства или людям, следующие из функционирования информационной системы. ОН включает оценку степени риска; анализ стоимости и эффективности; выбор, реализацию и оценку мер безопасности; и формальное санкционирование эксплуатации системы. Процесс рассматривает эффективность, действенность и ограничения, обусловленные законами, директивами, политиками или нормативными актами.
Safeguards Меры защиты [CNSS Inst. 4009, Уточнённая]	Защитные меры, предписанные для выполнения требований безопасности (то есть, конфиденциальности, целостности и доступности), определенных для информационной системы. Меры защиты могут включать средства защиты, ограничения управления, безопасность персонала и безопасность физических структур, областей и устройств. Синоним с мерами безопасности и контрмерами.
Sanitization Очистка [CNSS Inst. 4009, Уточнённая]	Процесс удаления информации из носителя информации таким образом, что восстановление информации становится не возможным. Он включает удаление всех меток, маркировок и журналов операций.
Scoping Guidance Руководство по учёту объектовых особенностей	Предоставляет организациям конкретные рассмотрения, связанные с технологией, связанные с инфраструктурой, связанные с открытым доступом, связанные с расширяемостью, связанные с управлением общей безопасностью и связанные с риском, по применимости и реализации отдельных мер безопасности в базовых наборах мер безопасности.
Security Category Категория безопасности [FIPS 199]	Характеристика информации или информационной системы, основанная на оценке потенциального воздействия, которое имелось бы на деятельность организации, активы организации или людей от потери конфиденциальности, целостности или доступности такой информации или информационной системы.
Security Controls Меры безопасности [FIPS 199]	Управленческие, эксплуатационные и технические меры (то есть, меры защиты или контрмеры), предписанные для информационной системы, чтобы защитить конфиденциальность, целостность и доступность системы и ее информации.
Security Control Baseline Базовый набор мер безопасности	Набор минимальных мер безопасности, определенный для информационной системы низкого воздействия, умеренного воздействия или высокого воздействия.
Security Control Enhancement Улучшение мер безопасности	Усиление мер безопасности с целью: (I) создания дополнительной, но связанной, функциональности мер безопасности; и/или (II) увеличение стойкости мер безопасности.
Security Impact Analysis Анализ воздействия на	Анализ, проводимый должностным лицом агентства, часто во время непрерывной фазы мониторинга процесса сертификации и

безопасность [NIST SP 800-37]	аккредитации безопасности, чтобы определить степень, до которой изменения к информационной системе влияли на положение безопасности системы.
Security Label Метка безопасности	Явная или неявная маркировка структуры данных или выходного носителя информации, связанных с информационной системой, представляющая содержащуюся в ней категорию безопасности по FIPS 199, или ограничения на распространение или предупреждения по обработке информации.
Security Objective Цель безопасности	Конфиденциальность, целостность или доступность.
Security Perimeter Периметр безопасности	См. *Граница аттестации*
Security Plan План безопасности	См. *План безопасности системы.*
Security Requirements Требования безопасности	Требования, накладываемые на информационную систему, которые получены из законов, правительственных распоряжений, директив, политик, инструкций, нормативных документов или потребностей организации (предназначения) чтобы гарантировать конфиденциальность, целостность и доступность обрабатываемой, хранимой или переданный информации.
Senior Agency Information Security Officer Высшее должностное лицо агентства по информационной безопасности, [44 U.S.C., Sec. 3544]	Должностное лицо, ответственное за выполнение обязанностей Директора по информации в отношение FISMA и служащее основной связью Директора по информации с санкционирующими должностными лицами агентства, владельцами информационной системы и сотрудниками безопасности информационной системы.
Spyware Шпионящее программное обеспечение	Программное обеспечение, которое тайно или скрытно установлено в информационную систему, чтобы собирать информацию о людях или организациях без их ведома.
Subsystem Подсистема	Основное подразделение или компонент информационной системы, состоящее из информации, информационных технологий и персонала, которое выполняет одну или более конкретные функции.
System Система	См. *Информационная система*.
System-Specific Security Control Мера безопасности, специфичная для системы [NIST SP 800-37]	Мера безопасности для информационной системы, которая не определялась как общая мера безопасности.
System Security Plan План безопасности системы [NIST SP 800-18]	Формальный документ, который представляет описание требований безопасности для информационной системы и описывает реализованные или планируемые меры безопасности для удовлетворения этим требованиям.
Technical Controls Технические меры	Меры безопасности (то есть, меры защиты или контрмеры) для информационной системы, которые прежде всего реализованы и

безопасности [NIST SP 800-18]	выполнены информационной системой через механизмы, содержавшиеся в аппаратных средствах, программном обеспечении, или компонентах встроенного микропрограммного обеспечения системы.
Threat Угроза [CNSSI 4009, уточненный]	Любое обстоятельство или событие с потенциалом к неблагоприятному воздействию на деятельность организации (включая предназначение, функции, имидж или репутацию), активы организации или людей через информационную систему посредством несанкционированного доступа, разрушения, раскрытия, модификации информации и/или отказа сервиса.
Threat Agent/Source Агент/источник угрозы [NIST SP 800-30]	Любое: (I) намерение и метод предназначенные для намеренной эксплуатации уязвимости; или (II) ситуация и метод, которые могут случайно инициировать уязвимость.
Threat Assessment Оценка угрозы [CNSSI 4009]	Формальное описание и оценка угрозы информационной системе.
Threat Source Источник угрозы [FIPS 200]	Намерение и метод, имеющие целью намеренное использование уязвимости или ситуации, и метод, который могут случайно инициировать уязвимость. Синоним с агентом угрозы.
Trusted Path Доверенный путь	Механизм, посредством которого пользователь (через устройство ввода данных) может связаться непосредственно с функциями безопасности информационной системы с необходимой доверительностью, чтобы поддержать политику безопасности системы. Этот механизм может быть активирован только пользователем или функциями безопасности информационной системы и не может быть имитирован недоверенным программным обеспечением.
User Пользователь [CNSSI 4009, уточненный]	Человек, или (системный) процесс, уполномоченный на доступ к информационной системе.
Vulnerability Уязвимость [CNSS Inst. 4009, Уточнённая]	Слабость в информационной системе, процедурах безопасности системы, внутренних мерах безопасности или реализации, которая может быть использована или инициирована источником угрозы.
Vulnerability Assessment Оценка уязвимостей [CNSSI 4009]	Формальное описание и оценка уязвимостей в информационной системе.

Приложение С: Ссылки

Публикация 199 стандартов обработки федеральной информации Национального института стандартов и технологий, *Стандарты для категорирования безопасности федеральной информации и информационных систем*, декабрь 2003.

Публикация 200 стандартов обработки федеральной информации, *Меры безопасности для федеральных информационных систем*, (планируется к публикации в феврале 2006).

Закон об управлении безопасностью федеральной информации (P.L. 107-347, Заголовок III), декабрь 2002.

Национальный институт стандартов и технологий Специальная Публикация 800-26, *Руководство по самооценке безопасности для систем информационных технологий,* ноябрь 2001.

Национальный институт стандартов и технологий Специальная Публикация 800-30, *Руководство по управлению рисками для систем информационных технологий,* июль 2002.

Национальный институт стандартов и технологий Специальная Публикация 800-37, *Руководство по аттестационным испытаниям и аттестации федеральных информационных систем*, май 2004.

Национальный институт стандартов и технологий Специальная Публикация 800-47, *Руководство по обеспечению безопасности для Соединения Систем Информационной технологии,* август 2002.

Национальный институт стандартов и технологий Специальная Публикация 800-53, *Рекомендуемые меры безопасности для федеральных информационных систем,* февраль 2005.

Национальный институт стандартов и технологий Специальная Публикация 800-59, *Руководство по идентификации информационных систем как систем национальной безопасности*, август 2003.

Национальный институт стандартов и технологий Специальная Публикация 800-60, *Руководство по отображению типов информации и информационных систем к категориям безопасности*, июнь 2004.

Национальный институт стандартов и технологий Специальная Публикация 800-64, Версия 1, *Рассмотрения безопасности в жизненном цикле разработки информационной системы*, июнь 2004.

Национальный институт стандартов и технологий Специальная Публикация 800-65, *Интегрирование безопасности ИТ-систем в процесс управления основным планированием и инвестициями,* январь 2005.

Национальный институт стандартов и технологий Специальная Публикация 800-70, *Программа контрольных списков конфигурации безопасности для продуктов ИТ - Руководство для пользователей и разработчиков контрольных списков,* май 2005.

Министерство управления и бюджета, Циркуляр А-130, Приложение III, Переходящий меморандум #4, *Управление ресурсами федеральной информации*, ноябрь 2000.