FIPS PUB 200

ПУБЛИКАЦИЯ СТАНДАРТОВ ОБРАБОТКИ ФЕДЕРАЛЬНОЙ ИНФОРМАЦИИ

Минимальные Требования безопасности для Федеральной информации и Информационных систем

Отдел Федеральной Компьютерной безопасности
Лаборатория Информационных технологий
Национальный институт стандартов и технологий

Гейтерсбург, Мэриленд 20899-8930

Март 2006

Американское Министерство торговли

Карлос М. Гутьеррез, Министр

Национальный институт стандартов и технологий

Уильям Джеффри, Директор

ПРЕДИСЛОВИЕ

Серия Публикации стандартов обработки федеральной информации (FIPS) Национального института стандартов и технологий (NIST) являются официальной серией публикаций, касающихся стандартов и руководств, принятых и провозглашенных в соответствии с положениями закона об управлении безопасностью Федеральной информации (FISMA) 2002. Комментарии относительно публикаций FIPS приветствуются и должны адресоваться Директору, Лаборатории Информационной технологии, Национальному институту стандартов и технологий, 100 Проезд Бюро, Остановка 8900, Гейтерсбург, Мэриленд 20899-8900.

- Cita M. Furlani, Исполняющая обязанности директора

Лаборатория информационных технологий

ПОЛНОМОЧИЯ

Публикации Стандартов обработки федеральной информации (FIPS PUBS) выпущены Национальным институтом стандартов и технологий (NIST) после санкционирования Министром торговли в соответствии с Разделом 5131 из Парламентской реформы управления информационными технологиями 1996 (Общественный закон 104-106) и Законом об управлении безопасностью Федеральной информации 2002 (Общественный закон 107-347).

Стандарты обработки федеральной информации 200

9 марта 2006

Анонс Стандарта
Минимальные требования безопасности для
Федеральная информации иИнформационных систем

Публикации Стандартов обработки федеральной информации (FIPS PUBS) выпущены Национальным институтом стандартов и технологий (NIST) после санкционирования Министром торговли в соответствии с законом об управлении безопасностью Федеральной информации (FISMA) 2002.

1. Название Стандарта.

Публикация FIPS 200: Минимальные требования безопасности для Федеральной информации и информационных систем.

2. Категория Стандарта.

Информационная безопасность.

3. Пояснения.

Закон об Электронном правительстве 2002 (Общественный закон 107-347), принятый сто седьмым Конгрессом и утвержденный Президентом в декабре 2002, определил важность информационной безопасности по отношению к интересам экономической и национальной безопасности Соединенных Штатов. Заголовок III закона об Электронном правительстве, названного Закон об управлении безопасностью Федеральной информации (FISMA), подчеркивает необходимость для каждого федерального агентства разработать, задокументировать и реализовать обще агентскую программу, чтобы обеспечить информационную безопасность для информации и информационных систем, которые поддерживают деятельность и активы агентства, включая обеспеченных или управляемых другим агентством, подрядчиком или другим источником. FISMA предписал обнародование федеральных стандартов для: (i) категорирования безопасности федеральной информации и информационных систем, основанного на целях обеспечения соответствующих уровней информационной безопасности согласно масштабу уровней риска; и (ii) минимальных требований безопасности для информации и информационных систем в каждой такой категории. Этот стандарт адресует спецификацию минимальных требований безопасности для федеральной информации и информационных систем.

4. Одобряющие полномочия.

Министр торговли.

5. Агентство по поддержке.

Министерство торговли, NIST, Лаборатория информационных технологий.

6. Применимость.

Эти стандарты должны примениться к: (i) всей информации в пределах Федерального правительства кроме той информации, которая была определена в соответствии с Правительственным распоряжением 12958, уточненным 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; и (ii) всем Федеральным информационным системам кроме тех информационных систем, которые определяются как системы национальной безопасности как определено в Разделе 3542 (b)(2) 44 кодекса Соединенных Штатов. Стандарт разработан открытым с технической перспективой к дополнению подобными стандартами для систем национальной безопасности. В дополнение к агентствам федерального правительства, правительства штатов, локальные и племенные правительства, и организации частного сектора, которые составляют критическую инфраструктуру Соединенных Штатов, поощрены рассмотреть использование этого стандарта, как соответствующего.

7. Спецификации.

Публикация FIPS 200, *Минимальные требования безопасности для Федеральной информации и информационных Систем.*

8. Реализации.

Этот стандарт определяет минимальные требования безопасности для федеральной информации и информационных систем в семнадцати связанных с безопасностью областях. Федеральные агентства должны реализовать минимальные требования безопасности, которые определены здесь, с помощью мер безопасности в соответствии с NIST Специальная Публикация 800-53, *Рекомендуемые меры безопасности для Федеральных информационных систем*, с учетом дополнений.

9. Дата вступления в силу.

Этот стандарт вступает в силу немедленно. Федеральные агентства должны соответствовать этому стандарту не позже одного года от его даты вступления в силу.

10. Развитие.

Приложение мер безопасности, определенных в NIST Специальная Публикация 800-53, определенное этим стандартом, представляет текущие практические меры защиты и контрмеры для информационных систем. Меры безопасности будут пересматриваться NIST, по крайней мере, ежегодно и, в случае необходимости, пересматриваться и расширяться, чтобы отразить: (i) опыт, извлеченный от использования мер безопасности; (ii) изменяющиеся требования безопасности в пределах федеральных агентств; и (iii) новые технологии безопасности, которые могут быть доступны. Минимальные меры безопасности, определенные в низком, умеренном и высоком уровнях базовых мер обеспечения безопасности, как ожидается, будут изменяться с течением времени также, как увеличение уровня безопасности и усилий по смягчению рисков в пределах федеральных агентств. Предложенные дополнения, удаления или модификации к каталогу мер безопасности и предложенные изменения к базовым мерам безопасности в NIST Специальная Публикация 800-53 будут проходить через строгий, общий процесс рассмотрения, чтобы получить обратную связь от правительственного сектора и частного сектора и прийти к согласию для изменений. Федеральные агентства будут иметь до одного года от даты заключительной публикации, чтобы полностью выполнить изменения, но поощрены сразу инициировать работы по их реализации.

11. Отказы.

FISMA не установлено оснований для отказов от FIPS, определенных обязательными Министром Торговля.

12. Где получить копии.

Эта публикация доступна на веб-сайте Отдела Компьютерной безопасности NIST, который доступен http://csrc.nist.go v/publications.

ОГЛАВЛЕНИЕ

1 НАЗНАЧЕНИЕ

Закон об Электронном правительстве 2002 (Общественный закон 107-347), принятый сто седьмым Конгрессом и утвержденный Президентом в декабре 2002, определил важность информационной безопасности по отношению к интересам экономической и национальной безопасности Соединенных Штатов. Заголовок III закона об Электронном правительстве, названного Закон об Управлении Безопасностью Федеральной Информации 2002 (FISMA), определил задачи для NIST с обязанностями по стандартам и руководствам, включая разработку:

- Стандартов, которые будут использоваться всеми Федеральными агентствами, чтобы категорировать всю информацию и информационные системы[1], принадлежащие или сопровождаемые непосредственно или от имени каждого агентства, основываясь на целях обеспечения соответствующих уровней информационной безопасности согласно масштабу уровней риска;
- Руководств, определяющих типы информации и информационных систем, которые должны быть включены в каждую категорию; и
- Минимальных требований информационной безопасности (т.е. организационных, эксплуатационных и технических мер), для информации и информационных систем в каждой такой категории.

Публикация 199 FIPS, *Стандарты для Категорирования Безопасности Федеральной информации и Информационных систем*, одобренная Министром торговли в феврале 2004, является первым из двух обязательных стандартов обеспечения безопасности, определенных законом FISMA.[2] Публикация FIPS 200, второй из обязательных стандартов обеспечения безопасности, определяет минимальные требования безопасности для информации и информационных систем, поддерживающих исполнительные агентства федерального правительства и основанные на риске процессы для того, чтобы выбрать меры безопасности, необходимые, чтобы удовлетворить минимальные требования безопасности. Этот стандарт будет способствовать разработке, реализации и эксплуатации более безопасных информационных систем в пределах федерального правительства, устанавливая минимальные уровни должной старательности для информационной безопасности и облегчая более непротиворечивый, сопоставимый и повторяемый подход для выбора и определения мер безопасности для информационных систем, которые обеспечивают минимальные требования безопасности.

2 УРОВНИ ВОЗДЕЙСТВИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Публикация 199 FIPS требует, чтобы агентства категорировали свои информационные системы как подверженные низкому воздействию, умеренному воздействию или высокому воздействию для целей безопасности конфиденциальности, целостности и доступности. Потенциальные значения воздействия, присвоенные соответствующим целям безопасности, являются самыми высокими значениями (то есть, наивысшее значение[3]) из числа категорий безопасности, которые были определены для каждого информационного типа, используемого в информационных системах.[4] Обобщенный формат для того, чтобы определить категорию безопасности (SC) информационной системы:

---

[1] *Информационная система* - дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или размещения информации. Информационные ресурсы включают информацию и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии.

[2] Стандарты обеспечения безопасности и руководства NIST, упомянутые в этой публикации, доступны в http://csrc.nist.gov.

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

[4] NIST Специальная Публикация 800-60, *Руководство для отображения типов информации и информационных систем к категориям безопасности*, обеспечивает руководство по реализации присвоения категорий безопасности к информации и информационным системам.

SCИнформационная система = {(**конфиденциальность**, *воздействие*), (**целостность**, *воздействие*), (**доступность**, *воздействие*)},
где приемлемые значения для потенциального воздействия низко, умеренно, или высоко.

Так как потенциальные значения воздействия для конфиденциальности целостности и доступности могут не всегда быть одинаковыми для определенной информационной системы, концепция наивысшего значения должна использоваться, чтобы определить полный уровень воздействия для информационной системы. Таким образом, *система низкого воздействия* - информационная система, в которой все три из целей безопасности низки. *Система умеренного воздействия* - информационная система, в которой, по крайней мере, одна из целей безопасности умеренна, и нет цели безопасности больше чем умеренная. И наконец, *система высокого воздействия* - информационная система, в которой, по крайней мере, одна цель безопасности высокая. Определение уровней воздействия информационной системы должно быть выполнено до рассмотрения минимальных требований безопасности и выбора соответствующих мер безопасности для этих информационных систем.

3 МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

Минимальные требования безопасности закрывают семнадцать связанных с безопасностью областей относительно защиты конфиденциальности, целостности и доступности федеральных информационных систем и информации, обработанной, хранившей и переданный этими системами. Связанные с безопасностью области включают: (i) контроль доступа; (ii) освоение и обучение; (iii) аудит и подконтрольность; (iv) аттестационные испытания, аттестация и оценка безопасности; (v) управление конфигурацией; (vi) планирование на случай непредвиденных ситуаций; (vii) идентификация и аутентификация; (viii) реакция на инциденты; (ix) поддержка; (x) защита носителей информации; (xi) физическая защита и защита окружающей среды; (xii) планирование; (xiii) безопасность персонала; (xiv) оценка риска; (xv) приобретение систем и сервисов; (xvi) защита систем и коммуникаций; и (xvii) целостность систем и информации. Эти семнадцать областей представляют всеобъемлющую, сбалансированную программу информационной безопасности, которая адресует организационные, эксплуатационные и технические аспекты защиты федеральной информации и информационных систем.

Политики и процедуры играют важную роль в эффективной реализации общих программ информационной безопасности в пределах федерального правительства и успех результирующих мер безопасности используется, чтобы защитить федеральную информацию и информационные системы. Таким образом, организации должны разработать и провозгласить формальные, задокументированные политики и процедуры, определяя минимальные требования безопасности, сформулированные в этом стандарте, и должны гарантировать их эффективную реализацию.

Спецификации для Минимальных Требований безопасности

Контроль доступа (AC): Организации должны ограничить доступ к информационной системе авторизованными пользователями, процессами, действующими от имени авторизованных пользователей или устройствами (включая другие информационные системы) и типами транзакций и функций, которые авторизованным пользователям разрешено использовать.

Освоение и обучение (AT): Организации должны: (i) гарантировать, что менеджеры и пользователи информационных систем организации информированы о рисках безопасности, связанных с их работами и о действующих законах, Правительственных распоряжениях, директивах, политиках, стандартах, инструкциях, правилах или процедурах, связанных с безопасностью информационных систем организации; и (ii) гарантировать, что персонал организации соответственно обучен, чтобы выполнить установленные им обязанности и ответственность, связанные с информационной безопасностью.

Аудит и подконтрольность (AU): Организации должны: (i) создавать, защищать, и сохранять записи аудита информационной системы до степени необходимой, чтобы обеспечить мониторинг, анализ, расследование и создание отчетов о незаконной, несанкционированной или несоответствующей работы информационной системы; и (ii) гарантируют, что действия отдельных пользователей информационной системы могут быть уникально прослежены до этих пользователей таким образом, что они могут быть признаны ответственными за свои действия.

Аттестационные испытания, аттестация и оценка Безопасности (CA): Организации должны: (i) периодически оценивать меры безопасности в информационных системах организации, чтобы определить, эффективны ли меры обеспечения в своем приложении; (ii) разрабатывать и реализовывать план действий, разработанный, чтобы исправить недостатки и уменьшить или устранить уязвимости в информационных системах организации; (iii) выдают разрешение на эксплуатацию информационных систем организации и любых связанных с информационной системой соединений; и (iv) мониторить меры безопасности информационной системы на непрерывной основе, чтобы гарантировать постоянную эффективность мер обеспечения безопасности.

Управление конфигурацией (CM):Организации должны: (i) устанавливать и сопровождать базовые конфигурации и материально-технические ресурсы информационных систем организации (включая аппаратные средства, программное обеспечение, встроенное микропрограммное обеспечение и документацию) всюду по соответствующим жизненным циклам разработки систем; и (ii) устанавливать и проводить в жизнь установки конфигурации безопасности для продуктов информационных технологий, используемых в информационных системах организации.

Планирование на случай непредвиденных ситуаций (CP): Организации должны устанавливать, сопровождать, и эффективно реализовывать планы аварийного реагирования, резервной деятельности, и поставарийного восстановления для информационных систем организации, чтобы гарантировать доступность ресурсов критической информации и непрерывность деятельности в чрезвычайных ситуациях.

Идентификация и аутентификация (IA): Организации должны идентифицировать пользователей информационной системы, процессы, действующие от имени пользователей, или устройства, и аутентифицировать (или проверять), идентификационные данные тех пользователей, процессов или устройств, как предпосылку к предоставлению доступа к информационным системам организации.

Реакция на инциденты (IR): Организации должны: (i) устанавливать способность обработки при эксплуатации инцидентов в информационных системах организации, которая включает адекватную подготовку, обнаружение, анализ, предупреждение, восстановление и пользовательские ответные действия; и (ii) прослеживание, документирование и составление отчетов об инцидентах соответствующим должностным лицам и/или уполномоченным сотрудникам организации.

Поддержка (MA): Организации должны: (i) выполнять периодическую и своевременную поддержку информационных систем организации; и (ii) обеспечивать эффективные меры обеспечения безопасности в отношении инструментов, технологий, механизмов и персонала, используемых при проведении поддержки информационной системы.

Защита носителей информации (MP): Организации должны: (i) защищать носители информации информационной системы, бумажные и цифровые; (ii) ограничивать доступ к информации на носителях информации информационной системы авторизованным пользователям; и (iii) санировать или уничтожать носители информации информационной системы перед уничтожением или предоставлением для повторного использования.

Физическая защита и защита окружающей среды (PE): Организации должны: (i) ограничивать физический доступ информационными системами, оборудованию и соответствующим операционным средам санкционированным людям; (ii) защищать материальную часть и поддерживающую инфраструктуру информационных систем; (iii) предоставлять поддерживающие коммунальные предприятия для информационных систем; (iv) защищать информационные системы от экологических опасностей; и (v) обеспечивать соответствующий контроль за состоянием окружающей среды в органах обслуживающих информационные системы.

Планирование (PL): Организации должны разрабатывать, документировать, периодически обновлять, и реализовывать планы обеспечения безопасности для информационных систем организации, которые описывают существующие или планируемые меры безопасности информационных систем и правила поведения для людей, получающих доступ к информационным системам.

Безопасность персонала (PS): Организации должны: (i) гарантировать, что люди, занимающие ответственные должности в организациях (включая сторонних поставщиков услуг), доверены и соответствуют установленным критериям безопасности для этих должностей; (ii) гарантировать, что информация и информационные системы организаций защищены в течение и после действий в отношении персонала, таких как увольнение и перемещение; и (iii) применять формальные санкции к персоналу, оказавшемуся не в состоянии выполнять организационную политику и процедуры безопасности.

Оценка риска (RA): Организации должны периодически оценивать риск в отношении деятельности организации (включая предназначение, функции, имидж или репутацию), активов организации и людей, следуя из применения информационных систем организации и связанной с ними обработки, хранения, или передачи информации организации.

Приобретение систем и сервисов (SA): Организации должны: (i) выделяют достаточные ресурсы, чтобы соответственно защитить информационные системы организации; (ii) использовать процессы жизненного цикла разработки систем, которые включают рассмотрение информационной безопасности; (iii) применять ограничения на использование и установку программного обеспечения; и (iv) гарантировать, что сторонние поставщики используют адекватные меры безопасности, чтобы защитить информацию, приложения и/или сервисы, предоставляемые от организации.

Защита систем и коммуникаций (SC): Организации должны: (i) мониторить, контролировать и защищать телекоммуникации организации (то есть, информацию, которая передается или получается информационными системами организации) на внешних границах и ключевых внутренних границах информационных систем; и (ii) использовать структурное проектирование, технологии разработки программного обеспечения и принципы проектирования систем, которые способствуют эффективной информационной безопасности в пределах информационных систем организации.

Целостность систем и информации (SI): Организации должны: (i) постоянно идентифицировать, протоколировать и исправлять дефекты информации и информационных систем; (ii) обеспечивать защиту от вредоносного кода в соответствующих областях информационных систем организации; и (iii) мониторить предупреждения и консультации в отношении безопасности информационных систем и принимать соответствующие ответные меры.

4 ВЫБОР МЕР БЕЗОПАСНОСТИ

Организации должны выполнять минимальные требования безопасности в этом стандарте, выбирая соответствующие меры безопасности и требования доверия как описано в NIST Специальная Публикация 800-53, *Рекомендуемые Меры безопасности для Систем*[5] Федеральной информации. Процесс выбора соответствующих мер безопасности и требований доверия для организационных информационных систем для достижения *адекватной безопасности*[6] есть многоаспектная, основанная на риске деятельность, затрагивающая управленческий и эксплуатационный персонал организации. Категорирование безопасности федеральной информации и информационных систем, как определено Публикацией 199 FIPS, является первым шагом в процессе управления рисками.[7] Вслед за процессом категорирования безопасности, организации должны выбрать соответствующий набор мер безопасности для их информационных систем, который удовлетворяет минимальным требованиям безопасности, определенным в этом стандарте. Выбранный набор мер безопасности должен включать один из трёх, соответственно адаптированных[8] базовых наборов мер безопасности из NIST Специальной Публикации 800-53, которые связаны с определёнными уровнями воздействия на информационные системы организации, которые определяются во время процесса категорирования безопасности.

- Для информационных систем организации *низкого воздействия*, как минимум, должны использоваться соответственно адаптированные меры безопасности из низкого базового набора мер безопасности, определенного в NIST Специальная Публикация 800-53, и должно гарантироваться, что минимальные требования доверия, связанные с низким базовым набором, удовлетворены.

- Для информационных систем организации *умеренного воздействия*, как минимум, должны использовать соответственно адаптированные меры безопасности из умеренного базового набора мер безопасности, определенного в NIST Специальная Публикация 800-53, и должно гарантироваться, что минимальные требования доверия, связанные с умеренным базовым набором, удовлетворены.

- Для информационных систем организации *высокого воздействия*, как минимум, должны использовать соответственно адаптированные меры безопасности от высокого базового набора мер безопасности, определенного в NIST Специальная Публикация 800-53, и должно гарантироваться, что минимальные требования доверия, связанные с высоким базовым набором, удовлетворены.

Организации должны использовать все меры безопасности в соответствующих базовых наборах мер безопасности, если конкретные исключения не допускаются на основании руководства по адаптации, представленного в NIST Специальной Публикации 800-53.

Чтобы гарантировать рентабельный, основанный на риске подход к достижению адекватной безопасности через организацию, работы базовый по адаптации мер безопасности, должны быть скоординированы с и одобрены соответствующими должностными лицами организации (такими, как

[5] Для процесса выбора меры безопасности организации должны использовать актуальнейшую версию NIST Специальная Публикация 800-53, с уточнениями.

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

[7] Категорирование безопасности должно быть выполнено как работа всего предприятия с участием высшего уровня должностных лиц организации включая, но нет ограничиваясь, директоров по информации, директоров по информационной безопасности агентства, санкционирующих должностных лиц (также известных как уполномоченные по аттестации), владельцев информационной системы и владельцев информации.

[8] Руководство по адаптации для базовых меры безопасности представлено в NIST Специальной Публикации 800-53.

директора по информации, директора по информационной безопасности агентства, санкционирующие должностные лица или уполномоченные представители санкционирующих должностных лиц). Результирующий набор мер безопасности должен быть задокументирован в плане обеспечения безопасности для информационной системы.

ПРИЛОЖЕНИЕ А ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АТТЕСТАЦИЯ: 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.

АДЕКВАТНАЯ БЕЗОПАСНОСТЬ: Безопасность, соразмерная с риском и величиной вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации. [Циркуляр OMB A-130, Приложение III]

АГЕНТСТВО: Любой исполнительный департамент, военный департамент, правительственная корпорация, контролируемая правительством корпорация или другое учреждение в исполнительных органах правительства (включая Администрацию Президента), или любой независимый контролирующий орган, но не включая: (i) Управление государственной ответственности; (ii) Федеральная избирательная комиссия; (iii) правительства Округа Колумбия и территорий и владений Соединенных Штатов, и их различных подразделений; или (iv) принадлежащие правительству управляемые подрядчиком организации, включая лаборатории участвующие в работах исследования и производства для национальной обороны. [44 U.S.C. США, Секция 3502]

АУТЕНТИФИКАЦИЯ: Проверка идентификационных данных пользователя, процесса или устройства, обычно как предпосылка к предоставлению доступа к ресурсам в информационной системе.

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.*

ДОСТУПНОСТЬ: Обеспечение своевременного и надежного доступа к и использования информации. [44 U.S.C. США, Секция 3542]

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.

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. [44 U.S.C. США, Секция 5125 (b)]

ДИРЕКТОР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: См. Директор по информационной безопасности Агентства.

КОНФИДЕНЦИАЛЬНОСТЬ: Сохранение санкционированных ограничений на доступ к и раскрытие информации, включая средства для защиты неприкосновенности личной жизни и конфиденциальной информации. [44 U.S.C. США, Секция 3542]

КОНТРМЕРЫ: Действия, устройства, процедуры, технологии или другие меры, которые уменьшают уязвимость информационной системы. [Инструкция 4009 CNSS] *Синонимично с мерами безопасности и мерами защиты.*

СРЕДА: Совокупность внешних процедур, условий и объектов, влияющих на разработку, эксплуатацию и поддержку информационной системы. [Инструкция 4009 CNSS]

ИСПОЛНИТЕЛЬНОЕ АГЕНТСТВО: исполнительный департамент, определенный в 5 U.S.C. США, Секция 101; военный департамент, определенный в 5 U.S.C. США, Секция 102; независимое учреждение как определено в 5 U.S.C. США, Секция 104 (1); и полностью находящаяся в собственности Правительства корпорация, полностью попадающая под действие 31 U.S.C. США, ГЛАВЫ 91. [41 U.S.C. США, Секция 403]

ФЕДЕРАЛЬНОЕ АГЕНТСТВО: См. Агентство.

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. США, Секция 11331]

СИСТЕМА ВЫСОКОГО 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 «высокий».

ИНЦИДЕНТ: Событие, которое фактически или потенциально подвергает опасности конфиденциальность, целостность, или доступность информационной системы или обрабатываемой, хранимой или передаваемой информации системы или которое представляет нарушение или непосредственную угрозу нарушения политик безопасности, мер безопасности или политик допустимого использования.

ИНФОРМАЦИЯ: Частный **с**лучай типа информации. [Публикация 199 FIPS]

ВЛАДЕЛЕЦ ИНФОРМАЦИИ: Должностное лицо с установленными законом или исполнительными полномочиями для указанной информации и ответственностью за установление мер по ее генерации, сбору, обработке, распространению и уничтожению. [Инструкция 4009 CNSS]

ИНФОРМАЦИОННЫЕ РЕСУРСЫ: Информация и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии. [44 U.S.C. США, Секция. 3502]

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. США, Секция 3542]

ИНФОРМАЦИОННАЯ СИСТЕМА: Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или уничтожения информации. [44 U.S.C. США, Секция 3502]

ВЛАДЕЛЕЦ ИНФОРМАЦИОННОЙ СИСТЕМЫ: Должностное лицо, ответственное за полное приобретение, разработку, интеграцию, модификацию или эксплуатацию и поддержку информационной системы. [Инструкция 4009 CNSS, Уточненная]

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ: Любое оборудование или взаимосвязанная система или подсистема оборудования, которое используется в автоматизированном приобретении, 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 реализации 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. США, Секция 1401]

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. [Публикация 199 FIPS]

ЦЕЛОСТНОСТЬ: Принятие мер против несанкционированной модификации или разрушения информации, включая гарантирование неотказуемости от информации и её аутентичности … [44 U.S.C. США, Секция 3542]

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».

ОРГАНИЗАЦИОННЫЕ МЕРЫ БЕЗОПАСНОСТИ: Меры безопасности (то есть, меры защиты или контрмеры) для информационной системы, которые сосредотачиваются на управлении риском и управлении безопасностью информационной системы.

НОСИТЕЛЬ ИНФОРМАЦИИ: Физические устройства или записывающие поверхности включающие, но не ограничивающиеся, магнитные ленты, оптические диски, магнитные диски, микросхемы памяти высокого уровня интеграции (LSI), распечатки (но нет включающие дисплейные устройства), на которых делается запись, хранение или печать информации в информационной системе.

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».

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.

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].

ЭКСПЛУАТАЦИОННЫЕ МЕРЫ: Меры безопасности (то есть, меры защиты или контрмеры) для информационной системы, которые реализованы и выполнены прежде всего людьми (в противоположность системам).

ОРГАНИЗАЦИЯ: Федеральное агентство или, если применимо, любой из его операционных элементов.

ПОТЕНЦИАЛЬНОЕ ВОЗДЕЙСТВИЕ: Потеря конфиденциальности, целостности или доступности, как ожидается, будет иметь ограниченное отрицательное воздействие, серьезное отрицательное воздействие или тяжелое или катастрофическое отрицательное воздействие на деятельность организации, активы организации или людей. [Публикация 199 FIPS]

ЗАПИСИ: Все книги, бумаги, карты, фотографии, машиночитаемые материалы или другие документальные материалы, независимо от физической формы или характеристик, сделанные или полученные агентством Правительства Соединенных Штатов в соответствии с Федеральным законом или в связи с общей деятельностью и сохраненные или подготовленные для сохранения этим агентством или его законным преемником как свидетельство структуры, функций, политик, решений, процедур, деятельности или других работ Правительства или из-за информационного значения данных в них. [44 U.S.C. США Секция 3301]

РИСК: Уровень воздействия на деятельность организации (включая предназначение, функции, имидж или репутацию), активы организации или людей, следующие из использования информационной системы, подвергаемой потенциальному воздействию угрозы, и вероятность появления угрозы.

УПРАВЛЕНИЕ РИСКАМИ: Процесс управления рисками в отношении деятельности организации (включая предназначение, функции, имидж, или репутацию), активов организации или людей, следующими из использования информационной системы, включающий: (i) проведение оценки степени риска; (ii) реализация стратегии уменьшения риска; и (iii) использование технологий и процедур для непрерывного мониторинга состояния безопасности информационной системы.

МЕРЫ ЗАЩИТЫ: Защитные меры, предписанные, чтобы выполнить требования безопасности (то есть, конфиденциальность, целостность и доступность), определенные для информационной системы. Меры защиты могут включать средства защиты, ограничения управления, безопасность персонала и безопасность физических структур, областей и устройств. [Инструкция 4009 CNSS, Уточненная] *Синонимично с мерами безопасности и контрмерами.*

ОЧИСТКА: Процесс удаления информации из носителя информации так, что информационное восстановление информации становится не возможным. Она включает удаление всех меток, маркировок и журналов операций. [Инструкция 4009 CNSS, Уточненная]

КАТЕГОРИЯ БЕЗОПАСНОСТИ: КАТЕГОРИЯ БЕЗОПАСНОСТИ: Характеристика информации или информационной системы, основанная на оценке потенциального воздействия, которое имелось бы на деятельность организации, активы организации или людей от потери конфиденциальности, целостности или доступности такой информации или информационной системы. [Публикация 199 FIPS]

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. [Публикация 199 FIPS]

БАЗОВЫЙ МЕРЫ БЕЗОПАСНОСТИ: Набор минимальных мер безопасности, определенных для информационной системы низкого воздействия, умеренного воздействия или высокого воздействия.

ЦЕЛЬ БЕЗОПАСНОСТИ: Конфиденциальность, целостность или доступность. [Публикация 199 FIPS]

ПЛАН ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ: См. План безопасности системы.

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ: Требования, предписанные информационной системе, которые получены из действующих законов, Правительственных распоряжений, директив, политик, стандартов, инструкций, нормативных документов или процедур, или предназначение/деятельности организации для того, чтобы гарантировать конфиденциальность, целостность и доступность обрабатываемой, хранимой или передаваемой информации.

ДИРЕКТОР АГЕНТСТВА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: Должностное лицо, ответственное за то, чтобы выполнять обязанности Директора по информации, определенные FISMA, и служить основной связью Директора по информации с санкционирующими должностными лицами агентства, владельцами информационной системы и сотрудниками безопасности информационной системы. [44 U.S.C. США, Секция 3544]

СИСТЕМА: См. информационная систему.

ПЛАН БЕЗОПАСНОСТИ СИСТЕМЫ: Формальный документ, который обеспечивает представление требований безопасности для информационной системы и описывает существующие или планируемые меры безопасности для того, чтобы удовлетворить эти требования. [NIST Специальная Публикация 800-18, Версия 1]

ТЕХНИЧЕСКИЕ МЕРЫ БЕЗОПАСНОСТИ: Меры безопасности (то есть, меры защиты или контрмеры) для информационной системы, которые реализованы и выполнены информационной системой прежде всего через механизмы, содержавшиеся в аппаратных средствах, программном обеспечении или компонентах встроенного микропрограммного обеспечения системы.

УГРОЗА: Любое обстоятельство или событие с потенциалом к неблагоприятному воздействию на деятельность организации (включая предназначение, функции, имидж или репутацию), активы организации или людей через информационную систему посредством несанкционированного доступа, разрушения, раскрытия, модификации информации и/или отказ сервиса. Также, потенциал источника угрозы, чтобы успешно использовать определенную уязвимость информационной системы. [Инструкция 4009 CNSS, Уточненная]

ИСТОЧНИК УГРОЗЫ: Намерение и метод , имеющий цель в намеренной эксплуатации уязвимости или ситуации, и метод, который может случайно инициировать уязвимость. *Синонимично с агентом угрозы.*

ПОЛЬЗОВАТЕЛЬ: Человек или (системный) процесс, авторизованный на доступ к информационной системе. [Инструкция 4009 CNSS]

УЯЗВИМОСТЬ: Слабость в информационной системе, процедурах обеспечения безопасности в системе, внутренних мерах безопасности или в их реализации, которая могла быть использована или инициирована источником угрозы. [Инструкция 4009 CNSS, Уточненная]

ПРИЛОЖЕНИЕ В ССЫЛКИ

[1] Комитет по Системам Национальной безопасности (CNSS) Инструкция 4009, *Национальный Глоссарий по Информационному доверию*, май 2003.

[2] Закон об электронном правительстве 2002 (Общественный закон 107-347), декабрь 2002.

[3] Публикация 199 Стандартов обработки федеральной информации, *Стандарты для Категорирования Безопасности Федеральной информации и Информационных систем*, февраль 2004.

[4] Закон об управлении безопасностью Федеральной информации 2002 (Общественный закон 107-347, Заголовок III), декабрь 2002.

[5] Парламентская реформа управления информационными технологиями 1996 (Общественный закон 104-106), август 1996.

[6] Национальный институт стандартов и технологий Специальная Публикация 800-18, Версия 1, *Руководство для Разработки Планов обеспечения безопасности для Федеральных информационных систем*, февраль 2006.

[7] Национальный институт стандартов и технологий Специальная Публикация 800-53, *Рекомендуемые Меры безопасности для Федеральных информационных систем*, февраль 2005.

[8] Национальный институт стандартов и технологий Специальная Публикация 800-60, *Руководство для Отображения Типов Информации и Информационных систем к Категориям безопасности*, июнь 2004.

[9] Министерство управления и бюджета, Циркуляр А-130, Переходящий Меморандум #4, У*правление Федеральными информационными Ресурсами*, Приложением III, *Безопасность Федеральных Автоматизированных Информационных Ресурсов*, ноябрь 2000.

ПРИЛОЖЕНИЕ С АКРОНИМЫ

CIO Директор по информации

CNSS Комитет по Системам Национальной безопасности

FIPS Стандарты обработки федеральной информации

FISMA Закон об управлении безопасностью Федеральной информации

NIST Национальный институт стандартов и технологий

OMB Министерство управления и бюджета

USC Кодекс Соединенных Штатов