NIST Специальная Публикация 800-60 Том 1
Версия 1

ТОМ I:
Руководство по отображению типов информации и информационных систем к категориям безопасности

Kevin Stine
Rich Kissel
William C. BArker
Jim Fahlsing
Jessica Gulick

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

Август 2008

МИНИСТЕРСТВО ТОРГОВЛИ США
Карлос М. Гутьеррез, Министр

НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И ТЕХНОЛОГИЙ
Джеймс М. Тернер, Заместитель директора

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 рентабельной безопасности и приватности в федеральных информационных системах за исключением информации, связанной с национальной безопасностью. 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

Эта публикация была разработана NIST в соответствии с ее обязанностями, установленными согласно Закону об управлении безопасностью федеральной информации (FISMA), Общественный закон (P.L). 107-347. NIST ответственен за разработку стандартов информационной безопасности и руководств, включая минимальные требования для федеральных информационных систем, но такие стандарты и руководства не должны применяться к системам национальной безопасности без специального санкционирования соответствующих федеральных должностных лиц, осуществляющих полномочия по таким системам. Это руководство непротиворечиво с требованиями Министерства управления и бюджета (OMB) Циркуляр A-130, Раздел 8b (3), Обеспечение безопасности информационных систем агентств, как указано в Циркуляре A-130, Приложение IV: Анализ ключевых разделов. Дополнительная информация предоставлена в Циркуляре A-130, Приложение III.

Это руководство было подготовлено к использованию федеральными агентствами. Оно может также использоваться неправительственными организациями на добровольной основе и не попадает под действие авторского права. (Упоминание ценилось 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.

NIST Специальная Публикация 800-60 Том I, Версия 1, 53 страницы

(Дата) CODEN: NSPUE2

Комментарии по этой публикации могут быть направлены в Отдел компьютерной безопасности, Лаборатория информационных технологий NIST на электронную почту sec-cert@nist.gov или почтовый адрес 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Благодарность

Авторы, Kevin Stine, Rich Kissel, и William C. Barker, хотят поблагодарить своих коллег, Jim Fahlsing и Jessica Gulick из Science Applications International Corporation (SAIC), которые помогали обновить этот документ, готовили проекты и рассматривали материалы. Кроме того, особая благодарность адресована нашим рецензентам, Arnold Johnson (NIST), Karen Quigg (Mitre Corporation), и Ruth Bandler (Управление по контролю за продуктами и лекарствами), которые значительно способствовали разработке документа. Специальная благодарность направляется Elizabeth Lennon за её превосходное техническое редактирование и административную поддержку. NIST также с благодарностью подтверждает и ценит большое содействие от людей в общественном и частном секторах, вдумчивые и конструктивные комментарии которых улучшили качество и полноценность этой публикации.

Том I: Руководство по отображению типов информации и информационных систем к категориям безопасности

Оглавление

РЕЗЮМЕ

Заголовок III закона об Электронном правительстве (Общественный закон 107-347), называемый Законом об управлении безопасностью Федеральной информации (FISMA), определил задачу для Национального института стандартов и технологий (NIST) по разработке:

- Стандартов, которые будут использоваться всеми Федеральными агентствами, чтобы категорировать всю информацию и информационные системы, имеющиеся в распоряжении или сопровождаемые непосредственно или от имени каждого агентства, основываясь на целях обеспечения соответствующих уровней информационной безопасности согласно масштабу уровней риска;
- Руководства, рекомендующие типы информации и информационных систем для включения в каждую такую категорию; и
- Минимальные требования информационной безопасности (то есть, управленческие, эксплуатационные и технические меры безопасности), для информации и информационных систем в каждой такой категории.

В ответ на вторую из этих задач было разработано это руководство, чтобы помочь агентствам Федерального правительства категорировать информацию и информационные системы. Цель руководства состоит в том, чтобы облегчить приложение соответствующих уровней информационной безопасности согласно масштабу уровней воздействия или последствий, которые могли бы следовать из несанкционированного раскрытия, модификации или использования информации или информационной системы. Это руководство предполагает, что пользователь знаком со *Стандартами по категорированию безопасности Федеральной информации и информационных* систем (стандарт обработки федеральной информации [FIPS] 199). Руководство и его приложения:

- Рассматривают термины категорирования безопасности и определения, установленные FIPS 199;
- Рекомендуют процесс категорирования безопасности;
- Описывают методологию для идентификации типов Федеральной информации и информационных систем;
- Предлагают ориентировочные[1] уровни воздействия безопасности для общих типов информации;
- Обсуждают атрибуты информации, которые могут варьироваться от предварительного присвоения уровня воздействия; и
- Описывают, как установить категорирование безопасности системы, основанное на использовании, связывании и агрегировании контента информации в системе.

Этот документ предназначен как ссылочный ресурс, а не как учебное пособие, и не весь материал будет применим ко всем агентствам. Этот документ включает два тома, основное руководство и том приложений. Пользователи должны рассмотреть руководства, представленные в Томе I, затем обратиться только к конкретному материалу из приложений, который применим к их собственным системам и приложениям. Назначение предварительных воздействий представлено в Томе II, Приложения C и D. Основанием, использованным в этом руководстве для идентификации типов информации, является публикация Офиса управления программой (PMO) Архитектуры федерального

[1] Ориентировочные уровни воздействия безопасности - начальные или условные определения воздействия, сделанные, пока все рассмотрения полностью не пересмотрены, проанализированы, и приняты в последующих шагах категорирования соответствующими должностными лицами.

предприятия (FEA) Офиса Управления и Бюджета, октябрь 2007, *Документ Консолидированная эталонная модель, Версия 2.3.*

1.0 Введение

Идентификация информации, обрабатываемой в информационной системе, важна для надлежащего выбора мер безопасности и обеспечения конфиденциальности, целостности и доступности системы и ее информации. Специальная Публикация (SP) 800-60 Национального института стандартов и технологий (NIST) была разработана, чтобы помочь агентствам Федерального правительства категорировать информацию и информационные системы.

1.1 Назначение и применимость

NIST SP 800-60, определенная FISMA, предназначена, чтобы разработать руководства, рекомендующие типы информации и информационных систем для включения в каждую категорию потенциального воздействия безопасности. Это руководство предназначено, чтобы помочь агентствам последовательно отобразить уровни воздействия безопасности на типы: (i) информации (например, приватная, медицинская, собственная, финансовая, чувствительная для подрядчиков, коммерческая тайна, следственная); и (ii) информационные системы (например, критического предназначения, поддержки предназначения, административная). Это руководство применяется ко всем Федеральным информационным системам кроме *систем национальной безопасности. Системы национальной безопасности* хранят, обрабатывают или передают *информацию национальной безопасности*.[2]

1.2 Целевая аудитория

Эта публикация предназначена, чтобы служить разнообразной федеральной аудитории по информационным системам и профессионалам информационной безопасности, включая: (i) людям с обязанностями по управлению и надзору за безопасностью информационных систем и информации (например, директора по информации, старшие сотрудники информационной безопасности агентств, уполномочивающие должностные лица); (ii) должностные лица организаций, имеющие личную заинтересованность в достижении предназначения организаций (например, владельцы сфер предназначения и деятельности, владельцев информации); (iii) людей с обязанностями по разработке информационных систем (например, менеджеры программ и проектов, разработчики информационных систем); и (iv) людей с обязанностями по реализации и эксплуатации информационной безопасности (например, владельцы информационных систем, владельцы информации, сотрудники безопасности информационных систем).

1.3 Отношение к другим документам

NIST Специальная Публикация (SP) 800-60 является элементом семейства публикаций NIST, связанных с безопасностью, включая:

- FIPS Публикация 199, Стандарты по категорирования безопасности федеральной информации и информационных систем;
- FIPS Публикация 200, Минимальные требования безопасности для федеральной информации и информационных систем;

[2] FISMA определяет *систему национальной безопасности* как любую информационную систему (включая любую телекоммуникационную систему) используемую или управляемую 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 является критической по отношению к прямому выполнению военных задач или задач разведки (исключая системы, которые должны использоваться для стандартных административных и бизнес приложений, например, платежей, финансов, логистики и приложений управления персоналом); или (ii), которая обрабатывает классифицированные данные. [См. Общественный закон 107-347, Раздел 3542 (b) (2) (A).]

- NIST SP 800-30, Руководство по управлению рисками для систем информационных технологий;[3]
- NIST SP 800-37, Руководство по оценке безопасности и аттестации Федеральных информационных систем;
- Проект NIST SP 800-39, Управление риском для информационных систем: Перспектива организации;
- NIST SP 800-53, Рекомендуемые меры безопасности для Федеральных информационных систем;
- NIST SP 800-53A, Руководство по оценке мер безопасности в Федеральных информационных системах; и
- NIST SP 800-59, Руководство по идентификации информационных систем как систем национальной безопасности.

Эта серия девяти документов предназначена, чтобы обеспечить структурированную и в то же время гибкую основу для того, чтобы выбирать, определять, использовать, оценивать и контролировать меры безопасности в федеральных информационных системах – и, таким образом, оказывает существенное содействие удовлетворению требований закона об управлении безопасностью Федеральной информации (FISMA) 2002. Хотя публикации взаимно дополняют и имеют некоторые зависимости, в большинстве случаев они могут эффективно использоваться независимо от друг друга.

SP 800-60 для типов информации и связанных уровней воздействия на безопасность основана на публикации Офиса управления программой (PMO) Архитектуры федерального предприятия (FEA) Офиса Управления и Бюджета, октябрь 2007, *Документ Консолидированная эталонная модель, Версия 2.3*, материалах участников предыдущих обсуждений NIST SP 800-60, и FIPS 199. Обоснование для рекомендаций по примерным уровням воздействия, представленных в приложениях, было получено из множественных источников и, как таковое, потребует, нескольких итераций пересмотра, комментариев и последующей модификации для обеспечения согласованности в терминологии, структуре и контенте.

1.4 Организация этой Специальной Публикации

Это Том I из двух томов. Он содержит основные руководства по отображению типов информации и информационных систем к категориям безопасности. Приложения, включая рекомендации по категорированию безопасности для типов информации, основанных на предназначении, и обоснование рекомендаций по категорированию безопасности, опубликованы как отдельный Том II.

Том I обеспечивает следующую вводную информацию и руководства по отображению:

- Раздел 2: Обеспечивает краткий обзор значения процесса категорирования для предназначения агентств, программ обеспечения безопасности и общего управления информационными технологиями (ИТ) и роль публикации в жизненном цикле разработки систем, процессе аттестации и Основах управления рисками NIST.
- Раздел 3: Определяет цели безопасности и соответствующие уровни воздействия безопасности, идентифицированные в стандарте обработки федеральной информации 199, *Стандарты для Категорирования Безопасности Федеральной информации и Информационных систем* [FIPS 199];

[3] Этот документ в настоящий момент находится в стадии пересмотра и будет переиздан как Специальная Публикация 800-30, Версия 1, *Руководство по проведению оценок степени риска*.

- Раздел 4: Определяет процесс, включающий руководства для идентификации типов информации, *основанных на предназначении*, и *управления и поддержки*, и процесс, используемый для выбора уровней воздействия на безопасность, общие рассмотрения, касающиеся присвоения воздействий на безопасность, руководства по категорированию безопасности систем и рассмотрения и руководства для применения и взаимосвязи результатов категорирования систем к предприятиям агентств, большим поддерживающим инфраструктурам и взаимосвязанным системам;
- Приложение A: Глоссарий; и
- Приложение B: Ссылки.

Том II включает следующие приложения:

- Приложение A: Глоссарий [Повторение];
- Приложение B: Ссылки [Повторение];
- Приложение C: Назначение ориентировочных уровней воздействия на безопасность и поддерживающее обоснование для информации *управления и поддержки* (административной, управленческой и сервисной информации);
- Приложение D: Назначение ориентировочных уровней воздействия на безопасность и поддерживающее обоснование для информации *основанной на предназначении* (информация предназначения и механизмов поставки сервисов); и
- Приложение E: Законодательные и исполнительные источники, которые определяют свойства чувствительности/критичности.

2.0 Краткий обзор публикации

Категорирование безопасности обеспечивает необходимый шаг в интегрировании безопасности в функции управления деятельностью и управления информационными технологиями правительственного учреждения и устанавливает основу для стандартизации безопасности их информационных систем. Категорирование безопасности начинается с определения какая информация поддерживает какие правительственные направления деятельности, как определено Архитектурой федерального предприятия (FEA). Последующие шаги сосредотачиваются на оценке потребности в безопасности с точки зрения конфиденциальности, целостности и доступности. Результат - тесная взаимосвязь между предназначениями, информацией и информационными системами и экономически выгодной информационной безопасностью.

2.1 Поддержка агентствами процесса категорирования безопасности

Агентства поддерживают процесс категорирования, устанавливая для организации типы информации, основанные на предназначении. Подход к установлению основанных на предназначении типов информации в агентстве начинается с документирования предназначения агентства и сферы деятельности. В случае информации, основанной на предназначении, ответственные люди, в координации с заинтересованными сторонами от управления, эксплуатации, архитектуры предприятия и безопасности, должны сформировать исчерпывающий набор направлений деятельности агентства и областей предназначения. Кроме того, ответственные люди должны идентифицировать применимые подфункции, необходимые, чтобы выполнить предназначение организации. Например, предназначение некоторой организации могло бы быть связано с экономическим развитием. Подфункции, которые являются частью предназначения экономического развития организации, могли бы включать разработку торгово-промышленной деятельности, защиту интеллектуальной собственности или надзор за финансовым сектором. Каждая из этих подфункций определяет тип информации.

Агентства должны провести категорирование безопасности их информационных систем по FIPS 199 как общую для агентства работу с участием высшего руководства и других ключевых должностных лиц в организации (такие, как владельцы предназначения и деятельности, уполномочивающие должностные лица, ответственные за риски, директора по информации, старшие сотрудники информационной безопасности агентства, владельцы информационных систем и владельцы информации) чтобы гарантировать, что каждая информационная система подвергается соответствующему управленческому надзору и отражает потребности организации в целом. Надзор высшего руководства за процессом категорирования безопасности важен для того, чтобы следующие шаги в Основах управления рисками NIST[4] (например, выбор мер безопасности) могли бы быть выполнены эффективным и непротиворечивым способом во всём агентстве.

2.2 Значение агентства предназначениям, программ обеспечения безопасности и управления ИТ

Федеральные агентства в значительной степени зависят от информации и информационных систем, чтобы успешно осуществлять критические предназначения. С повышением значимости надежности и растущей сложностью информационных систем, а так же постоянным изменением среды риска, информационная безопасность стала функцией, существенной для предназначения. Эта функция должна быть осуществлена в способе, который уменьшает риски для информации, поручаемой агентством, его общему предназначению и его возможности осуществлять деятельность и служить американскому обществу. В результате, информационная безопасность, как функция, становится механизмом реализации деятельности через надлежащее и эффективное управление риском к конфиденциальности, целостности и доступности информации.

[4] См. Раздел 2.5, рисунок 1: Основа управления рисками NIST

Поэтому, значение категорирования информационной безопасности состоит в том, чтобы дать возможность агентствам заранее реализовать соответствующие меры обеспечения информационной безопасности, основанные на оцененном потенциальном воздействии на конфиденциальность, целостность и доступность информации и, в свою очередь, поддержать их предназначение в рентабельном способе. Неправильный анализ воздействия на информационные системы (то есть, неправильное категорирование безопасности по FIPS 199) может иметь результат для агентства или по защите информационной системы, тратя, таким образом, впустую ценные ресурсы безопасности, или при защите информационной системы и нахождении важной деятельности и активов в опасности. Агрегирование таких ошибок на уровне предприятия может далее породить проблемы.

Напротив, проведение исследований воздействия по FIPS 199 в отношении всего агентства с участием ключевых должностных лиц (например, директора по информации [CIO], высшего должностного лица Агентства по информационной безопасности [SAISO], уполномочивающих должностных лиц, владельцев предназначения/систем) на всех уровнях, может дать агентству возможность повысить экономию через эффективное управление и реализацию мер безопасности на уровне предприятия. Результирующее значение реализации этого систематизированного процесса по определению категорий безопасности и применения соответствующих средств обеспечения безопасности состоит в улучшении общего понимания предназначения агентства, процессов деятельности и владения системами и информацией.

Совет реализации

Чтобы обеспечить соответствующий уровень поддержки предназначения и надлежащей реализация текущих и будущих требований информационной безопасности, каждое агентство должно установить формальный процесс, чтобы подтвердить категорирование уровня безопасности систем с точки зрения приоритетов агентства. Это будет не только способствовать сопоставимой оценке систем, но также даст дополнительные преимущества по усилению общих мер обеспечения безопасности и установлению глубокой защиты.

2.3 Роль в жизненном цикле разработки систем

Начальное категорирование безопасности должно произойти в начале жизненного цикла разработки систем агентства (SDLC). Результирующее категорирование безопасности должно способствовать идентификации требований безопасности (чтобы затем развиться в меры безопасности) и другим связанным работам, таким как анализ воздействия на приватность или анализ критической инфраструктуры. В конечном счете, идентифицированные требования безопасности и выбранные меры безопасности включаются в стандартный процесс проектирования систем, чтобы эффективно интегрировать меры безопасности с функциональными и эксплуатационными требованиями к информационным системам, так же как другие соответствующие требования к системам (например, надежность, пригодность для обслуживания, поддерживаемость).

2.4 Роль в процессе сертификации и аккредитации

Категорирование безопасности устанавливает основу работ по аттестации (C&A), определяя уровни строгости, требуемой для аттестационных испытаний и полной проверки доверия к мерам безопасности, а так же для дополнительных действий, которые могут требоваться (то есть, защита приватности и критической инфраструктуры (CIP)). Таким образом, это помогает в определении уровня усилий по аттестации и продолжительности связанных работ.

Категорирование безопасности это необходимая предпосылка для процесса аттестации. Категорирование должно быть пересмотрено, по крайней мере, каждые три года или когда происходят существенное изменения в системе или поддерживающих сферах деятельности. Переоценки категорирования могут потребовать ситуативные изменения вне системы или агентства (такие, как предписанные изменения предназначения, изменения в управлении, повышение или изменение направленности действия угроз). Для получения дополнительной информации, см. NIST SP 800-64, Рассмотрения безопасности в жизненном цикле разработки информационных систем и NIST SP 800-37, Руководство по аттестации безопасности федеральных информационных систем.

Совет реализации

Важно обычно пересмотреть категорирование безопасности когда изменяется предназначение / деятельность, потому что при этом, вероятно, уровни могут измениться также воздействия или даже типы информации.

2.5 Роль в основах управления рисками NIST

Категорирование безопасности это первый ключевой шаг в основах управление рисками[5] из-за его влияния на все другие шаги в основах от выбора мер безопасности до уровня усилия в оценке эффективности мер безопасности.

Рисунок 1, Основа управления рисками NIST, отображает роль стандартов и руководств по обеспечению безопасности NIST для безопасности информационных систем.

[5] NIST SP 800-39, *Управление риском информационных систем: Организационная перспектива, (Начальный публичный проект), октябрь 2007.*

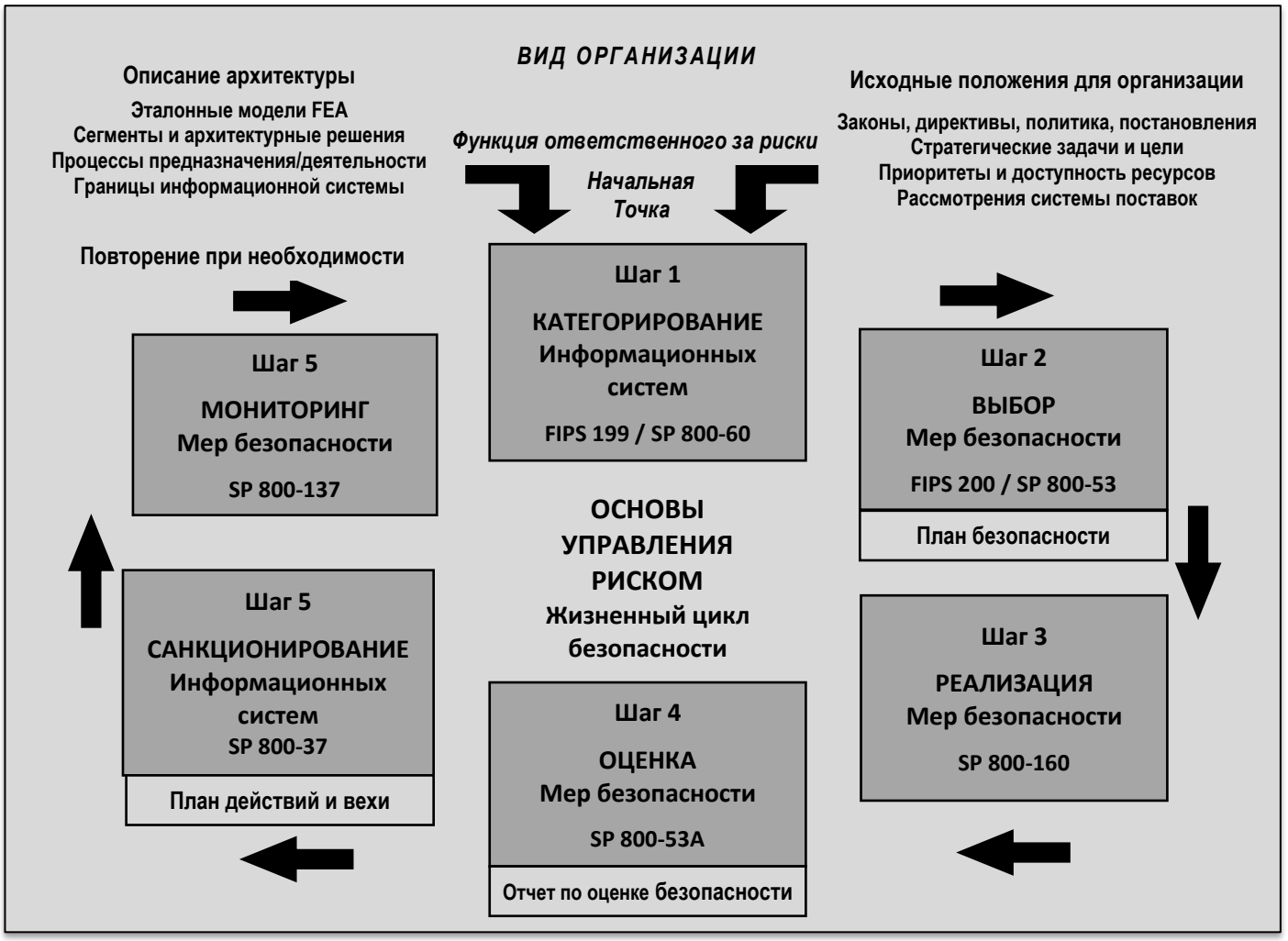

Рисунок 1: Основы управления рисками NIST

Процесс категорирования безопасности, задокументированный в эту публикацию, включает следующие процессы:

- Шаг 2: Выбор начального набора мер безопасности для информационной системы, основанный на категорировании безопасности по FIPS 199, и применение руководства по адаптации, как соответствующе, чтобы получить начальную точку для требуемых мер безопасности, как определено в FIPS 200, *Минимальные требования безопасности для Федеральной информации и информационных систем* и NIST SP 800-53, *Рекомендуемые меры безопасности для Федеральных информационных систем.* Дополнение начального набора адаптированных мер безопасности с использованием NIST SP 800-53 и SP 800-30, *Руководство управления рисками для систем информационных технологий,* основываясь на оценке риска и локальных условий, включая специфичные для организации требования безопасности, конкретную информацию об угрозах, анализ стоимости и эффективности или особые обстоятельства.
- Шаг 3: Реализация мер безопасности в информационной системе.
- Шаг 4: Оценка мер безопасности, используя соответствующие методы и процедуры, чтобы определить степень, до которой меры безопасности реализованы правильно, работают как предназначено и производят желаемый результат относительно требований безопасности для системы. (Ссылка на NIST 800-53A SP, *Руководство для оценки мер безопасности в Федеральных информационных системах*).

- Шаг 5: Санкционирование применения информационной системы, основываясь на определении риска к деятельности организации, активам организации или людям, следующего из применения информационной системы и решения, что этот риск приемлем, как определено в NIST SP 800-37, *Руководство по аттестации Федеральных информационных систем.*
- Шаг 6: Контроль и оценка выбранных мер безопасности в информационной системе на непрерывной основе, включая документирование изменений в системе, проведение исследования воздействий на безопасность, связанных с изменениями и составление на регулярной основе отчетов о состоянии безопасности системы соответствующим должностным лицам организации. (Ссылка на NIST SP 800-37 и 800-53A SP).

3.0 КАТЕГОРИРОВАНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ИНФОРМАЦИОННЫХ СИСТЕМ

Стандарт обработки федеральной информации 199 (FIPS 199), *Стандарты по категорированию безопасности Федеральной информации и информационных систем*, определяет категории безопасности, цели безопасности и уровни воздействия к которым SP 800-60 отображает типы информации. FIPS 199 устанавливает категории безопасности, основываясь на величине вреда, который, как ожидается, будет следовать из компрометации, а не на результатах оценки, которая включает попытку определить вероятность компрометации. FIPS 199 также описывает контекст, используемый в этом руководстве. Часть контента FIPS 199 включена в этот раздел, чтобы упростить использование этого руководства.

3.1 Категории и цели безопасности

3.1.1 Категории безопасности

FIPS 199 устанавливает категории безопасности и для информации[6] и для информационных систем. Категории безопасности основаны на потенциальном воздействии на организацию в результате реализации некоторых событий, которые подвергают опасности информацию и информационные системы, необходимые организации, чтобы выполнять установленную ей задачу, защищать её активы, выполнять её юридическую ответственность, сопровождать её ежедневные функции и защищать людей. Категории безопасности должны использоваться в сочетании с информацией об уязвимостях и угрозах в оценке риска к организации.

FIPS 199 устанавливает три уровня потенциального воздействия (низкое, умеренное и высокое) относящихся к обеспечению безопасности Федеральной информации и информационных систем для каждой из трех заявленных целей безопасности (конфиденциальность, целостность и доступность).

3.1.2 Цели безопасности и типы возможных потерь

Как представлено в Таблице 1, FISMA и FIPS 199 определяют три цели безопасности для информации и информационных систем.

Таблица 1: Цели безопасности информация и информационных систем

Цель безопасности	Определение FISMA [44 U.S.C., Раздел 3542]	Определение FIPS 199
Конфиденциальность	“Сохранение авторизованных ограничений на доступ и раскрытие информации, включая средства по защите неприкосновенности частной жизни и конфиденциальной информации …”	Потеря *конфиденциальности* - несанкционированное разглашение информации
Целостность	“Принятие мер против несанкционированной модификации или разрушения информации, включая гарантирование неотказуемости от информации и её аутентичности …”	Потеря *целостности* - несанкционированная модификация или разрушение информации
Доступность	“Гарантирование своевременного и надежного доступа к и использования информации …”	Потеря *доступности* - прекращение доступа к или использования информации или информационной системы

[6] Информация категорируется согласно ее *типу информации*. Тип информации - конкретная категория информации (например, приватная, медицинская, частная, финансовая, следственная, чувствительная для подрядчика, управления безопасностью) определенная организацией или, в некоторых случаях, согласно конкретному закону, Правительственному распоряжению, директиве, политике или регулированию.

3.2 Оценка воздействия

FIPS 199 определяет три уровня *потенциального воздействия* на организации или людей, являющегося нарушением безопасности (то есть, потерей конфиденциальности, целостности, или доступности). Эти определения должны применяться в соответствии с контекстом каждой организации и общего национального интереса. Таблица 2 содержит определения потенциальных воздействия из FIPS 199.

Таблица 2: Потенциальные уровни воздействия

Потенциал воздействия	Определение
Низкий	Потенциальное воздействие **низко** если - потеря конфиденциальности, целостности или доступности, как ожидается, будет иметь **ограниченное** отрицательное воздействие на деятельность организации, активы организации или людей.[7] Ограниченное отрицательное воздействие означает, что, например, потеря конфиденциальности, целостности или доступности могла бы: (i) вызывать ухудшение в способности выполнять предназначение до степени и продолжительности, что организация в состоянии выполнить свои основные функции, но эффективность функций заметно уменьшена; (ii) результат в незначительном ущербе к активам организации; (iii) иметь результат в незначительных финансовых убытках; или (iv) иметь результат в незначительном вреде людям.
Умеренный	Потенциальное воздействие **умеренно** если - потеря конфиденциальности, целостности или доступности, как ожидается, будет иметь **серьезное** отрицательное воздействие на деятельность организации, активы организации или людей. Серьезное отрицательное воздействие означает, что, например, потеря конфиденциальности, целостности или доступности могла бы: (i) вызывать существенное ухудшение в способности выполнять предназначение до степени и продолжительности, что организация в состоянии выполнить свои основные функции, но эффективность функций значительно уменьшена; (ii) иметь результат в существенном ущербе активам организации; (iii) иметь результат в существенных финансовых убытках; или (iv) иметь результат в существенном вреде людям, который не включает потерю жизни или серьезные опасные для жизни повреждения.
Высокий	Потенциальное воздействие **высоко** если - потеря конфиденциальности, целостности, или доступности, как ожидается, будет иметь тяжелое или **катастрофическое** отрицательное воздействие на деятельность организации, активы организации или людей. Тяжелое или катастрофическое отрицательное воздействие означает, что, например, потеря конфиденциальности, целостности, или доступности могла бы: (i) вызывать тяжелое ухудшение или потерю способности выполнять предназначение до степени и продолжительности, при которой организация не в состоянии выполнить одну или более ее основных функций; (ii) иметь результат в крупном ущербе активам организации; (iii) иметь результат в крупных финансовых убытках; или (iv) иметь результат в тяжелом или катастрофическом вреде людям, включающим потерю жизни или серьезные опасные для жизни повреждения.

В FIPS 199, Категория безопасности типа информации может быть связана и с пользовательской информацией и с системной информацией[8] и может быть применимой к информации или в электронной или в неэлектронной форме. Она может также использоваться как входные данные в рассмотрении соответствующей категории безопасности информационной системы (см. описание категорий безопасности для информационных систем ниже). Установление соответствующей категории безопасности типа информации по существу требует определения *потенциального воздействия* для каждой цели безопасности, связанной с определенным типом информации. Обобщенный формат для того, чтобы определить категорию безопасности, *SC*, типа информации:

[7] Отрицательные воздействия на людей могут включать, но не ограничены, потерей приватности, на которую люди наделены правом в соответствии с законом.

[8] Системная информация (например, сетевые таблицы маршрутизации, файлы пароля и информация управления криптографическим ключом) должна быть защищена на уровне, соразмерном с самой критической или чувствительной пользовательской информацией, обрабатываемой, хранимой или передаваемой информационной системой, чтобы гарантировать конфиденциальность, целостность и доступность.

Категория безопасности $_{\text{тип информации}}$ = {(конфиденциальность, воздействие), (целостность, воздействие), (доступность, воздействие)},

где приемлемые значения для потенциального *воздействия* низко, умеренно, высоко или не применимо[9]

[9] Потенциальное значение воздействия *не применимо* применяется только к цели безопасности конфиденциальность.

4.0 Назначение уровней воздействия и категорий безопасности

В этом разделе представлена методология для назначения уровней воздействия на безопасность и категорирования безопасности для типов информации и информационных систем, соответствующих установленному предназначению организации и функциям деятельности, основанным на FIPS 199, Стандарты для категорирования безопасности Федеральной информации и информационных систем. Этот документ предполагает, что пользователь читал и знаком с FIPS 199. Рисунок 2 иллюстрирует процесс категорирования безопасности с четырьмя шагами и как он приводит к выбору базового уровня мер обеспечения безопасности.

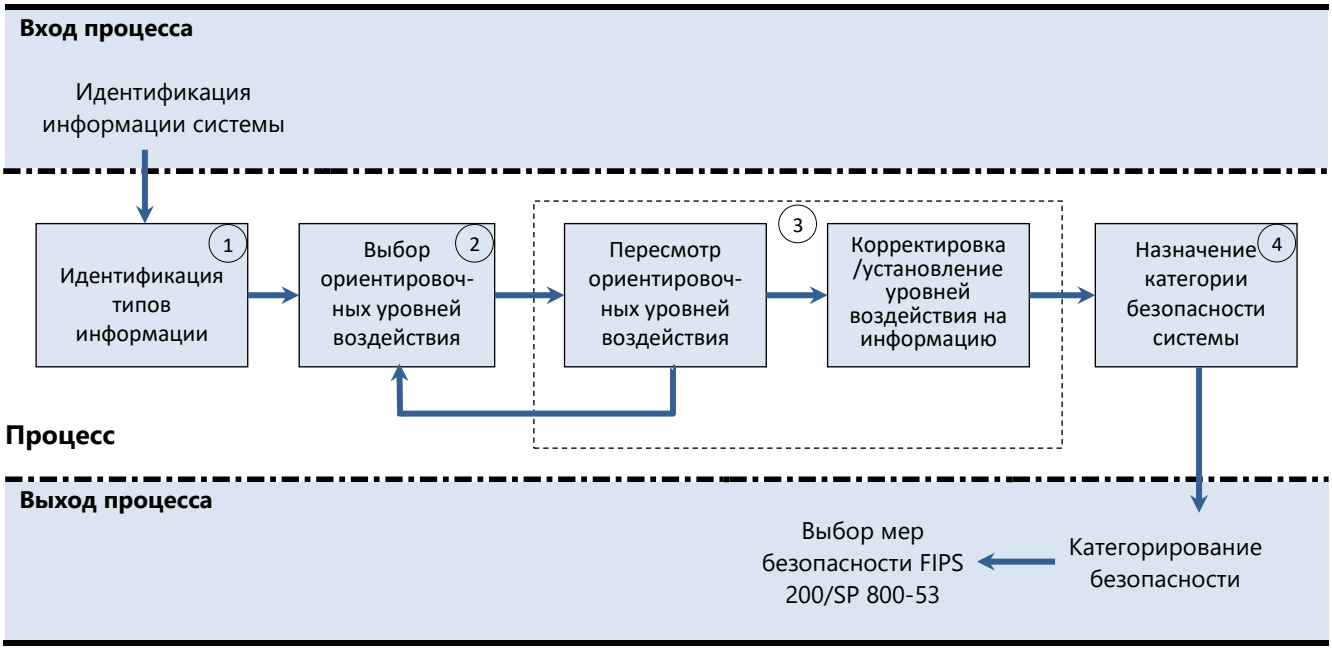

Рисунок 2: Выполнение процесса категорирования безопасности SP 800-60

Таблица 3 обеспечивает пошаговый путеводитель для идентифицирования типов информации, установления уровней воздействия на безопасность по потере конфиденциальности, целостности и доступности типов информации и назначения категорий безопасности для типов информации и для информационных систем. Категорирование безопасности - основание для того, чтобы идентифицировать начальный исходный набор мер безопасности для информационной системы.[10] Каждый функциональный шаг в процессе объяснен подробно в Разделах от 4.1 до 4.4.

[10] Информационная система - дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или уничтожения информации. [Источник: SP 800-53; FIPS 200; FIPS 199; 44 конгресса США, Раздел 3502; Циркуляр OMB A-130, Приложение. III]

Таблица 3: Путеводитель процесса SP 800-60

Шаг процесса	Действия	Роли
Вход: Идентификация информационных систем	• Агентства должны разработать свои собственные политики относительно идентификации информационных систем для целей категорирования безопасности. Система в целом ограничена периметром безопасности.[11]	CIO; SAISO; Владельцы предназначения
Шаг 1 Идентификация типов информации	• Задокументируйте области деятельности и предназначения агентства • Идентифицируйте все типы информации, которые вводятся, хранятся, обрабатываются и/или выводятся из каждой системы [Раздел 4.1] o Идентифицируют типы информации категории *основанные на предназначении*, основываясь на поддержке FEA направлений деятельности [Раздел 4.1.1] o Если применимо, идентифицируйте типы информации категории *управление и поддержка*, основываясь на поддержке FEA направлений деятельности [Раздел 4.1.2] o Определите применимые подфункции для идентифицированных категорий *основанные на предназначении* и *управление и поддержка* [II объема, Приложения C и D] o По мере необходимости, идентифицируйте другие требуемые типы информации [Разделы 4.1.3, 4.1.4] • Задокументируйте применимые типы информации для идентифицированной информационной системы наряду с выбором основанном на типе информации [Раздел 4.5]	Владельцы предназначения; Владельцы информации
Шаг 2 Выбор ориентировочных уровней воздействия	• Выберите уровни воздействия на безопасность для идентифицированных типов информации o из рекомендуемых предварительных уровней воздействия для каждого идентифицированного типа информации [Том II, Приложения C и D] o или, из FIPS 199 критериев представленных в Таблице 7 Раздел 4.2.1, и Раздел 4.2.2 • Определите категорию безопасности (SC) для каждого типа информации: $SC_{\text{тип информации}}$ = {(конфиденциальность, воздействие), (целостность, воздействие), (доступность, воздействие)} • Задокументируйте предварительный уровень воздействия на конфиденциальность, целостность и доступность, связанный с типом информации системы [Раздел 4.5]	Сотрудник безопасности информационной системы (ISSO)
Шаг 3 Пересмотр ориентировочных уровней воздействия Корректировка/ установление уровней воздействия на информацию	• Рассмотрите применимость предварительных уровней воздействия, основываясь на организации, среде, предназначении, использовании и совместном использовании данных [Раздел 4.3] • Если необходимо, скорректируйте уровни воздействия, основываясь на следующих рассмотрениях: o Факторах конфиденциальности, целостности и доступности [Раздел 4.2.2] o Ситуативные и эксплуатационные побуждения (синхронизация, жизненный цикл, и т.д.) [Раздел 4.3] o Законные или нормативные причины • Задокументируйте все корректировки уровней воздействия и обеспечьте обоснование или оправдание для корректировок [Раздел 4.5]	SAISO; ISSO; Владельцы предназначения; Владельцы информации
Шаг 4 Назначение категории безопасности системы	• Рассмотрите идентифицированные категории безопасности для совокупности типов информации. • Определите категорию безопасности системы, идентифицируя наивысшее значение уровня воздействия на безопасность для каждой из целей безопасности (конфиденциальность, целостность, доступность): $SC_{\text{Система X}}$ = {(конфиденциальность, воздействие), (целостность, воздействие), (доступность, воздействие)} • Скорректируйте наивысшее значение уровня воздействия на безопасность для каждой цели безопасности системы, применяя, при необходимости, факторы, обсужденные в разделе 4.4.2. • Назначьте полный уровень воздействия для информационной системы, основанный на самом высоком уровне воздействия для целей безопасности системы (конфиденциальность, целостность, доступность) • Следуйте надзорному процессу агентства для того, чтобы пересмотреть, одобрить и задокументировать все определения или решения [Раздел 4.5]	CIO, SAISO; ISSO; Владельцы предназначения; Владельцы информации
Выход: Категорирование безопасности	• Выход, который может использоваться как вход к выбору набора мер безопасности, необходимых для каждой системы и оценки риска для системы • Минимальные меры безопасности, рекомендуемые для каждой категории безопасности системы, могут быть найдены в NIST SP 800-53, с учетом обновлений	CIO; ISSO; Должностные лица авторизации; Разработчики

[11] Периметр безопасности синонимичен с термином граница аттестации и включает все компоненты информационной системы, которая будет аттестована официальным санкционированием и не включает отдельно аккредитованные системы, с которыми соединена информационная система.

4.1 Шаг 1: Идентифицируйте типы информации

В соответствии с FIPS 199, агентства должны идентифицировать все применимые типы информации, которые являются соответствующими для входных, хранимых, обрабатываемых и/или выходных данных каждой системы. Начальная работа в отображении типов Федеральной информации и информационных систем к целям безопасности и уровням воздействия - разработка информационной таксономии, или создание каталога типов информации.[12] Основание для идентификации типов информации - Эталонная модель деятельности OMB (BRM), описанная в публикации в октябре 2007, *Документ FEA Консолидированная Эталонная модель, Версия 2.3*. BRM описывает четыре сферы деятельности, содержащие 39 FEA направлений деятельности.[13] Эти четыре сферы деятельности разделяют деятельность правительства на высокоуровневые категории, включающие:

- Назначение правительства (*услуги для граждан*);
- Механизмы, используемые правительством, чтобы достигнуть его назначения (*режим предоставления*);
- Функции поддержки, необходимые чтобы осуществлять деятельность правительства (*поддерживают предоставление услуг*); и
- Функции управления ресурсами, которые поддерживают все области деятельности правительства (*управление правительственными ресурсами*).

Первые две сферы деятельности, *услуги для граждан* и *режима предоставления,* представляют NIST SP 800-60 Типы информации, основанные на предназначении, и будут обсуждены первыми в следующем разделе, а *поддержка поставки сервисов* и *управление правительственными ресурсами* представляют Типы информации Управление и Поддержка и будут представлены в Разделе 4.1.2.

Хотя это руководство идентифицирует много типов информации и базирует свою таксономию на BRM, вероятно только несколько из идентифицированных типов будут обрабатываться каждой отдельной системой. Кроме того, каждая система может обрабатывать информацию, которая не обязательно полностью попадает в один из перечисленных типов информации. Как только будет выбран набор типов информации, идентифицированных в этом руководстве, целесообразно рассмотреть информацию, обрабатываемую каждой системой, рассматриваемой, чтобы увидеть, должны ли дополнительные типы быть идентифицированы для целей оценки воздействия. Кроме того, рекомендуется, чтобы должностные лица организации обеспечили надлежащее документирование идентифицированных типов информации для информационной системы вместе с основанием для выбора типов информации. Руководство для документирования типов информации представлено в Разделе 4.5.

4.1.1 Идентификация типов информации, основанных на предназначении

Этот раздел описывает процесс идентификации типов информации, основанных на предназначении, и определения воздействий, связанных с несанкционированным раскрытием, модификацией или недоступностью этой информации. Типы информации, основанные на предназначении, по определению, конкретны к отдельным департаментам и агентствам или к конкретным наборам департаментов и агентств. BRM сфера деятельности *услуги для граждан* обеспечивает основную систему отсчета для определения уровней воздействия на цели безопасности для информации и

[12] Некоторой проблемой, связанной с работой по таксономии, является определение степени детализации. Если категории будут слишком широки, то руководства по назначению уровней воздействия, вероятно, будут слишком общими, чтобы быть полезными. С другой стороны, если будет предпринята попытка обеспечить руководства для каждого элемента информации, обрабатываемой каждым правительственным учреждением, то руководство, вероятно, будет громоздким и требовать чрезмерно частых изменений.

[13] Определения для терминов BRM, таких как "Сферы деятельности", "Направления деятельности" и "Подфункции"представлены в SP 800-60 Приложение A.

информационных систем, основанных на предназначении. Последствия или воздействие несанкционированного разглашения информации, модификации или разрушения информации, и нарушения доступа к или использования информации, определяются сущностью и владельцем предоставленной или поддержанной услуги. BRM устанавливает 26 предписанных сервисов и направлений предоставления поддержки деятельности с 98 связанными типами информации (указанными в таблице 4). Два типа дополнительной информации были включены, чтобы определить Исполнительные функции Исполнительного управления Президента и Обеспечения выполнения торгового права. Эти дополнения идентифицированы курсивом в Таблице 4.

Таблица 4: Типы информации, основанные на предназначении и механизмы предоставления[14]

Области предназначения и типы информации [Услуги для граждан]		
D.1 Оборона & Национальная безопасность	**D.7 Энергетика**	**D.14 Здоровье**
Стратегическая национальная & театров военных действий оборона	Энергоснабжение	Доступность здравоохранения
Оперативная оборона	Энергосбережение и энергетическая готовность	Управление здоровьем населения & Безопасность потребителей
Тактическая оборона	Управление энергоресурсами	Администрирование здравоохранения
D.2 Безопасность отечества	Производство энергии	Предоставление услуг здравоохранения
Безопасность границ и перевозок	**D.8 Меры по охране окружающей среды**	Исследования и практическое обучение в здравоохранении
Защита ключевых активов и критической инфраструктуры	Мониторинг и прогнозирование окружающей среды	**D.15 Безопасность доходов**
Защита от катастроф	Восстановление окружающей среды	Общие пенсии и инвалидность
Исполнительные функции Исполнительного управления Президента (EOP)	Контроль предотвращение загрязнения	Пособия по безработице
D.3 Разведывательные операции	**D.9 Экономическое развитие**	Помощь в предоставлении жилья
Планирование разведки	Торгово-промышленные разработки	Поддержка продовольствием и питанием
Сбор разведывательных данных	Защита интеллектуальной собственности	Компенсации оставшимся в живых
Разведывательный анализ & продукция	Надзор за финансовым сектором	**D.16 Обеспечение правопорядка**
Распространение разведывательных данных	Укрепление доходов индустриального сектора	Прогнозирование преступлений
Обработка разведывательных данных	**D.10 Общественные работы & Социальное обеспечение**	Расследование преступлений и надзор
D.4 Борьба со стихийными бедствиями	Поощрение домовладения	Защита граждан
Мониторинг и прогнозирование стихийных бедствий	Общественное и региональное развитие	Защита руководителей
Планирование и подготовка к стихийным бедствиям	Социальное обеспечение	Защита собственности
Ремонт и восстановление после стихийных бедствий	Почтовая связь	Контроль веществ
Аварийное реагирование	**D.11 Перевозки**	Предупреждение преступности
D.5 Международные отношения & Торговля	Наземные перевозки	*Правоприменение торговых законов*
Международные отношения	Водные перевозки	**D.17 Тяжбы & Судебные действия**
Международное развитие и гуманитарная помощь	Воздушные перевозки	Судебные слушания
Международная торговля	Космические операции	Судебная защита
D.6 Природные ресурсы	**D.12 Образование**	Судебные расследования
Управление водными ресурсами	Начальное, вторичное и профессиональное образование	Судебные преследования и тяжбы
Управление заповедниками, морское и наземное	Высшее образование	Содействие разрешению
Управление рекреационными ресурсами и туризм	Охрана памятников истории и культуры	**D.18 Федеральные исправительные работы**
Сельскохозяйственное инновации и сервисы	Культурные и исторические экспозиции	Уголовные тюремные наказания
	D.13 Управление Трудовыми ресурсами	Реабилитация правонарушителей
	Обучение и занятость	**D.19 Естественные науки & Инновации**
	Управление трудовыми правами	Научные и технологические исследования и инновации
	Охрана труда	Космические исследования и инновации

[14] Рекомендуемые типы информации, представленные в NIST SP 800-60, получены из "сфер деятельности" и "направлений деятельности" Эталонной модели деятельности OMB (BRM) раздел Архитектура федерального предприятия (FEA), Документа Консолидированная эталонная модель Версия 2.3, октябрь 2007.

Таблица 4: Типы информации, основанные на предназначении и механизмы предоставления

Механизмы предоставления услуг и Типы информации [Режим предоставления]		
D.20 Создание знаний & Управление	**D.22 Создание общественных благ & Управление**	**D.24 Кредиты и страхование**
Исследования и разработки	Производство	Прямые ссуды
Данные общего назначения и статистика	Конструирование	Кредитные поручительства
Консультирование и консалтинг	Публичные ресурсы, возможности и управление инфраструктурой	Общее страхование
Распространение знаний	Управление информационной инфраструктурой	**D.25 Предоставления правительств штатов/ локальных**
D.21 Соответствие установленным требованиям & соблюдение правопорядка	**D.23 Федеральная финансовая помощь**	Государственные субсидии
Инспекции и ревизии	Федеральные субсидии (не штатов)	Субсидии на программы/конкурсные
Стандарты устанавливающие/ фиксирующие направления развития	Прямое предоставление индивидуальных субсидий	Адресные субсидии
Разрешения и лицензирование	Налоговые льготы	Ссуды штатов
		D.26 Прямые услуги для Граждан
		Военные операции
		Гражданские операции

Подход к установлению основанных на предназначении типов информации на уровне агентства начинается с документирования деятельности агентства и области предназначения. Владелец или уполномоченный, каждой информационной системы ответственны за идентификацию типов информации, хранимых в, обрабатываемых или формируемых этой информационной системой. В случае информации основанной на предназначении ответственные люди, в координации с заинтересованными сторонами в управлении, эксплуатации и безопасности, должны составить исчерпывающий набор направлений деятельности и областей предназначения относящихся к агентству. Кроме того, ответственные люди должны идентифицировать применимые поддфункции, необходимые, чтобы осуществлять деятельность агентства и последовательно выполнять предназначение агентства. Например, одно предназначение, осуществляемое агентством, могло бы быть обеспечением правопорядка. Под - функции, которые являются частью предназначения обеспечения правопорядка агентства, могли бы включать расследование преступлений и надзор, прогнозирование преступлений, уголовные тюремные наказания, защиту гражданина, предупреждение преступности и защиту собственности. Каждая из этих поддфункций представила бы тип информации.

Рекомендуемые основанные на предназначении направления деятельности и составляющие поддфункции, которые могут обрабатываться информационными системами идентифицированы в Таблице 4 с деталями, представленными в Томе II, Приложение D, "Примеры определения воздействия для информации и информационных систем, основанных на предназначении."

Совет реализации

Все правительственные учреждения на уровне агентства выполняют по крайней мере одну из *областей предназначения* и используют по крайней мере один из *механизмов предоставления услуг*, описанных в Таблице 4. Однако, некоторые информационные системы могут обеспечивать только поддерживающую роль для предназначения агентства и не обрабатывать непосредственно любой из *основанных на предназначении* типов информации.

4.1.2 Идентификация информации управления и поддержки

Много информации Федерального правительства и многие поддерживающие информационные системы не используются для непосредственного предоставления основанных на предназначении сервисов, а предназначены главным образом для поддержки поставки сервисов или управления ресурсами. *Поддержки поставка сервисов* и *управление ресурсами* сфер деятельности вместе включают 13 направлений деятельности (Таблицы 5 и 6). BRM подразделяет направления деятельности на 72

подфункции. *Поставка поддержки сервисов* и *управление ресурсами* сфер деятельности являются общими для большинства агентств Федерального правительства и информация, связанная с каждой из их подфункций, идентифицирована в этом руководстве как тип информации *поддержки и управление*. Четыре дополнительных под-фактора типов информации *управления и поддержки* предназначены для определения информации приватности. Один дополнительный под-фактор типа информации *управления и поддержки* предназначен для определения Общей информации, как всеобъемлющего типа информации, который может быть не определен FEA BRM. Также агентства могут счесть необходимым идентифицировать типы дополнительной информации, не определенные в BRM и назначить связанные уровни воздействия на безопасность для этих типов.

4.1.2.1 Информация поддержки поставки сервисов

Большинство информационных систем, используемых и в поддержке предоставления услуг и в работах управления ресурсами, участвует в одном или более восьми направлений деятельности *поддержки поставки сервисов*. Каждый из типов информации, связанный с подфункцией *поддержки поставкой сервисов*, представлен в Таблице 5. Приложение C.2 Тома II, "Функции поддержки поставки сервисов," рекомендует предварительные уровни воздействия для целей безопасности конфиденциальность, целостность и доступность. Эти функции поддержки сервиса - ежедневные работы, необходимые, чтобы обеспечить критическую политику, программную и организаторскую основа для поддержки деятельности Федерального правительства. Непосредственное предназначение сервиса и, в конечном счете, избиратели, поддерживаемые функциями поддержки сервиса, представляют значимый фактор в определении воздействий на безопасность, связанных с компрометацией информации, связанной с областью деятельности *поддержки поставки услуг*.

Таблица 5: Функции и типы информации Поддержки предоставления сервисов[15]

C.2.1 Меры и надзор	**C.2.4 Управление & Сокращение внутренними рисками**	**C.2.8 Государственное управление**
Корректирующие действия	Планирование на случай чрезвычайных ситуаций	Централизованная фискальная деятельность
(Политика/ Регулирование)	Непрерывность деятельности	Законодательные функции
Программа оценки	Восстановление сервисов	Исполнительные функции
Программа мониторинга	**C.2.5 Сбор доходов**	Управление центральной собственностью
C.2.2 Регулирование развития	Взыскание долгов	Управление центральным персоналом
Политика & Руководство развитием	Сбор платы за пользование	Управление налогообложением
Отслеживание общественного мнения	Продажа федеральных активов	Управление централизованной отчетностью & статистика
Формирование регулирования	**C.2.6 Общественные отношения**	*Информация о доходах*
Публикация правил	Услуги потребителям	*Персональные идентификационные и аутентификационные данные*
C.2.3 Планирование & Бюджетирование	Распространение официальной информации	*Информация о правовых событиях*
Подготовка бюджета	Программа продовольственной помощи	*Информация об уполномоченных получателях платежей*
Планирование капиталовложений	Связи с общественностью	*Общая информация*
Архитектура предприятия	**C.2.7 Законодательные отношения**	
Стратегическое планирование	Отслеживание законодательства	
Исполнение бюджета	Законодательные свидетельства	
Планирование трудоресурсов	Разработка предложений	
Управление развитием	Деятельность по связи с конгрессом	
Интеграция бюджетирование & исполнение		
Налоговая & фискальная политика		

4.1.2.2 Информация по управлению ресурсами Правительства

Сфера деятельности, связанная с *информацией по управлению ресурсами правительства* включает дополнительную поддерживающую деятельность, дающие возможность Федеральному правительству работать эффективно. Пять направлений деятельности, *относящихся к информации по управлению ресурсами правительства* и подфункции, связанные с каждым типом информации, представлены в

[15] Рекомендуемые типы информации, представленные в NIST SP 800-60, получены из "сфер деятельности" и "направлений деятельности" Эталонной модели деятельности OMB (BRM) раздел Архитектура федерального предприятия (FEA), Документа Консолидированная эталонная модель Версия 2.3, октябрь 2007.

Таблице 6. Приложение C.3 тома II , " Информация по управлению правительственными ресурсами" рекомендует предварительные уровни воздействия для целей безопасности конфиденциальность, целостность и доступность. Многие департаменты и агентства управляют своими собственными системами поддержки. Другие получают, по крайней мере, некоторую часть услуг поддержки от других организаций. Предназначение некоторых агентств состоит, прежде всего, в том, чтобы поддерживать другие ведомства и агентства в предоставлении услуг, определенных их предназначением. Как определено выше, цели безопасности и связанные уровни воздействия на безопасность для административной и управленческой информации и систем определены сущностью поддерживаемых установленных сервисов и поддерживаемых избирателей.

Таблица 6: Функции и типы информации Управления правительственными ресурсами[16]

C.3.1 Административное управление	**C.3.3 Управление людскими ресурсами**	**C.3.5 Управление информацией & технологиями**
Управление сооружениями, парками средств и оборудованием	HR (кадровая) стратегия	Разработка систем
Услуги технической поддержки	Набор персонала	Управление жизненным циклом/изменениями
Управление безопасностью	Управление организационными структурами и должностями	Поддержка (сопровождение) систем
Перемещения	Управление компенсациями	Поддержка ИТ-инфраструктуры
Разработка & управление политикой рабочих мест	Управление вознаграждениями	Информационная безопасность
C.3.1 Управление финансами	Управление деятельностью служащих	Сохранение записей
Бухгалтерская учёт	Взаимоотношения между сотрудниками	Управление информацией
Фондовый контроль	Трудовые отношения	Мониторинг систем и сетей
Платежи	Управление увольнением	Распространение информации
Сбор денежных средств и дебиторская задолженность	Развитие человеческих ресурсов	
Управление активами и обязательствами	**C.3.4 Управление цепями поставок**	
Отчётность и информирование	Приобретение товаров	
Учёт издержек / измерение результатов	Контроль за состоянием запасов	
	Управление логистикой	
	Приобретение сервисов	

4.1.3 Полномочия на законодательную и исполнительную информацию

Во время идентификации типов информации в информационной системе персонал агентства должен предоставить специальное рассмотрение для соответствующих властей, определяющее обрабатываемую информацию и поддерживаемое назначение агентства. Приложение E тома II перечисляет законодательные и исполнительные полномочия, определяющие руководства по чувствительности и критичности для конкретных типов информации.

4.1.4 Идентификация типов информации, не перечисленных в этом руководстве

Типы информации FEA BRM представлены только как руководство по таксономии. Не вся информация, обрабатываемая информационными системами, может быть идентифицирована по Таблицам 4 - 6. Поэтому, агентство может идентифицировать уникальные типы информации, не перечисленные в этом руководстве, или может не выбирать предварительные уровни воздействия из Приложения C тома II, (для типов информации управления и поддержки) или Приложения D тома II, (для типов информации, основанных на предназначении). Разделы от 4.2.1 до 4.2.3 из этого руководства обеспечивают помощь агентствам в назначении предварительных категорий безопасности для идентифицированных агентством типов информации и информационным системам.

Дополнительно, SP 800-60 обеспечивает подфункцию *управление и поддержка*, Тип общей информации, который может использоваться агентствами в качестве средства идентифицировать и категорировать

[16] Рекомендуемые типы информации, представленные в NIST SP 800-60, получены из "сфер деятельности" и "направлений деятельности" Эталонной модели деятельности OMB (BRM) раздел Архитектура федерального предприятия (FEA), Документа Консолидированная эталонная модель Версия 2.3, октябрь 2007.

информацию не содержавшийся в FEA BRM. Полное описание информации Типа общей информации должно быть охвачено в процессе агентства сбор и документирование.

4.2 Шаг 2: Выберите предварительный уровень воздействия

В Шаге 2 организации должны установить предварительные уровни воздействия[17] основанные на идентифицированных в Шаге 1 типах информации. Предварительные уровни воздействия - исходные уровни воздействия, назначенные целям безопасности конфиденциальность, целостность и доступность для типов информации из тома II до внесения любых корректировок. Также в этом шаге устанавливается и документируется начальное категорирование безопасности для типа информации.

Приложение C тома II, содержит предварительные уровни воздействия для конфиденциальности, целостности и доступности для типов информации управления и поддержки, а Приложение D тома II, обеспечивает примеры присвоений предварительных уровней воздействия для типов информации, основанных на предназначении. Используя критерии оценки воздействия, идентифицированные в Разделе 3.2 для целей безопасности и типов возможных потерь, идентифицированных в Разделе 3.1.2, лицо организации, ответственное за определение воздействия, должно назначить уровни воздействия и далее категорировать безопасность для типов информации, *базирующихся на предназначении,* и *управления и поддержки*, идентифицированных для каждой информационной системы.

4.2.1 Критерии категорирования безопасности FIPS 199

Когда тип информации, обрабатываемый информационной системой, не категорируется посредством этого руководства [основываясь на типах информации, определённых в Приложениях C и D тома II], начальное определение воздействия должно быть сделано, основываясь на критериях категорирования FIPS 199 (приведенных в Таблице 7).

Агентства могут назначить категории безопасности для типов информации и информационных систем, выбирая и корректируя соответствующие значения Таблицу 7 для потенциальных воздействий компрометаций целей безопасности конфиденциальность, целостность и доступность. Ответственные за выбор уровня воздействия и последующее категорирование безопасности должны применять критерии, представленные в Таблице 7, к каждому типу информации, получаемому, обрабатываемому, хранимому и/или генерируемому каждой системой, за которую они ответственны. Категорирование безопасности должно вообще быть определено, основываясь на наиболее чувствительной или критической информации, получаемой, обрабатываемой, хранимой и/или генерируемой рассматриваемой системой.

[17] Уровни воздействия (множественное число), используемые здесь, относятся к *низкому*, *умеренному*, *высоко*му или *не применимому* значениям, назначенным для каждой цели безопасности (то есть, конфиденциальности, целостности и доступности), используемой в выражении категории безопасности типа информации или информационной системы. Значение *не применимо* применяется только к типам информации и не применяется к информационным системам.

Таблица 7: Категорирование Федеральной информации и информационных систем

	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 **серьёзное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированное разглашение информации, как ожидается, будет иметь **тяжёлое 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 **серьёзное** отрицательное воздействие на деятельность организации, активы организации или людей.	Несанкционированная модификация или разрушение информации, как ожидается, будет иметь **тяжёлое 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 **серьёзное** отрицательное воздействие на деятельность организации, активы организации или людей.	Прекращение доступа к или использования информации или информационной системы, как ожидается, будет иметь **тяжёлое или катастрофическое** отрицательное воздействие на деятельность организации, активы организации или людей.

4.2.2 Общие факторы для выбора уровней воздействия

Когда агентство определяет уровни воздействия на безопасность и категорирование безопасности, основываясь на локальном применении критериев FIPS 199, рекомендуется, чтобы были рассмотрены следующие факторы относительно воздействий на безопасность для каждого типа информации.

4.2.2.1 Факторы конфиденциальности

Используя критерии потенциальных воздействий FIPS 199, суммированные в Таблице 7, каждый тип информации должен быть оценен для конфиденциальности относительно уровня воздействия, связанного с несанкционированным раскрытием (i) каждой известной разновидности информации, принадлежащей к типу, и (ii) каждого использования информации рассматриваемой системой. Ответы на следующие вопросы помогут в процессе оценки:

- Как злонамеренный противник может использовать несанкционированное разглашение информации, чтобы причинить ограниченный/серьёзный/тяжёлый вред деятельности агентства, активам агентства или людям?
- Как злонамеренный противник может использовать несанкционированное разглашение информации, чтобы получить контроль над активами агентства, который мог бы иметь результат в несанкционированной модификации информации, разрушении информации или отказе системных сервисов, которые будут иметь результат в ограниченном/серьёзном/тяжёлом вреде деятельности агентства, активам агентства или людям?

- Будет ли несанкционированное раскрытие/распространение элементов типа информации нарушать законы, правительственные распоряжения или нормативные документы агентства?

4.2.2.2 Факторы целостности

Используя критерии потенциальных воздействий FIPS 199, суммированные в Таблице 7, каждый тип информации, должны быть оценён для целостности относительно уровня воздействия, связанного с несанкционированной модификацией или разрушением (i) каждой известной разновидности информации, принадлежащей типу, и (ii) каждого использования информации рассматриваемой системой. Ответы на следующие вопросы помогут в процессе оценки:

- Как злонамеренный противник может использовать несанкционированную модификацию или разрушение информации, чтобы причинить ограниченный/серьёзный/тяжёлый вред деятельности агентства, активам агентства или людям?
- Будет ли несанкционированная модификация/разрушение элементов типа информации нарушать законы, правительственные распоряжения или нормативные документы агентства?

Несанкционированная модификация или разрушение информации могут принимать много форм. Изменения могут быть незначительными и трудными для обнаружения или они могут иметь широкий масштаб. Можно построить чрезвычайно широкий диапазон сценариев для модификации информации и ее вероятных последствий. Вот только несколько примеров, включающих подделывание или изменение информации для:

- Уменьшения общественного доверия к агентству;
- Мошеннического достижения финансовой выгоды;
- Создания путаницы или противоречий через опубликование мошеннической или неправильной процедуры;
- Инициирования путаницы или противоречий через ложное приписывание мошеннической или ложной политики;
- Влияния на решения персонала;
- Вмешательства в или манипулирования обеспечением правопорядка или судебными процессами;
- Влияния на законодательство; или
- Достижения несанкционированного доступа к правительственной информации или средствам.

В большинстве случаев, самые серьезные воздействия компрометации целостности происходят, когда предпринимаются некоторые меры, основываясь на измененной информации, или измененная информация распространяется к другим организациям или обществу.

Необнаруженная потеря целостности может быть катастрофической для многих типов информации. Последствия компрометации целостности могут быть или прямыми (например, модификация финансовой записи, медицинского предписания или досье) или косвенными (например, облегчение несанкционированного доступа к чувствительной или приватной информации или лишение доступа к информации или сервисам информационной системы). Злонамеренное использование доступа для записи к информации и информационным системам может причинить огромный вред предназначению агентства и может быть использован, чтобы использовать систему агентства в качестве прокси для атак на другие системы.

Во многих случаях, последствия несанкционированной модификации или разрушения информации по функциям предназначения агентства и общественному доверию к агентству, как можно ожидать, будут ограничены. В других случаях компрометации целостности может иметь результат в подвергании опасности человеческой жизни или в других тяжелых последствиях. Воздействие может быть особенно тяжелым в случае срочной информации.

4.2.2.3 Факторы доступности

Используя критерии потенциальных воздействий FIPS 199, суммированные в Таблице 7, каждый тип информации, должны быть оценены для доступности относительно уровня воздействия, связанного с нарушением доступа к, или использования информации (i) каждой известной разновидности информации, принадлежащей типу, и (ii) каждого использования информации рассматриваемой системой. Ответы на следующие вопросы помогут в процессе оценки:

- Как злонамеренный противник может использовать нарушение доступа к или использования информации, чтобы причинить ограниченный/серьёзный/тяжёлый вред деятельности агентства, активам агентства или людям?
- Будет ли нарушение доступа к, или использования элементов типа информации, нарушать законы, правительственные распоряжения или нормативные документы агентства?

Для многих типов информации и информационных систем, уровень воздействия на доступность зависит от того, сколько времени информация или система остаются недоступными. Необнаруженная потеря доступности может быть катастрофической для многих типов информации. Например, постоянная потеря информации исполнения бюджета, планирования на случай непредвиденных ситуаций, непрерывности деятельности, восстановления услуг, взыскания долгов, управления налогообложением, управления персоналом, управления заработной платой, управления безопасностью, контроля за состоянием запасов, управления логистикой или учетной информации баз данных была бы катастрофической почти для любого агентства. Полная реконструкция таких баз данных была бы трудоёмкой и дорогой.

В большинстве случаев, отрицательные воздействия компрометации доступности ограниченной продолжительности на функции предназначения организаций и общественное доверие будут ограничены. Напротив, для критических к срочности типов информации, менее вероятно, что доступность будет восстановлена прежде, чем серьезный вред будет причинен активам, деятельности или персоналу агентства (или общему благосостоянию). В таких случаях документированные рекомендации по уровням воздействия на доступность должны указывать, что информация критична к срочности и является основанием для критичности.

4.2.3 Примеры выбор уровней воздействия на основе FIPS 199

Примеры выбора воздействия на цели безопасности и категорирования безопасности на основе FIPS 199 для типовых типов информации следующие:

ПРИМЕР 1: организация, управляющая *публичной информацией* на её веб-сервере, решает, что нет потенциального воздействия от потери конфиденциальности (то есть, требования конфиденциальности не применимы), умеренное потенциальное воздействие от потери целостности и умеренное потенциальное воздействие от потери доступности. Результирующая категория безопасности этого типа информации выражается как:

> Категории безопасности $_{\text{публичная информация}}$ = {(конфиденциальность, n/a), (целостность, умеренно), (доступность, умеренно)}.

ПРИМЕР 2: организация обеспечения правопорядка, управляющая чрезвычайно чувствительной *следственной информацией*, решает, что потенциальное воздействие от потери конфиденциальности высоко, потенциальное воздействие от потери целостности умеренно и потенциальное воздействие от потери доступности умеренно. Результирующая категория безопасности для этого типа информации выражена как:

Категория безопасности $_{\text{следственная информация}}$ = {(конфиденциальность, высоко), (целостность, умеренно), (доступность, умеренно)}.

ПРИМЕР 3: финансовая организация, управляющая стандартной *административной информацией* (информация не относящаяся к приватности) решает, что потенциальное воздействие от потери конфиденциальности низко, потенциальное воздействие от потери целостности низко и потенциальное воздействие от потери доступности низко. Результирующая категория безопасности этого типа информации выражена как:

Категории безопасности $_{\text{административная информация}}$ = {(конфиденциальность, низко), (целостность, низко), (доступность, низко)}.

В общем, оценка воздействия на цели безопасности независима от механизмов, используемых, чтобы смягчить последствия компрометации.

4.3 Шаг 3: Рассмотрите предварительные уровни воздействия и скорректируйте/примите окончательные уровни воздействия для типа информации

В Шаге 3 организации должны рассмотреть и скорректировать предварительные уровни воздействия на безопасность для целей безопасности каждого типа информации и получить окончательные значения. Чтобы выполнить это, организации должны: (i) рассмотреть уместность предварительных уровней воздействия, основанных на организации, среде, предназначении, использовании и совместном использовании данных; (ii) корректировать уровни воздействия на цели безопасности, по мере необходимости используя специальное руководство по факторам[18], представленное в Приложениях C и D тома II; и (iii) задокументировать все корректировки уровней воздействия и представить обоснование или оправдание для корректировок.

Когда уровни воздействия для категорирования безопасности, рекомендованные в Разделе 4.2 или Приложения C и D тома II, приняты как предварительные уровни воздействия на безопасность, агентство должно рассмотреть уместность предварительных уровней воздействия в контексте организации, среды, предназначения, использования и совместного использования данных, связанных с рассматриваемой информационной системой. Это рассмотрение должен учитывать важность предназначения агентства; жизненный цикл и своевременность последствий; соответствующую информацию по конфигурации и политике безопасности; специальные требования обработки; и т.д. Факторы FIPS 199, представленные в Разделе 4.2.2 этого документа, должен использоваться в качестве основания для решений относительно корректировки или признания окончательными предварительных уровней воздействия. Уровни воздействия на конфиденциальность, целостность и доступность могут корректироваться один или более раз в ходе пересмотра. Когда процесс пересмотра и корректировки заканчивается, отображение уровней воздействия к типам информации может быть завершено.

Воздействие на информацию, компрометирующее определенный тип, может отличаться для различных агентств или в различных контекстах эксплуатации. Кроме того, воздействие для типа информации может изменяться в течении жизненного цикла. Например, контрактная информация, которая имела ***умеренный*** уровень воздействия на конфиденциальность во период существования контракта, может иметь ***низкий*** уровень воздействия, когда контракт завершен. Информация политики может иметь ***умеренные*** уровни воздействия на конфиденциальность и целостность во время процесса разработки политики, ***низкий*** для конфиденциальности и ***умеренный*** для целостности уровни воздействия, когда политика реализована, и ***низкие*** уровни воздействия на конфиденциальность и целостность когда политика больше не используется.

[18] Специальное руководство по факторам в NIST SP 800-60, том II, обеспечивает конкретное руководство для рассмотрений по корректировке каждой цели безопасности (конфиденциальности, целостности и доступности) для каждого типа информации. Специальное руководство по факторам применено к каждому типу информации, основываясь на том, как тип информации используется, предназначении организации или среды эксплуатации системы.

Уровни воздействия, связанные с информацией *управления и поддержки*, общей для многих агентств, сильно зависят от информации, *основанной на предназначении*, с которой они связаны. Таким образом, у общей для агентств информации управления и поддержки, используемой с очень чувствительными или критическими типами информации, основанными на предназначении, могут быть более высокие уровни воздействия, чем у той же самой общей для агентств информации, используемой с менее критическими основанными на предназначении типами информации.

Далее, информационные системы обрабатывают много типов информации. Не для всех этих типов информации, вероятно, будут те же самые уровни воздействия на безопасность. Компрометация некоторых типов информации подвергнет опасности функциональность систем и предназначение агентства больше, чем компрометация других типов информации. Уровни воздействия на безопасность систем должны быть оценены в контексте предназначения и функций систем, а так же на основе совокупности компонентных типов информации.

Дополнительно, должны быть пересмотрены конфигурационная информация и информация по соблюдению политики безопасности и скорректирован, соответственно, информационный процесс в системе. Конфигурационная информация и информация политики безопасности включают файлы пароля, правила сетевого доступа, другие аппаратные и программные установки конфигурации и документацию, влияющую на доступ к данным информационной системы, программам и/или процессам. Как минимум, к этому набору информации и процессам применяется низкий уровень воздействия на конфиденциальность и целостность, соответствующий потенциалу для повреждения, неправильного употребления или злоупотребления системной информацией и процессами.

Фактором, специфичным для цели конфиденциальность, является информация, подвергаемая особой обработки (например, информация согласно Закону о неприкосновенности частной жизни от 1974, 5 U.S.C. § 552A). Независимо от других рассмотрений, некоторый минимальный уровень воздействия на конфиденциальность должен быть назначен для любой информационной системы, которая хранит, обрабатывает или генерирует такую информацию. Примеры такой информации включают информацию согласно закону о Коммерческой тайне, Закону о неприкосновенности частной жизни, Информация мер защиты Министерства энергетики, Информация только для служебного пользования Налогового управления и Конфиденциальная информация о деятельности управления по охране окружающей среды (например, согласно закону о контроле токсичных веществ; закону о сохранении и восстановлении ресурсов; закону о комплексной экологической ответственности, компенсациях и обязанностях). Некоторые из этих законодательных и нормативных спецификаций перечислены в Приложении E в тома II "Законодательные и исполнительные источники, устанавливающие чувствительность/критичность."

4.4 Шаг 4: Назначьте категорию безопасности системы

Как только уровни воздействия на безопасность были выбраны, пересмотрены и скорректированы по мере необходимости для целей безопасности каждого отдельного типа информации, обрабатываемого информационной системой, необходимо назначить категорию безопасности системы, основанную на совокупности типов информации. Работы Шага 4 включают следующее: (i) рассмотрение идентифицированных категорий безопасности для совокупности типов информации; (ii) определение категории безопасности системы, идентифицируя наивысшее значение для каждой из целей безопасности (конфиденциальность, целостность, доступность), основываясь на совокупности типов информации; (iii) коррекция, по мере необходимости, наивысшего значения для каждой цели безопасности системы, применяя факторы, обсужденные в разделе 4.4.2; (iv) назначение полного уровня воздействия на информационную систему, основываясь на самом высоком уровне воздействия для целей безопасности системы; и (v) документирование всех определённых категорий безопасности и решений.

4.4.1 Процесс FIPS 199 для категорирования безопасности системы

FIPS 199 отдаёт должное, что определение категории безопасности информационной системы требует дополнительного анализа и должно рассматривать категории безопасности всех типов информации, присутствующих в информационной системе. Для информационной системы, потенциальные уровни воздействия на безопасность, назначаемые для каждой из соответствующих целей безопасности (конфиденциальность, целостность, доступность), являются высшим уровнем (то есть, наивысшим значение) для любой из этих целей, который был определён для типов информации, присутствующих в информационной системе.

Информационные системы состоят из компьютерных программ и информации. Программы, выполняемые в пределах информационной системы (то есть, системные процессы), облегчают обработку, хранение и передачу информации и необходимы для организации, чтобы выполнять ее существенные коммерческие функции и деятельность. Эти, связанные с системными процессами функции, также требуют защиты и также могли бы быть подчинены категорированию безопасности. Однако, в интересах упрощения, предполагается, что категории безопасности для всех типов информации, связанных с информационной системой, обеспечивает соответствующий худший случай потенциала для всей информационной системы, устраняя, таким образом, потребность рассматривать системные процессы при категорировании безопасности информационной системы. При этом учитываются:

- Фундаментальное требование защищать целостность, доступность и, для ключевой информации, такой как пароли и ключи шифрования, конфиденциальность функций обработки и информации на уровне системы по наивысшему значению; и
- Сильная взаимозависимость между конфиденциальностью, целостностью и доступностью.

Поэтому, в FIPS 199 отмечается, что, в то время как значение (то есть, уровень) *не применимо* может примениться к целям безопасности для конкретных типов информации, обрабатываемых системами, это значение не может быть назначено ни какой цели безопасности для информационной системы. Есть минимальное предварительное воздействие (то есть, низшее значение) для компрометации конфиденциальности, целостности и доступности в информационной системе. Это необходимо, чтобы защитить функции обработки и информацию на уровне системы, критические по отношению к эксплуатации информационной системы.

Обобщенный формат для определения категории безопасности, или SC, информационной системы:

$SC_{\text{Информационная система}}$ = {(конфиденциальность, *воздействие*), (целостность, *воздействие*), (доступность, *воздействие*)},

где приемлемые значения для потенциального воздействия НИЗКО, УМЕРЕННО или ВЫСОКО. Следующие примеры иллюстрируют процесс категорирования безопасности системы, описанный в FIPS 199.

ПРИМЕР СИСТЕМЫ 1: информационная система, используемая для больших приобретений в подрядной организации, содержит и чувствительную информация о контракта фазы перед ходатайством и стандартную административную информация. Управление в пределах подрядной организации решает что: (i) для чувствительной информации контракта, потенциальное воздействие от потери конфиденциальности умеренно, потенциальное воздействие от потери целостности умеренно, и потенциальное воздействие от потери доступности низко; и (ii) для стандартной административной информации (не - связанная с приватностью информация), потенциальное воздействие от потери конфиденциальности низко, потенциальное воздействие от потери целостности низко, и потенциальное воздействие от потери доступности низко. Результирующие категории безопасности, или *SC*, этих типов информации выражены как:

$SC_{\text{контрактная информация}}$ = {(конфиденциальность, УМЕРЕННО), (целостность, УМЕРЕННО), (доступность, НИЗКО)}, и

$SC_{\text{административная информация}}$ = {(конфиденциальность, НИЗКО), (целостность, НИЗКО), (доступность, НИЗКО)}.

Результирующая категория безопасности информационной системы, выраженная как:

$SC_{\text{система приобретения}}$ = {(конфиденциальность, УМЕРЕННО), (целостность, УМЕРЕННО), (доступность, НИЗКО)},

представляет наивысшее значение или максимальную величину потенциального воздействия на каждую цель безопасности для типов информации в системе приобретения.

ПРИМЕР СИСТЕМЫ 2: электростанция содержит SCADA (диспетчерское управление и сбор данных) систему, контролирующую распределение электроэнергии для большой военной установки. Система SCADA содержит и данные датчиков в реальном времени и стандартную административную информацию. Управление в электростанции решает что: (i) для данных датчиков, получаемых системой, SCADA, нет потенциального воздействия от потери конфиденциальности, высокое потенциальное воздействие от потери целостности и высокое потенциальное воздействие от потери доступности; и (ii) для административной информации, обрабатываемой системой, есть низкое потенциальное воздействие от потери конфиденциальности, низкое потенциальное воздействие от потери целостности и низкое потенциальное воздействие от потери доступности. Результирующие категории безопасности, или *SC*, этих типов информации выражены как:

$SC_{\text{данные датчика}}$ = {(конфиденциальность, НЕТ), (целостность, ВЫСОКО), (доступность, ВЫСОКО)}, и

$SC_{\text{административная информация}}$ = {(конфиденциальность, НИЗКО), (целостность, НИЗКО), (доступность, НИЗКО)}.

Результирующая категория безопасности информационной системы первоначально, выраженная как:

$SC_{\text{система SCADA}}$ = {(конфиденциальность, НИЗКО), (целостность, ВЫСОКО), (доступность, ВЫСОКО)},

представляет наивысшее значение или максимальную величину потенциального воздействия на каждую цель безопасности для типов информации в системе SCADA. Управление в электростанции хочет увеличивать потенциальное воздействие от потери конфиденциальности с низко до умеренно, отражающее более реалистическое представление потенциального воздействия на информационную систему, вызванного нарушением защиты вследствие несанкционированное раскрытие информации на уровне системы или функций обработки. Заключительная категория безопасности информационной системы выражается как:

$SC_{\text{система SCADA}}$ = {(конфиденциальность, УМЕРЕННО), (целостность, ВЫСОКО), (доступность, ВЫСОКО)}.

4.4.2 Руководства по категорированию систем

В некоторых случаях, уровень воздействия для категории безопасности системы будет выше, чем любой уровень воздействия на цели безопасности для любого типа информации, обрабатываемого системой.

Первичными факторами, которые обычно повышают уровни воздействия категории безопасности системы выше составляющих её типов информации является агрегирование и критическая функциональность системы. Дополнительно, изменения в чувствительности/критичности относительно времени должны быть, возможно, учтены в процессе присвоения воздействия. Какая-то информация теряет свою чувствительность во времени (например, экономические/товарные прогнозы после того, как они были опубликованы). Другая информация является особенно критической в некоторый момент времени (например, погодные данные в конечной области захода на посадку во время осуществления приземления самолета). Этот раздел обеспечивает некоторые общие руководящие принципы относительно того, как агрегирование, критическая функциональность и другие системные факторы могут влиять на категорирование безопасности систем.

Совет реализации

Персонал агентства должен знать, что есть несколько факторов которые должны быть рассмотрены во время агрегирования типов информации системы. При рассмотрении факторов, могут появиться ранее непредвиденные обстоятельства, влияющие на уровни воздействия на конфиденциальность, целостность и/или доступность на уровне системы. Эти факторы включают агрегирование данных, критическую функциональность систем, учёт обстоятельств и другие системные факторы.

Чтобы эффективно выполнить этот шаг, различные заинтересованные стороны (например, управленческий, эксплуатационный персонал или специалисты по безопасности), возможно, должны быть вовлечены в получение оценок воздействия на уровне системы. Следующие разделы рассматривают факторы, которые должны рассматриваться при корректировке уровней воздействия на цели безопасности системы.

4.4.2.1 Агрегирование

Некоторая информация может быть немного или вообще не чувствительна в отдельности, но может быть очень чувствительной в совокупности. В некоторых случаях, агрегирование большого количества информации одного типа может раскрыть чувствительные образцы и планы, или облегчить доступ к чувствительным или критическим системам. В других случаях, может иметь подобный эффект объединение нескольких различных и на вид безвредных типов информации. В общем, чувствительность элемента определенных данных, вероятно, будет больше в контексте чем в изоляции (например, ассоциация номера счета с идентификационными данными человека и/или учреждения). Доступность, сложность использования и изощренность агрегации данных и инструментов вывода постоянно увеличиваются. Если рассмотрение показывает повышение чувствительности или критичности, связанное с агрегированием информации, то уровни воздействия на цели безопасности системы, возможно, должны быть скорректированы к более высокому уровню, чем тот, который мог бы быть определен по уровням воздействия на безопасность, связанным с любым отдельным типом информации. Это может быть реализовано, путём добавления описания, которое объясняет агрегацию и потенциальную цель безопасности, на которую это влияет, а так же уточнения к уровням воздействия.

4.4.2.2 Критическая функциональность систем

Компрометация некоторых типов информации может оказать малое влияние в контексте основной функции системы, но может иметь намного большее значение когда рассматривается в контексте потенциального воздействия, ставящего под угрозу:

- Другие системы, с которыми рассматриваемая система соединена, или
- Другие системы, которые зависят от информации этой системы.

Информация контроля доступа в системе, которая обрабатывает информацию только низкого воздействия, как первоначально можно было бы предположить, имела бы только цели безопасности с низким воздействием. Однако, если доступ к этой системе мог бы иметь результат в некоторой форме доступа к другим системам (например, по сети), нужно рассмотреть влияние на чувствительность и атрибуты критичности всех систем, к которым может быть такой косвенный доступ. Аналогично, некоторая информация может, в общем, иметь низкую чувствительность и/или критичность целей безопасности. Однако, эта информация может быть используемой другими системами, чтобы выполнять чрезвычайно чувствительные или критичные функции (например, авиадиспетчерская служба пользуется погодной информацией или коммерческой информацией о полетах, чтобы идентифицировать военные боевые транспортные системы). Потеря целостности, доступности данных, временного контекста или другого контекста может иметь катастрофические последствия.

4.4.2.3 Учёт обстоятельств

Эта публикация сосредотачивается на категорировании информационных систем, основываясь на типах их информации и связанных воздействиях на цели безопасности. Существуют моменты, когда уровень воздействия на цели безопасности системы должен быть повышен, основанный на других причинах помимо их информации. Например, информационная система обеспечивает критический технологический маршрут или возможности безопасности, доступность системы для общества, значительное число других систем полагается на её эксплуатацию или возможная стоимости её полной замены. Эти примеры, учитывая конкретную ситуацию, могут являться причиной для владельца системы повысить полный уровень воздействия на безопасность системы.

Повышение, основанное на учёте обстоятельств, может быть более очевидным при сравнении исходного категорирования безопасности с анализом влияния на деятельность. Если система была категорирована на основании FIPS 199 как Умеренного полного уровня воздействия, но владелец системы определил, что она должна быть в действии в течение 4-8 часов после разрушения независимо от уровня воздействия на безопасность, назначенного доступности агрегированного типа информации, то имеет место расхождение, которое вызвано учётом обстоятельств системы. Агентства должны настраивать уровень воздействия на доступность информационной системы таким образом, чтобы получить окончательное значение и точность.

4.4.2.4 Другие факторы систем

Целостность публичной информации

Большинство Федеральных агентств сопровождает веб-страницы, которые доступны для общества. Огромное большинство этих страниц государственной сети разрешает взаимодействие между сайтом и обществом. В некоторых случаях, сайт предоставляет только информацию. В других случаях, через вебсайт могут быть представлены формы (например, приложения для сервиса или заявления о приеме на работу). В некоторых случаях, сайт - посредник для деловых сделок. Несанкционированная модификация или разрушение информации, влияющей на внешние коммуникации (например, веб-страницы, электронная почта), могут оказать негативное влияние на деятельность и/или общественное доверие к агентству. В большинстве случаев, ущерб может быть исправлен в пределах относительно короткого периода времени и ущерб ограничен (уровень воздействия ***низко***). В других случаях (например, очень большие мошеннические транзакции или модификация веб-страницы, принадлежащей члену сообщества разведки/безопасности), ущерб функции предназначения и/или общественному доверию к агентству может быть серьезным. В таких случаях воздействие на целостность, связанное с несанкционированной модификацией или разрушением страницы государственной сети, было бы, по крайней мере, ***умеренно***.

Катастрофическая потеря доступности систем

Физическое или логическое разрушение главных активов может иметь результат в очень больших расходах на восстановление активов и/или большие периоды времени для восстановления. Постоянный ущерб/недоступность возможностей информационной системы может серьезно препятствовать деятельности агентства и, там где предписано, чтобы сервисы к обществу были включены, иметь тяжелое отрицательное воздействие на общественное доверие к Федеральным агентствам. Особенно в случае больших систем, критерии FIPS 199 предполагают, что катастрофическая потеря доступности систем может иметь результат в уровне воздействия на доступность ***высоко***. Должен ли уровень воздействия доступности систем быть ***высоко*** (и как следствие уровень воздействия на безопасности системы ***высоко***) зависит от других факторов, таких, как стоимость и критичность системы, а не от уровней воздействия на безопасность для типов информации, обрабатываемых системой.

Большие поддерживающие и взаимодействующие системы

Большие или сложные информационные системы, составленные из множества систем низкого уровня, часто требуют дополнительного рассмотрения относительно присвоения категории безопасности системы. Этот раздел обеспечивает руководства по применению и взаимосвязи результатов категорирования безопасности отдельных систем к предприятиям организаций, большим поддерживающим инфраструктурам (таким, как системы общей поддержки, приложения хранилищ данных, большие устройства хранения данных, фермы серверов и информационные репозитарии) и взаимосвязанным системам.
После идентификации категорий безопасности для всех информационных систем, взаимодействующих с большими инфраструктурными системами, старшее ИТ должностное лицо и должностное лицо службы безопасности владеют ценной информацией, которая может теперь установить глобальную перспективу безопасности предприятия. Первая существенная работа включает сбор полного категорирования безопасности для поддерживающей сетевой инфраструктуры агентства. Так как сети, так же как и другие системы общей поддержки, не "имеют", по своей сути, основанные на предназначении или управленческие и поддерживающие типы информации, категорирование инфраструктуры основано на агрегировании категорий безопасности информационных систем. Другими словами, категория безопасности инфраструктуры - наивысшее значение для поддерживаемых информационных систем и основана на типах информации обрабатываемых, передаваемых или хранимых в сети или системе общей поддержки. Совместно, нисходящая оценка угроз в целом для предприятия и восходящая оценка безопасности, получаемая агрегированием, позволяет организации смотреть на свой профиль риска со всестороннего и сбалансированного представления. Далее, этот анализ гарантирует, что надлежащее приложение общих мер безопасности, поддерживающих множественные информационные системы и защиты, обеспечиваемой этими мерами безопасности, наследуется отдельными системами.

Критические инфраструктуры и ключевые ресурсы

Когда предназначение, предоставляемое информационной системой, или информация, которую обрабатывает система, влияет на безопасность критических инфраструктур и ключевых ресурсов, вред, который следует из компрометации, требует особенно пристального внимания. В этом случае, влияние на безопасность может состоять в значительном сокращении эффективности механизмов защиты физической безопасности или кибербезопасности, или в помощи террористической атаки на критические инфраструктуры и ключевые ресурсы. Соответственно, когда потеря конфиденциальности, целостности или доступности будет иметь результат в негативном воздействии на критические инфраструктуры и ключевые ресурсы, категорирование безопасности системы должно быть тщательно определено.

Закон об Инфраструктуре Критической информации 2002, Общественный закон 107-296 §§ 211-215 от 25 ноября 2002 (кодифицированный как 6 U.S.C. 131-134), определяет термин "критическая информация инфраструктуры", чтобы обозначить информацию не обычную для публичного домена а связанную с безопасностью критической инфраструктуры или защищенных систем. Если типы информации соответствуют типам Критических инфраструктур, то должны быть предприняты меры, чтобы гарантировать соответствие Президентской Директиве по безопасности отечества № 7 (HSPD 7) и инициировать анализ взаимозависимости.

Приватная информация

Закон об Электронном правительстве 2002 дополняет требования защиты приватности Закона о неприкосновенности частной жизни 1974. В соответствии с этими публичными законами, агентства

Федерального правительства имеют конкретные обязанности относительно сбора, распространения или разглашения информации, касающейся людей.[19]

26 сентября 2003 Меморандум OMB M-03-22, "Руководство OMB по реализации положений приватности закона об Электронном правительстве 2002," вводит в действие положения приватности Электронного Правительственного закона 2002. Руководство применяется к информации, которая идентифицирует людей в распознаваемой форме, включая имя, адрес, номер телефона, номер социального страхования, и адрес электронной почты. OMB инструктировал руководителей агентств "описывать, как правительство обрабатывает информацию, которую люди предоставляют электронно, так, чтобы у американского общества имело доверие, что персональные данные защищены." В соответствии с этими публичными законами и исполняющими их политиками, необходимо расширить определение "несанкционированного раскрытия", чтобы охватить *любой* доступ, использование, раскрытие или совместное использование защищенной по приватности информации между агентствами Федерального правительства, когда такие действия запрещены законами о приватности и политиками. Так как основное регулирование приватности сосредотачивается на доступе, использовании, раскрытии или обмене информацией, это руководство имеет дело с рассмотрениями приватности как специальными факторами, влияющими на уровень воздействия на конфиденциальность. В установлении уровней воздействия на конфиденциальность для каждого типа информации ответственные стороны должны рассмотреть последствия несанкционированного раскрытия приватной информации (относительно нарушений федеральной политики и/или закона).

Агентства обязаны проводить Оценки воздействия на приватность (PIAs) прежде, чем разработать IT-системы, которые содержат идентифицирующую персональную информацию или прежде, чем собирать электронно идентифицирующую персональную информацию. Воздействиями на нарушение приватности должны считаться любые отрицательные воздействия, испытываемые людьми или организациями в результате потери конфиденциальности PII. Примеры отрицательных воздействий, испытываемых людьми, могут включать шантаж, хищение личных данных, дискриминацию или эмоциональное страдание. Примеры отрицательных воздействий, испытываемых организациями, могут включать административное бремя, финансовые убытки, потерю общей репутации и уверенности и штрафы, связанных с нарушением соответствующих законодательных актов и политик.

Должно быть пересмотрено категорирование, чтобы гарантировать, что отрицательные эффекты от потери конфиденциальности PII были соответственно сопоставлены определённым воздействиям. Уровень воздействия на конфиденциальности должен обычно соответствовать ***умеренному*** уровню.

Коммерческие тайны

Есть несколько законов, которые конкретно запрещают несанкционированное раскрытие коммерческих тайн (например, 7 U.S.C., Глава 6, Подглава II, 136-ой Раздел и 42 U.S.C., Глава 6A, Подглава XII, Часть E, Раздел 300j-4 (d) (1)). Системы, которые хранят, передают или обрабатывают коммерческие тайны, должен обычно назначаться, по крайней мере, ***умеренный*** уровень воздействия на конфиденциальность.

4.4.3 Полное воздействие на информационную систему

Так как значения воздействия (то есть, уровни) для определенной информационной системы на конфиденциальность, целостность и доступность нет всегда являются одинаковыми, для определения полного уровня воздействия на информационную систему используется концепция наивысшего

[19] OMB определяет человека как, "гражданин Соединенных Штатов или иностранец, законно получивший разрешение на постоянное место жительства." Агентства могут применять положения закона о неприкосновенности частной жизни и закона об Электронном правительстве к коммерческим предприятиям, индивидуальным предпринимателям, иностранцам и т.д.

значения[20]. Уровень воздействия на безопасность для информационной системы обычно будет самым высоким уровнем воздействия на цели безопасности (конфиденциальность, целостность и доступность), соответствующие совокупности типов информации системы. Таким образом, система низкого воздействия определяется как информационная система, в которой все три цели безопасности низкие. Система умеренного воздействия - информационная система, в которой, по крайней мере, одна из целей безопасности умеренна, и нет цели безопасности большей чем умеренная. И наконец, система высокого воздействия - информационная система, в которой, по крайней мере, одна цель безопасности высокая.

4.5 Документирование процесса категорирования безопасности

Для процесса категорирования безопасности является важным документирование исследований, ключевых решений и санкционирований, и поддерживающих обоснований, задающих категорирование безопасности информационной системы. Эта информация является ключевой к поддержанию жизненного цикла безопасности и должна быть включена в план обеспечения безопасности информационной системы.

Рисунок 3 обеспечивает пример деталей информации, которые должны быть собраны.

[20] Концепция наивысшего значения использована, потому что есть существенные зависимости среди целей безопасности конфиденциальность, целостность и доступность. В большинстве случаев, компрометация одной цели безопасности также, в конечном счете, влияет на другие цели безопасности.

Имя системы: Система SCADA [и Агентство конкретный идентификатор]

Название информационной системы: SCADA система [и специфический идентификатор агентства]			
Поддержка деятельности и предназначения: SCADA (диспетчерское управление и сбор данных) система обеспечивает в реальном времени контроль и информационную поддержку основной электростанции. Электростанция обеспечивает критическое распределение электроэнергии к военной установке.			
Типы информации			
[D.7.1] Энергоснабжение	Данные датчика, контролирующего доступность энергии для военной установки, ее солдат и командования. Эта функция включает управление распределением и передачу энергии. Возможности дистанционного управления SCADA могут принять такие меры, как инициирование необходимых действий переключения, чтобы облегчить условия энергетической перегрузки. Воздействия на эту информацию и систему SCADA могут влиять на критическую инфраструктуру установки.		
[C.2.8.12] Общая информация	Стандартная административная информация, обрабатываемая информационной системой SCADA		
Шаг 1 **Идентификация типов информации**	**Шаг 2 [Предварительный] / Шаг 3a [Корректировка]**		
	Воздействие на конфиденциальность	**Воздействие на целостность**	**Воздействие на доступность**
	Шаг 3b - Подтверждение корректировки воздействия		
Энергоснабжение	L/M	L/H	L/H
	Раскрытие информации датчика может серьезно воздействовать на предназначение, если показания & предупреждения о полных возможностях будут предоставлены противнику.	Тяжелые воздействия или последствия могут произойти, если соперник модифицирует информационные результаты в некорректные действия по регулированию или управлению энергией системой.	Тяжелое воздействие на возможности предназначения, обусловленное потерей доступности, может иметь результат и может трансформироваться в катастрофические последствия для критической инфраструктуры средств и возможную потерю человеческой жизни.
Общая информация	L	L	L
	Без корректировки	Без корректировки	Без корректировки
Шаг 4: Категорирование системы	**Умеренно**	**Высоко**	**Высоко**
	Полное воздействие на информационную систему: Высоко		

Рисунок 3: Совокупность информации категорирования безопасности

Кроме того, агентства могут рассмотреть улучшение их SSPs с учётом других исследований, решений, назначений и или санкционирований, которые использовались в процессе категорирования. Примеры могут включать:

- Области деятельность и предназначения агентства (Шаг 1 в Таблице 1)
- Законодательная и исполнительная информация, оказывающая влияние на назначение или корректировку информационного воздействия (Раздел 4.1.3)
- Указание на то, является ли информация критичной по времени в обоснованиях по назначению уровней воздействия на доступность (Раздел 4.2.2.3)
- Обоснования по назначению информации типа общей информации (Раздел 4.1.2, Совет реализации)
- Результаты пересмотров уместности предварительных уровней воздействия на информацию (Раздел 4.3)

- Результаты рассмотрения потенциальных воздействий на другие организации и рассмотрения, "потенциальных воздействий национального уровня в категорировании информационной системы в соответствии с Патриотическим актом США 2001 и Президентской директивой по безопасности отечества" (NIST SP 800-53 мера безопасности RA-2)
- Результаты рассмотрения идентифицированных категорий безопасности для совокупности типов информации (Шаг 4 в Таблице 1)
- Влияние различных факторов и обстоятельств (например, агрегация данных, критическая системная функциональность, приватность, коммерческие тайны, критическая инфраструктура, агрегация, критическая системная функциональность, учёт обстоятельств) на категорию системы (Раздел 4.4.2)
- На основании чего и почему агентство определило, что системный уровень воздействия должен быть выше чем любой из уровней типов информации, которые обрабатывает система (Раздел 4.4)
- Санкционирование всех определений или решений (Шаг 4 в Таблице 1)

4.6 Использование информации категорирования

Результаты категорирования безопасности системы могут и должны использоваться или быть доступными для соответствующего персонала агентства, чтобы поддержать деятельность агентства включая:

- Анализ влияния на деятельность (BIA): персонал Агентства должен рассмотреть перекрестное использование категорирования безопасности и информации BIA при выполнении каждой работы. Их общие цели дают возможность агентствам взаимно исходить из них, обеспечивая, таким образом, сдержки и противовесы, чтобы гарантировать соответствие для каждой информационной системы. Конфликтная информация и аномальные условия, такие как низкое воздействие на доступность и BIA цель трехчасового времени восстановления, должны инициировать переоценку владельцами предназначения и данных.
- Основное планирование и контроль инвестиций (CPIC) и Архитектура предприятия (EA): Так же, как инвестиции в IT не должны делаться без одобренной архитектуры, [21] категорирование безопасности, которое начинает жизненный цикл безопасности, является действием дающим возможность непосредственно представлять архитектуру предприятия и процессы CPIC для новых инвестиций, а так же для решений по обновлению и миграции. Конкретно, категорирование безопасности может обеспечить прочный базис для выравнивания определённых капиталовложений, а также может обеспечить аналитические посылки, чтобы избежать ненужных инвестиций.
- Системное проектирование: Понимание и проектирование архитектуры системы с различными уровнями чувствительности информации могут помочь в достижении положительного эффекта, сопоставимого с сервисами безопасности и защитой по зонам коллективной безопасности в пределах предприятия. Например, информационная система, содержащая информацию приватности, может располагаться в одной зоне безопасности с другими информационными системами, содержащими подобную чувствительную информацию. У каждой зоны могут быть различные уровни безопасности. Например, более критические зоны могут требовать аутентификации с 3 факторами, тогда как открытая область может требовать только обычного контроля доступа. Этот тип подхода требует основательного понимания типов информации агентства и типов данных, полученных посредством процесса категорирования безопасности.

[21] Документ FEA консолидированная эталонная модель, Версия 2.3, октябрь 2007

- Планирование непредвиденных ситуаций и аварийного восстановления: Персонал планирования непредвиденных ситуаций и аварийного восстановления должен анализировать информационные системы, которые имеют множественные типы данных различных уровней воздействия и принимать во внимание группирование приложений с подобными уровнями воздействия информационных систем с достаточно защищенными инфраструктурами. Это гарантирует эффективное применение корректных мер безопасности для непредвиденных ситуаций и защиты от аварий и избегать чрезмерной защиты информационных систем более низкого воздействия.
- Совместное использование информации и соглашения о взаимодействии систем: персонал Агентства должен использовать агрегированную и частную информацию категорирования безопасности, оценивая межведомственные соединения. Например, знание того, что информация, обрабатываемая в информационной системе высокого воздействия, передаётся информационной системе умеренного воздействия другого агентства, должно заставить оба агентства оценить информацию категорирования безопасности, реализованные или планируемые меры безопасности и риск, связанный со взаимосвязанными системами. Результаты этой оценки могут показать потребность в дополнительных мерах безопасности в форме Соглашения об уровне обслуживания, модернизации информационных систем, дополнительных смягчающих мер безопасности или альтернативных средств для того, чтобы обмениваться требуемой информацией.

ПРИЛОЖЕНИЕ А: Глоссарий терминов

Accreditation Санкционирование	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 или людей, основанное на реализации согласованного набор мер безопасности. [FIPS 200, NIST SP 800-37]
Accreditation Boundary Границы санкционирования	Все компоненты информационной системы, которая санкционирована для эксплуатация в результате официального санкционирования, исключая отдельно санкционированные системы, с которыми соединена информационная система. Синоним термина периметр безопасности, определённого в инструкции CNSS 4009 и DCID 6/3. [NIST SP 800-37]
Accrediting Authority Орган санкционирования	См. Санкционирующее должностное лицо
Agency Агентство	Исполнительный департамент, определенный в 5 U.S.C., Раздел 101; военный департамент, определеный 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. [41 U.S.C., Sec. 403]
Authentication Аутентификация	Проверка идентификационных данных пользователя, процесса или устройства, обычно как предпосылка к предоставлению доступа к ресурсам в информационной системе. [FIPS 200]
Authenticity Аутентичность	Свойство, определяющее подлинность и возможность проверять и доверять; уверенность в законности передачи, сообщения или автора сообщения. См. Аутентификация.
Authorizing Official Санкционирующее должностное лицо	Должностное лицо с полномочиями, 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. Синоним с Уполномоченным по аттестации. [FIPS 200, NIST SP 800-37]
Availability Доступность	Обеспечение своевременного и надежного доступа к и использования информации. [44 U.S.C., Sec. 3542]

Business Areas Сферы деятельности	"Сферы деятельности" разделяют правительственную деятельность на высокоуровневые категории, касающиеся назначения правительства, механизмы, которые правительство использует, чтобы достигнуть его назначений, поддерживающие функции, необходимые чтобы осуществлять правительственную деятельность и функции управления ресурсами, которые поддерживают все области деятельности правительства. "Сферы деятельности" подразделены на "области применения" или "направления деятельности." Рекомендуемые типы информации, представленные в NIST SP 800-60, получены от "сфер деятельности" и "направлений деятельности" раздела Эталонная модель деятельности OMB (BRM) *Документа Архитектура федерального предприятия (FEA) Консолидированная эталонная модель Версия 2.3*
Certification Аттестационные испытания	Всесторонняя оценка организационных, эксплуатационных и 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. [FIPS 200, NIST SP 800-37]
Chief Information Officer Директор по информации	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, правилами 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. [PL 104-106, Sec. 5125(b)]
Classified Information Классифицированная информация	Информация, которая была определена в соответствии с Правительственным распоряжением (E.O). 13292 или любым предшествующим распоряжением, требующая защиты против несанкционированного раскрытия, и помеченная, чтобы указать на её классифицированный статус в документальной форме.

Command and Control Руководство и управление	Использование полномочий и руководство должным образом назначенным командующим приписанными и присоединенными силами в достижении предназначения. Функции руководства и управления осуществляются через соглашение с персоналом, оборудование, коммуникации, средства и процедуры, используемые командующим при планировании, указаниях, координировании и контроле сил и действий в достижении предназначения.
Confidentiality Конфиденциальность	Сохранение установленных ограничений на доступ к и раскрытие информации, включая средства для защиты неприкосновенности частной жизни и конфиденциальной информации. [44 U.S.C., Sec. 3542]
Counterintelligence Контрразведка	Сбор информации и действия, проводимые для защиты от электронного шпионажа, другой разведывательной деятельности, саботажа или убийств, проведенных от имени иностранных правительств или их структур, внешних организаций, или внешних людей, или международной террористической деятельности.
Criticality Критичность	Мера степени, до которой организация зависит от информации или информационной системы для достижения успеха предназначения или функций деятельности.
Cryptologic Криптологический	Принадлежащий или имеющий отношение к криптологии.
Cryptology Криптология	Наука, которая имеет дело со скрытыми, замаскированными или зашифрованными коммуникациями. Она включает коммуникационную безопасность и коммуникационную разведку.
Executive Agency Исполнительное агентство	Исполнительный департамент, определенный в 5 U.S.C., Раздел 101; военный департамент, определеный 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. [41 U.S.C., Sec. 403]
Federal Enterprise Architecture [FEA Program Management Office] 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	Информационная система, которая используется или управляется исполнительным агентством, подрядчиком исполнительного агентства или другой организацией от имени исполнительного агентства. [40 U.S.C., Sec. 11331]

General Support System Система общей поддержки	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. [OMB Circular A-130, Appendix III]
High-Impact System Система высокого 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 «высокий». [FIPS 200]
Impact Воздействие	Эффект на деятельность организации, активы организации, людей, другие организации или Нацию (включая интересы национальной безопасности Соединенных Штатов) от потери конфиденциальности, целостности или доступности информации или информационной системы.
Independent Regulatory Agency Независимый Контролирующий орган	Совет управляющих Федеральной резервной системы, Комиссия по торговле товарными фьючерсами, Комиссия по безопасности потребительских товаров, Федеральная комиссия по связи, Федеральная корпорация страховки депозитов, Федеральная энергетическая комиссия, Федеральный совет по финансированию жилья, Федеральная морская комиссия, Федеральная торговая комиссия, Комиссия межгосударственной торговли, Комиссия по рассмотрению охраны труда и здоровья на шахтах, Национальное управление по занятости населения, Комиссия по ядерному урегулированию, Комиссия по рассмотрению охраны труда и здоровья, Комиссия по почтовым тарифам, Комиссия по ценным бумагам и биржам и любое другое подобное агентство, определяемое уставом как федеральный независимый контролирующий орган или комиссия.
Individual Человек	Гражданин Соединенных Штатов или иностранец, законно получивший разрешение на постоянное место жительства." Агентства могут применять положения закона о неприкосновенности частной жизни и закона об Электронном правительстве к коммерческим предприятиям, индивидуальным предпринимателям, иностранцам и т.д.
Information Информация	Частный случай типа информации. [FIPS 199]
Information Owner Владелец информации	Должностное лицо с установленными законом или исполнительными полномочиями для указанной информации и ответственностью за установление мер безопасности по ее генерации, сбору, обработке, распространению и уничтожению. [CNSS Inst. 4009]
Information Resources Информационные ресурсы	Информация и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии. [44 U.S.C., Sec. 3502]
Information Security Информационная безопасность	Защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения, с целью обеспечения конфиденциальности, целостности и доступности. [44 U.S.C., Sec. 3542]

Information System Информационная система	Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или уничтожения информации. [44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III]
Information System Owner (or Program Manager) Владелец информационной системы (или менеджер программы)	Должностное лицо, ответственное в целом за приобретение, разработку, интеграцию, модификацию или эксплуатацию и поддержку информационной системы. [CNSS Inst. 4009, Adapted]
Information System Security Officer Сотрудник безопасности информационной системы	Человек с возложенной ответственностью высшего сотрудника по информационной безопасности агентства, санкционирующего должностного лица, управляющего должностного лица или владельца информационной системы для поддержания соответствующего состояния эксплуатационной безопасности для информационной системы или программы. [CNSS Inst. 4009, Уточненная]
Information Technology Информационная технология	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. [40 U.S.C., Sec. 1401]
Information Type Тип информации	Конкретная категория информации (например, приватная, медицинская, имущественная, финансовая, следственная, чувствительная для подрядчика, управления безопасностью) определенная организацией или, в некоторых случаях, согласно конкретному закону, Правительственному распоряжению, директиве, политике или постановлению. [FIPS 199]
Integrity Целостность	Защита против неправомерной модификации или уничтожения информации, включающая обеспечение неотказуемости и аутентичности информации. [44 U.S.C., Sec. 3542]
Intelligence Разведка	(i) продукт, получаемый из сбора, обработки, интеграции, анализ, оценка и интерпретация доступной информации относительно зарубежных стран или областей; или (ii) информация и знания о противнике, полученные через наблюдение, исследование, анализ или понимание. Термин 'разведка' включает внешнюю разведку и контрразведку.

Intelligence Activities Разведывательная деятельность	Термин 'разведывательная деятельность' включает все действия, которые агентства Разведывательного сообщества уполномочены проводить в соответствии с Правительственным распоряжением 12333, Разведывательная деятельность Соединенных Штатов.
Intelligence Community Разведывательное сообщество	Термин 'разведывательное ведомство' относится к следующим агентствам или организациям: (i) Центральное разведывательное управление США (CIA); (ii) Агентство национальной безопасности (NSA); (iii) Разведывательное управление Министерства обороны (DIA); (iv) офисы Министерства обороны для набора специализированной национальной внешней разведки через программы рекогносцировки; (v) Бюро разведки и исследований Государственного департамента; vi) разведывательные подразделения армии, флота, воздушных сил и корпуса морской пехоты, Федерального бюро расследований (FBI), Департамента казначейства и Министерства энергетики; и (vii) персонал подразделений Директора Центральной разведки.
Lines of Business Направления деятельности	"Направления деятельности" или "области применения" описывают назначение правительства в функциональных терминах или описывают функции поддержки, которые правительство должно выполнять, чтобы эффективно предоставлять сервисы гражданам. *Направления деятельности*, касающиеся назначения правительства и механизмов, которые правительство использует, чтобы достигнуть его назначения, основываются на предназначении. *Направления деятельности*, касающиеся функций поддержки и функций управления ресурсами, которые необходимы, чтобы осуществлять деятельность правительства, являются общими для большинства агентств. Рекомендуемые типы информации, представленные в NIST SP 800-60, определены из "сфер деятельности" и "направлений деятельности" Эталонной модели деятельности OMB (BRM) Документа Архитектура федерального предприятия (FEA) Консолидированная эталонная модель Версия 2.3.
Low-Impact System Система низкого воздействия	Информационная система, в которой всем трем целям безопасности (то есть, конфиденциальности, целостности и доступности) назначено в соответствии с FIPS 199 значение потенциала воздействия «низкий». [FIPS 200]
Mission Critical Критическое предназначение	Любые телекоммуникации или информационные системы, которые определены как *системы национальной безопасности* (FISMA), или обрабатывают любую информацию потеря, неправильное употребление, раскрытие или несанкционированный доступ к или модификация которой, оказали бы ослабляющее влияние на предназначение агентства.

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 Публикацией FIPS 199 значение потенциала воздействия «умеренный» и нет цели безопасности, которой назначено в соответствии с Публикацией FIPS 199 значение потенциала воздействия «высокий». [FIPS 200]
National Security Information Информация национальной безопасности	Информация, которая была определена в соответствии с Правительственным распоряжением 12958, уточнённым 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	Любая информационная система (включая любую телекоммуникационную систему) используемая или управляемая агентством или подрядчиком агентства, или другой организации 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. [44 U.S.C. США, Секция 3542].
Non-repudiation Неотказуемость	Доверие, что отправителю информации предоставляется доказательство поставки, а получателю предоставляется доказательство подлинности отправителя, таким образом, ни один не может позже отрицать обработку информацию. [CNSS Inst. 4009 Уточнённое]
Potential Impact Пртенциал воздействия	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. [FIPS 199]

Privacy Impact Assessment (PIA) Оценка воздействия на приватность	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. [OMB Memorandum 03-22]
Public Information Публичная информация	Любая информация, независимо от формы или формата, которую агентство раскрывает, распространяет или делает доступной общественности.
Risk Риск	Уровень воздействия на деятельность организации (включая предназначение, функции, имидж или репутацию), активы организации, людей, другие организации или Нацию, следующие из использования информационной системы, подвергаемой потенциальному воздействию угрозы, и вероятность появления угрозы. [FIPS 200, Уточнённое]
Security Category Категория безопасности	Характеристика информации или информационной системы, основанная на оценке потенциального воздействия, которое имелось бы на деятельность организации, активы организации, людей, другие организации и Нацию при потере конфиденциальности, целостности или доступности такой информации или информационной системы. [FIPS 199, Уточнённое]
Security Controls Меры безопасности	Организационные, эксплуатационные и технические меры (то есть, меры защиты или контрмеры), предписанные для информационной системы, чтобы защитить конфиденциальность, целостность и доступность системы и ее информации. [FIPS 199]
Security Objectives Цели безопасности	Конфиденциальность, целостность и доступность. [FIPS 199]
Senior Agency Information Security Officer Высшее должностное лицо агентства по информационной безопасности	Должностное лицо, ответственное за выполнение обязанностей Директора по информации в отношение FISMA и служащее основной связью Директора по информации с должностными лицами агентства по санкционированию, владельцами информационной системы и сотрудниками безопасности информационной системы. [44 U.S.C., Sec. 3544]
Sensitivity Чувствительность	Используется в этом руководстве, чтобы определить меру важности, установленную для информации ее владельцем с целью обозначения потребности в ее защите.

Sub-functions Подфункции	*Подфункции* - основные действия, осуществляемые для предоставления системных сервисов в каждой области применения или направлении деятельности. Рекомендуемые типы информации, представленные в NIST SP 800-60, определены из "сфер деятельности" и "направлений деятельности" Эталонной модели деятельности OMB (BRM) Документа Архитектура федерального предприятия (FEA) Консолидированная эталонная модель Версия 2.3.
System Система	См. Информационная система
Telecommunications Телекоммуникации	Передача выбранной пользователем информации, между или среди точек, определенных пользователем, без изменения в форме или контенте информации при отправке и получении.
Threat Угроза	Любое обстоятельство или событие с потенциалом к неблагоприятному воздействию на деятельность организации (включая предназначение, функции, имидж или репутацию), активы организации, людей, другие организации или Нацию через информационную систему посредством несанкционированного доступа, разрушения, раскрытия, модификации информации и/или отказа сервиса. [CNSS Inst. 4009, Уточнённое]
Vulnerability Уязвимость	Слабость в информационной системе, процедурах безопасности системы, внутренних мерах безопасности или реализации, которая может быть использована или инициирована источником угрозы. [CNSS Inst. 4009, Уточнённое]
Weapons System Система оружия	Комбинация одного или более оружия со всем связанным оборудованием, материалами, сервисами, персоналом и средствами доставки и развертывания (если применимо), требуемыми для самодостаточности.

ПРИЛОЖЕНИЕ B: Ссылки

S. 3418 [5 U.S.C.§ 552A через Общественный закон 93-579], 93-ий американский Конгресс, 2d Sess., *Закон о неприкосновенности частной жизни 1974*, 31 декабря 1974 (имеющий силу от 27 сентября 1975).

S. 244 [Общественный закон 104-13], 104-ый американский Конгресс, 1t Sess., *Закон о сокращении документов 1995*, 22 мая, 1995.

S. 1124, Отдел E [Общественный закон 104-106], 104-ый американский Конгресс, 2d Sess., *Парламентская реформа управления информационными технологиями от 1996*, 10 февраля 1996.

H.R. 3162, Заголовок VII и Заголовок IX [Общественный закон 107-56], 107-ой американский Конгресс, 1t Sess., *ПАТРИОТИЧЕСКИЙ АКТ США от 2001*, 26 октября 2001.

Общественный закон 107-296, *Закон об инфраструктуре критической информации 2002*, §§211-215, 25 ноября, 2002.

H.R. 2458 [Общественный закон 107-347], 107-ой американский Конгресс, 2-ой Sess., *Закон об электронном правительстве 2002*, 17 декабря 2002.

H.R. 2458, Заголовок III [Общественный закон 107-347], 107-ой американский Конгресс, 2d Sess., *Закон об управлении безопасностью федеральной информация 2002*, 17 декабря 2002.

Исполнительное управление президента, *Президентская Директива 63 Решения, Защита Американской критической инфраструктуры*, 22 мая 1998.

Министерство управления и бюджета Соединенных Штатов, Циркуляр № A-130, Приложение III, Переходящий Меморандум #4, *Управление федеральными информационными ресурсами*, ноябрь 2000.

Министерство управления и бюджета Соединенных Штатов, *Руководство OMB по реализации положений по приватности закона об электронном правительстве 2002*, 29 сентября 2003.

Министерство управления и бюджета Соединенных Штатов (OMB), Архитектура федерального предприятия (FEA) Офис управления программой (PMO), *Консолидированная эталонная модель FEA 2.3*, октябрь 2007.

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, Стандарты обработки федеральной информации Публикация 199, *Стандарты для категорирования безопасности Федеральной информации и информационных систем*, декабрь 2003.

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, Стандарты обработки федеральной информации Публикация 200, *Минимальные требования безопасности для федеральной информации и информационных систем*, март 2006.

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, Специальная Публикация 800-18, *Руководство по разработке планов обеспечения безопасности для федеральных информационных систем*, Версия 1, февраль 2006.

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

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, Специальная Публикация 800-34, *Руководство по планированию на случай непредвиденных ситуаций для систем информационных технологий*, июнь 2002.

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, Специальная Публикация 800-37, *Руководство по сертификации безопасности и аттестации федеральных информационных систем*, май 2004.

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, Специальная Публикация 800-39, *Проект, Управление риском информационных систем: Организационная перспектива*, апрель 2008.

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, Специальная Публикация 800-53, *Рекомендуемые меры безопасности для федеральных информационных систем*, Версия 2, декабрь 2007.

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, Специальная публикация800-53A, *Руководство по оценке мер безопасности в федеральных информационных системах*, июль 2008.

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, Специальная публикация 800-59, *Руководство по идентификации информационных систем как систем национальной безопасности*, август 2003.

Министерство торговли Соединенных Штатов, Национальный институт стандартов и технологий, специальная Публикация 800-64, *Рассмотрение безопасности в жизненном цикле разработки информационных систем*, июнь 2004.