Специальная публикация NIST 800-53
Пересмотр 4

Меры обеспечения безопасности и приватности для Федеральных информационных систем и организаций

ОБЪЕДИНЕННАЯ ЭКСПЕРТНАЯ ГРУППА
ПО ИНИЦИАТИВЕ ПРЕОБРАЗОВАНИЯ

Эта публикация доступна бесплатно на:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

Специальная публикация NIST 800-53
Пересмотр 4

Меры обеспечения безопасности и приватности для Федеральных информационных систем и организаций

ОБЪЕДИНЕННАЯ ЭКСПЕРТНАЯ ГРУППА
ПО ИНИЦИАТИВЕ ПРЕОБРАЗОВАНИЯ

Эта публикация доступна бесплатно на:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

Апрель 2013
Включая дополнения от 01-22-2015

Министерство торговли США
Rebecca M. Blank, ИО Министра

Национальный институт стандартов и технологий
Patrick D. Gallagher, Заместитель министра торговли по стандартам и технологиям и Директор

Полномочия

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

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. Эта публикация может быть использована на добровольной основе неправительственными организациями и это не попадает по действие авторского права в Соединенных Штатах. Однако упоминание приветствовалось бы NIST.

Национальный институт стандартов и технологий, Специальная публикация 800-53, Пересмотр 4
462 страницы (Апрель 2013)
CODEN: NSPUE2

Эта публикация доступна бесплатно на: http://dx.doi.org/10.6028/NIST.SP.800-53r4

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

В этой публикации могут быть ссылки к другим разрабатываемым в настоящий момент публикациям NIST в соответствии с возложенными на него законными обязанностями. Информация в этой публикации, включая концепции и методологию, может быть использована федеральными агентствами ещё до завершения таких сопутствующих публикаций. Таким образом, до тех пор, пока каждая публикация не завершена, текущие требования, руководства и процедуры, где они существуют, остаются действующими. Для целей планирования и перехода федеральные агентства имеют возможность постоянно отслеживать разработку этих новых публикаций в NIST.

Организации поощрены рассматривать все черновые публикации во время периодов для публичных комментариев и предоставлять обратную связь в NIST. Все публикации Отдела компьютерной безопасности NIST, кроме некоторых указанных выше, доступны в http://csrc.nist.gov/publications.

Комментарии по этой публикации могут быть направлены в:

Национальный институт стандартов и технологий
Для: Отдел компьютерной безопасности, Лаборатория информационных технологий
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Электронная почта: sec-cert@nist.gov

Отчёты по технологиям компьютерных систем

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

Краткий обзор

Эта публикация обеспечивает каталог мер обеспечения безопасности и приватности для федеральных информационных систем и организаций и процесса выбора мер безопасности для защититы деятельности организаций (включая предназначение, функции, имидж и репутацию), активов, организаций, людей, других организаций и Нации от набора разнообразных угроз, включая враждебные кибератаки, стихийные бедствия, структурные отказы и человеческие ошибки. Меры обеспечения адаптируются и реализуются как часть общего для организации процесса, который управляет информационными рисками безопасности и приватности. Меры обеспечения определяются разнообразным набором требований безопасности и приватности для федерального правительства и критической инфраструктуры, полученных из законодательства, Правительственных распоряжений, политик, директив, нормативных актов, стандартов и/или потребностей предназначения и деятельности. Публикация также описывает, как разработать специализированные наборы мер обеспечения или оверлеи, адаптированные для определенных типов функций предназначения/ деятельности, технологий или сред эксплуатации. Наконец, каталог мер безопасности определяет безопасность и с точки зрения функциональности (обеспечиваемой стойкостью функций и механизмов безопасности) и с точки зрения доверия (мер уверенности в реализованных возможностях безопасности). Обеспечение и функциональности безопасности и доверия к безопасности гарантирует, что продукты информационных технологий и информационные системы, созданные из этих продуктов, используя системные и инженерные принципы обеспечения безопасности, достаточно доверенны.

Ключевые слова

Доверие; компьютерная безопасность; FIPS публикация 199; FIPS публикация 200, FISMA; Закон о неприкосновенности частной жизни; Основы управления рисками; меры безопасности; требования безопасности.

Благодарность

Эта публикация была разработана Межведомственной рабочей группой *объединенной экспертной группы по инициативе преобразования* совместно с представителями Гражданского, Оборонного и Разведывательного ведомств в продолжение усилий по созданию единой основы информационной безопасности для федерального правительства. Национальный институт стандартов и технологий хочет выразить благодарность и признательность высшим руководителям от Министерств Торговли и Обороны, Офиса Директора Национальной Разведки, Комитета по Системам Национальной безопасности и членам межведомственной технической рабочей группы, чьи объединенные усилия значительно способствовали публикации. Высшие руководители, члены межведомственной рабочей группы и их организационная принадлежность включают:

Министерство обороны

Teresa M. Takai
Директор по информации МО

Robert J. Carey
Первый заместитель Директора по информации МО

Richard Hale
Заместитель Директора по информации по кибербезопасности

Dominic Cussatt
Заместитель директора, политика кибербезопасности

Офис Директора Национальной Разведки

Adolpho Tarasiuk Jr.
Помощник DNI и Директор по информации Разведывательного ведомства

Charlene Leubecker
Заместитель Директора по информации Разведывательного ведомства

Catherine A. Henson
Директор, управление данными

Greg Hall
Руководитель, Отдел программ управления рисками и информационной безопасности

Национальный институт стандартов и технологий

Charles H. Romine
Директор, Лаборатория информационных технологий

Donna Dodson
Советник по вопросам кибербезопасности, Лаборатория информационных технологий

Donna Dodson
Руководитель, Отдел компьютерной безопасности

Ron Ross
Руководитель проекта реализации FISMA

Комитет по Системам национальной безопасности

Teresa M. Takai
Председатель, CNSS

Richard Spires
Сопредседатель, CNSS

Dominic Cussatt
Сопредседатель подкомитета CNSS

Jeffrey Wilk
Сопредседатель подкомитета CNSS

Richard Tannich
Сопредседатель подкомитета

Межведомственная рабочая группа Объединенной экспертной группы по инициативе преобразования

Ron Ross *NIST, Лидер JTF*	Gary Stoneburner *APL Джонса Хопкинса*	Richard Graubart *MITRE Corporation*	Kelley Dempsey *NIST*
Esten Porter *MITRE Corporation*	Bennett Hodge *Буз Аллен Гамильтон*	Karen Quigg *MITRE Corporation*	Christian Enloe *NIST*
Kevin Stine *NIST*	Jennifer Fabius *MITRE Corporation*	Daniel Faigin *Aerospace Corporation*	Arnold Johnson *NIST*
Lisa Kaiser *DNS*	Pam Miller *MITRE Corporation*	Sandra Miravalle *MITRE Corporation*	Victoria Pillitteri *NIST*

В дополнение к вышеупомянутым выражаем специальную благодарность Peggy Himes и Elizabeth Lennon NIST за их превосходное техническое редактирование и административную поддержку. Авторы также хотят выделить Marshall Abrams, Nadya Bartol, Frank Belz, Deb Bodeau, Dawn Cappelli, Corinne Castanza,

Matt Coose, George Dinolt, Kurt Eleam, Jennifer Guild, Cynthia Irvine, Cass Kelly, Steve LaFountain, Steve Lipner, Tom Macklin, Tim McChesney, Michael McEvilley, John Mildner, Joji Montelibano, George Moore, LouAnna Notargiacomo, Dorian Pappas, Roger Schell, Carol Woody и весь научный персонал Отдела компьютерной безопасности NIST за их исключительное содействие в помощи по улучшению текста публикации. И наконец, авторы также с благодарностью подтверждают и ценят существенные содействия от людей, рабочих групп и организаций в общественных и частных секторах, на национальном и международном уровне, чьи вдумчивые и конструктивные комментарии улучшили общее качество, завершённость и полноценность этой публикации.

FIPS 200 И SP 800-53

РЕАЛИЗАЦИЯ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РУКОВОДСТВ

Публикация FIPS 200, *Минимальные требования безопасности для федеральной информации и информационных систем*, является обязательным федеральным стандартом, разработанным NIST в ответ на FISMA. Чтобы соответствовать федеральному стандарту, организации сначала определяют категорию безопасности своей информационной системы в соответствии с FIPS Публикацией 199, *Стандартами для классификации безопасности федеральной информации и информационных систем*, исходя из категории безопасности, получают уровень воздействия на информационную систему в соответствии с FIPS 200, и затем применяют соответствующий специализированный набор мер базового уровня безопасности из Специальной публикации NIST 800-53, *Меры обеспечения безопасности и приватности для федеральных информационных систем и организаций*. У организаций есть гибкость в применении мер обеспечения базового уровня безопасности в соответствии с руководством, представленным в Специальной публикации 800-53. Это позволяет организациям адаптировать соответствующий базовый набор мер безопасности так, чтобы он более близко соответствовал их предназначением, требованиями к деятельности и средой эксплуатации.

FIPS 200 и Специальная публикация NIST 800-53 совместно гарантируют, что ко всей федеральной информации и информационным системам применены соответствующие требования безопасности и меры безопасности. Оценка организациями риска обеспечивает проверку начального выбора мер безопасности и определение, необходимы ли дополнительные меры, чтобы защитить деятельность организаций (включая задачу, функции, имидж или репутацию), активы организаций, людей, другие организации или Нацию. Результирующий набор мер безопасности устанавливает уровень должной безопасности для организаций.

РАЗРАБОТКА ОБЩИХ ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОТРУДНИЧЕСТВО СРЕДИ СУЩНОСТЕЙ ОБЩЕСТВЕННОГО И ЧАСТНОГО СЕКТОРА

При разработке стандартов и руководств, требуемых FISMA, NIST консультируется с другими федеральными агентствами и с частным сектором, чтобы улучшить информационную безопасность, избежать ненужного и дорогостоящего дублирования усилий и гарантировать, что его публикации соотносятся со стандартами и руководствами, используемыми для защиты систем национальной безопасности. В дополнение к всестороннему публичному процессу рассмотрения и исследования, NIST сотрудничает с Офисом Директора национальной разведки (ODNI), Министерством обороны (DoD) и Комитетом по системам национальной безопасности (CNSS), чтобы установить унифицированную основу информационной безопасности для федерального правительства. Общая основа информационной безопасности обеспечит Гражданский, Оборонный и Разведывательный сектора федерального правительства и их подрядчиков более рентабельными и непротиворечивыми способами управления риском, связанным с информационной безопасностью, в отношении деятельности организаций, активов организаций, людей, других организаций и Нации. Унифицированная основа также обеспечит прочное основание для взаимного принятия решений по санкционированию и облегчит совместное использование информации. NIST также работает со многими сущностями общественного и частного сектора, чтобы установить отображения и отношения между стандартами обеспечения безопасности и руководствами, разработанными NIST и Международной организацией по стандартизации и Международной электротехнической комиссией (ISO/IEC).

ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

С ТОЧКИ ЗРЕНИЯ РАЗЛИЧНЫХ СООБЩЕСТВ ПО ИНТЕРЕСАМ

Термин *требования безопасности* используется различными сообществами и группами по-разному и требуется дополнительное объяснение чтобы установить определеный контекст для различных вариантов использования. Требования безопасности могут быть заявлены на очень высоком уровне абстракции, например, в законодательстве, Правительственных распоряжениях, директивах, политиках, стандартах и описаниях потребностей предназначения/деятельности. FISMA и FIPS публикация 200 ясно формулируют требования безопасности на таком уровне.

Персонал приобретения разрабатывает требования безопасности для целей заключения контракта, которые определяют необходимость защиты, чтобы достигнуть потребности предназначения/ деятельности. Системные инженеры, инженеры по безопасности, разработчики систем и системные интеграторы разрабатывают проектные требования безопасности для информационных систем, разрабатывают архитектуру безопасности систем и архитектурно-зависимые требования безопасности, и впоследствии, реализуют конкретные функции безопасности в аппаратных средствах, программном обеспечении и на уровне компонентов встроенного микропрограммного обеспечения.

Требования безопасности также отражены в различных нетехнических мерах безопасности, которые определяют такие вопросы как политика и процедуры в управленческих и эксплуатационных элементах организаций в различных уровнях детализации. Важно определить контекст для каждого использования термина требования безопасности таким образом, чтобы соответствующие сообщества (включая людей, ответственных за политику, архитектуру, приобретение, технику и защиту предназначения/ деятельности) могли ясно передать свое намерение.

Организации могут определить некоторые *возможности безопасности*, необходимые для удовлетворения требованиям безопасности, и обеспечить соответствующую защиту предназначения и деятельности. Возможности безопасности, как правило, определяются объединением в конкретный набор мер защиты/контрмер (то есть, мер безопасности), полученных из соответственно уточненных базовых наборов мер, которые вместе формируют необходимые возможности.

НЕЙТРАЛЬНОСТЬ ТЕХНОЛОГИИ И ПОЛИТИКИ

ХАРАКТЕРИСТИКИ МЕР БЕЗОПАСНОСТИ

Меры безопасности в каталоге, за редким исключением, были разработаны, чтобы быть нейтральными в отношении политик и технологий. Это означает, что меры безопасности и улучшения мер безопасности сосредотачиваются на фундаментальных мерах защиты и контрмерах, необходимых, чтобы защитить информацию при обработке, во время хранения и при передаче. Поэтому, за рамки этой публикации выходит представление о приложении мер безопасности к конкретным технологиям, средам эксплуатации, сообществам интереса или функциям предназначения/деятельности. Специализированные области определяются при помощи процесса адаптации, описанного в Главе Три и использования оверлеев, описанных в Приложении I. Нужно также отметить, что в то время как меры безопасности в значительной степени нейтральны в отношении полит и технологий, это в действительности не подразумевает, что меры безопасности не подразумевают политик и технологий. Понимание политик и технологий необходимо, чтобы меры безопасности были значимы и соответствующе реализованы.

В немногих случаях, когда конкретные технологии упомянуты в мерах безопасности (например, мобильные устройства, PKI, беспроводная связь, VOIP), организациям дается предостережение, что потребность обеспечить адекватную безопасность находится вне требований к отдельной мере безопасности, связанной с определенной технологией. Многие из необходимых мер и контрмер защиты получаются из других мер безопасности в каталоге, выделением начального базоввого набора мер безопасности как начальной точки для разработки планов обеспечения безопасности и оверлеев, используя процесс адаптации. Может также быть некоторое перекрытие в защите, связанное с мерами безопасности в различных семействах мер безопасности.

В дополнение к управляемой клиентом разработке специализированных планов обеспечения безопасности и оверлеев, Специальные публикации NIST и Межведомственные отчеты могут дать представление о рекомендуемых мерах безопасности для конкретных технологий и специфичных для сектора приложений (например, программно-управляемые сети, здравоохранение, промышленные системы управления и мобильные устройства).

Использование каталога мер безопасности, нейтрального в отношении технологий и политик, обладает следующими преимуществами:

- Это поощряет организации сосредотачиваться на *возможностях безопасности*, требуемых для успеха в предназначении/деятельности и защите информации, независимо от информационных технологий, которые используются в информационных системах организаций.
- Это поощряет организации анализировать каждую меру безопасности для ее применения в конкретных технологиях, средах эксплуатации, функциях предназначения/деятельности и сообществах интересов.
- Это поощряет организации определять политику безопасности как часть процесса адаптации для мер безопасности, у которых есть переменные параметры.

Специализация планов обеспечения безопасности, с использованием руководства по адаптации и оверлеев, вместе с устойчивым набором нейтральных в отношении технологий и политик мер безопасности, способствует рентабельной, основанной на риске информационной безопасности для организаций в любом секторе, для любой технологии и в любой среде применения.

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДОЛЖНУЮ СТАРАТЕЛЬНОСТЬ

УПРАВЛЕНИЕ РИСКОМ В ОТНОШЕНИИ ФУНКЦИЙ ПРЕДНАЗНАЧЕНИЯ/ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИЙ

Меры безопасности в Специальной публикации NIST 800-53 разработаны, чтобы облегчить согласие с применимыми федеральными законами, Правительственными распоряжениями, директивами, политиками, нормативными актами, стандартами и руководствами. Согласие это *не* соблюдение статических контрольных списков или генерирование не требуемых FISMA отчетных документов. Скорее, согласие требует *должной старательности* организаций относительно информационной безопасности и управления рисками. Должная старательность в информационной безопасности включает использование всей соответствующей информации как часть общей для организации программы управления рисками, чтобы эффективно использовать руководство адаптации и свойственную публикациям NIST гибкость в том, чтобы выбранные меры безопасности, задокументированные в планы обеспечения безопасности организаций, выполняли требования по предназначению и деятельности организаций. Использование инструментов управления рисками и технологий, которые доступны организациям, важно в разработке, реализации и поддержании мер защиты и контрмер с необходимой и достаточной стойкостью механизмов, чтобы противостоять текущим угрозам деятельности и активам организаций, людям, другим организациям и Нации. Применение эффективных, основанных на риске процессов, процедур и технологий поможет гарантировать то, что у всех федеральных информационных систем и организаций есть необходимая устойчивость, чтобы поддерживать имеющиеся федеральные обязанности, критические приложения инфраструктуры и непрерывность руководства.

МЕРЫ ОБЕСПЕЧЕНИЯ ПРИВАТНОСТИ

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ПРИВАТНОСТИ ДЛЯ ФЕДЕРАЛЬНОЙ ИНФОРМАЦИИ

Приложение J, *Каталог Мер приватности*, является новым дополнением к NIST Специальной публикации 800-53. Оно предназначено, чтобы обеспечить потребности в приватности для федеральных агентств. Приложение приватности:

- Обеспечивает структурированный набор мер приватности, основанных на лучших методах, что поможет организациям выполнять применимые федеральные законы, Правительственные распоряжения, директивы, инструкции, нормативные акты, политики, стандарты, руководства и специфичные для организаций публикации;
- Устанавливает зависимости и отношения между мерами обеспечения приватности и безопасности с целью определения соответствующих требований приватности и безопасности, которые могут наложиться в проектах и в реализации для федеральных информационных систем, программ и организаций;
- Демонстрирует применимость основ управления рисками NIST при выборе, реализации, оценке и постоянном мониторинге мер приватности, реализуемых в федеральных информационных системах, программах и организациях; и
- Способствует более тесному сотрудничеству между должностными лицами по приватности и безопасности в рамках федерального правительства, чтобы помочь в достижении целей высших лидеров/руководителей по установлению требований в федеральном законодательстве, политиках, нормативных актах, директивах, стандартах и руководствах по приватности.

Есть большое сходство в структуре мер приватности в Приложении J и мер безопасности в Приложениях F и G. Например, мера AR-1 (Управление и программа приватности) требует, чтобы организации разработали планы обеспечения приватности, которые могут быть реализованы на уровне организации или на уровне программы. Эти планы могут также использоваться в соединении с планами обеспечения безопасности, что предоставляет возможность организациям выбрать соответствующий набор мер обеспечения безопасности и приватности в соответствии с требованиями к предназначению/деятельности организаций и средами, в которых действуют организации. Включение аналогичных концепций, используемых в управлении рисками информационной безопасности, помогает организациям реализовать меры приватности в более рентабельном, основанном на анализе риска способе, одновременно защищая отдельно приватность и удовлетворяя взаимоувязанным требованиям. Стандартизированные меры приватности обеспечивают более дисциплинированный и структурированный подход для того, чтобы он удовлетворил федеральным требованиям приватности и демонстрировал согласие с другими требованиями.

ПРЕДОСТЕРЕЖЕНИЕ

РЕАЛИЗАЦИЯ ИЗМЕНЕНИЙ, ОСНОВАННЫХ НА ПЕРЕСМОТРАХ СПЕЦИАЛЬНОЙ ПУБЛИКАЦИИ 800-53

Когда NIST публикует пересмотры Специальной публикации 800-53, есть четыре основных типа изменений, произведенных в документе: (i) меры безопасности или улучшения мер безопасности добавлены или удалены из Приложений F и G и/или для низкого, умеренного и высокого базовых уровней; (ii) изменено дополнительное руководство; (iii) изменен материал в основных главах или приложениях; и (iv) стиль изложения уточнен и/или обновлен всюду по документу.

Когда изменяются существующие специализированные базовыенаборы мер безопасности на Уровне 3 в иерархии управления рисками (как описано в Специальной публикации 800-39) и обновляются меры безопасности на любом уровне как результат пересмотра Специальной публикации 800-53, организации должны применять проверенный, основанный на риске подход, в соответствии с допустимым риска для организаций и текущими оценками степени риска. Если иначе не определено политикой OMB, следующие работы рекомендуется реализовать при изменениях в Специальной публикации 800-53:

- Во-первых, организации определяют, применимы ли какие-либо дополнительные меры безопасности/улучшения мер безопасности к информационным системам организаций или средам эксплуатации после адаптации руководств в этой публикации.
- Затем, организации пересматривают изменения в дополнительных руководствах, руководствах в основных главах и приложениях и обновления/разъяснения стиля изложения всюду по публикации, чтобы определить, применимы ли изменения к каким-либо информационным системам организаций и требуются ли любые немедленные действия.
- Наконец, как только организации определили полноту изменений, требуемых ами публикации, изменения интегрируются в установленный непрерывный процесс контроля до самой большой возможной степени. Реализация новых или измененных мер безопасности, направленных на устранение специфических, актуальных угроз, всегда является самым высоким приоритетом для упорядочивания и реализации изменений. Модификации, такие как изменения к шаблонам или незначительные изменения стиля изложения в политиках или процедурах, являются обычно самым низким приоритетом и делаются в соответствии с установленным циклом пересмотра.

Оглавление

Пролог

"... Посредством процесса управления рисками лидеры должны рассмотреть риск к интересам США от противников, использующих киберпространство для достижения ими преимущества, и от наших собственных усилий использовать глобальную природу киберпространства для достижения целей в военных, разведывательных и бизнес операциях..."

"... Для разработки планов деятельности должна быть оценена комбинация угроз, уязвимостей и воздействий, чтобы определить важные тенденции и решить, где усилие должно быть применено, чтобы устранить или уменьшить возможности угрозы; устранить или уменьшить уязвимости; и оценить, скоординировать и устранить конфликты во всех операциях в киберпространстве..."

"... Лидеры на всех уровнях являются ответственными за обеспечение готовности и безопасности до той же самой степени как в любом другом домене..."

- НАЦИОНАЛЬНАЯ СТРАТЕГИЯ ОПЕРАЦИЙ В КИБЕРПРОСТРАНСТВЕ

ОФИС ПРЕДСЕДАТЕЛЯ, ОБЪЕДИНЕННЫЙ КОМИТЕТ НАЧАЛЬНИКОВ ШТАБОВ, АМЕРИКАНСКОЕ МИНИСТЕРСТВО ОБОРОНЫ

Предисловие

Специальная публикация NIST 800-53, Пересмотр 4, представляет самое всестороннее обновление каталога мер безопасности начиная с его первого выпуска в 2005г. Публикация была разработана NIST, Министерством обороны, Разведывательным ведомством и Комитетом по системам национальной безопасности в рамках Совместной экспертной группы, межведомственного партнерства, сформированного в 2009г. Это обновление было мотивировано преимущественно расширяющимся пространством угроз, характеризуемым увеличивающейся изощренностью кибератак и темпом действий противников (то есть, частотой таких атак, профессионализмом атакующих и целеустремленностью атакующих). Практические меры безопасности и улучшения мер были разработаны и интегрированы в каталог, адресованный к таким областям, как: мобильные и облачные вычисления; безопасность приложений; защищенность, доверие и устойчивость информационных систем; инсайдерские угрозы; безопасность системы поставок и постоянные развивающиеся угрозы. Кроме того, Специальная публикация 800-53 была расширена, чтобы включить восемь новых семейств мер приватности, основанных на принятых на международном уровне Принципах честной информационной практики.

Специальная публикация 800-53 Пересмотр 4 обеспечивает более *целостный* подход для управления информационной безопасностью и управления рисками, предоставляя организациям охват и глубину мер безопасности, необходимых, чтобы существенно усилить их информационные системы и среды, в которых эти системы применяются - содействие системам, чтобы они были более устойчивы перед лицом кибератак и других угроз. Эта стратегия "Стройте правильно" применяется вместе со множеством мер безопасности для "Непрерывного мониторинга", чтобы дать организациям информацию близко к реальному времени, которая важна для высших руководителей, принимающих долговременные, *основанные на риске* решения, влияющие на их критические функции предназначения и деятельности.

Чтобы использовать в своих интересах расширенный набор мер обеспечения безопасности и приватности и дать организациям большую гибкость и оперативность в защите их информационных систем, в этом пересмотре была представлена концепция *оверлеев*. Оверлеи обеспечивают структурированный подход, чтобы помочь организациям адаптировать базовые наборы мер безопасности и разработать специализированные планы обеспечения безопасности, которые могут быть применены к конкретным функциям предназначения/деятельности, средам эксплуатации и/или технологиям. Этот подход специализации важен, так как число управляемых угрозами мер безопасности и улучшений меры безопасности в каталоге увеличивается и организации разрабатывают стратегии управления рисками, чтобы определить их конкретные потребности защиты в пределах определенных допусков риска.

Наконец, было несколько новых опций, добавленных к этой версии, чтобы облегчить простоту её использования организациями. Они включают:

- Предположения, касающиеся мер безопасности, принимаемых за основу разработки;
- Расширенное, обновленное и оптимизированное руководство адаптации;
- Дополнительные параметры операций назначения и выбора для мер обеспечения безопасности и приватности;
- Описательные имена для мер улучшения безопасности и приватности;
- Консолидированные таблицы для мер безопасности и улучшений мер по семействам с распределением по базовым наборам мер;
- Таблицы для мер безопасности, которые поддерживают разработку, оценку и применение доверия; и
- Таблицы отображения для международного стандарта безопасности ISO/IEC 15408 (Общие Критерии).

Меры обеспечения безопасности и приватности в Специальной публикации 800-53 Пересмотр 4 были разработаны, чтобы быть в значительной степени нейтральными в отношении политик и технологий для облегчения гибкости в реализации. Меры обеспечения удобно расположены, чтобы поддержать интеграцию информационной безопасности и приватности в процессы организаций, включая архитектуру предприятия, проектирование систем, жизненный цикл разработки систем и приобретение/снабжение. Успешная интеграция мер обеспечения безопасности и приватности в долговременные процессы организаций будет демонстрировать большую зрелость программ безопасности и приватности и обеспечивать более тесную связь инвестиций в безопасность и приватность с базовыми функциями предназначения и деятельности организаций.

Совместная экспертная группа

Опечатки

Следующие изменения были включены в Специальную публикацию 800-53, Пересмотр 4.

ДАТА	ТИП	ИЗМЕНЕНИЕ	СТРАНИЦА
07.05.2013	Редакция	Изменение Приоритетного кода CA-9 с P1 на P2 в таблице D-2.	D-3
07.05.2013	Редакция	Изменение Приоритетного кода CM-10 с P1 на P2 в таблице D-2.	D-4
07.05.2013	Редакция	Изменение Приоритетного кода MA-6 с P1 на P2 в таблице D-2.	D-5
07.05.2013	Редакция	Изменение Приоритетного кода MP-3 с P1 на P2 в таблице D-2.	D-5
07.05.2013	Редакция	Изменение Приоритетного кода PE-5 с P1 на P2 в таблице D-2.	D-5
07.05.2013	Редакция	Изменение Приоритетного кода PE-16 с P1 на P2 в таблице D-2.	D-5
07.05.2013	Редакция	Изменение Приоритетного кода PE-17 с P1 на P2 в таблице D-2.	D-5
07.05.2013	Редакция	Изменение Приоритетного кода PE-18 с P2 на P3 в таблице D-2.	D-5
07.05.2013	Редакция	Изменение Приоритетного кода PL-4 с P1 на P2 в таблице D-2.	D-6
07.05.2013	Редакция	Изменение Приоритетного кода PS-4 с P2 на P1 в таблице D-2.	D-6
07.05.2013	Редакция	Изменение Приоритетного кода SA-11 с P2 на P1 в таблице D-2.	D-6
07.05.2013	Редакция	Изменение Приоритетного кода SC-18 с P1 на P2 в таблице D-2.	D-7
07.05.2013	Редакция	Изменение Приоритетного кода SI-8 с P1 на P2 в таблице D-2.	D-8
07.05.2013	Редакция	Удаление рекомендации к SA 5(6) в таблице D-17.	D-32
07.05.2013	Редакция	Удаление CM 4(3) из Таблицы E-2.	E-4
07.05.2013	Редакция	Удаление CM 4(3) от Таблицы E-3.	E-5
07.05.2013	Редакция	Удаление рекомендации к SA 5(6).	F-161
07.05.2013	Редакция	Изменение Приоритетного кода SI-16 с P0 на P1.	F-233
01-15-2014	Редакция	Удаление “(и намеренные и неумышленные)” в строке 5 в Кратком обзоре.	iii
01-15-2014	Редакция	Удаление "безопасности и приватности" в строке 5 в Кратком обзоре.	iii
01-15-2014	Редакция	Изменение “ начального набора базовых мер безопасности ” на “применимого базового набора мер безопасности ” в Разделе 2.1, Шаге 2 RMF.	9
01-15-2014	Редакция	Удаление следующего абзаца: “Раздел улучшений меры безопасности обеспечивает … в Приложении F.”	11
01-15-2014	Редакция	Изменение “базовых мер безопасности” на “базовых наборов мер безопасности” в Разделе 2.3, 2-ом абзаце, строка 6.	13
01-15-2014	Редакция	Изменение “начального набор мер безопасности” на “применимого базового набора мер безопасности” в Разделе 3.1, абзаце 2, строка 4.	28
01-15-2014	Редакция	Изменение “ базовых наборов мер безопасности ” на “ базовых наборов, идентифицированных в Приложении D ” в Разделе 3.1, абзаце 2, строка 5.	28
01-15-2014	Редакция	Изменение “соответствующего набора базовых мер безопасности” на “соответствующего базового набора мер безопасности ” в Разделе 3.1, абзаце 3, строка 3.	29
01-15-2014	Редакция	Удаление "начального" перед “ базового набора мер безопасности ” и добавленние “FIPS 200” перед "уровне воздействия" в Разделе 3.1, абзаце 3, строка 4.	29
01-15-2014	Редакция	Изменение “наборов базовых мер безопасности ” на “базовых наборов мер безопасности ” в Разделе 3.1, абзаце 3, строка 6.	29
01-15-2014	Редакция	Изменение “начального набора базовых мер безопасности ” на “применимого базового набора мер безопасности ” в Разделе 3.2, абзаце 1, строка 1.	30
01-15-2014	Редакция	Изменение “начального набора базовых мер безопасности ” на “применимого базового набора мер безопасности ” в Разделе 3.2, абзаце 3, строка 5.	31
01-15-2014	Редакция	Удаление “набор” перед "мерами безопасности" в Разделе 3.2, Использование объектовых особенностей, абзац Мобильность, строка 1.	33
01-15-2014	Редакция	Удаление "начальный" перед “набор” в Разделе 3.2, Использование объектовых особенностей, абзац Мобильность, строка 2.	33

01-15-2014	Редакция	Изменение “базовые” на “каждый базовый” в Разделе 3.2, Использование объектовых особенностей, абзац Мобильность, строка 3.	33
01-15-2014	Редакция	Изменение “начальный набор мер безопасности” на “ базовый набор мер безопасности ” в Разделе 3.2, Использование объектовых особенностей, абзац	33
01-15-2014	Редакция	Добавление "конкретных" перед "мест" в Разделе 3.2, Использование объектовых особенностей, абзац Мобильность, строка 6.	33
01-15-2014	Редакция	Изменение "начальных" на "трёх" в Разделе 3.2, Использование объектовых особенностей, абзац Мобильность, строка 8.	33
01-15-2014	Редакция	Изменение “начальному набору базовых мер безопасности” на “ применимому базовуму набору мер безопасности ” в Разделе 3.2, Выбор компенсирующих мер	36
01-15-2014	Редакция	Изменение “набора начальных базовых мер безопасности” на “ базовых наборов мер безопасности ” в Разделе 3.3, строка 1.	40
01-15-2014	Редакция	Добавление "." после “C.F.R” в №3, ПОЛИТИКИ, ДИРЕКТИВЫ, ИНСТРУКЦИИ, НОРМАТИВНЫЕ АКТЫ И МЕМОРАНДУМЫ.	A-1
01-15-2014	Редакция	Добавление “Пересмотр 1 (Проект)” Специальной публикации NIST 800-52 в Ссылках.	A-7
01-15-2014	Редакция	Добавленние "конфигурированию", к заголовку Специальной публикации NIST 800-52, Пересмотр 1.	A-7
01-15-2014	Редакция	Изменение даты NIST Специальная публикация 800-52, Пересмотр 1 на сентябрь 2013.	A-7
01-15-2014	Редакция	Перемещение определения для Риска информационной безопасности после Плана программы информационной безопасности в Глоссарии.	B-11
01-15-2014	Редакция	Добавление AC 2(11) к высокому базовому набору мер в Таблице D-2.	D-2
01-15-2014	Редакция	Изменение Приоритетного кода AC-10 с P2 на P3 в Таблице D-2.	D-2
01-15-2014	Редакция	Изменение Приоритетного кода AC-14 с P1 на P3 в Таблице D-2.	D-2
01-15-2014	Редакция	Изменение Приоритетного кода AC-22 с P2 на P3 в Таблице D-2.	D-2
01-15-2014	Редакция	Изменение Приоритетного кода AU-10 с P1 на P2 в Таблице D-2.	D-3
01-15-2014	Редакция	Изменение Приоритетного кода CA-6 с P3 на P2 в Таблице D-2.	D-3
01-15-2014	Редакция	Изменение Приоритетного кода CA-7 с P3 на P2 в Таблице D-2.	D-3
01-15-2014	Редакция	Изменение Приоритетного кода CA-8 с P1 на P2 в Таблице D-2.	D-3
01-15-2014	Редакция	Изменение Приоритетного кода IA-6 с P1 на P2 в Таблице D-2.	D-4
01-15-2014	Редакция	Изменение Приоритетного кода IR-7 с P3 на P2 в Таблице D-2.	D-5
01-15-2014	Редакция	Изменение Приоритетного кода MA-3 с P2 на P3 в Таблице D-2.	D-5
01-15-2014	Редакция	Изменение Приоритетного кода MA-4 с P1 на P2 в Таблице D-2.	D-5
01-15-2014	Редакция	Изменение Приоритетного кода MA-5 с P1 на P2 в Таблице D-2.	D-5
01-15-2014	Редакция	Удаление мер Управление программой из Таблицы D-2.	D-8/9
01-15-2014	Редакция	Удаление следующего предложения в конце абзаца: “Семейство Управление программой (PM) не включено в сводную таблицу, так как меры безопасности PM не связаны с каким либо определенным базовым набором мер безопасности.”	D-9
01-15-2014	Редакция	Добавление AC-2(12) и AC-2(13) к высокому базовому набору мер в Таблице D-3.	D-10
01-15-2014	Редакция	Изменение AC-17(5), включено в, ссылки с AC-17 на SI-4 в Таблице D-3.	D-12
01-15-2014	Редакция	Изменение AC-17(5), включено в, ссылки с AC-3 на AC-3(10) в Таблице D-3.	D-12
01-15-2014	Редакция	Изменение AC-6 на AC-6(9) в AU 2(4) уведомление вывода войск в Таблице D-5.	D-15
01-15-2014	Редакция	Изменение "Training" на "Scanning" в заголовке SA 19(4) в Таблице D-17.	D-34
01-15-2014	Редакция	Удаление SC-9(1), SC-9(2), SC-9(3), и SC-9(4) из Таблицы D-18.	D-37
01-15-2014	Редакция	Добавление AC-2 и AC-5 к SC-14 и удаление SI-9 из SC-14 в Таблице D-18.	D-37
01-15-2014	Редакция	Удаление CA-3(5) из Таблицы E-2.	E-4
01-15-2014	Редакция	Добавление CM-3(2) в Таблицу E-2.	E-4

01-15-2014	Редакция	Добавление RA-5(2) и RA-5(5) в Таблицу E-2.	E-4
01-15-2014	Редакция	Удаление CA-3(5) из Таблицы E-3.	E-5
01-15-2014	Редакция	Добавление CM-3(2) в Таблицу E-3.	E-5
01-15-2014	Редакция	Удаление полужирного текста для RA-5(2) и RA-5(5) в Таблице E-3.	E-5
01-15-2014	Редакция	Добавление CM-8(9) в Таблицу E-4.	E-7
01-15-2014	Редакция	Добавление CP-4(4) в Таблицу E-4.	E-7
01-15-2014	Редакция	Добавление IR-3(1) в Таблицу E-4.	E-7
01-15-2014	Редакция	Добавление RA-5(3) в Таблицу E-4.	E-7
01-15-2014	Редакция	Удаление SA-4(4) из Таблицы E-4.	E-7
01-15-2014	Редакция	Изменение в SA-21(1) с «улучшения» на «улучшение» в Таблице E-4.	E-7
01-15-2014	Редакция	Удаление SI-4(8) из Таблицы E-4.	E-7
01-15-2014	Редакция	Изменение “процессе управления риском” на “RMF” в Использование каталога, строка 4.	F-6
01-15-2014	Редакция	Изменение “соответствующий набор мер безопасности” на “соответствующий базовый набор мер безопасности” в Использование каталога, строка 5.	F-6
01-15-2014	Редакция	Удаление лишней “,” из AC-2 g.	F-7
01-15-2014	Редакция	Добавление AC-2(11) в высокий базовый набор.	F-10
01-15-2014	По существу	Добавление следующего текста в AC-3(2) Supplemental Guidance: “Dual authorization may also be known as two-person control.”	F-11
01-15-2014	Редакция	Изменение “ucdmo.gov” на “None” в AC-4 References.	F-18
01-15-2014	Редакция	Добавление “.” после “C.F.R” в AT-2 References.	F-38
01-15-2014	Редакция	Изменение AC-6 на AC-6(9) в AU-2(4) withdrawal notice.	F-42
01-15-2014	Редакция	Удаление “csrc.nist.gov/pcig/cig.html” и добавление “http://” к URL в AU-2 References.	F-42
01-15-2014	Редакция	Изменение “identify” на “identity” в AU-6(6) Supplemental Guidance.	F-46
01-15-2014	По существу	Добавление следующего текста к AU-9(5) Supplemental Guidance: “Dual authorization may also be known as two-person control.”	F-49
01-15-2014	Редакция	Добавление “Control Enhancements: None.” к AU-15.	F-53
01-15-2014	Редакция	Удаление лишней “.” из CM-2(7) Supplemental Guidance.	F-66
01-15-2014	Редакция	Added “)” after “board” in CM-3 g.	F-66
01-15-2014	По существу	Added CA-7 to related controls list in CM-3.	F-66
01-15-2014	По существу	Added the following text to CM-5(4) Supplemental Guidance: “Dual authorization may also be known as two-person control.”	F-69
01-15-2014	Редакция	Добавление “http://” к URLs в CM-6 References.	F-71
01-15-2014	Редакция	Добавление “component” перед “inventories” в CM-8(5).	F-74
01-15-2014	Редакция	Изменение “tsp.ncs.gov” на “http://www.dhs.gov/telecommunications-service-priority-tsp” в CP-8 References.	F-86
01-15-2014	По существу	Добавление следующего текста к CP-9(7) Supplemental Guidance: “Dual authorization may also be known as two-person control.”	F-87
01-15-2014	Редакция	Изменение “HSPD 12” на “HSPD-12” и добавление “http://” к URL в IA-2 References.	F-93
01-15-2014	Редакция	Изменение “encrypted representations of” на “cryptographically-protected” в IA-5(1) (c).	F-96

01-15-2014	Редакция	Изменение “Encrypted representations of” на “Cryptographically-protected” в IA-5(1) Supplemental Guidance.	F-97
01-15-2014	По существу	Добавление следующего текста к IA-5(1) Supplemental Guidance: “To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.”	F-97
01-15-2014	Редакция	Добавление “http://” к URL в IA-5 References.	F-99
01-15-2014	Редакция	Добавление “http://” к URL в IA-7 References.	F-99
01-15-2014	Редакция	Добавление “http://” к URL в IA-8 References.	F-101
01-15-2014	Редакция	Изменение “:” на “;” после “800-61” и добавление “http://” к URL в IR-6 References.	F-108
01-15-2014	По существу	Добавление следующего текста к MP-6(7) Supplemental Guidance: “Dual authorization may also be known as two-person control.”	F-124
01-15-2014	Редакция	Добавление “http://” к URL в MP-6 References.	F-124
01-15-2014	Редакция	Изменение “DoDI” на “DoD Instruction” и добавление “http://” к URLs в PE-3 References.	F-130
01-15-2014	Редакция	Удаление “and supplementation” после “tailoring” в PL-2 a. 8.	F-140
01-15-2014	Редакция	Добавление “Special” перед “Publication” в PL-4 References.	F-141
01-15-2014	Редакция	Добавление “Control Enhancements: None.” к PL-7.	F-142
01-15-2014	Редакция	Удаление AT-5 и AC-19(6), AC-19(8) и AC-19(9) из PL-9 Supplemental Guidance.	F-144
01-15-2014	Редакция	Добавление “Control Enhancements: None.” к PL-9.	F-144
01-15-2014	Редакция	Добавление “Special” перед “Publication” в PL-9 References.	F-144
01-15-2014	Редакция	Изменение “731.106(a)” на “731.106” в PS-2 References.	F-145
01-15-2014	Редакция	Изменение “Publication” на “Publications” и добавление “http://” к URL в RA-3 References.	F-153
01-15-2014	Редакция	Добавление “http://” к URLs в RA-5 References.	F-155
01-15-2014	Редакция	Добавление “http://” к URLs в SA-4 References.	F-160
01-15-2014	По существу	Добавление следующего текста к SA-11(8) Supplemental Guidance: “To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms).”	F-169
01-15-2014	Редакция	Добавление “http://” к URLs в SA-11 References.	F-169
01-15-2014	Редакция	Добавление “Control Enhancements: None.” к SA-16.	F-177
01-15-2014	Редакция	Изменение “Training” на “Scanning” в SA-19(4) title.	F-181
01-15-2014	Редакция	Изменение “physical” на “protected” в SC-8 Supplemental Guidance.	F-193
01-15-2014	Редакция	Изменение “140-2” на “140” идобавление “http://” к URLs в SC-13 References.	F-196
01-15-2014	Редакция	Добавление “authentication” после “data origin” в SC-20, Part a.	F-199
01-15-2014	Редакция	Добавление “verification” после “integrity” в SC-20, Part a.	F-199
01-15-2014	Редакция	Добавление “Control Enhancements: None.” к SC-35.	F-209
01-15-2014	Редакция	Удаление лишнего “References: None” из SI-7.	F-228

01-15-2014	По существу	Добавление следующего текста как нового третьего абзаца в Приложение G: “Таблица G-1 представляет сводку мер безопасности семейства управления программой из Приложения G. Организации могут использовать рекомендуемые *приоритетные коды*, связанные с каждой мерой управления программой, для помощи в принятии решений по упорядочиванию для реализации (то есть, у меры безопасности с Приоритетным Кодом 1 [P1], есть более высокий приоритет для реализации чем у меры безопасности с Приоритетным Кодом 2 [P2]; и у меры безопасности с Приоритетным Кодом 2 [P2] есть более высокий приоритет для реализации чем у меры безопасности с Приоритетным Кодом 3 [P3].”	G-1/2
01-15-2014	Редакция	Добавление Таблицы G-1 в Приложение G.	G-2
01-15-2014	Редакция	Добавление “http://” к URL в Ссылках PM-5.	G-5
01-15-2014	Редакция	Удаление “Web: www.fsam.gov” из Ссылок PM-7.	G-5
01-15-2014	Редакция	Добавление “http://” к URL в Сноске 124.	J-22
01-22-2015	Редакция	Изменение соглашения о присвоении имен улучшениям мер безопасности (то есть, формата), путём удаления пробела между основной мерой безопасности и пронумерованным обозначением улучшения.	Везде
01-22-2015	Редакция	Изменение “ (iv) и” на “и (iv)” в определении Глоссария для Разработчика.	B-6
01-22-2015	Редакция	Изменение “IR-2 (1) в высоком базовом наборе для записи IR-2” на “запись IR-2 (1) (2) в высоком базовом наборе для IR-2” в Приложении D, абзац 1, строка 8.	D-1
01-22-2015	Редакция	Изменение “улучшение (1)” на “улучшения (1) и (2)” в Приложении D, абзац 1, строка 10.	D-1
01-22-2015	Редакция	Удаление “в каталоге мер безопасности“ в Приложении D, абзац 1, строка 10.	D-1
01-22-2015	Редакция	Изменение “ SHARED GROUPS / ACCOUNTS “ на “ SHARED / GROUPS ACCOUNTS ” в Таблице D-3, AC 2 (9) название.	D-10
01-22-2015	Редакция	Добавление “ROLE-BASED“ перед “SECURITY TRAINING” в теблице D-4, AT-3(1) название.	D-14
01-22-2015	Редакция	Добавление “ROLE-BASED“ перед “SECURITY TRAINING” в теблице D-4, AT-3(2) название.	D-14
01-22-2015	Редакция	Добавление “ROLE-BASED“ перед “SECURITY TRAINING” в теблице D-4, AT-3(3) название.	D-14
01-22-2015	Редакция	Добавление “ROLE-BASED“ перед “SECURITY TRAINING” в теблице D-4, AT-3(3) название.	D-14
01-22-2015	Редакция	Добавление “-BASED“ к “BIOMETRIC” в таблице D-9, IA-5(12) название.	D-23
01-22-2015	Редакция	Удаление “/ ANALYSIS“ после “PENETRATION TESTING” в таблице D-17, SA-11(5) название.	D-33
01-22-2015	Редакция	Изменение “(1)” с нормального шрифта на полужирныйв таблице E-4, SI-4(1).	E-7
01-22-2015	Редакция	Изменение “SHARED GROUPS / ACCOUNTS“ на “SHARED / GROUP ACCOUNTS” в AC-2(9) название.	F-10
01-22-2015	Редакция	Изменение “use“ на “usage” в AC-2(12) часть (a).	F-10
01-22-2015	Редакция	Изменение “policies“ на “policy” в AC-3(3).	F-11
01-22-2015	Редакция	Удаление “specifies that” в AC-3(3).	F-11
01-22-2015	Редакция	Изменение “The policy is“ на “Is” в AC-3(3) часть (a).	F-11
01-22-2015	Редакция	Изменение “A“ на “Specifies that a” в AC-3(3) часть (b).	F-11
01-22-2015	Редакция	Добавление “Specifies that“ к AC-3(3) часть (c).	F-11
01-22-2015	Редакция	Изменение “Organized-defined“ на “organization-defined” в AC-3(3) часть (c).	F-11
01-22-2015	Редакция	Изменение “policies“ на “policy” в AC-3(4).	F-12
01-22-2015	Редакция	Добавление “information“ перед “flows” в AC-4(7).	F-15

01-22-2015	Редакция	Добавление “ROLE-BASED“ перед “SECURITY TRAINING” в AT-3(1) название.	F-39
01-22-2015	Редакция	Добавление “ROLE-BASED“перед “SECURITY TRAINING” в AT-3(2) название.	F-39
01-22-2015	Редакция	Добавление “ROLE-BASED“перед “SECURITY TRAINING” в AT-3(3) название.	F-39
01-22-2015	Редакция	Добавление “ROLE-BASED“перед “SECURITY TRAINING” в AT-3(4) название.	F-39
01-22-2015	Редакция	Добавление “the” перед “relationship” в AU-12(1).	F-52
01-22-2015	Редакция	Перенос “.”за пределы закрывающей квадратной скобки в изъятом разделе.	F-61
01-22-2015	Редакция	Изменение “that“ на “those” в CP-7 часть c.	F-84
01-22-2015	Редакция	Удаление “list of“ в IA-2(10).	F-92
01-22-2015	Редакция	Удаление “such as documentary evidence or a combination of documents and biometrics“ в IA-4(3).	F-95
01-22-2015	Редакция	Добавление “, such as documentary evidence or a combination of documents and biometrics,“ в IA-4(3) Supplemental Guidance.	F-95
01-22-2015	Редакция	Добавление “-BASED“ к “BIOMETRIC” в IA-5(12) название.	F-98
01-22-2015	Редакция	Изменение “testing/exercises“ на “testing” в IR-4 часть c.	F-105
01-22-2015	Редакция	Удаление “and“ перед “prior” в MA-4(3) часть (b).	F-115
01-22-2015	Редакция	Изменение “Sanitation“ на “Sanitization” в MP-7(2) Supplemental Guidance (два раза).	F-125
01-22-2015	Редакция	Изменение “resign“ на “re-sign” в PL-4 часть d.	F-141
01-22-2015	Редакция	Удаление “security categorization decision is reviewed and approved by the“ перед “authorizing” (первый раз) в RA-2 часть c.	F-151
01-22-2015	Редакция	Добавление “reviews and approves the security categorization decision“ после “representative” RA-2 часть c.	F-151
01-22-2015	Редакция	Изменение “;“ на “,” после IA-2 в SA-4(10) Supplemental Guidance.	F-160
01-22-2015	Редакция	Добавление “takes“ перед оператором присваивания в SA-5 часть c.	F-161
01-22-2015	Редакция	Изменение “either is“ на “is either” в SA-11(3) часть (b).	F-167
01-22-2015	Редакция	Удаление “has been“ перед “granted” в SA-11(3) часть (b).	F-167
01-22-2015	Редакция	Удаление “/ ANALYSIS“ после “PENETRATION TESTING” в SA-11(5) название.	F-168
01-22-2015	Редакция	Удаление “enhancement“ после “control” в SA-12 Supplemental Guidance.	F-169
01-22-2015	Редакция	Удаление “Related control: PE-21.” из SA-12(9) Supplemental Guidance.	F-171
01-22-2015	Редакция	Изменение “reference to source“ на “references to sources” в SC-5.	F-187
01-22-2015	Редакция	Добавление “to be“ перед “routed to” в SC-7(11).	F-190
01-22-2015	Редакция	Изменение “i“ на “1” и “ii” на “2” в SI-4 часть c.	F-219
01-22-2015	Редакция	Изменение “USER“ на “USERS” в SI-4(20) название.	F-223
01-22-2015	Редакция	Удаление “for“ в SI-6(2).	F-225
01-22-2015	Редакция	Изменение “interfaces” на “interactions” в SI-10(4) Supplemental Guidance.	F-229
01-22-2015	Редакция	Изменение “-“ на “,” после AU-7 в PM-12 Дополнительное руководство.	G-8
01-22-2015	По существу	Обновление введения к Приложению H и Таблицам H-1 и H-2 в соответствии с версией ISO/IEC 27001 2013 года и пересмотр методологии отображения мер безопасности.	H-1 до H-12
01-22-2015	Редакция	Удаление UL-3 из связанных мер безопасности, перечисленных в SE-1.	J-20

ГЛАВА ОДИН

ВВЕДЕНИЕ

ПОТРЕБНОСТЬ ЗАЩИТИТЬ ИНФОРМАЦИЮ И ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Выбор и реализация *мер безопасности* для организаций и информационных систем[1] являются важными задачами, которые могут оказывать существенное влияние на деятельность[2] и активы организаций,[3] а так же на благосостояние людей и Нации. Меры безопасности - меры защиты/контрмеры, предписанные для информационных систем или организаций, которые разработаны для: (i)защиты конфиденциальности, целостности и доступности информации, которая обрабатывается, хранится и передается в этих системах/ организациях; и (ii) удовлетворяют набору определенных требований безопасности[4]. Есть несколько ключевых вопросов, на которые должны ответить организации, когда рассматривают информационную безопасность для информационных систем:

- Какие меры безопасности необходимы, чтобы удовлетворить требованиям безопасности и соответственно смягчить риск, существующий при использовании информации и информационных систем в выполнении задач и коммерческих функций организаций?
- Реализованы ли меры безопасности или существует ли план их реализации?
- Каков желаемый или требуемый уровень доверия, что выбранные меры безопасности, при реализации, были эффективны в их применении?[5]

Ответы на эти вопросы необходимы не в отдельности, а скорее в контексте эффективного *процесса управления рисками* для организации, который идентифицирует, смягчает насколько необходимо и контролирует на непрерывной основе риски,[6] связанные с её информацией и информационными системами. Специальная публикация NIST 800-39 дает представление об управлении рисками информационной безопасности на трёх различных уровнях: уровне организации, уровне процесса предназначения/деятельности и уровне информационной системы. Меры безопасности, определенные в этой публикации и рекомендуемые организациям для использования при удовлетворении их требованиям безопасности, должны быть использованы как часть четко определенного и задокументированного процесса управления рисками, который поддерживает программы информационной безопасности организаций.[7]

---

[1] Информационная система - дискретный набор *информационных ресурсов*, специально организованных для сбора, обработки, поддержки, использования, распределения, распространения или ликвидации информации. Информационные системы также включают специализированные системы, такие как промышленные системы/системы управления процессами, телефонные коммутаторы/офисные мини-АТС и системы контроля за состоянием окружающей среды. Информационные системы могут быть рассмотрены с логической и физической точек зрения, как сложная система систем, когда есть множественные системы, объединенные с высокой степенью связности и взаимодействия между системами.

[2] Деятельность организаций включает предназначение, функции, имидж и репутацию.

[3] Термин "организация" описывает сущность любого размера, сложности или позиции в пределах организационной структуры (например, федеральное агентство или, если применимо, любой из его операционных элементов).

[4] Требования безопасности получены из предназначения/потребностей деятельности, законов, Правительственных распоряжений, директив, постановлений, политик, инструкций, стандартов, нормативных актов и/или процедур, чтобы гарантировать конфиденциальность, целостность и доступность информации, обрабатываемой, хранимой или передаваемой информационными системами организаций.

[5] *Эффективность* мер безопасности определяет степень, до которой меры безопасности реализованы правильно, применяются как предназначено и производят желаемый результат относительно соответствия требованиям безопасности для информационной системы в ее среде эксплуатации или осуществляют/проводят установленную политику безопасности.

[6] Риски, связанные с информационной безопасностью, - это риски, которые являются результатом потери конфиденциальности, целостности или доступности информации или информационных систем и оказывают потенциально неблагоприятные воздействия на деятельность и активы организаций, людей, другие организации и Нацию.

[7] Меры безопасности управления программой (Приложение G) дополняют меры безопасности для информационной системы (Приложение F), сосредотачиваясь на требованиях информационной безопасности общих для организации, которые независимы от любой определенной информационной системы и важны для управления программами информационной безопасности.

Первостепенную важность имеет то, что ответственные должностные лица понимают риски и другие факторы, которые могут оказать негативное влияние на деятельность и активы организации, людей, другие организации и Нацию[8]. Эти должностные лица должны также понимать текущий статус своих программ обеспечения безопасности и мер безопасности, планируемых или существующих для защиты их информации и информационных систем, чтобы сделать обоснованные суждения и инвестиции, которые смягчают риски до допустимого уровня. Конечная цель состоит в том, чтобы вести повседневную деятельность организации и выполнять установленные функции предназначение и деятельности организации таким образом, что Циркуляр OMB A-130 определяет как *адекватная безопасность*, или безопасность, соразмерная с риском, следующим из несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения информации.

1.1 НАЗНАЧЕНИЕ И ПРИМЕНИМОСТЬ

Назначение этой публикации состоит в том, чтобы обеспечить руководство для выбора и определения мер безопасности для организаций и информационных систем, поддерживающих исполнительные агентства федерального правительства, чтобы удовлетворить требованиям FIPS публикация 200, *Минимальные Требования безопасности для федеральной информации и информационных систем*. Руководство применяется ко всем компонентам[9] информационной системы, которые обрабатывают, хранят, или передают федеральную информацию. Руководство было разработано, чтобы достигнуть более безопасных информационных систем и эффективного управления рисками в пределах федерального правительства:

- Облегчить более непротиворечивый, сопоставимый и повторяемый подход для выбора и определения мер безопасности для информационных систем и организаций;
- Обеспечить постоянный, тем не менее гибкий каталог мер безопасности, чтобы встретить текущие потребности в защите информации и требования будущих потребностей защиты, основанные на изменяющихся угрозах, требованиях и технологиях;
- Обеспечить рекомендации для минимальных мер безопасности для информационных систем, категорированных в соответствии с FIPS публикация 199, *Стандарты для классификации безопасности федеральной информации и информационных систем*;
- Создать основы для разработки методов и процедур оценки для того, чтобы определить эффективность меры безопасности; и
- Улучшить связи среди организаций, обеспечивая общий словарь, который поддерживает обсуждение концепций управления рисками.

В дополнение к мерам безопасности, описанным выше, эта публикация: (i) обеспечивает набор мер управления программой информационной безопасности (PM), которые, как правило, реализуются на уровне организации и не предписываются отдельным информационным системам организации; (ii) обеспечивает ряд мер приватности, основанных на международных стандартах и лучших практиках, которые помогают организациям провести в жизнь требования приватности, полученные из федерального законодательства, директив, политик, нормативных актов и стандартов; и (iii) устанавливает взаимосвязь и отношение между мерами приватности и безопасности для целей определения соответствующих требований приватности и безопасности, которые могут перекрываться в концепции и в реализации в пределах федеральных информационных систем, программ и организаций. Стандартизированные меры приватности обеспечивают более дисциплинированный и структурированный подход для того, чтобы он удовлетворял федеральным требованиям приватности и демонстрировал согласие с теми требованиями. Объединение с такими же

[8] Это включает риск для американской критической инфраструктуры/ключевых ресурсов, как описано в Президентской Директиве национальной безопасности 7.

[9] Компоненты информационной системы включают, например, мэйнфреймы, рабочие станции, серверы (например, баз данных, электронной почты, аутентификации, сети, прокси, файлов, доменных имён), устройства ввода-вывода (например, сканеры, копировальные устройства, принтеры), сетевые компоненты (например, межсетевые экраны, маршрутизаторы, шлюзы, переключатели речи и данных, контроллеры обработки, точки доступа, сетевые устройства, датчики), операционные системы, виртуальные машины, промежуточное программное обеспечение и приложения.

концепциями, которые используются в управлении рисками информационной безопасности, помогает организации реализовать меры приватности в более рентабельном, основанном на анализе риска способе.

Руководства в этой специальной публикации применимы ко всем федеральным информационным системам[10] кроме тех систем, которые определены как системы национальной безопасности в соответствии с 44 U.S.C., Раздел 3542[11]. Руководства разработаны с широкой технической перспективой до дополнения подобных руководств для систем национальной безопасности и может использоваться для таких систем с санкционирования соответствующих федеральных должностных лиц, имеющих полномочия по таким системам[12]. Правительства штатов, локальные и племенные правительства, а так же организации частного сектора поощрены рассматривать использование этих руководств где соответствующе.

1.2 ЦЕЛЕВАЯ АУДИТОРИЯ

Эта публикация предназначена, чтобы служить разнообразной аудитории профессионалов по информационным системам и информационной безопасности, включая:

- Людей с обязанностями по информационным системам, безопасности и/или управлению и надзору за рисками (например, уполномоченных должностных лиц, директоров по информации, высших сотрудников по информационной безопасности,[13] менеджеров по информационным системам, менеджеров по информационной безопасности);
- Людей с обязанностями по разработке информационных систем (например, диспетчеров программ, проектировщиков и разработчиков систем, инженеров по информационной безопасности, системных интеграторов);
- Людей с обязанностями по реализации и применению информационной безопасности (например, владельцев предназначения/деятельности, владельцев информационных систем, поставщиков общих мер безопасности, владельцев/управляющих информацией, системных администраторов, сотрудников безопасности информационных систем);
- Людей с обязанностями по оценке и контролю информационной безопасности (например, аудиторов, Генеральных инспекторов, оценщиков систем, инспекторов, независимых верификаторов/валидаторов, аналитиков, владельцев информационных систем); и
- Коммерческие компании, производящие продукты и системы информационных технологий, создающие технологии, связанные с информационной безопасностью или предоставляющие услуги по информационной безопасности.

1.3 ОТНОШЕНИЕ К ДРУГИМ ПУБЛИКАЦИЯМ ПО МЕРАМ БЕЗОПАСНОСТИ

Чтобы создать технически осмысленный и широко применимый набор мер безопасности для информационных систем и организаций, во время разработки этой специальной публикации было рассмотрено множество источников. Источники включали меры безопасности от сообществ обороны, аудита, финансов, здравоохране-

[10] *Федеральная информационная система* - информационная система, которая используется или управляется исполнительным агентством, подрядчиком исполнительного агентства или другой организацией от имени исполнительного агентства.

[11] *Система национальной безопасности* - любая информационная система (включая любую телекоммуникационную систему) используемая или управляемая агентством или подрядчиком агентства, или другой организацией от имени агентства - (i) функция, деятельность или использование которой включает разведывательную деятельность; включает криптологические работы, связанные с национальной безопасностью; включает руководство и управление вооруженными силами; включает оборудование, которое является неотъемлемой частью оружия или системы оружия; или 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) защищена постоянно 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].

[12] Инструкция 1253 CNSS обеспечивает руководство реализации для систем национальной безопасности.

[13] На уровне *агентства* эта позиция известна как Высший сотрудник по информационной безопасности Агентства. Организации могут также именовать эту позицию как *Высший сотрудник информационной безопасности* или *Директор по информационной безопасности*.

ния, управления промышленными/технологическими процессами и разведывательного, а так же меры безопасности, определенные организациями по национальным и международным стандартам. Цель Специальной публикации NIST 800-53 состоит в том, чтобы обеспечить набор мер безопасности, которые могут удовлетворить охват и глубину требований безопасности[14], накладываемых на организации, процессы предназначения/деятельности и информационные системы, и которые непротиворечивы с и дополнительны к другим, установленным стандартами информационной безопасности.

Каталог мер безопасности в Специальной публикации 800-53 может эффективно использоваться, чтобы защитить информацию и информационные системы от традиционных и постоянных развивающихся угроз в различных вариантах применения, сред и техники. Меры безопасности могут также использоваться, чтобы демонстрировать согласие с множеством требований безопасности, установленных правительством, организацией или ведомством. Организации несут ответственность за выбор соответствующих мер безопасности, правильную реализацию мер и демонстрацию эффективности мер в удовлетворении установленных требований безопасности.[15] Меры безопасности облегчают разработку методов и процедур оценки, которые могут использоваться, чтобы демонстрировать эффективность мер безопасности в непротиворечивом/повторяемом способе - таким образом, способствуя доверию организаций к тому, что требования безопасности продолжают удовлетворяться на непрерывной основе. Кроме того, меры безопасности могут использоваться в разработке *оверлеев* для специализированных информационных систем, информационных технологий, сред эксплуатации или сообществ интересов (см. Приложение I).

1.4 ОБЯЗАННОСТИ ОРГАНИЗАЦИЙ

Организации используют FIPS Публикацию 199, чтобы категорировать их информацию и информационные системы. Категорирование безопасности выполняется как деятельность общая для общеорганизации[16] с участием персонала организации высшего уровня, включая, например, уполномочивающих должностных лиц, директоров по информации, высших сотрудников по информационной безопасности, информационных владельцев и/или управляющих, владельцев информационных систем и ответственных за риски (как функция).[17] Информация категорируется на Уровне 1 (уровень организации) и Уровне 2 (уровень процесса предназначения/деятельности). В соответствии с FIPS Публикацией 200, организации используют результаты категорирования безопасности Уровней 1 и 2, чтобы определять информационные системы организации на Уровне 3 (уровень информационной системы) как системы низкого воздействия, умеренного воздействия или высокого воздействия. Для каждой информационной системы организации на Уровне 3, рекомендации для мер безопасности от *базовых мер безопасности*, определенных в Приложении D, являются начальной точкой для процесса *адаптации* мер безопасности. Хотя процесс выбора мер безопасности в основном фокусируется на информационных системах на Уровне 3, процесс в целом применим для всех трех уровней управления рисками.

Категорирование безопасности в соответствии с FIPS Публикацией 199 связывает информацию и эксплуатацию и использование информационных систем с потенциально худшим случаем неблагоприятное воздействие на деятельность и активы организации, людей, другие организации и Нацию.[18] Оценки риска организаций, включая использование конкретной и достоверной информации об угрозах, информации об уязвимостях и вероятности угроз, использующих уязвимости, чтобы вызвать неблагоприятные воздействия, являются руководством и обеспечением информацией для процесса адаптации и заключительного выбор мер

[14] Требования безопасности - требования, предписанные информационной системе, которые получены из законов, Правительственных распоряжений, директив, политик, инструкций, нормативных актов, стандартов, руководств, или потребностей организации (предназначения) гарантировать конфиденциальность, целостность и доступность обрабатываемой, хранимой или передаваемой информации.

[15] Специальная публикация NIST 800-53A представляет руководство по оценке эффективности мер безопасности.

[16] См. Публикацию 200 FIPS, Сноску 7.

[17] Организации, как правило, используют управленческий, эксплуатационный и финансовый контроль за своими информационными системами и безопасностью, обеспеченной для этих систем, включая полномочия и возможности, чтобы реализовать или потребовать, чтобы меры безопасности считались необходимыми для защиты деятельности и активов организаций, людей, других организаций и Нации.

[18] Соображения по потенциальным воздействиям национального уровня и воздействиям на другие организации при категорировании информационных систем организаций получают из ПАТРИОТИЧЕСКОГО АКТА США и Президентских Директив по безопасности отечества (HSPDs).

безопасности.[19] Заключительный, согласованный набор мер безопасности, соответствующий конкретному потребностям предназначения/деятельности организаций и допуску для риска, документируется с соответствующим обоснованием в плане обеспечения безопасности для информационной системы.[20] Использование мер безопасности из Специальной публикации 800-53 (включая базовые меры безопасности как начальной точки в процессе выбора мер безопасности), облегчает более непротиворечивый уровень безопасности для федеральных информационных систем и организаций, одновременно сохраняя гибкость и оперативность организаций, необходимые чтобы соответствовать все более и более сложному и враждебному пространству угроз, конкретным функциям предназначения/деятельности организаций, быстро меняющимся технологиям и, в некоторых случаях, уникальным средам эксплуатации.

Достижение адекватной информационной безопасности для организаций, процессов предназначения/ деятельности и информационных систем - многоаспектная задача, которая требует:

- Ясно сформулированных требований безопасности и спецификаций безопасности;
- Хорошо спроектированных и хорошо разработанных продуктов информационных технологий, базирующихся на проверенных на практике аппаратных средствах, встроенном микропрограммном обеспечении и процессах разработки программного обеспечения;
- Обоснованных системных/обеспечения безопасности инженерных принципов и методов для того, чтобы эффективно интегрировать продукты информационных технологий в информационные системы организаций;
- Обоснованных методов безопасности, которые хорошо задокументированы и эффективно интегрируются в требования обучения и повседневной деятельности персонала организаций с обязанностями по безопасности;
- Непрерывного мониторинга организаций и информационных систем, чтобы определить долговременную эффективность развернутых мер безопасности, изменения в информационных системах и средах эксплуатации и согласие с законодательством, директивами, политиками и стандартами; [21] и
- Управления планированием информационной безопасности и жизненным циклом разработки систем.[22]

С технической точки зрения информационная безопасность - только одна из многих требуемых эксплуатационных возможностей информационных систем, которые поддерживают процессы предназначения/деятельности организаций - возможностей, которые должны быть консолидированы организациями всюду по жизненному циклу разработки систем, чтобы достигнуть успеха в предназначении/деятельности. Важно, чтобы организации *реалистично* оценили риск деятельности и активам организаций, людям, другим организациям и Нации, являющейся результатом процессов предназначения/деятельности при принятии информационных систем в эксплуатацию или при продолжении эксплуатации. Реалистичная оценка риска требует понимания угроз для и уязвимостей в пределах организаций и вероятности и потенциала неблагоприятных воздействий по успешному использованию таких уязвимостей этими угрозами.[23] Наконец, требования информационной безопасности должны быть удовлетворены с полным знанием и рассмотрением стратегии управления

[19] Оценки степени риска могут быть выполнены множеством способов в зависимости от конкретных потребностей организаций. Специальная публикация NIST 800-30 дает представление об оценке риска как части полного процесса управления рисками.

[20] Уполномочивающие должностные лица или их назначенные представители, принимая окончательные планы обеспечения безопасности, соглашаются на набор мер безопасности, предложенных, чтобы выполнить требования безопасности для организаций (включая процессы предназначения/деятельности) и/или определенных информационных систем.

[21] Специальная публикация NIST 800-137 дает представление о непрерывном мониторинге информационных систем организаций и сред эксплуатации.

[22] Специальная публикация NIST 800-64 дает представление о соображениях информационной безопасности в жизненном цикле разработки систем.

[23] Специальная публикация NIST 800-30 дает представление о процессе оценки степени риска.

рисками организаций, в свете потенциальной стоимости, сроков и проблем функционирования, связанных с приобретением, развертыванием и эксплуатацией информационных систем организаций.[24]

1.5 ОРГАНИЗАЦИЯ ЭТОЙ СПЕЦИАЛЬНОЙ ПУБЛИКАЦИИ

Оставшаяся часть этой специальной публикации организована следующим образом:

- **Глава Два** описывает фундаментальные концепции, связанные с выбором мер и спецификаций безопасности включая: (i) многоуровневое управление рисками; (ii) структуру мер безопасности и организацию мер безопасности в семейства; (iii) базовые наборы мер безопасности как начальные точки для процесса адаптации; (iv) использование общих мер безопасности и наследование возможностей безопасности; (v) внешние среды и поставщиков услуг; (vi) доверие и доверенность; и (vii) версии и расширения мер безопасности и базовых наборов мер безопасности.
- Глава Три описывает процесс выбора и определения мер безопасности для информационных систем организаций, включая: (i) выбор соответствующих базовых наборов мер безопасности; (ii) адаптация базовых наборов мер безопасности, включая разработку специализированных оверлеев; (iii) документирование процесса выбора мер безопасности; и (iv) применение процесса выбора к новым и унаследованным системам.
- **Поддерживающие приложения** существенно обеспечивают выбор мер безопасности и связанной со спецификацией информации, включая: (i) общие ссылки;[25] (ii) термины и определения; (iii) акронимы; (iv) базовые наборы мер безопасности для информационных систем низкого, умеренного и высокого уровней воздействия; (v) руководство по доверию и доверенности в информационных системах; (vi) каталог мер безопасности;[26] (vii) каталог мер упраления программой информационной безопасности; (viii) отображения к международным стандартам информационной безопасности; (ix) руководство по разработке оверлеев организациями или сообществами интересов; и (x) каталог мер приватности.

[24] В дополнение к требованиям информационной безопасности организации должны также определять требования приватности, которые вытекают из федерального законодательства и политик. Организации могут использовать меры приватности в Приложении J в сочетании с мерами безопасности в Приложении F, чтобы достигнуть всесторонней защиты безопасности и приватности.

[25] Если иначе не заявлено, все ссылки на публикации NIST в этом документе (то есть, стандарты обработки федеральной информации и Специальные публикации) относятся к самой последней версии публикации.

[26] Меры безопасности в Специальной публикации 800-53 доступны онлайн и могут быть загружены в различных форматах с веб-сайта NIST по адресу http://web.nvd.nist.gov/view/800-53/home.

ГЛАВА ДВА

ОСНОВНЫЕ ПРИНЦИПЫ

СТРУКТУРА МЕРЫ БЕЗОПАСНОСТИ, ОРГАНИЗАЦИЯ, ОСНОВЫ И ДОВЕРИЕ

Эта глава представляет фундаментальные концепции, связанные с выбором и спецификацией мер безопасности включая: (i) трехуровневое управление рисками; (ii) структура мер безопасности и организация мер в каталоге мер безопасности; (iii) базовые меры безопасности; (iv) идентификация и использование мер обеспечения коллективной безопасности; (v) меры безопасности во внешних средах; (vi) меры доверия к безопасности; и (vii) будущие версии мер безопасности, каталога мер и базовых мер безопасности.

2.1 МНОГОУРОВНЕВОЕ УПРАВЛЕНИЕ РИСКАМИ

Выбор и спецификация мер безопасности для информационной системы выполняются как часть общей для организации программы информационной безопасности для управления риском - то есть, риском к деятельности и активам организации, людям, другим организациям и Нации, связанным с применением информационных систем. Основанные на риске подходы к выбору и спецификации мер безопасности рассматривают эффективность, действенность и ограничения обусловленные применимыми федеральными законами, Правительственными распоряжениями, директивами, политиками, нормативными актами, стандартами и руководствами. Чтобы интегрировать процесс управления рисками всюду по организации и эффективнее определять интересы предназначения/деятельности, использован трехуровневый подход, который адресует риски на: (i) уровень *организации*; (ii) *уровень* процесса предназначения/деятельности; и (iii) уровень информационной системы. Процесс управления рисками осуществляется на трех уровнях с главной целью непрерывного совершенствования в связанных с риском работах организации и эффективного межуровневого и внутриуровневого взаимодействия всех заинтересованных сторон, имеющих общий интерес в успехе предназначения/ деятельности организации. Рисунок 1 иллюстрирует трехуровневый подход к управлению рисками.

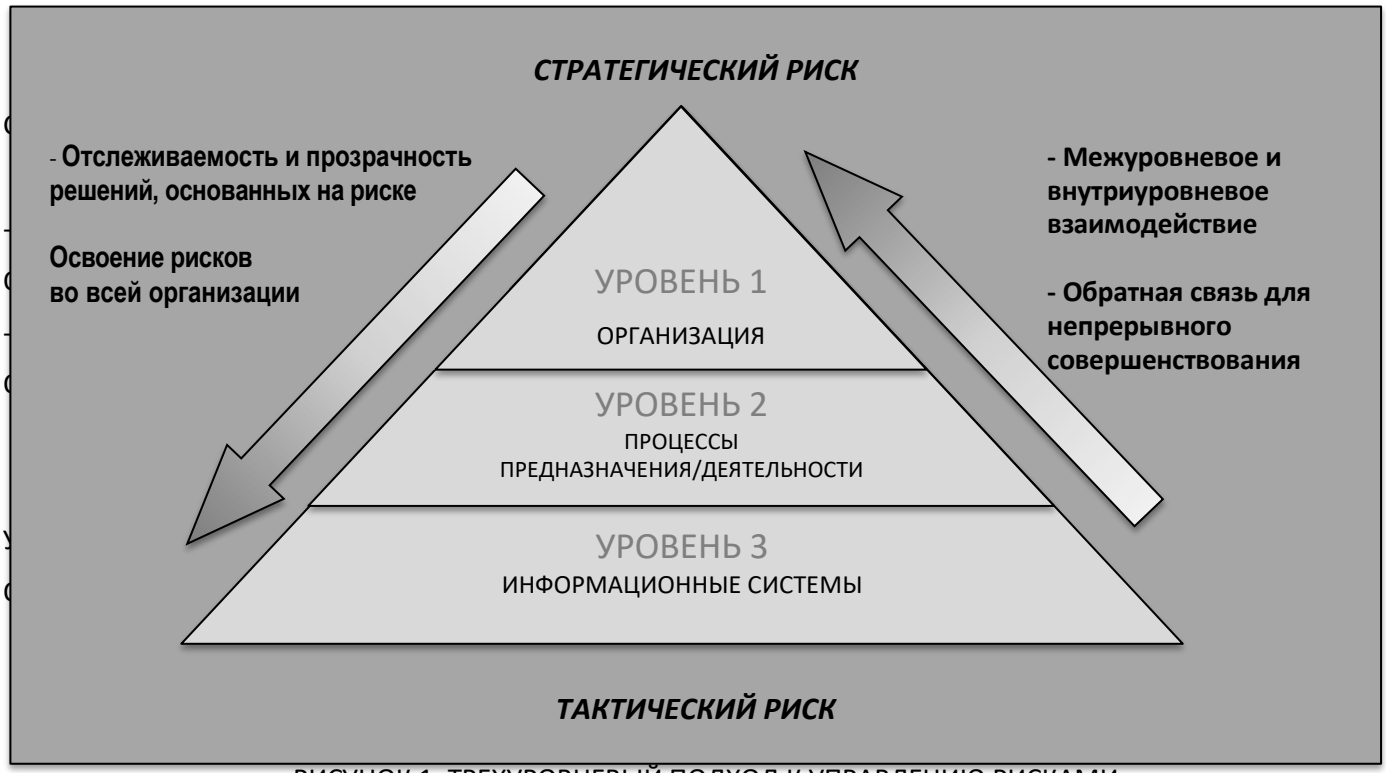

РИСУНОК 1: ТРЕХУРОВНЕВЫЙ ПОДХОД К УПРАВЛЕНИЮ РИСКАМИ

Уровень 1 обеспечивает назначение приоритетов функций предназначения/деятельности организаций, которые, в свою очередь, управляют инвестиционными стратегиями и финансированием конструктивных рентабельных эффективных решений для информационных технологий, непротиворечивых со стратегическими задачами и целями организации и показателями деятельности. Уровень 2 включает: (i) определение процессов предназначения/деятельности, необходимых для поддержания функций предназначения/деятельности организаций; (ii) определение категорий безопасности информационных систем, необходимых для выполнения процессов предназначения/деятельности; (iii) включение требований информационной безопасности в процессы предназначения/деятельности; и (iv) установление архитектуры предприятия (включая встроенную архитектуру информационной безопасности), чтобы облегчить выделение мер безопасности к информационным системам организации и средам, в которых работают эти системы. Основы управления рисками (RMF), изображенные в рисунке 2, являются первичным средством для того, чтобы определить риск на Уровне 3.[27] Эта публикация сосредотачиваются на Шаге 2 RMF, процесса выбора мер безопасности, в контексте трех уровней в иерархии управления рисками организации.

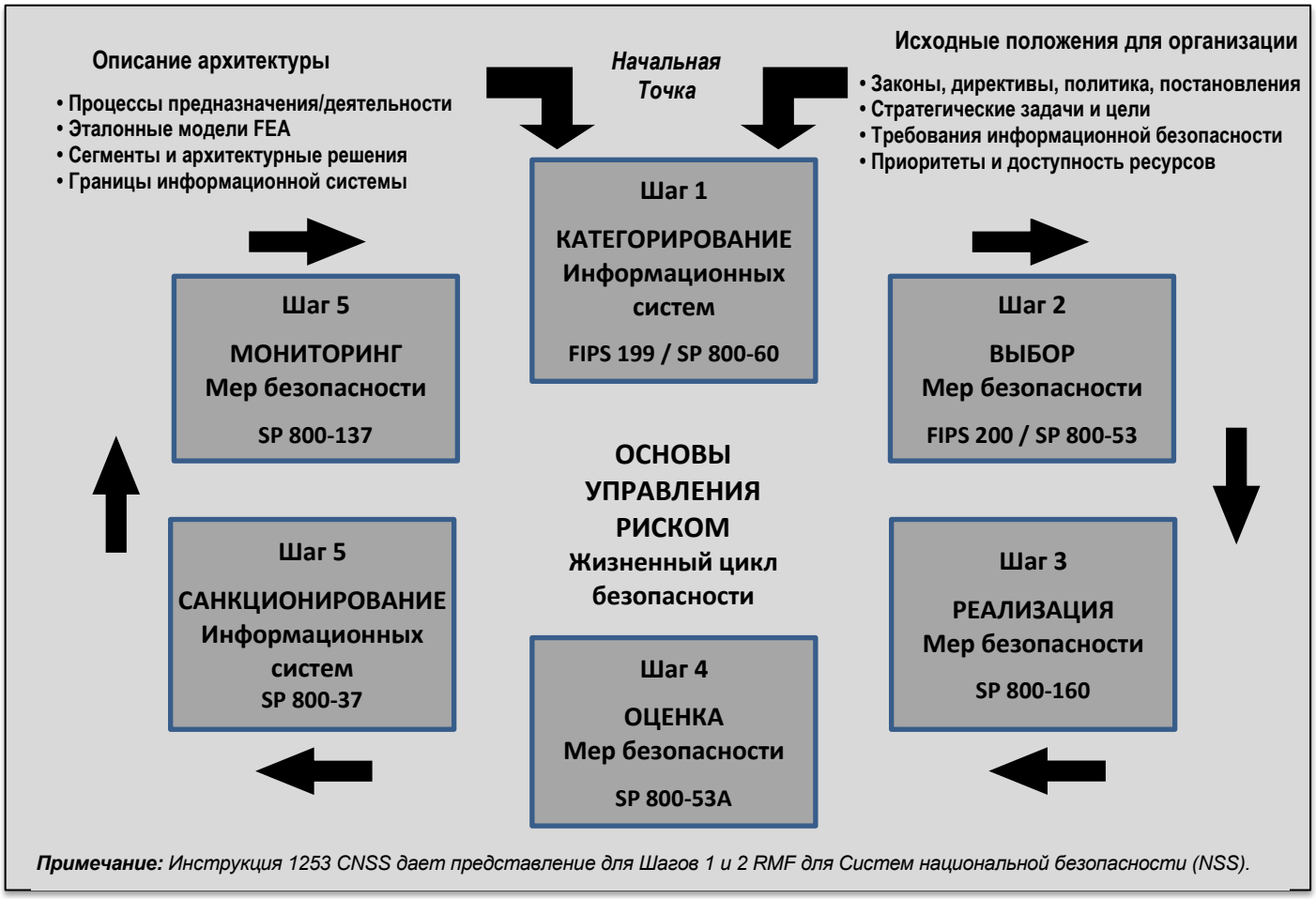

РИСУНОК 2: ОСНОВЫ УПРАВЛЕНИЯ РИСКОМ

RMF определяет проблемы безопасности организаций, связанные с проектированием, разработкой, реализацией, эксплуатацией и ликвидацией информационных систем и сред, в которых работают эти системы. RMF состоит из следующих шести шагов:

[27] Специальная публикация NIST 800-37 дают представление о реализации Основ управления рисками. Полный список всех публикаций, поддерживающих RMF и упомянутый на рисунке 2, представлен в Приложении А.

Шаг 1: *Категорирование* информационной системы, основанное на оценке воздействия в соответствии с FIPS Публикацией 199;[28]

Шаг 2: *Выбор* применимого базового набора мер безопасности, основанный на результатах категорирования безопасности и применении руководства по адаптации (включая потенциальное использование оверлеев);

Шаг 3: *Реализация* меры безопасности и документирование деталей проектирования, разработки и реализации для мер безопасности;

Шаг 4: *Оценка* мер безопасности для того, чтобы определить степень, до которой меры безопасности реализованы правильно, работают как предназначено и производят желаемый результат относительно выполнения требований безопасности для системы;[29]

Шаг 5: *Санкционирование* эксплуатации информационной системы, основанное на определении риска к деятельности и активам организации, людям, другим организациям и Нации, следующего из эксплуатации и использования информационной системы и решения, что этот риск приемлем; и

Шаг 6: *Контроль* на непрерывной основе мер безопасности в информационной системе и среде эксплуатации для определения эффективности мер безопасности, изменений в системе/среде и соответствия законодательству, Правительственным распоряжениям, директивам, политикам, нормативным актами и стандартам.

2.2 СТРУКТУРА МЕР БЕЗОПАСНОСТИ

У мер безопасности, описанных в этой публикации, есть четко определенная организация и структура. Для простоты использования в процессе выбора и спецификации мер безопасности, меры организованы в восемнадцать *семейств*.[30] Каждое семейство содержит меры безопасности, связанные с общей темой семейства безопасности. Двухсимвольный идентификатор однозначно определяет семейство мер безопасности, например, PS (Безопасность Персонала). Меры безопасности могут включать аспекты политики, надзора, контроля, ручных процессов, действий людей или автоматизированных механизмов, реализованных информационными системами/устройствами. Таблица 1 содержит список семейства мер безопасности и соответствующих идентификаторов семейств в каталоге мер безопасности.[31]

ID	FAMILY	ID	FAMILY
AC	Контроль доступа	MP	Защита носителей информации
AT	Освоение и обучение	PE	Физическая защита и защита среды
AU	Аудит и подконтрольность	PL	Планирование
CA	Оценка безопасности и санкционирование	PS	Безопасность персонала
CM	Управление конфигурацией	RA	Оценка риска
CP	Планирование на случай непредвиденных ситуаций	SA	Приобретение систем и сервисов
IA	Идентификация и аутентификация	SC	Защита систем и коммуникаций
IR	Реакция на инциденты	SI	Целостность систем и информации
MA	Поддержка	PM	Управление программой

[28] Инструкция CNSS 1253 обеспечивает руководство по категорированию безопасности для систем национальной безопасности.

[29] Специальная публикация NIST 800-53A дает представление об оценке эффективности мер безопасности.

[30] Из восемнадцати семейств мер безопасности в Специальной публикации NIST 800-53, семнадцать семейств описаны в каталоге мер безопасности в Приложении F, и близко соответствуют семнадцати минимальным требованиям безопасности для федеральной информации и информационных систем в FIPS публикации 200. Одно дополнительное семейство (семейство Управление программой [PM]) определяет меры безопасности для программ информационной безопасности, требуемых FISMA. Это семейство, которое непосредственно не упомянуто в FIPS публикации 200, обеспечивает меры безопасности на уровне организации, а не на уровне информационной системы. Для определения и руководства по реализации для мер безопасности PM см. Приложение G.

[31] Меры приватности, перечисленные в Приложении J, имеют организацию и структуру подобные мерам безопасности, включая использование двухсимвольных идентификаторов для восьми семейств приватности.

Структура мер безопасности включает следующие компоненты: (i) раздел *мера безопасности*; (ii) раздел *дополнительное руководство*; (iii) раздел *улучшения меры безопасности*; (iv) раздел *ссылки*; и (v) раздел *приоритет* и *принадлежность к базовому набору мер безопасности*. Следующий пример из семейства Аудит и подконтрольность иллюстрирует структуру типичной меры безопасности.

AU-3 КОНТЕНТ ЗАПИСЕЙ АУДИТА

Мера безопасности: Информационная система генерирует записи аудита, содержащие информацию, которая устанавливает, какое событие имело место, когда событие имело место, где событие имело место, источник события, результат события и идентификационные данные людей или субъектов, связанных с событием.

Дополнительное Руководство: Контент записи аудита, который может быть необходим, чтобы удовлетворить требование этой меры безопасности включает, например, отметки времени, источник и адреса получателя, идентификаторы пользователя/процесса, описание события, индикация успеха/неуспеха, имена затронутых файлов и связанные правила контроля доступа или управления потоками. Результаты события могут включать индикаторы успеха или неуспеха события и специфичных для события результатов (например, состояние безопасности информационной системы после того, как событие имело место). Соответствующие меры безопасности: AU-2, AU-8, AU-12, SI-11.

Улучшения меры безопасности:

(1) *КОНТЕНТ ЗАПИСЕЙ АУДИТА | ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ АУДИТА*
Информационная система генерирует записи аудита, содержащие следующую дополнительную информацию: [Назначение: определенная организацией дополнительная, более подробная информация].
Дополнительное Руководство: Подробная информация, которую организации могут рассматривать в записях аудита, включает, например, полнотекстовые записи привилегированных команд или индивидуальные идентификаторы групп учтенных пользователей. Организации ограниченно рассматривают дополнительную информацию аудита только для той информации, которая явно необходима для конкретных требований аудита. Это облегчает использование журналов аудита и журналов регистрации, не включая информацию, которая может потенциально вводить в заблуждение или может сделать более трудным определение местоположения интересующей информации.

(2) *КОНТЕНТ ЗАПИСЕЙ АУДИТА | ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ ПЛАНОВЫМ КОНТЕНТОМ ЗАПИСЕЙ АУДИТА*
Информационная система обеспечивает централизованное управление и конфигурацию контента, который будет охвачен в сгенерированных записях аудита [Назначение: определенные организацией компоненты информационной системы].
Дополнительное Руководство: Это улучшение мер безопасности требует, чтобы контент, который будет охвачен в записях аудита, был сконфигурирован из центрального местоположения (требует автоматизации). Организации координируют выбор требуемого контента аудита, чтобы поддержать централизованное управление и возможность конфигурации, обеспеченные информационной системой. Связанные меры безопасности: AU-6, AU-7.

Ссылки: Нет.

Приоритет и принадлежность к базовому набору мер безопасности:

P1	**НИЗКИЙ** AU-3	**СРЕДНИЙ** AU-3(1)	**ВЫСОКИЙ** AU-3(1)(2)

Раздел мер безопасности определяет конкретные связанные с безопасностью работы или действия, которые должны быть выполнены организациями или информационными системами. Термин и*нформационная система* обращается к тем функциям, которые обычно составляют реализацию информационной технологии (например, аппаратные средства, программное обеспечение и встроенное микропрограммное обеспечение). Наоборот, термин *организация* обращается к действиям, которые обычно являются процессом – управляемыми или сущностью-управляемыми – то есть, меры безопасности обычно реализуется посредством человеческих или основанных на процедуре действиях. Меры безопасности, которые используют термин организация, могут кроме того требовать, чтобы определенная степень автоматизации была выполнена. Точно так же у мер безопасности, которые используют термин информационная система, могут быть некоторые элементы, которые являются процессом-управляемыми или сущностью-управляемыми. Использование терминов организация и/или информационная система не устраняет применение мер безопасности на любом из уровней в иерархии управления рисками (то есть уровне организации, уровне процесса предназначения/ деятельности, уровне информационной системы), как соответствующе.

Для некоторых мер безопасности в каталоге мер обеспечена степень гибкости, позволяющая организациям определять значения для некоторых параметров, связанных с мерами безопасности. Эта гибкость достигнута с помощью операторов *назначения* и *выбора*, включенных в состав мер безопасности и улучшений мер безопасности. Операторы назначения и выбора предоставляют организациям возможность адаптировать меры безопасности и улучшения мер, основываясь на: (i) требованиях безопасности по поддержке функций предназначения/деятельности организаций и эксплуатационных потребностях; (ii) оценке степени риска и допустимого риска для организаций; и (iii) требованиях безопасности, определенных в федеральных законах, Правительственных распоряжениях, директивах, политиках, нормативных актах, стандартах, или руководствах.[32]

Например, организации могут определить дополнительную информацию, необходимую для записей аудита, чтобы поддержать обработку событий аудита. См. выше пример для AU-3(1) (то есть, [*Назначение: определенная организацией дополнительная, более подробная информация*]). Эти назначения могут включать определенные действия, которые будут использованы информационными системами в случае отказов аудита, частоты проведения системного резервного копирования, ограничений на использование паролей или списков рассылки для политик и процедур организации.[33] После задания,[34] определенные организацией значения для операторов назначения и выбора становятся частью меры безопасности, и реализация меры безопасности оценивается в соответствии с полным описанием меры безопасности. Операторы назначения предлагают высокую степень гибкости, позволяя организациям определять значения параметров не требуя, чтобы эти значения были одними из двух или более конкретных предопределенных вариантов. Напротив, операторы выбора сужают потенциальные входные значения, обеспечивая конкретный список элементов, из которых должны выбрать организации.[35]

Раздел дополнительного руководства обеспечивает не предписывающую, дополнительную информацию для конкретной меры безопасности. Организации могут применить дополнительное руководство как соответствующе, определяя, разрабатывая и/или реализуя меры безопасности. Дополнительное руководство может обеспечить важные соображения для реализации мер безопасности в контексте эксплуатационных сред, требований предназначения/деятельности или оценок риска и может также объяснять назначение или значение определенных мер. Улучшения мер безопасности могут также содержать дополнительное руководство, когда руководство применяется не ко всей мере безопасности, а сосредотачивается на определенном улучшении меры. Разделы дополнительного руководства для мер безопасности и улучшений мер могут содержать список *связанных мер безопасности*. Связанные меры безопасности: (i) непосредственно воздействуют или поддерживают реализацию конкретной меры безопасности или улучшения меры; (ii) определяют тесно связанную *возможность безопасности*; или (iii) упоминаются в дополнительном руководстве. Улучшения мер безопасности по определению связаны с основной мерой. Связанные меры безопасности, которые перечислены в дополнительном руководстве для основных мер, не повторяются в дополнительном руководстве для улучшений мер. Однако, там могут быть связанные меры безопасности, идентифицированные для улучшений мер, которые нет перечислены в основной мере безопасности.

Раздел улучшений мер безопасности обеспечивает описание возможностей безопасности для: (i) добавления функциональности/специфики к мере безопасности; и/или (ii) увеличения стойкости меры безопасности. В обоих случаях, улучшения меры безопасности используются в информационных системах и средах эксплуатации, требующих большей защиты, чем обеспеченно основной мерой вследствие потенциально неблагоприят-

[32] Как правило, определенные организацией *параметры*, используемые в операторах назначении и выбора в основных мерах безопасности, применяются также ко всем улучшениям мер безопасности, связанным с этими мерами безопасности.

[33] Организации определяют, выполняются ли конкретные операторы назначения или выбора на Уровне 1 (уровень организации), Уровне 2 (уровень процесса предназначения/деятельности), Уровне 3 (уровень информационной системы) или их комбинации.

[34] Организации могут определять конкретные значения для параметров мер безопасности в политиках, процедурах или руководствах (которые могут быть применимыми к более чем одной информационной системе), ссылаясь на исходные документы в плане обеспечения безопасности, вместо явного определения операторов назначения/выбора в мерах безопасности как части плана.

[35] Меры безопасности в целом разработаны, чтобы быть независимыми от технологий и реализации, и поэтому не содержат конкретные требования в этих областях. Организации определяют такие требования, какие считают необходимыми, в плане обеспечения безопасности для информационной системы.

ных воздействий на организацию или когда организации ищут дополнения к основной функциональности/ специфике меры, основанной на оценках риска для организации. Улучшения мер безопасности пронумерованы последовательно в пределах каждой меры так, чтобы улучшения могли быть легко идентифицированы когда выбраны для добавления к основной мере. У каждого улучшения меры безопасности есть короткий подзаголовок, чтобы указать на возможности безопасности, обеспечиваемые улучшением меры. В примере для AU-3, если первое улучшение меры выбрано, обозначение меры становится AU-3(1). Числовое обозначение улучшения меры безопасности используется только для того, чтобы идентифицировать определенное улучшение в пределах меры безопасности. Обозначение не указывает ни на стойкость улучшения меры ни на любое иерархическое отношение среди улучшений. Улучшения меры безопасности не предназначены, чтобы быть выбранными независимо (то есть, если улучшение меры безопасности выбрано, то соответствующая основная мера также должна быть выбрана). Это отражено в спецификациях базовых наборов мер в Приложении D и в разделе базовой принадлежности для каждой меры в Приложении F.

Справочный раздел включает список применимых федеральных законов, Правительственных распоряжений, директив, политик, нормативных актов, стандартов и руководств (например, Циркуляры/Меморандумы OMB, Президентские Директивы по безопасности отечества, FIPS публикации и Специальные публикации NIST), которые относятся к определенной мере безопасности.[36] Рекомендации, обеспечиваемые федеральным законодательством и политикой, предоставляют полномочия вместе с поддерживающей информацией для реализации мер безопасности и улучшений мер безопасности. Справочный раздел также содержит подходящие вебсайты для организаций, чтобы использовать в получении дополнительной информации для реализации и оценки мер безопасности.

Раздел приоритета и базовой принадлежности мер безопасности обеспечивает: (i) рекомендуемые приоритетные коды, используемые для упорядочивания решений при реализации мер безопасности; и (ii) начальную принадлежность мер безопасности и улучшений мер безопасности к базовым наборам мер. Организации могут использовать обозначение *приоритетного кода*, связанное с каждой мерой безопасности, чтобы помочь в принятии решений по упорядочиванию при реализации меры безопасности (то есть, Приоритетный Код 1 [P1] меры безопасности имеет более высокий приоритет для реализации, чем Приоритетный Код 2 [P2] меры безопасности, Приоритетный Код 2 [P2] меры безопасности имеет более высокий приоритет для реализации, чем Приоритетный Код 3 [P3] меры безопасности, и Приоритетный Код 0 [P0] указывает, что мера безопасности не выбрана ни в одном из базовых наборов). Это рекомендованное упорядочивание приоритетов помогает гарантировать, что основополагающие меры, от которых зависят другие меры безопасности, реализованы первыми, давая, таким образом, возможность организациям развернуть меры безопасности в более структурированном и своевременном способе в соответствии с доступными ресурсами. Реализация мер безопасности в последовательности приоритетных кодов, однако, не подразумевает достижение какого либо определенного уровня снижения риска до тех пор, пока *все* меры безопасности в плане обеспечения безопасности не будут реализованы. Приоритетные коды предназначены только для упорядочивания реализации, а не для того, чтобы принимать решения по выбору мер безопасности.

2.3 БАЗОВЫЕ НАБОРЫ МЕР БЕЗОПАСНОСТИ

Организации обязаны соответственно смягчать риск, являющийся результатом использования информации и информационных систем в выполнении функций предназначения и деятельности. Существенная проблема для организаций состоит в том, как определить самый рентабельный, соответствующий набор мер, которые если будут реализованы и определены быть эффективными, смягчили бы риск, выполняя требования безопасности, определенных применимыми федеральными законами, Правительственными распоряжениями, нормативными актами, политиками, директивами или стандартами (например, FISMA, Циркуляр OMB A-130, HSPD-12, FIPS публикация 200). Нет какого либо корректного набора мер безопасности, который решает все проблемы безопасности организаций во всех ситуациях. Выбор самого подходящего набора мер

[36] Публикации, перечисленные в справочном разделе, относятся к последним версиям публикаций. Рекомендации предназначены, чтобы помочь организациям в применении мер безопасности и не предназначены, чтобы быть содержательными или полными.

безопасности для конкретной ситуации или информационной системы, чтобы соответственно смягчить риск, является важной задачей, которая требует фундаментального понимания приоритетов предназначения/деятельности организации, функций предназначения и деятельности, которые поддерживают информационные системы и среды эксплуатации, в которых системы будут находиться. С таким пониманием организации могут демонстрировать, как наиболее эффективно гарантировать конфиденциальность, целостность и доступность информации и информационных систем организаций в способе, который поддерживает потребности предназначения/деятельности, демонстрируя должную старательность. Выбор, реализация и поддержание соответствующего набора мер безопасности для адекватной защиты информационных систем, применяемых организациями, требует тесного сотрудничество с владельцами систем для понимания происходящих изменений в функциях предназначения/деятельности, средах эксплуатации и того, как системы используются.

Чтобы помочь организациям в осуществлении соответствующего выбора мер безопасности для информационных систем, представлена концепция *базовых наборов мер безопасности*. Базовые наборы мер безопасности являются начальной точкой для процесса выбора мер безопасности, описанного в этом документе, и выбираются, основываясь на категории безопасности и связанном уровне воздействия на информационные системы, которые определены в соответствии с FIPS Публикацией 199 и FIPS Публикацией 200, соответственно.[37] Приложение D содержит перечень базовых наборов мер безопасности. Идентифицированы три базовых набора мер безопасности, соответствующих информационным системам низкого воздействия, умеренного воздействия и высокого воздействия, используя наивысшее значение, определенное в FIPS публикации 200, использованные в Разделе 3.1 этого документа, чтобы определить начальный набор мер безопасности для каждого уровня воздействия.[38]

Приложение F содержит всеобъемлющий каталог мер безопасности для информационных систем и организаций, расположенных по семействам меры безопасности. Глава Три обеспечивает дополнительную информацию о том, как использовать категории безопасности FIPS публикации 199 и уровни воздействия на системы из FIPS публикации 200 в использовании руководства адаптации к мерам базового уровня безопасности, чтобы достигнуть адекватного снижения риска. Руководство по адаптации, описанное в Разделе 3.2, помогает организациям настроить выбранные базовые наборы мер безопасности, используя результаты оценок риска для организаций. Базовые действия по адаптации включают: (i) идентификацию и определение общих мер безопасности; (ii) применение объектовых особенностей; (iii) выбор компенсирующих меры безопасности; (iv) назначение конкретны значений для параметров мер безопасности; (v) дополнение начальных базовых наборов мер дополнительными мерами безопасности или улучшениями мер безопасности; и (vi) обеспечение дополнительной информацией для реализации мер безопасности.

Совет по реализации

Есть меры безопасности и улучшения мер, представлены в каталоге мер безопасности (Приложение F), которые находятся только в базовых наборах высокого воздействия или не используются ни в одном из базовых наборов. Эти дополнительные меры безопасности и улучшения мер для информационных систем доступны организациям и могут использоваться в адаптации базовых наборов мер безопасности, чтобы достигнуть необходимого уровня защиты в соответствии с оценками риска для организаций. Набор мер безопасности в плане обеспечения безопасности должен быть достаточным, чтобы соответственно смягчить риски к деятельности и активам организации, людям, другим организациям и Нации, основываясь на допустимом риске для организации.

[37] CNSS Инструкция 1253 дает представление о базовых меры безопасности для систем национальной безопасности.

[38] Базовые наборы мер безопасности, содержавшиеся в Приложении D, не являются абсолютно обязательными. Руководство, описанное в Разделе 3.2, предоставляет организациям возможность адаптировать меры безопасности в соответствии с положениями и условиями, установленными их санкционирующими должностными лицами и задокументированными в их соответствующих планах обеспечения безопасности.

2.4 ХАРАКТЕРИСТИКИ МЕР БЕЗОПАСНОСТИ

Есть три различных типа характеристик, связанных с мерами безопасности в Приложении F, которые определяют: (i) область применимости для мер безопасности; (ii) общность мер безопасности; и (iii) ответственность за разработку, реализацию, оценку и санкционирование мер безопасности. Эти характеристики охватывают *общие* меры безопасности, *специфичные для системы* меры безопасности и *гибридные* меры.

Общие меры безопасности - меры, результаты реализации которых в возможности безопасности являются *наследуемыми* одной или более информационными системами организации. Меры безопасности считают наследуемыми информационными системами или компонентами информационных систем, когда системы или компоненты получают защиту от реализованных мер безопасности, но меры разработаны, реализованы, оценены, санкционированы и контролируются сущностями, не являющимися ответственными за системы или компоненты - сущностями, внутренними или внешними к организациям, где системы или компоненты находятся. Возможности безопасности, обеспеченные общими мерами безопасности, могут быть наследованы от многих источников включая, например, организации, сферы предназначения/деятельности организаций, объекты информатизации, анклавы, среды эксплуатации или другие информационные системы. Многие из мер безопасности, необходимые для защиты информационных систем организации (такие, как обучение безопасности, планы реакции на инциденты, физический доступ к средствам, правила поведения), превосходные кандидаты на статус общих мер безопасности. Кроме того, может также быть множество основанных на технологии общих мер безопасности (например, Инфраструктура публичных ключей [PKI], разрешенные безопасные стандартные конфигурации для клиентов/серверов, системы управления доступом, защита периметра, междоменные решения). При централизованном документировании и управлении разработкой, реализацией, оценкой, санкционированием и контролем общих мер безопасности, стоимость безопасности может быть амортизирована по многим информационным системам.

Организация возлагает ответственность за общие меры безопасности на соответствующих должностных лиц организации (то есть, поставщиков общих мер безопасности) и координирует разработку, реализацию, оценку, санкционирование и мониторинг мер безопасности.[39] Идентификация общих мер достигает наибольшего эффекта, если осуществляется в целом для организации с активным участием директоров по информации, высших сотрудников по информационной безопасности, ответственных за риски (функция), санкционирующих должностных лиц, владельцев/управляющих информации, владельцев информационных систем и сотрудников безопасности информационных систем. Осуществлять рассмотрение категорий безопасности информационных систем и мер безопасности для всей организации необходимо, чтобы соответственно смягчать риски, являющиеся результатом использования этих систем (см. *базовый набор* мер безопасности в Разделе 2.3).[40] Идентификация общих мер безопасности проводится для мер, которые влияют на многие информационные системы, но не все системы организации получают пользу от применения подобного подхода. Ключевые заинтересованные стороны сотрудничают, чтобы идентифицировать возможности эффективно использовать общие меры на уровне сферы предназначения/ деятельности, объекта информатизации или анклава.

Когда общие меры безопасности защищают многие информационные системы организации, отличающиеся уровнями воздействия, меры безопасности реализуются относительно самого высокого уровня воздействия среди этих систем. Если общие меры безопасности не будут реализованы на самом высоком уровне воздействия на информационные системы, то владельцы систем будут нуждаться в учете этой ситуации в своих оценках риска и должны предпринимать соответствующие меры снижения риска (например, добавляя меры безопасности или улучшения мер, изменяя назначаемые значения параметров мер безопасности, реализуя компенсирующие меры безопасности или изменяя определенные аспекты процессов предназначения/

[39] Директор по информации, Высший сотрудник по информационной безопасности или другие, назначенные организацией должностные лица на высшем уровне руководства, возлагают ответственность за разработку, реализацию, оценку, санкционирование и мониторинг общих мер безопасности на соответствующие сущности (внутренние или внешние к организации).

[40] Каждая общая мера безопасности, идентифицированная организацией, как правило, рассматривается владельцами информационной системы и санкционирующими должностными лицами для применимости в каждой конкретной информационной системе организации.

деятельности). Реализация общих мер безопасности, которые недостаточно эффективны или которые обеспечивают недостаточную возможность безопасности в отношении информационных систем более высокого воздействия, может оказать существенное неблагоприятное влияние на функции предназначения или деятельности организации.

Общие меры безопасности обычно документируются в общем для организации *плане программы информационной безопасности*, если не реализуются как часть конкретной информационной системы, когда меры безопасности документируются в плане обеспечения безопасности для этой системы.[41] У организаций есть возможность, или описать общие меры безопасности в отдельном документе или в нескольких документах со ссылками или указателями, как соответствующе. В случае нескольких документов документы, описывающие общие меры безопасности, включаются как приложения к плану программы информационной безопасности. Если план программы информационной безопасности содержит несколько документов, организации определяют в каждом документе должностных лиц организации, ответственных за разработку, реализацию, оценку, санкционирование и мониторинг соответствующих общих мер безопасности. Например, организация может потребовать, чтобы Офис управления средствами разработал, реализовал, оценил, аттестовал и непрерывно контролировал меры обеспечения физической защиты и защиты окружающей среды семейства PE, когда такие меры безопасности не связаны с определенной информационной системой, но при этом, поддерживают несколько систем. Когда общие меры безопасности включены в отдельный план обеспечения безопасности для информационной системы (например, меры безопасности использованы как часть системы обнаружения вторжений, обеспечивающей защиту периметра, наследуемую одной или более информационными системами организации), в плане программы информационной безопасности указывается, какой отдельный план обеспечения безопасности содержит описание общих мер безопасности.

Совет по реализации

Выбор общих мер безопасности выполняется наиболее эффективно на основе всей организации с участием высшего руководства (то есть, владельцев предназначения/деятельности, санкционирующих должностных лиц, директоров по информации, высших сотрудников по информационной безопасности, владельцев информационной системы, владельцев/управляющих информации, ответственных за риски). Эти люди имеют коллективное знание, чтобы понимать приоритеты организации, значимость деятельности и активов организации и важность информационных систем, которые поддерживают эту деятельность/активы. Высшие руководители находятся также в лучшей позиции, чтобы выбрать общие меры для каждого базового набора мер безопасности и назначить конкретные обязанности по разработке, реализации, оценке, санкционированию и контролю этих мер безопасности.

Общие меры, используемые в информационных системах организации или средах эксплуатации, санкционируются высшими должностными лицами, по крайней мере, с тем же самым уровнем санкционирования/ ответственности по управлению риском, с каким должностные лица санкционировали информационные системы, наследовавших меры безопасности. Результаты санкционирования для общих мер используются совместно владельцами соответствующих информационных систем и санкционирующими должностными лицами. План действий и вехи разрабатываются и сопровождаются для общих мер безопасности, которые были определены через независимые оценки, как менее стойкие, чем эффективные. Владельцы информационных систем, зависящих от общих мер, которые менее стойкие, чем эффективные, рассматривают, готовы ли они принять связанный с этим риск или требуется дополнительная адаптация, чтобы устранить слабые места или недостатки в мерах безопасности. Такие основанные на риске решения принимаются санкционирующими должностными лицами и организациями с учетом доступных ресурсов, трастовых моделей, используемых организацией, и допустимого риска.[42]

[41] Планы программы информационной безопасности описаны в Приложении G. Организации гарантируют, что любые возможности безопасности, обеспеченные общими мерами безопасности (то есть, возможности безопасности, наследуемые другими сущностями организации), описаны в достаточных деталях, чтобы облегчить адекватное понимание реализации мер безопасности наследуемыми сущностями.

[42] NIST Специальная публикация 800-39 дает представление о трастовых моделях, включая оцененные, проверенные временем, установленные и предписанные трастовые модели.

Общие меры безопасности являются предметом такой же самой оценки и требований мониторинга, как специфичные для систем меры, используемые в отдельных информационных системах организации. Поскольку общие меры безопасности воздействуют более чем на одну систему, может требоваться более высокая степень доверительности относительно эффективности этих мер безопасности.

Меры безопасности, не определенные как общие меры, считаются *специфичными для системы* или *гибридными* мерами безопасности. Специфичные для системы меры безопасности - основная ответственность владельцев информационной системы и соответствующих должностных лиц их санкционирования. Организации назначают *гибридный* статус мерам безопасности, когда одна часть меры является общей, и другая часть меры специфична для системы. Например, организация может реализовать меру безопасности Политика и процедуры реакции на инциденты (IR-1), как гибридную меру, определяемую как общая в части политики, и определяемую как специфичная для системы в части процедур. Гибридные меры могут также служить предопределенными шаблонами для дальнейшего усовершенствования мер безопасности. Организации могут, например, реализовать меру безопасности Планирование на случай непредвиденных ситуаций (CP-2) как предопределенный шаблон для обобщенного плана действий при непредвиденных ситуациях для всех информационных систем организации с адаптацией плана владельцами информационных систем, где необходимо, для специфичного использования систем.

Деление мер безопасности на общие, гибридные и специфичные для систем меры может иметь для организаций результат в существенной экономии в стоимости реализации и оценки, а так же в более непротиворечивом применении мер для всей организации. В то время как разделение мер безопасности на общие, гибридные и специфичные для систем меры является простым и интуитивно понятным, фактическое применение требует существенного планирования и координации. На уровне информационной системы, определение общих, гибридных или специфичных для системы мер следует за разработкой конкретного базового набора. Необходимо сначала определить, какая возможность безопасности необходима прежде, чем организации примут ответственность за то, как меры должны быть реализованы, управляться и сопровождаться.

Планы обеспечения безопасности для отдельных информационных систем идентифицируют, какие меры безопасности, требуемые для этих систем, определены организациями как общие меры и какие меры определены как специфичные для системы или гибридные. Владельцы информационной системы ответственны за любые специфичные для системы детали реализации, связанные с общими мерами безопасности. Эти детали реализации идентифицируются и описываются в планах обеспечения безопасности для конкретных информационных систем. Высшие сотрудники по информационной безопасности организаций взаимодействуют с *поставщиками общих мер безопасности* (например, менеджерами средств/объектов, менеджерами людских ресурсов, владельцами системы обнаружения вторжений), чтобы гарантировать, что требуемые меры разработаны, реализованы и оценены как эффективные. Планы обеспечения безопасности для отдельных информационных систем и общесистемные планы программ информационной безопасности в совокупности обеспечивают полное покрытие для всех мер безопасности, используемых в организации.

Определение того, является ли мера безопасности общей, гибридной или специфичной для системы, основано на контексте. Меры безопасности не могут быть определены как общие, гибридные или специфичные для системы только на основании рассмотрения описания мер. Например, мера безопасности может быть специфичной для определенной информационной системы, но в то же самое время эта мера может быть общей мерой для другой системы, которая наследует меру безопасности от первой системы. Один индикатор того, может ли специфичная для системы мера также быть общей мерой безопасности для другой информационной системы, состоит в рассмотрении того, кто или что зависит от функциональности этой конкретной меры безопасности. Если некоторая часть информационной системы или решения, внешнего к периметру системы, зависит от меры безопасности, то эта мера может быть кандидатом на идентификацию её как общей меры безопасности.

Совет по реализации

- Организации рассматривают *наследованный риск* от использования общих мер безопасности. Планы обеспечения безопасности, отчеты об оценке безопасности и план действий и вехи для общих мер безопасности (или сводка такой информации) являются доступными для владельцев информационных систем (для систем, наследовавших меры безопасности) после того, как информация рассмотрена и одобрена высшим должностным лицом или руководителем, ответственным и подотчетным за меры безопасности.
- Организации гарантируют, что поставщики общих мер безопасности обеспечивают актуальность информации о статусе мер безопасности, так как меры, как правило, поддерживают многие информационные системы организации. Планы обеспечения безопасности, отчеты об оценке безопасности и план действий и вехи для общих мер безопасности используются санкционирующими должностными лицами для принятия основанных на риске решений в процессе санкционирования безопасности для их информационных систем и поэтому, наследованный риск от общих мер безопасности - значимый фактор в таких основанных на риске решениях.
- Организации гарантируют, что у поставщиков общих мер безопасности есть возможность быстро и циркулярно доводить изменения в статусе общих мер безопасности, которые оказывают негативное влияние на защиту, обеспечиваемую и ожидаемую от общих мер безопасности. Поставщики общих мер безопасности сообщают владельцам систем информацию о том, когда проблемы возникают в наследованных общих мерах безопасности (например, когда оценка или переоценка общих мер безопасности указывают, что мера безопасности нарушена или не отвечает в некотором смысле требованиям, или когда появляется новый метод угрозы или атаки, который делает общие меры безопасности менее эффективными в защите от нового метода угрозы или атаки).
- Организации поощрены использовать системы автоматизированного управления для поддержки записей о конкретных общих мерах безопасности, используемых в каждой информационной системе организации, чтобы улучшить возможности поставщиков общих мер безопасности быстро связаться с владельцами систем.
- Если общие меры безопасности предоставлены организациям сущностями, внешними к организации (например, общие и/или внешние поставщики услуг), делаются соглашения с внешними/общими поставщиками услуг организации, чтобы получать информацию относительно эффективности развернутых мер безопасности. Информация, получаемая от внешних организаций относительно эффективности общих мер безопасности, является элементом решения о санкционировании.

2.5 ВНЕШНИЕ ПОСТАВЩИКИ УСЛУГ

Организации становятся все более и более уверенными в услугах информационных систем, предоставляемых внешними поставщиками для выполнения важных функций предназначения и деятельности. Внешние услуги информационной системы это вычислительные и информационно-технологические сервисы, реализуемые за пределами традиционных границ санкционирования безопасности, установленных организациями для их информационных систем. Традиционные границы санкционирования, связанные с физическим пространством и контролем за активами, расширяются (и физически и логически) с ростом использования внешних услуг. В этом контексте внешние услуги могут быть предоставлены: (i) сущностями в рамках организации, но за пределами границ санкционирования безопасности, установленных для информационных систем организации; (ii) сущностями за пределами организации в любом общественном секторе (например, федеральными агентствами) или частном секторе (например, поставщиками коммерческих услуг); или (iii) некоторой комбинацией сущностей общественного и частного сектора. Внешние услуги информационной системы включают, например, использование сервис-ориентированных архитектур (SOA), услуг, основанных на облачных вычислениях (инфраструктура, платформа, программное обеспечение), или применение дата-центров. Внешние услуги информационной системы могут использоваться, но, как правило, не являются частью информационных систем организации. В некоторых ситуациях внешние услуги информационной системы могут полностью заменить или в значительной степени увеличить стандартную функциональность внутренних информационных систем организации.

FISMA и политики OMB требуют, чтобы федеральные агентства, используя внешних поставщиков услуг для обработки, хранения или передачи федеральной информации или управления информационными системами

от имени федерального правительства, гарантировали, что при таком использовании выполняются те же самые требования безопасности, которые федеральные агентства обязаны выполнять. Требования безопасности для внешних поставщиков услуг, включая меры безопасности для внешних информационных систем, отражаются в контрактах или других формальных соглашениях.[43] Организации являются ответственными и подотчетными за риск информационной безопасности, понесенный при использовании услуг информационной системы, предоставленных внешними поставщиками. Такой риск определяется в соответствии с Основами управления рисками (RMF) как часть положений и условий контрактов с внешними поставщиками. Организации могут потребовать, чтобы внешние поставщики реализовывали все, определенные в RMF шаги, кроме шага санкционирования безопасности, который остается, неотъемлемой федеральной ответственностью, непосредственно связанной с управлением риском информационной безопасности, связанным с использованием внешних сервисов информационной системы.[44] Организации могут также потребовать, чтобы внешние поставщики представили соответствующие свидетельства, которые демонстрируют, что они выполнили RMF для защиты федеральной информации. Однако, федеральные агентства несут прямую ответственность за полную безопасность таких сервисов, санкционируя информационные системы, предоставляющие услуги.

Отношения с внешними поставщиками услуг устанавливаются множеством путей, например, через совместные предприятия, коммерческие партнерства, соглашения взаимодействия с соисполнителями (то есть, через контракты, межведомственные соглашения, соглашения направлений деятельности, соглашения об уровне обслуживания), лицензионные соглашения и/или системы обмена поставками. Рост использования внешних поставщиков услуг и новые отношения, устанавливаемые с этими поставщиками, представляют собой новые и трудные проблемы для организаций, особенно в области безопасности информационных систем. Эти проблемы включают:

- определение типов внешних услуг информационных систем, предоставляемых для организаций;
- описание, как эти внешние услуги защищены в соответствии с требованиями информационной безопасности организаций; и
- получение необходимого доверия, что риск для деятельности и активов организации, людей, других организаций и Нации, являющийся результатом использования внешних услуг, приемлем.

Степень доверительности, что риск от использования внешних сервисов на допустимом уровне, зависит от доверия, которое организации возлагают на внешних поставщиков услуг. В некоторых случаях, уровень доверия основан на объеме непосредственного управления, которым организация в состоянии влиять на внешних поставщиках услуг относительно использования мер безопасности, необходимых для защиты сервисов/информации, и свидетельства, ясно показывающего эффективность этих мер безопасности.[45] Уровень управления обычно устанавливается положениями и условиями контрактов или соглашений об уровне обслуживания с внешними поставщиками услуг и может колебаться от всеобъемлющего управления (например, согласовывая контракты или соглашения, которые определяют подробные требования безопасности для поставщиков) до очень ограниченного управления (например, используя контракты или

[43] Организации консультируются с Федеральной Программой управления риском и санкционированием (FedRAMP), получая "облачные" услуги от внешних поставщиков. FedRAMP адресует требуемые меры безопасности и независимые оценки для множества "облачных" услуг. Дополнительная информация доступна в http://www.fedramp.gov.

[44] Чтобы эффективно управлять риском информационной безопасности, организации *санкционируют* информационные системы внешних поставщиков, которые являются частью информационных технологий или сервисов (например, инфраструктура, платформа или программное обеспечение), предоставленных федеральному правительству. Требования санкционирования безопасности отражаются в положениях и условиях контрактов с внешними поставщиками информационных технологий и сервисов.

[45] Уровень доверия, в зависимости от места, которое организации занимают среди внешних поставщиков услуг, может значительно различаться, в пределах от тех, кто чрезвычайно доверен (например, деловые партнеры по совместному предприятию, которые совместно используют общую бизнес-модель и общие цели) до тех, кто менее доверен и представляет большие источники риска (например, деловые партнеры в одной акции, которые являются также конкурентами в другом секторе рынка). NIST Специальная публикация 800-39 описывает различные трастовые модели, которые могут использовать организации, устанавливая отношения с внешними поставщиками услуг.

соглашения об уровне обслуживания для получения серийных услуг[46], таких как коммерческие телекоммуникационные сервисы). В других случаях уровни доверия основываются на факторах, которые убеждают организации, что требуемые меры безопасности были использованы и что существует определение эффективности мер безопасности. Например, отдельно санкционированные внешние услуги информационной системы, предоставленные организациям через известные отношения направлений деятельности, могут обеспечить уровни доверия в таких сервисах в пределах допустимого масштаба риска должностных лиц санкционирования и организаций, использующих услуги.

Предоставление сервисов внешними поставщиками может осуществляться для некоторых сервисов без явных соглашений между организациями и поставщиками. Всякий раз, когда явные соглашения выполнимы и практичны (например, через контракты, соглашения об уровне обслуживания), организации разрабатывают такие соглашения и требуют использования мер из Приложения F этой публикации. Когда организации не имеют возможность требовать явных соглашений с внешними поставщиками услуг (например, услуги предписаны организации, услуги - серийные сервисы), организации устанавливают и документируют явные предположения о возможностях услуг относительно безопасности. В ситуациях, где организации обеспечивают сервисы информационной системы через централизованные механизмы приобретения (такие как общеправительственные контракты Администрации служб общего назначения или других привилегированных и/или обязательных организаций приобретения), это может быть более эффективно и экономически выгодно для источников контракта, чтобы установить и сопроводить заявленные уровни доверия с внешними поставщиками услуг (включая определение требуемых мер безопасности и уровней доверия относительно обеспечения таких мер безопасности). Организации, впоследствии получающие сервисы информационных систем из централизованных контрактов, могут использовать в своих интересах согласованные уровни доверия, установленные источниками приобретения, и таким образом избежать дорогостоящего повторения работ, необходимых чтобы установить такое доверие.[47] Централизованные механизмы приобретения (например, контракты) могут также требовать активного участия организаций. Например, организации, могут требовать через положения в контрактах или соглашениях установить клиентское программное обеспечение, поддерживающее шифрование с открытым ключом, рекомендуемое внешними поставщиками услуг.

В конечном счете, ответственность за адекватное смягчение недопустимых рисков, являющихся результатом использования внешних сервисов информационной системы, остается за санкционирующими должностными лицами. От организаций требуется, чтобы соответствующие *цепочки доверия* были установлены с внешними поставщиками услуг, когда имеется дело со многими проблемами, связанными с безопасностью информационной системы. Организации устанавливают и сохраняют уровень доверия, который участвующим поставщикам услуг в потенциально сложном отношении поставщик - потребитель обеспечивает надлежащую защиту для услуг, оказанных организациям. Цепочка доверия может быть усложнена вследствие числа сущностей, участвующих в отношении поставщик – потребитель, и типов отношений между сторонами. Внешние поставщики услуг могут также получать выбранные сервисы у других внешних сущностей, делая цепочку доверия более трудной и сложной для управления. В зависимости от сущности сервисов, организации могут счесть невозможным надеяться на внешних поставщиков. Эта ситуация соответствует не некоторой свойственной незащищенности со стороны поставщиков, а внутреннему уровню риска в сервисах.[48]

[46] Коммерческие поставщики сервисов товарного типа, как правило, организуют свои бизнес-модели и сервисы вокруг концепции совместно используемых ресурсов и устройств для широкой и разнообразной клиентской базы. Поэтому, если организации не получают полностью выделенные сервисы от поставщиков коммерческих сервисов, то может потребоваться большая уверенность в компенсации мер безопасности, чтобы обеспечить необходимую защиту для информационной системы, которая полагается на эти внешние сервисы. Оценки риска и действия по снижению риска организациями отражают эту ситуацию.

[47] Например, источники приобретения могли санкционировать информационные системы, предоставляющие внешние услуги федеральному правительству согласно конкретным положениям и условиям контрактов. Федеральные агентства, запрашивающие такие услуги в соответствии с контрактами, были бы не обязаны повторно санкционировать информационные системы, получая такие услуги (если запрос не включает услуги вне области исходных контрактов).

[48] Риск может также быть в отклонении некоторой функциональности из-за проблем безопасности. Безопасность - это одно из многих соображений в полном определении риска.

Когда достаточный уровень доверия для внешних сервисов и/или поставщиков не может быть установлен, организации могут: (i) смягчать риск, используя компенсирующие меры безопасности; (ii) принимать риск в пределах уровня допустимого риска организации; (iii) передавать риск, приобретая страховку, чтобы закрыть возможные потери; или (iv) избегать риска, предпочитая не получать услуги от некоторых поставщиков (в результате исполняя предназначение/деятельность с уменьшенными уровнями функциональности или возможно без функциональности вообще).[49] Например, в случае информационных систем и/или сервисов, основанных на облачных вычислениях, организации могли бы потребовать как компенсирующую меру, что бы вся информация, хранящаяся в облаке была зашифрована для дополнительной защиты информации. Альтернативно, организации могут потребовать шифрования части информации, хранящейся в облаке (в зависимости от критичности или чувствительности такой информации) - принимая дополнительный риск, но ограничивая риск того, чтобы не хранить всю информацию в незашифрованной форме.

2.6 ДОВЕРИЕ И ДОВЕРЕННОСТЬ

Доверие и доверенность информационных систем, системных компонентов и сервисов информационной системы становятся все более и более важной частью стратегий управления рисками, разрабатываемых организациями. Развернуты ли информационные системы, чтобы поддержать, например, эксплуатацию национальной системы авиадиспетчерской службы, главного финансового учреждения, атомной электростанции, обеспечивающей электричество для большого города или военные службы и войска, системы должны быть надежны, доверенны и устойчивы перед лицом все более и более сложных и распространяющихся угроз. Чтобы понять, как организации достигают доверенности систем и роль доверия, играемую в факторе доверенности, важно сначала определить термин *доверие*. Доверие, вообще, есть *вера* в то, что сущность будет вести себя предсказуемым образом, выполняя конкретные функции, в конкретных средах и при указанных условиях или обстоятельствах. Сущностью может быть человек, процесс, информационная система, системный компонент, система систем или любая комбинация этого.

С точки зрения информационной безопасности доверие – вера в то, что сущность, важная для безопасности, будет вести себя предсказуемым образом, удовлетворяя определенному набору требований безопасности при указанных условиях/обстоятельствах, подвергаясь разрушениям, человеческим ошибкам, компонентным сбоям и отказам и целеустремленным атакам, которые могут произойти в среде эксплуатации. Доверие обычно определяется относительно конкретных *возможностей безопасности*[50] и может быть решено относительно отдельного системного компонента или всей информационной системы. Однако доверие на уровне информационной системы не достигается в результате создания возможностей безопасности от совокупности доверенных системных компонентов – скорее, доверие на системном уровне есть по сути субъективное определение, которое получается из сложных взаимозависимостей между сущностями (то есть, техническими компонентами, физическими компонентами и людьми), принимая во внимание действия в жизненном цикле, которые связаны с руководством, разработкой, эксплуатацией и поддержкой систем. По сути, наличие доверия к возможностям безопасности требует, чтобы было достаточное основание для доверия, или *доверенность,* в наборе сущностей, важных для безопасности, которые должны быть объединены, чтобы обеспечить такую возможность.

Доверенность в отношении информационных систем, определяет степень, до которой системы, как может ожидаться, сохранят с определенной степенью уверенности, конфиденциальности, целостности и доступности информацию, которая обрабатывается, хранится или передается системами с учетом масштаба угроз. Доверенные информационные системы - системы, которые, как полагают, способны к действию в пределах определенного допустимого риска несмотря на экологические разрушения, человеческие ошибки,

[49] Могут быть доступными альтернативные поставщики, предлагающие более высокое основание для доверия, обычно по более высокой стоимости.

[50] *Возможности безопасности* - комбинация взаимно усиливающих мер безопасности (то есть, мер защиты и контрмер), реализованная техническими средствами (то есть, функциональностью в аппаратных средствах, программном обеспечении и встроенном микропрограммном обеспечении), физическими средствами (то есть, физическими устройствами и мерами защиты), и процедурными средствами (то есть, процедурами, выполняемыми людьми).

структурные отказы и целенаправленные атаки, которые, как ожидается, произойдут в средах в которых системы функционируют - системы, которые имеют доверенность для успешного выполнения установленных функций предназначения/деятельности при условиях нагрузки и неопределенности.[51]

Возможности безопасности

Организации могут рассматривать определение совокупности возможностей безопасности как действие предшествующее процессу выбора мер безопасности. Концепция возможностей безопасности - конструкция, которая определяет, что защита информации, обрабатываемой, хранимой или переданный информационными системами, редко получается из отдельной меры защиты или контрмеры (то есть, меры безопасности). В большинстве случаев, такая защита следует из выбора и реализации ряда взаимно подкрепляемых мер безопасности. Например, организации могут хотеть определить возможности безопасности для безопасной удаленной аутентификации. Эти возможности могут быть достигнуты выбором и реализацией ряда мер безопасности из Приложения F (например, IA-2 [1], IA-2 [2], IA-2 [8], IA-2 [9], и SC-8 [1]). Кроме того, возможности безопасности могут определять множество областей, которые могут включать, например, технические средства, физические средства, процедурные средства или любую комбинацию их. Таким образом, в дополнение к вышеупомянутым функциональным возможностям безопасного удаленного доступа, организациям, возможно, также понадобятся возможности безопасности, которые определяют физические средства, такие как обнаружение вторжений на криптографический модуль или обнаружение/анализ аномалий в орбитальном космическом корабле.

Поскольку число мер безопасности в Приложении F растет в течение продолжительного времени в ответ на все более и более сложное пространство угрозы, для организаций важно иметь возможность описать ключевые возможности безопасности, необходимые для защиты базовых функций предназначения/деятельности организаций, и впоследствии определить ряд мер безопасности, которые, если будут должным образом спроектированы, разработаны и реализованы, предоставят такие возможности. Это упрощает концептуальное рассмотрение проблемы защиты. По сути, использование конструкции возможностей безопасности обеспечивает простой метод группирования мер безопасности, которые используются для общей цели или достижения общей цели. Это становится важным соображением, например, когда проводятся оценки для эффективности мер безопасности.

Традиционно, оценки производятся на основе мера-по-мере получения результата, который характеризуются как принятие (то есть, мера удовлетворительна), или отклонение (то есть, мера не удовлетворительна). Однако, отказ от отдельной меры или, в некоторых случаях, отказ от нескольких мер безопасности, может не влиять на полные возможности безопасности, необходимые организации. Кроме того, использование более широкой конструкции возможностей безопасности позволяет организациям оценивать серьезность уязвимостей, обнаруженных в их информационных системах и определять, влияет ли отклонение определенной меры безопасности (связанное с уязвимостью) или решение не разворачивать некоторую меру безопасности, на полные возможности, необходимые для защиты предназначения/деятельности. Это также облегчает проведение исследования *первопричины*, чтобы определить, может ли отклонение одной меры безопасности быть прослежено до отклонений других мер, основанных на установленных отношениях среди мер безопасности. В конечном счете, решения о санкционировании (то есть, решения приемлемости риска) делаются основаясь на степени, до которой требуемые возможности безопасности были эффективно достигнуты и выполняют требования безопасности, определенные организацией. Эти основанные на риске решения непосредственно связаны с допустимым риском для организации, который определен как часть стратегии управления рисками организации.

Два фундаментальных компонента, влияющие на доверенность информационных систем, являются *функциональность безопасности* и *доверие к безопасности*. Функциональность безопасности, как правило, определяется с точки зрения средств, функций, механизмов, сервисов, процедур и архитектур безопасности, реализованных в информационных системах организаций или средах, в которых работают эти системы. Доверие к безопасности - мера уверенности, что функциональность безопасности реализована правильно, работает как предназначено и производит желаемый результат относительно соответствия требованиям безопасности для системы – то есть, обладает возможностью точно добиться и провести в жизнь

[51] В то время как информация - основная проблемная область, доверенность применяется к защите для всех *активов, которые* организации считают критическими. Наряду с информацией, защитой обеспечиваются технологии (то есть, аппаратные средства, программное обеспечение, встроенное микропрограммное обеспечение), физические элементы (то есть, двери, блокировки, наблюдение) и элементы, связанные с людьми (то есть, люди, процессы, процедуры).

установленную политику безопасности. Меры безопасности определяют и функциональность безопасности и доверие к безопасности. Некоторые меры фокусируются прежде всего на функциональности безопасности (например, PE-3, Физическое управление доступом; IA-2, Идентификация и аутентификация; SC-13, Криптографическая защита; AC-2, Ведение счетов). Другие меры фокусируются прежде всего на доверии к безопасности (например, CA-2, Оценка безопасности; SA-17, Архитектура и проект безопасности разработчика; CM-3, Конфигурационных контроль изменений). Наконец, некоторые меры безопасности могут поддерживать и функциональность безопасности и доверие (например, RA-5, Сканирование уязвимостей; SC-3, Изоляция функций безопасности; AC-25, Монитор обращений). Меры безопасности, связанные с функциональностью, объединяются для разработки возможностей безопасности со связанными с доверием мерами безопасности, реализованными, чтобы обеспечить степень уверенности в возможностях в пределах допуска риска для организации.

Свидетельство доверия - от действий по разработке и эксплуатации

Организации получают доверие к безопасности через *меры,* предпринятыми разработчиками, внедренцами, операторами, специалистами по поддержке и оценщиками информационной системы. Действия людей и/или групп во время разработки/эксплуатации информационных систем производят *свидетельство безопасности*, которое способствует доверию, или степени уверенности, в функциональности безопасности, необходимой чтобы предоставить возможности безопасности. Глубина и покрытие этих действий (как описано в Приложении E) также способствуют эффективности свидетельства и степени уверенности. Свидетельства, произведенные разработчиками, внедренцами, операторами, оценщиками и специалистами по поддержке во время жизненного цикла разработки систем (например, образцы проекта/разработки, результаты оценки, декларации и сертификаты об оценке/подтверждении соответствия), способствуют пониманию мер безопасности, реализованных организациями.

Стойкость функциональности безопасности[52] играет важную роль в возможности достижения необходимых возможностей безопасности и впоследствии удовлетворении требованиям безопасности организаций. Разработчики информационной системы могут увеличить стойкость функциональности безопасности, используя, как часть процесса разработки аппаратного/программного/встроенного микропрограммного обеспечения: (i) четко определенную политику безопасности и модели политики; (ii) структурированные/строгие технологии проектирования и разработки; и (iii) осмысленные системные/обеспечения безопасности инженерные подходы. Образцы, сгенерированные этими действиями при разработке (например, функциональные спецификации, проекты высокого/низкого уровня, представления реализации [исходный код и схемотехника аппаратных средств], результаты статического/динамического тестирования и анализа кода), могут представить важные свидетельства, что информационные системы (включая компоненты, которые составляют эти системы) будут более надежны и доверенны. Свидетельство безопасности может также быть получено из проверки безопасности, проведенного независимыми, аккредитованными, сторонними организациями оценки (например, испытательными лабораториями Общих критериев, испытательными лабораториями по криптографической защите и других работ по оценке организаций правительственного и частного секторов[53]).

В дополнение к свидетельствам, полученным в среде разработки, организации могут получить свидетельства от среды эксплуатации, которые способствует доверию к функциональности и, в конечном счете, к возможностям безопасности. Эксплуатационные свидетельства включают, например, отчеты о недостатках, записи о восстановительных мероприятиях, результаты отчетности об инцидентах безопасности и результаты работ организации по постоянному мониторингу. Такие свидетельства помогают определить эффективность развернутых мер, изменений в информационных системах и средах эксплуатации и согласию с федеральным

[52] *Стойкость безопасности* компонента информационной системы (то есть, аппаратных средств, программного обеспечения или встроенного микропрограммного обеспечения) определена степенью, с которой функциональность безопасности, реализованная в том компоненте, является корректной, полной, устойчивой чтобы противостоять атакам (стойкость механизма) и устойчивой к обходу или вмешательству.

[53] Например, сторонние организации оценивают "облачные" сервисы и поставщиков услуг в поддержку федеральной Программы управления риском и санкционированием (FedRAMP). Испытательные лаборатории Общих критериев испытывают и оценивают продукты информационных технологий, используя стандарт ISO/IEC 15408. Испытательные лаборатории по криптографической защите испытывают криптографические модули, используя стандарт FIPS 140-2.

законодательством, политиками, директивами, нормативными актами и стандартами. Свидетельства безопасности, полученные из действий по разработке или эксплуатации, обеспечивают лучшее понимание мер безопасности, реализованных и используемых организациями. Вместе, меры, предпринятые разработчиками во время жизненного цикла разработки систем, реализуемые, операторами, специалистами по поддержке и оценщиками и свидетельства, полученные как часть этих действий, помогают организациям определить степень, до которой функциональность безопасности в пределах их информационных систем реализована правильно, работает как предписано и производит желательный результат относительно соответствия заявленным требованиям безопасности и проводит в жизнь или способствует установленной политике безопасности - таким образом, обеспечивая большую уверенность в возможностях безопасности.

Неотразимый аргумент за доверие

Организации специфицируют связанные с доверием меры безопасности, чтобы определить действия, выполняемые чтобы получить соответствующее и заслуживающее доверия свидетельство о функциональности и поведении информационных систем организации и проследить свидетельство до элементов, которые обеспечивают такую функциональность/поведение. Это свидетельство используется, чтобы получить степень уверенности, что системы удовлетворяют заявленным требованиям безопасности - и делают это, эффективно поддерживая функции предназначения/деятельности организаций, будучи подвергнутыми угрозам в установленных средах эксплуатации.

Что касается получаемых свидетельств безопасности, *глубина* и *покрытие* таких свидетельств могут влиять на уровень доверия к реализованной функциональности. Глубина и покрытие - атрибуты, связанные с методами оценки и получением свидетельств безопасности. Методы оценки могут быть применены к доверию связанному и с разработкой и с эксплуатацией. Для доверия связанного с разработкой глубина связана со строгостью, уровнем детализации и формальностью образцов, полученных при проектировании и разработке аппаратных средств, программного обеспечения и компонентов встроенного микропрограммного обеспечения информационных систем (например, функциональные спецификации, высокоуровневый проект, низкоуровневый проект, исходный код). Уровень детализации, доступный в образцах разработки, может влиять на тип тестирования, оценки и анализа, проведенного во время жизненного цикла разработки систем (например, тестирование "черного ящика", тестирование «серого ящика», тестирование "белого ящика", статический/динамический анализ). Для эксплуатационного доверия атрибут глубины определяет количество и типы связанных с доверием мер безопасности, выбранных и реализованных. Напротив, атрибут покрытия связан с методами оценки, используемыми во время разработки и эксплуатации, определяя область и размер объектов оценки, включенных в оценки (например, число/типы тестов, проведенных на исходном коде, число проанализированных программных модулей, число сетевых узлов/мобильных устройств, проверенных на уязвимость, число людей, у которых взяли интервью, чтобы проверить понимание обязанностей по непредвиденным ситуациям).[54]

Определение связанных с доверием мер безопасности при приобретении и разработке систем может помочь организациям получить достаточно доверенные информационные системы и компоненты, которые более надежны и с меньшей вероятностью могут быть нарушены. Эти меры безопасности включают гарантию, что разработчики используют обоснованные инженерные принципы и процессы обеспечения безопасности, включая, например, обеспечение комплексной архитектуры безопасности и претворение строгого управления конфигурацией и контроля изменений в информационных системах и программном обеспечении. После того как информационные системы развернуты, связанные с доверием меры безопасности могут помочь организациям продолжать быть уверенными в доверенности систем. Эти меры безопасности включают, например, осуществление проверки целостности программного обеспечения и компонентов встроенного микропрограммного обеспечения, проведение тестирования на возможность проникновения, чтобы найти уязвимости в

[54] NIST Специальная публикация 800-53A даёт представление о получении свидетельств безопасности, связанных с оценками безопасности, проведенными во время жизненного цикла разработки систем.

информационных системах организации, контроль установленных безопасных параметров конфигурации и разработку политик/процедур, которые поддерживают эксплуатацию и применение систем.

Концепции, описанные выше, включая требования безопасности, возможности безопасности, меры безопасности, функциональность безопасности и доверие к безопасности, объединены в модели доверенности для системных компонентов и информационных систем. Рисунок 3 иллюстрирует ключевые компоненты в модели и отношения между компонентами.

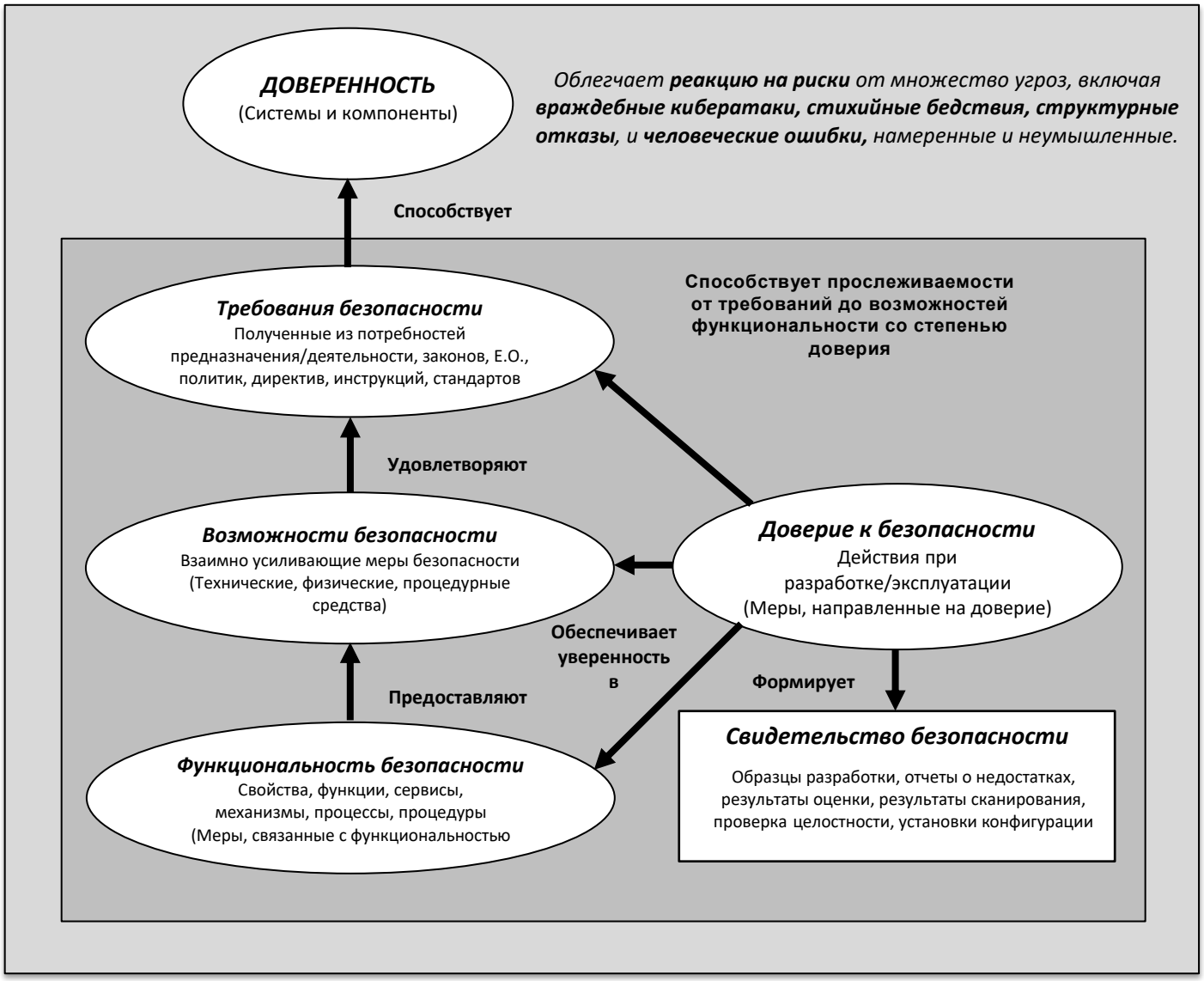

РИСУНОК 3. МОДЕЛЬ ДОВЕРЕННОСТИ

Действия, связанные с разработкой и эксплуатацией, для достижения высокого доверия

Повышение планки доверия может быть трудным и дорогостоящим для организаций, но иногда важным для критических приложений, предназначения или функций деятельности. Определение какие части инфраструктуры информационных технологий организации требуют более высокого доверия при реализации функциональности безопасности осуществляется на уровне 1/уровне 2 действий по управлению рисками (см. рисунок 1 в Главе Два). Этот тип действий возникает когда организации определяют *требования безопасности*, необходимые чтобы защитить деятельность организации (то есть, предназначение, функции, имидж и репутацию), активы организации, людей, другие организации и Нацию. Определение требований безопасности и связанных *возможностей безопасности,* необходимых для осуществления соответствующей защиты, неотъемлемая часть процесса управления рисками организации, представленного в Специальной публикации NIST 800-39, - конкретно, в разработке *стратегии реакции на риски* после шагов структурирования риска и оценки степени риска (где организации устанавливают приоритеты, предположения, ограничения, допустимые риски и оценивают угрозы, уязвимости, воздействие на предназначение/ деятельность, и вероятность осуществления угрозы). После того, как требования безопасности и возможности безопасности определены на Уровнях 1 и 2 (включая необходимые требования доверия, чтобы обеспечить степень уверенности в требуемых возможностях), эти требования/возможности отражаются в проекте архитектуры предприятия, связанной с процессами предназначения/деятельности и информационными системами организации, которые необходимы, чтобы поддержать эти процессы. Организации могут использовать Основу управления рисками (RMF), описанные в Специальной публикации NIST 800-37, чтобы гарантировать, что соответствующие уровни доверия достигнуты для информационных систем и системных компонентов, развернутых, чтобы выполнить базовые функции предназначения и деятельности. Это, прежде всего, работы Уровня 3, но могут иметь некоторое перекрытие с Уровнями 1 и 2, например, в области выбора общих мер безопасности.

Доверенные информационные системы трудно создать из программного обеспечения и систем перспективной разработки. Однако есть много проектных, архитектурных принципов и принципов реализации, которые, если используются, могут иметь результат в более доверенных системах. Эти базовые *принципы безопасности* включают, например, простоту, модульность, иерархическое представление, изоляцию доменов, наименьшее количество полномочий, наименьшее количество функциональности и изоляцию/инкапсуляцию ресурсов. Продукты и системы информационных технологий, показывающие более высокую степень доверенности (то есть продукты/системы, имеющие необходимую функциональность безопасности и доверие к безопасности), как, ожидается, будут показывать более низкий уровень скрытых дефектов проекта/реализации и более высокую степень сопротивления проникновениям в отношении масштабных угроз включая, например, сложные кибератаки, стихийные бедствия, аварии и намеренные/неумышленные ошибки.[55] Уязвимость и чувствительность функций предназначения/ деятельности организаций и поддерживающих информационных систем к известным угрозам, средам эксплуатации, где эти системы развернуты, и максимально допустимый уровень риска информационной безопасности, являются руководством по степени необходимой доверенности.

Приложение E содержит минимальные требования доверия для федеральных информационных систем и организаций и выделяет, связанные с доверием меры безопасности в базовых наборах мер безопасности из Приложения D, которые необходимы, чтобы гарантировать, что требования удовлетворены.[56]

[55] Организации также полагаются в значительной степени на доверие к безопасности с эксплуатационной точки зрения, как представлено связанными с доверием мерами в Таблицах E-1…E-3. Эксплуатационное доверие получается другими действиями, чем действия связанные с разработкой, включая, например, определение и применение установок конфигурации безопасности к продуктам информационных технологий, установление политик и процедур, оценка мер безопасности и проведение строгой непрерывной программы мониторинга. В некоторых ситуациях, чтобы достигнуть необходимых возможностей безопасности со слабыми или несовершенными информационными технологиями, организации осуществляют компенсацию, увеличивая их эксплуатационное доверие.

[56] Инструкция CNSS 1253 определяет базовые меры безопасности для систем национальной безопасности. Поэтому, связанные с доверием меры безопасности в базовых наборах мер, установленных для сообщества национальной безопасности, если установлены, могут отличаться от тех мер, которые определены для систем, не относящихся к национальной безопасности.

Почему доверие имеет значение

Важность доверия к безопасности может быть описана при использовании примера выключателя света на стене в гостиной вашего дома. Люди могут наблюдать, что просто включая и выключая переключатель, кажется, что переключатель должен действовать согласно его функциональной спецификации. Это походит на проведение тестирования функциональности безопасности в информационной системе или системном компоненте методом "черного ящика". Однако, более важными вопросами могли бы быть -

делает ли выключатель света что-либо еще помимо того, что он, как предполагается, делает?
на что выключатель света похож изнутри?
какие типы компонентов использовались, чтобы сконструировать выключатель света и как выключатель был собран?
следовал ли производитель выключателя в процессе разработки лучшим методам отрасли?

Этот пример походит на многие действия, связанные с разработкой, которые определяют качество функциональности безопасности в информационной системе или системном компоненте, включая, например, принципы разработки, технологии программирования, анализ кода, тестирование и оценку.

Требования доверия к безопасности и ассоциированные, связанные с доверием, меры безопасности в Приложении Е рассматривают проблему выключателя света на наружной стороне стены и, потенциально, изнутри стены, в зависимости от меры доверительности, необходимой для рассматриваемого компонента. Для функций предназначения/деятельности организаций, которые являются менее критическими (то есть, низкого воздействия), могли бы быть соответствующими более низкие уровни доверия. Однако, по мере того как функции предназначения/ деятельности становятся более важными (то есть, умеренного или высокого воздействия) и информационные системы и организации, становятся восприимчивыми к постоянным развивающимся угрозам высококвалифицированных противников, могут требоваться повышенные уровни доверия. Кроме того, поскольку организации становятся более зависящими от внешних сервисов информационных систем и поставщиков, доверие становится более важным, обеспечивая большую способность проникновения в суть и степень уверенности организаций в понимании и проверке возможностей безопасности внешних поставщиков и услуг, предоставленных федеральному правительству. Таким образом, когда потенциальное воздействие на деятельность и активы организаций, людей, другие организации или Нацию является большим, увеличивающийся уровень усилия должен быть направлен на то, что происходит внутри.

2.7 ВЕРСИИ И РАСШИРЕНИЯ

Меры безопасности, перечисленные в этой публикации, представляют практические меры защиты и контрмеры для федеральных информационных систем и организаций. Меры безопасности[57] будут тщательно рассматриваться и периодически перевыпускаться, чтобы отразить:

- опыт, извлекаемый при использовании мер безопасности;
- новое федеральное законодательство, правительственные распоряжения, директивы, нормативные акты или политики;
- изменение требований безопасности;
- появляющиеся угрозы, уязвимости и методы атак; и
- доступность новых технологий.

Меры в каталоге мер безопасности, как ожидается, будут изменяться по истечении времени, так как меры будут исключаться, пересматриваться и добавляться. Меры безопасности, определённые в базовых наборах мер низкого, умеренного и высокого уровней безопасности, как ожидается, также будут изменяться с течением времени, как в части уровня безопасности так и необходимых усилий для того, чтобы смягчить риски в соответствии с изменениями в организациях. В дополнение к необходимости в изменении, необходимость в устойчивости определяет потребность, чтобы предлагаемые модификации к мерам безопасности проходили

[57] Меры обеспечения приватности, перечисленные в Приложении J, будут также обновляться на регулярной основе, используя подобные критерии.

через строгий публичный процесс рассмотрения, чтобы получить обратную связь от общественного и частного секторов и прийти к согласию для такого изменения. Это обеспечивает в течение долгого времени устойчивый, гибкий и технически осмысленный набор мер безопасности для федерального правительства, подрядчиков и любых других организаций, использующих каталог мер безопасности.

ГЛАВА ТРИ

ПРОЦЕСС

ВЫБОР И СПЕЦИФИКАЦИЯ МЕР БЕЗОПАСНОСТИ

Эта глава описывает процесс выбора и определения мер безопасности и улучшений мер безопасности для информационных систем организаций, что включает: (i) выбор соответствующих базовых наборов мер безопасности; (ii) адаптация базовых наборов мер; (iii) документирование процесса выбора мер безопасности; и (iv) применение процесса выбора мер безопасности к новым разработкам и унаследованным системам.

3.1 ВЫБОР БАЗОВЫХ НАБОРОВ МЕР БЕЗОПАСНОСТИ

При подготовке к выбору и определению надлежащих мер безопасности для информационных систем организаций и соответствующих сред эксплуатации, организации сначала определяют критичность и чувствительность информации, которая будет обрабатываться, храниться или передаваться этими системами. Этот процесс, известный как категорирование безопасности, описан в FIPS публикации 199.[58] Стандарт категорирования безопасности основан на простой и известной концепции - определении потенциального неблагоприятного воздействия для информационных систем организации. Результаты категорирования безопасности помогают в руководстве и информации для выбора соответствующих мер безопасности (то есть, мер защиты и контрмер), чтобы соответственно защитить эти информационные системы. Меры безопасности, выбранные для информационных систем, соразмерны с потенциальным неблагоприятным воздействием на деятельность и активы организаций, людей, другие организации или Нацию, если имеется потеря конфиденциальности, целостности или доступности. FIPS публикация 199 требует, чтобы организации категорировали информационные системы как системы низкого, умеренного или высокого уровней воздействия для заявленных целей безопасности конфиденциальности, целостности и доступности (**Шаг 1 RMF**). Потенциальные значения воздействия, назначенные для целей безопасности, являются самыми высокими значениями (то есть, наивысшими значениями) для категорий безопасности, которые были определены для каждого типа обрабатываемой, хранимой или передаваемой информации этими информационными системами.[59] Обобщенный формат для того, чтобы определить категорию безопасности (SC) информационной системы следующий:

SC Информационная 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 тем же самыми для конкретной информационной системы, концепция наивысшего значения (представленная в FIPS публикации 199) используется в FIPS публикации 200, чтобы определить уровень воздействия на информационную систему с целью выбора применимого набора мер безопасности как одного из трех базовых наборов, идентифицированных в Приложении D.[60] Таким образом, система *низкого воздействия* определена как информационная система, в которой все три из целей безопасности низки. Система *умеренного воздействия* - информационная система, в которой по крайней мере одна из целей

[58] Инструкция CNSS 1253 обеспечивает руководство по категорированию безопасности для систем национальной безопасности.

[59] Специальная публикация NIST 800-60, Руководство по отображению типов информации и информационных систем к категориям безопасности, дает представление о назначении категорий безопасности для информационных систем.

[60] Концепция наивысшего значения использована, потому что есть существенные зависимости среди целей безопасности конфиденциальности, целостности и доступности. В большинстве случаев, компрометация одной из целей безопасности, в конечном счете, также влияет на другие цели безопасности. Следовательно, меры безопасности не категорированы по целям безопасности. Скорее меры безопасности сгруппированы в базовые наборы, чтобы обеспечить общую возможность защиты для классов информационных систем, основанных на уровне воздействия.

безопасности умеренна, и нет цели безопасности большей чем умеренная. Наконец, система высокого воздействия - информационная система, в которой, по крайней мере, одна цель безопасности высокая.

Совет по реализации

Определение уровня воздействия для информационной системы:

Во-первых, определите различные типы информации, которые обрабатываются, хранятся или передаются информационной системой. Специальная публикация NIST 800-60 содержит общие типы информации.
Во-вторых, используя значения воздействий в FIPS публикации 199 и рекомендациях Специальной публикации NIST 800-60, прокатегорируйте конфиденциальность, целостность и доступность для каждого типа информации.
В-третьих, проведите категорирование безопасности информационной системы, то есть, определите самые высокие значения воздействий для каждой цели безопасности (конфиденциальности, целостности, доступности) из числа категорированных для типов информации, связанных с информационной системой.
В-четвертых, определите полный уровень воздействия для информационной системы как самого высокого значения воздействия среди трех целей безопасности в категорировании безопасности системы.

Примечание: *Для систем национальной безопасности организации используют для категорирования безопасности CNSSI 1253.*

Как только уровень воздействия для информационной системы определен, организации начинают процесс выбора мер безопасности (**Шаг 2 RMF**). Первый шаг в выборе и определении мер безопасности для информационной системы состоит в выборе соответствующего базового набора мер безопасности.[61] Выбор базового набора мер безопасности основан на FIPS 200 уровне воздействия на информационную систему, определенного в процессе категорирования безопасности, описанном выше. Организация выбирает один из трех базовых наборов мер безопасности из Приложения D, соответствующих низкому воздействию, умеренному воздействию или высокому воздействию, оцененному для информационной системы.[62] Следует заметить, что не все меры безопасности назначены в базовые наборы, что обозначено в Таблице D-2 фразой, *не выбрано*. Точно так же, как иллюстрировано в Таблицах от D-3 до D-19, не все улучшения мер безопасности назначены в базовые наборы. Те улучшения мер безопасности, которые назначены в базовые наборы обозначены "**x**" в столбцах, соответствующих низкому, умеренному или высокому уровням. Использование термина *базовый набор* является намеренным. Меры безопасности и улучшения мер безопасности в базовых наборах - начальная точка, из которой меры безопасности/улучшения могут быть удалены, добавлены или специализированы, основываясь на руководстве адаптации в Разделе 3.2.

Базовые наборы мер безопасности в Приложении D определяют потребности безопасности широкого и разнообразного набора потребителей (включая отдельных пользователей и организации). Некоторые *предположения*, которые в целом лежат в основе базовых наборов в Приложении D, включают, например: (i) среды, в которых работают информационные системы организаций; (ii) тип эксплуатации, применяемый организациями; (iii) функциональность, используемая в информационных системах; (iv) типы угроз, направленных на организации, процессы предназначения/деятельности и информационные системы; и (v) типы информации, обрабатываемой, хранимой или передаваемой информационными системами. Точное формулирование базовых предположений является основным элементом в начальном шаге *структурирования риска* процесса управления рисками, описанного в Специальной публикации NIST 800-39. Некоторые из предположений, которые лежат в основе базовых наборов в Приложении D, включают:

[61] Общий процесс выбора мер безопасности может расширяться или больше детализироваться дополнительным, специфичным для сектора руководством, как описано в Разделе 3.3, *Создание оверлеев*, и Приложении I, *шаблон* для разработки *оверлеев*.
[62] Инструкция CNSS 1253 определяет базовые наборы мер безопасности для систем национальной безопасности.

- Информационные системы расположены в физических сооружениях;
- Пользовательские данные/информация в информационных системах организаций являются относительно постоянными;63
- Информационные системы являются многопользовательскими (или последовательно или одновременно) в эксплуатации;
- Некоторые пользовательские данные/информация в информационных системах организаций не являются общими для других пользователей, у которых есть санкционированный доступ к тем же самым системам;
- Информационные системы существуют в сетевых средах;
- Информационные системы, по сути, имеют общее назначение; и
- У организаций есть необходимая структура, ресурсы и инфраструктура, чтобы реализовать меры безопасности.64

Если одно или более из этих предположений нет допустимо, то некоторые из мер безопасности, назначенных в начальные базовые наборы в Приложении D, могут быть не применимы - ситуация, которая может легко решаться, применяя руководство по адаптации в Разделе 3.2 и результаты оценок риска организации. Наоборот, есть также некоторые возможные ситуации, которые конкретно не определены в базовых наборах. Они включают:

- в организациях существуют инсайдерские угрозы;
- информационными системами обрабатываются, хранятся или передаются классифицированные данные;
- для организаций существуют постоянные развивающиеся угрозы (APT);
- выборочные данные/информация требуют специализированной защиты, основанной на федеральном законодательстве, директивах, нормативных актах или политиках; и
- информационные системы должны взаимодействовать с другими системами через различные домены безопасности.

Если какое-либо из вышеупомянутых предположений применяется, то, вероятно, были бы необходимы дополнительные меры безопасности из Приложения F, чтобы гарантировать надлежащую защиту - ситуация, которая также может эффективно решаться, применяя руководство адаптации из Раздела 3.2 (а именно, дополнением мер безопасности) и результаты оценок риска организаций.

3.2 АДАПТАЦИЯ БАЗОВОГО НАБОРА МЕР БЕЗОПАСНОСТИ

После выбора применимого базового набора мер безопасности из Приложения D организации инициируют процесс адаптации, чтобы соответственно изменить и выровнять меры безопасности более близко с особыми условиями в организациях (то есть, условиями, связанными с функциями предназначения/ деятельности, информационными системами или средами эксплуатации организаций). Процесс адаптации включает:

- идентификацию и определение общих мер безопасности в начальных базовых наборах мер безопасности;
- применение объектовых особенностей к остальным мерам базового набора мер безопасности;
- выбор компенсирующих мер безопасности, если необходимо;

63 Постоянство данных/информации относится к данным/информации, являющихся востребованными в течение относительно долгого времени (например, дни, недели).

64 Вообще, федеральные департаменты и агентства удовлетворяют этому предположению. Предположение становится более проблемным для нефедеральных сущностей, таких как муниципалитеты, службы оперативного реагирования и мелкие (комерческие) подрядчики. Такие сущности могут не быть достаточно большими или достаточно оснащенными, чтобы иметь возможность выделить элементы для обеспечения масштаба возможностей безопасности, которые приняты базовыми. Организации рассматривают такие факторы в своих основанных на риске решениях.

- назначение конкретных значений для определенных организациями параметров мер безопасности через операции явного назначения и выбора;
- дополнение базовых наборов дополнительными мерами безопасности и улучшениями мер безопасности, если необходимо; и
- предоставление дополнительной специфичной информации для реализации мер безопасности, если необходимо.

Процесс адаптации, как неотъемлемая часть выбора и спецификации мер безопасности, является частью всестороннего процесса управления рисками организации – структурирования, оценки, реакции на и мониторинга риска информационной безопасности. Организации используют руководство управления рисками, чтобы облегчить основанное на риске принятие решений относительно применимости мер безопасности в базовых наборах мер безопасности. В конечном счете, организации используют процесс адаптации, чтобы достигнуть рентабельной, основанной на риске безопасности, которая поддерживает потребности предназначения/деятельности организаций. Работы по адаптации санкционируются уполномоченными должностные лица в координации с выбранными должностными лицами организаций (например, ответственными за риски [функция], директорами по информации, высшими сотрудниками информационной безопасности, владельцами информационных систем, поставщиками общих мер безопасности) до реализации мер безопасности. У организаций есть гибкость по выполнению процесса адаптации на уровне организации для всех информационных систем (если или требуется адаптация базового набора мер или как начальная точка для работ по адаптации, специфичных для системы), в поддержку определенного направления деятельности или процесса предназначения/деятельности, на уровне отдельной информационной системы или при использовании комбинации вышеупомянутого.[65]

Однако, организации не удаляют меры безопасности исходя из удобства эксплуатации. Адаптация решений относительно мер безопасности должна быть оправдана основываясь на потребностях предназначения/ деятельности и сопровождаться явными основанными на риске решениями.[66] Адаптация решений, включая конкретное обоснование для этих решений, документируется в планы обеспечения безопасности для информационных систем организации. Каждая мера безопасности применимого базового набора мер безопасности рассматривается организацией (например, поставщиком общих мер безопасности) или владельцем информационной системы. Если некоторые меры безопасности адаптированы, то соответствующее обоснование документируется в планах обеспечения безопасности (или делаются рекомендации/указания на другую соответствующую документацию) для информационных систем, и одобряются ответственными должностными лицами организаций, как часть процесса санкционирования плана обеспечения безопасности.[67]

Документирование существенных решений управления рисками в процессе выбора мер безопасности обязательно для того, чтобы санкционирующие должностные лица имели необходимую информацию, для принятия верных, основанных на риске решений относительно санкционирования информационных систем. Так как информационные системы, среды эксплуатации и персонал, связанные с жизненным циклом разработки систем, подвержены изменениям, обеспечение предположений, ограничений и обоснований, поддерживающих эти важные решения риска, позволяет лучшее понимать в будущем состояния безопасности информационных систем или сред эксплуатации для того времени, когда исходные решения риска были приняты, и облегчает идентификацию изменений, когда предыдущие решения риска пересматриваются.

[65] См. также Раздел 3.3, *Создание оверлеев*, и Приложение I, *шаблон* для разработки *оверлеев*.

[66] Адаптация решений может также быть основана на синхронизации и приспособлении выбранных мер безопасности под некоторые определенные условия. Таким образом, меры безопасности могут не применяться в каждой ситуации, или значения параметра для операторов присваивания могут измениться при определенных обстоятельствах. Оверлеи могут определять эти конкретные ситуации, условия или связанные с синхронизацией соображения.

[67] Уровень детализации, требуемый в документировании решений адаптации в процессе выбора мер безопасности выбирается на усмотрение организаций и отражает уровни воздействия соответствующей реализации информационных систем или наследования мер безопасности.

Идентификация и обозначение общих мер безопасности

Общие меры безопасности являются мерами, которые могут быть наследованными одной или более информационными системами организации. Если информационная система наследовала общие меры безопасности, то эта система не должна явно реализовывать эти меры безопасности - то есть, возможности безопасности обеспечиваются другой сущностью. Поэтому, когда меры безопасности в Приложении F указывают на то, чтобы информационная система реализовала или выполнила определенную функцию безопасности, это не должно быть интерпретировано так, чтобы означать, что все системы, которые являются частью больших, более сложных систем или все компоненты определенной системы, должны реализовать эту меру или функцию. Решения организации, в соответствии с которыми меры безопасности определяются как общие меры безопасности, могут значительно влиять на обязанности отдельных владельцев систем относительно реализации мер безопасности в конкретном базовом наборе мер. Выбор общих мер безопасности может также влиять на полные расходы ресурсов организаций (то есть, чем больше число реализованных общих мер безопасности, тем больше потенциальное снижение издержек).

Использование объектовых особенностей

Объектовые особенности, когда используются совместно с руководством управления рисками, предоставляют организациям более гранулированную основу, на которой можно сделать основанные на риске решения.[68] Использование объектовых особенностей может устранить ненужные меры безопасности из начальных базовых наборов мер безопасности и помочь гарантировать, что организации выбирают *только* те меры безопасности, которые необходимы, чтобы обеспечить соответствующий уровень защиты для информационных систем организации - защиту, основанную на функциях предназначения и деятельности, поддерживаемых этими системами и средами, в которых работают системы. Организации могут применить объектовые особенности, описанные ниже, чтобы помочь с разработкой основанных на риске решений относительно выбора и спецификации мер безопасности - решений, которые могут потенциально влиять на то, как меры базового уровня безопасности применены и реализованы организациями:

- СООБРАЖЕНИЯ ВЫДЕЛЕНИЯ И РАЗМЕЩЕНИЯ МЕР БЕЗОПАСНОСТИ -

  Термин и*нформационная система* может относиться к системам различных уровней абстракции в диапазоне от системы систем к отдельным однопользовательским системам. Растущая сложность многих информационных систем требует тщательного анализа в выделении/размещении мер безопасности в рамках трех уровней в иерархии управления рисками (уровень организации, уровень процесса предназначения/деятельности и уровень информационной системы), без наложения конкретных архитектурных представлений или решений.[69] Меры безопасности в начальных базовых наборах представляют информацию набора мер безопасности масштаба всей системы, которые могут быть не применимы к каждому компоненту в системе. Меры безопасности применимы только к компонентам информационной системы, которые обеспечивают или поддерживают возможности информационной безопасности, определяемые мерами безопасности.[70] Организации принимают явные, основанные на риске решения относительно того, где применять или выделять конкретные меры безопасности в информационных системах организаций, чтобы достигнуть необходимых возможностей безопасности и удовлетворить требованиям безопасности.[71] Пример этого типа выделения применяется в требованиях от AC-18(1) (то есть, защиты беспроводного доступа к информационным системам, используя

[68] Объектовые особенности, перечисленные в этом разделе, являются примерами и не предназначены, чтобы ограничить организации в представлении основанных на риске решений, базирующихся на других определенных организацией соображениях с соответствующим обоснованием.

[69] Это особенно справедливо с появлением сервис-ориентированных архитектур, где конкретные услуги предоставляются, чтобы реализовать отдельную функцию.

[70] Например, меры аудита безопасности, как правило, применяются к компонентам информационной системы, которые обеспечивают возможность аудита (например, серверы, и т.д.) и не обязательно применимы к каждой рабочей станции на уровне пользователя в организации. Организации должны тщательно оценить материально-технические ресурсы компонентов, которые составляют их информационные системы, чтобы определить, какие меры безопасности применимы к различным компонентам.

[71] Поскольку информационные технологии развиваются, более мощная и разнообразная функциональность может быть найдена в смартфонах, планшетах и других типах мобильных устройств. В то время как руководство по адаптации может не поддерживать выделение определенной меры безопасности к конкретной технологии или устройству, любой остаточный риск, связанный с отсутствием такой меры, должен определяться в оценках степени риска, чтобы соответственно защитить эксплуатацию и активы организации, людей, другие организации и Нацию.

аутентификацию/шифрование) до всего беспроводного доступа за исключением беспроводного доступа к подсетям посетителей, которые не соединены с другими компонентами систем.

- СООБРАЖЕНИЯ, СВЯЗАННЫЕ С ЭКСПЛУАТАЦИЕЙ/ОКРУЖЕНИЕМ -

  Некоторые из мер безопасности в базовых наборах основаны на предположении о существовании некоторых факторов эксплуатации/окружения. Там где эти факторы отсутствуют или значительно отклоняются от базовых предположений допустимо адаптировать базовый набор. Некоторые из более общих факторов эксплуатации /окружения включают:

  - *Мобильность*
    Мобильность среды физического размещения может оказывать воздействие на меры безопасности, выбираемые для информационных систем организации. Как отмечено выше, набор мер безопасности, включенных в каждый базовый набор в Приложении D, предполагает эксплуатацию информационных систем в установленных средствах и немобильных расположениях. Если информационные системы работают прежде всего в мобильных средах, базовый набор мер безопасности должен быть соответственно адаптирован, чтобы учесть различия в мобильности и доступности конкретных мест, где системы находятся. Например, многие из мер безопасности в семейство Физическая защита и защита среды (PE), которые имеются во всех трёх базовых наборах, отражает предположение, что информационные системы находятся в физических сооружениях/комплексах, которые требуют соответствующей физической защиты. Такие меры безопасности, вероятно, не обеспечили бы достаточную защиту для мобильных сред, таких как корабли, самолеты, автомобили, фургоны или системы космического базирования.[72]

  - *Однопользовательские системы и режимы*
    Для информационных систем, которые разработаны, чтобы работать как однопользовательские системы (например, смартфоны), некоторые из мер безопасности, которые определяют общее использование рядом пользователей, могут не быть необходимы. Однопользовательская система или устройство относятся к системам/устройствам, которые предназначены только для того, чтобы использоваться единственным человеком в течение долгого времени (т.е., монопольное использование). Системы или устройства, которые используются совместно несколькими пользователями в течение долгого времени, не считаются однопользовательскими. Меры безопасности, такие как AC-10, Меры безопасности параллельных сеансов, SC-4, Информация в общих ресурсах и AC-3, Обеспечение доступа[73] могут быть не требованы в однопользовательских системах/режимах и могут быть разумно адаптированы в базовом наборе на усмотрение организаций.

  - *Передача данных и пропускная способность*
    Несмотря на то, что многие информационные системы взаимосвязаны, есть некоторые системы, в которых в силу безопасности или эксплуатационных причин отсутствуют сетевые возможности - то есть, системы с воздушным зазором от сети. Для несетевых систем меры безопасности, такие как AC-17, Удаленный доступ, SC-8, Конфиденциальность и целостность передачи и SC-7, Защита границ, не применимы и могут быть адаптированы из базовых меры безопасности на усмотрение организаций. В дополнение к несетевым информационным системам есть системы, у которых есть очень ограниченная или спорадическая пропускная способность (например, тактические системы, которые поддерживают войска или предназначены для обеспечения правопорядка). Для таких систем приложение мер безопасности должно было бы быть исследовано тщательнее, поскольку ограниченная и/или спорадическая пропускная способность могут иметь воздействие на практичность реализации этих мер безопасности и эффективность противников, организовывающих кибератаки при ограниченной пропускной способности.

[72] Мобильная сущность устройств означает возможность того, что в течение некоторого промежутка времени устройства могут находиться в фиксированных сооружениях или комплексах в фиксированных местах. В течение этого времени должны, вероятно, применяться меры обеспечения PE.
[73] Организации должны рассмотреть, есть ли у отдельных пользователей полномочия администратора прежде, чем удалить A- 3 из базовых мер безопасности.

- *Ограниченная функциональность систем или системных компонентов*
  То, что составляет информационную систему, согласно закону об Электронном правительстве 2002, довольно широко. Факсы, принтеры, сканеры, пейджеры, смартфоны, планшеты, электронные книги и цифровые фотоаппараты могут быть все категорированы как информационные системы (или системные компоненты). Эти типы систем и компонентов могут испытать недостаток в основных возможностях, принятые в базовых мерах безопасности. Сущность этих ограничений может лимитировать типы угроз, которые относятся к этим системам и, следовательно, уместность некоторых из мер безопасности. Таким образом, мера безопасности, такая как SI-3, Защита от вредоносного кода (требуемая во всех базовых мерах безопасности) может не быть практичной для информационных систем или компонентов, которые не допускают исполняемый код (например, пейджеры только для текста). Однако, потому что часто нет четкого разграничения между этими типами информационных систем или компонентов (например, смартфоны содержат цифровые возможности телефонов, камер и компьютеров), важно, чтобы приложение мер безопасности к системам или компонентам ограниченной функциональности было сделано обдуманно и всегда принимало во внимание намеченное использование систем, системных возможностей и риск компрометации.

- *Непостоянство информации и систем*
  Часто делается предположение, что пользовательская информация в пределах информационных систем организации является постоянной в течение значительного промежутка времени. Однако, для некоторых приложений и сред эксплуатации (например, тактические системы, промышленные системы управления), постоянство пользовательской информации часто очень ограничено по продолжительности. Для информационных систем обрабатывающих, хранящих или передающих такую непостоянную информацию, некоторые меры безопасности в семействе Планирование на случай непредвиденных ситуаций (CP), такие, как CP-6, Альтернативный объект хранения информации, CP-7, Альтернативный объект обработки информации и CP-9, Резервное копирование информационной системы, могут быть не практичными и могут быть адаптированы на усмотрение организаций. По подобным причинам меры безопасности, такие как MP-66, Очистка носителей информации и SC-28, Защита остаточной информации, являются хорошими кандидатами на удаление посредством адаптации.[74] В дополнение к непостоянству информации, информационные системы/сервисы, могут также быть непостоянными. Это может быть достигнуто при помощи технологий виртуализации, чтобы устанавливать непостоянные инсталляции операционных систем и приложений. В зависимости от продолжительности инсталляций некоторые базовые меры безопасности могут быть не применимыми.

- *Открытый доступ*
  Когда позволен открытый доступ к информационным системам организаций, меры безопасности должны применяться разумно, так как некоторые меры из определенных базовых наборов мер (например, идентификация и аутентификация, меры безопасности персонала) могут быть не применимыми для открытого доступа. Таким образом, в случае широкого публичного доступа к вебсайтам федерального правительства (например, чтобы загружать публично доступную информацию такую, как формы, информация готовности к чрезвычайным ситуациям), такие меры безопасности, как AC-7, Неудачные попытки входа в систему, AC-17, Удаленный доступ, IA-2, Идентификация и аутентификация, IA-4, управление идентификаторами и IA-5, управление аутентификаторами, как правило, не были бы соответствующими для того, чтобы проверять санкционирование доступа или полномочий. Однако многие из этих мер, возможно, были бы необходимы для идентификации и аутентификации персонала организации, который сопровождает и поддерживает информационные системы, обеспечивающие такие вебсайты и сервисы открытого доступа. Точно так же, многие из мер безопасности могут быть требованы для пользователей, получающих доступ к непубличным информационным системам через такие открытые интерфейсы, например, для доступа или изменения персональных данных.

[74] Организации балансируют постоянство информации с чувствительностью информации. Непостоянная информация может, кроме того, потребовать очистки после удаления. Кроме того, организации рассматривают продолжительность информационной чувствительности - некоторая информация может быть постоянноий, но быть чувствительной только на ограниченный срок.

- СООБРАЖЕНИЯ, СВЯЗАННЫЕ С ЦЕЛЯМИ БЕЗОПАСНОСТИ -

  Меры безопасности, которые поддерживают только одну или две из целей безопасности конфиденциальность, целостность или доступность, могут быть понижены до соответствующих мер безопасности в более низком базовом наборе мер(или изменены или исключены, если не определены в более низком базовом наборе мер) только если действие понижения: (i) отражает категорию безопасности FIPS публикации 199 для поддерживаемой цели (ей) безопасности до перехода на уровень воздействия FIPS публикации 200 (то есть, наивысшего значения);[75] (ii) поддержано оценкой риска организации; и (iii) действительно не оказывает негативное влияние на уровень защиты для информации, важной для безопасности, в информационной системе.[76] Например, если информационная система категорирована как система умеренного воздействия, используя концепцию наивысшего значения, потому, что конфиденциальность и/или целостность умеренны, а доступность низка, и есть несколько мер безопасности, которые поддерживают только цель безопасности доступность и они, потенциально, могли бы быть понижены до более низких базовых требований - то есть, это может быть соответствующе, чтобы *не* реализовывать CP-2(1) потому, что изменение меры безопасности поддерживает только доступность и выбрано в умеренном базовом наборе, а не в низком базовом наборе мер. Следующие меры безопасности и улучшения мер безопасности - потенциальные кандидаты на понижение:[77]

  - *Конфиденциальность:* AC-21, MA-3(3), MP-3, MP-4, MP-5, MP-5(4), MP-6(1), MP-6(2), PE-4, PE 5, SC-4, SC-8, SC-8(1);

  - *Целостность:* УК-5, УК-5(1), УК-5(3), SC-8, SC-8(1), SI-7, SI-7(1), SI-7(5), SI-10; и

  - *Доступность:* CP-2(1), CP-2(2), CP-2(3), CP-2(4), CP-2(5), CP-2(8), CP-3(1), CP-4(1), CP-4(2), CP-6, CP-6(1), CP-6(2), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-7(4), CP-8, CP-8(1), CP-8(2), CP-8(3), CP-8(4), CP-9(1), CP-9(2), CP-9(3), CP-9(5), CP-10(2), CP-10(4), MA-6, PE-9, PE-10, PE-11, PE-11(1), PE-13(1), PE-13(2), PE-13(3), PE-15(1).

- СООБРАЖЕНИЯ, СВЯЗАННЫЕ С ТЕХНОЛОГИЕЙ -

  Меры безопасности, которые обращаются к конкретным технологиям (например, беспроводная связь, криптография, инфраструктура публичных ключей) применимы, только если эти технологии использованы или обязаны быть использованы в информационных системах организаций. Меры безопасности, которые могут быть явно или неявно поддержаны автоматизированными механизмами, не требуют разработки таких механизмов, если механизмы ещё не существуют или легко не доступны в коммерческих или правительственных стандартных продуктах. Если автоматизированные механизмы легко не доступны, не рентабельны или технически не выполнимы, используются компенсирующие меры безопасности, реализуемые через неавтоматизированные механизмы или процедуры, чтобы удовлетворить

[75] Когда применяется наивысшее значение в Разделе 3.1, часть исходных целей безопасности - конфиденциальность, целостность или доступность из FIPS публикации 199, возможно, может быть обновлена до более высокого базового набора мер безопасности. Как часть этого процесса, меры безопасности, которые уникально поддерживают цели безопасности конфиденциальность, целостность или доступность, возможно, были обновлены излишне. Следовательно, рекомендуется, чтобы организации рассматривали соответствующие и допустимые действия понижения, чтобы гарантировать рентабельное, основанное на риске использование мер безопасности.

[76] Информацию, которая важна для безопасности на уровне информационной системы (например, файлы пароля, таблицы сетевой маршрутизации, информация управления криптографическими ключами), надо отличать от пользовательской информации в той же самой системе. Некоторые меры безопасности используются, чтобы поддержать цели безопасности конфиденциальность и целостность и для информации на уровне системы и на уровне пользователя. Следует действовать с осторожностью при понижении мер безопасности связанных с конфиденциальностью или целостностью, чтобы гарантировать, что действия понижения не дают результат в недостаточной защите информации, важной для безопасности в информационной системе. Информация, важная для безопасности, должна быть защищена в наивысшем значении, чтобы достигнуть подобного уровня защиты для любой из целей безопасности, связанной с информацией на уровне пользователя.

[77] Действия понижения применяются только к умеренным и высоким базовым наборам мер. Меры безопасности, которые являются уникальными по отношению к конфиденциальности, целостности или доступности, которые обычно рассматривали бы как потенциальные кандидаты на понижение (например, AC 16, AU 10, IA-7, PE 12, PE 14, SC-5, SC-13, SC-16) устранены из рассмотрения, потому что меры безопасности или выбраны для использования во всех базовых наборах и не имеют улучшений, которые могли бы быть понижены, или меры безопасности являются дополнительными, и не выбраны для использования в каком либо базовом наборе. Организации должны действовать с осторожностью, понижая меры безопасности, которые не находятся в списке в Разделе 3.2, чтобы гарантировать, что действия понижения действительно нет влияют на цели безопасности кроме целей, предназначенных для понижения.

определенные меры безопасности или улучшения мер безопасности (см. положения и условия по применению компенсирующих мер безопасности ниже).

- СООБРАЖЕНИЯ, СВЯЗАННЫЕ С ТРЕБОВАНИЯМИ ПРЕДНАЗНАЧЕНИЯ -

  Некоторые меры безопасности могут быть не применимыми (или не соответствующими), если при реализации этих мер безопасности есть возможность ухудшить, ослабить или иначе препятствовать критическим функциям предназначения и/или деятельности организаций. Например, если предназначение требует, чтобы для решения ответственных задач в консоли оператора был непрерывно доступен показ информации (например, консоли авиадиспетчера), реализация AC-11, Блокировка сеанса или SC-10, Сетевое разъединение, может быть не соответствующей.

Выбор компенсирующих мер безопасности

Организации могут счесть необходимым иногда использовать компенсирующие меры безопасности. Компенсирующие меры безопасности - альтернативные меры, используемые организациями вместо соответствующих мер безопасности в низком, умеренном или высоком базовых уровнях, описанных в Приложения D - меры безопасности которые обеспечивают эквивалентную или сопоставимую защиту для информационных систем организации и информации, обрабатываемой, хранимой или передаваемой этими системами.[78] Это может произойти, например, когда организации не способны эффективно реализовать конкретные базовые меры безопасности или когда, вследствие специфического характера информационных систем или сред эксплуатации, меры в базовых наборах не являются рентабельным средством получения необходимого снижения риска. Компенсирующие меры безопасности, как правило, выбираются после применения объектовых особенностей в руководстве адаптации к применимому базовуму набору мер безопасности. Компенсирующие меры безопасности могут быть использованы организациями при следующих условиях:

- Организации выбирают компенсирующие меры безопасности из Приложения F; если соответствующие компенсирующие меры безопасности не доступны, организации принимают подходящие компенсирующие меры безопасности из других источников;[79]
- Организации представляют поддерживающее обоснование того, что компенсирующие меры безопасности обеспечивают эквивалентные возможности безопасности для информационных систем организаций и почему меры базового уровня безопасности не могут быть использованы; и
- Организации оценивают и принимают риск, связанный с реализацией компенсирующих мер безопасности в информационных системах организаций.

Назначение значений параметрам мер безопасности

Меры безопасности и улучшения мер, содержащие встроенные параметры (то есть, операторы назначения и выбора), дают организациям гибкость по определению некоторой части мер безопасности и улучшений мер для поддержки конкретных требований организаций. После начального приложения объектовых особенностей и выбора компенсирующих мер безопасности, организации рассматривают операции назначения/выбора для мер безопасности и улучшений мер и устанавливают соответствующие определенные организацией значения для идентифицированных параметров. Значения параметров могут быть предписаны применимыми федеральными законами, Правительственными распоряжениями, директивами, нормативных актами, политиками или стандартами. Как только организации определяют значения параметров для мер

[78] Может требоваться более чем одна компенсирующая мера безопасности, чтобы обеспечивать эквивалентную защиту для определенной меры безопасности в Приложении F. Например, организации с существенными ограничениями персонала могут компенсировать меры безопасности раздельного режима работы, усиливая аудит, подконтрольность и меры безопасности персонала.

[79] Организации должны всегда предпринять попытку выбрать компенсирующие меры безопасности из каталога мер безопасности в Приложении F. Определенные организацией компенсирующие меры безопасности используются *только тогда*, когда организации решают, что каталог мер безопасности действительно не содержит подходящие компенсирующие мер безопасности.

безопасности и улучшений мер, назначения и выборы становятся частью мер безопасности и улучшений.[80] Организации могут хотеть определять значения для параметров мер безопасности, прежде чем выбрать компенсирующие меры безопасности, так как спецификация параметров завершает определение мер безопасности и может влиять на требования к компенсирующим мерам безопасности. Могут также быть существенные преимущества в сотрудничестве по разработке значений параметров. Для организаций, которые сотрудничают на частой основе, может быть полезно, разработать для этих организаций взаимно удовлетворяющий набор универсальных значений для параметров мер безопасности. Выполнение этого может помочь организациям в достижении большей степени взаимности, когда есть зависимость от информационных систем и/или услуг, предлагаемых другими организациями.

Дополнение базовых мер безопасности

Заключительное определение соответствующего набора мер безопасности, необходимых, чтобы обеспечить адекватную безопасность для информационных систем организаций и сред, в которых работают эти системы, является функцией оценки риска и требуется, чтобы в достаточной степени смягчать риски к деятельности и активам организаций, людям, другим организациям и Нации.[81] Во многих случаях, дополнительные меры безопасности или улучшения мер (сверх мер безопасности и улучшений, содержащихся в базовых наборах в Приложении D) будут требоваться, чтобы противодействовать конкретным угрозам и уязвимостям в организациях, процессах предназначения/деятельности и/или информационных системах и удовлетворять требованиям применимых федеральных законов, Правительственных распоряжений, директив, политик, стандартов или нормативных актов.[82] Оценка степени риска в процессе выбора мер безопасности обеспечивает важную информацию в определении потребности и достаточности мер безопасности и улучшений мер в начальных базовых наборах. Организации поощрены максимально использовать Приложение F, чтобы облегчить процесс дополнения начальных базовых наборов дополнительными мерами безопасности и/или улучшениями мер безопасности.[83]

Ситуации, требующие потенциальных дополнений базовых наборов

Организации могут быть поставлены в условия, которые, в зависимости от эксплуатационных, экологических или перспективных угроз, являются основанием для выбора и реализации дополнительных мер безопасности, чтобы достигнуть надлежащей защиты функций предназначения/деятельности организаций и информационных систем, поддерживающих эти предназначения/функции. Примеры условий и дополнительных мер безопасности, которые могли бы требоваться, приведены ниже.

- ПОСТОЯННАЯ РАЗВИВАЮЩАЯСЯ УГРОЗА

  Базовые наборы мер безопасности не предполагают, что текущая среда угрозы является такой, где противники достигли существенной точки опоры и присутствия в организациях и информационных систем организаций - то есть, организации имеют дело с постоянной развивающейся угрозой (APT). Противники продолжают атаковать информационные системы организации и инфраструктуру информационных технологий и успешны в некоторых аспектах таких атак. Чтобы более полно определить постоянную развивающуюся угрозу, можно рассмотреть такие концепции, как защита от инсайдерских угроз (УК-5(4)), неоднородность (SC-29), обман (SC-26 и SC-30), непостоянство (SC-25 и SC-34) и сегментация (SC-7(13)).

[80] Инструкция 1253 CNSS обеспечивает назначение минимальных значений для определяемых организацией переменных, применимых к системам национальной безопасности. Значения параметров могут также быть определены как часть оверлеев, описанных в Разделе 3.4.

[81] Соображения для потенциальных воздействий национального уровня и воздействий но другие организации при категорировании информационных систем организаций получают из ПАТРИОТИЧЕСКОГО АКТА США и Президентских Директив по безопасности отечества.

[82] В предыдущих версиях Специальной публикации 800-53, адаптация относилась только к удалению мер безопасности из базовых наборов, а дополнение относилось только к добавлению мер безопасности к базовым наборам. В этом документе термин адаптация был пересмотрен, чтобы включать и добавление мер безопасности к базовым наборам (то есть, адаптация вверх) и удаление мер безопасности из базовых наборов(то есть, адаптация вниз).

[83] Меры безопасности и улучшения мер безопасности, выбранные, чтобы дополнить базовые наборы, назначаются соответствующим компонентам информационной системы таким же самым способом, как назначения мер безопасности, выполненные организациями в начальных базовых наборах мер.

- МЕЖДОМЕННЫЕ СЕРВИСЫ

  Базовые меры безопасности не предполагают, что информационные системы должны работать через множественные домены безопасности. Базовые наборы предполагают плоское представление информационных потоков (то есть, одна и та же политика безопасности в различных доменах, когда информация проходит через границы санкционирования). В отношении междоменных сервисов и транзакций, можно полагать, что некоторое подмножество улучшений меры безопасности AC-4 гарантирует надлежащую защиту информации, когда она передается между информационными системами с различной политикой безопасности.

- МОБИЛЬНОСТЬ

  Использование мобильных устройств может иметь результат в потребности в дополнительных мерах безопасности и улучшениях мер, нет выбранных в начальных базовых наборах. Например, AC-7(2), которая требует уничтожение/стирания информации после определенного организацией числа неудачных попыток входа в систему, или MP-6(8), которая требует возможности удаленного уничтожения/стирания, могут быть выбранными, чтобы противостоять угрозе воровства или потери мобильных устройств.

- КЛАССИФИЦИРОВАННАЯ ИНФОРМАЦИЯ

  В некоторых средах, классифицированная и чувствительная информация[84] может быть резидентным объектом в системах национальной безопасности, где не все пользователи имеют необходимое санкционирование по доступу ко всей информации. В этих ситуациях дополнительные меры безопасности обязаны гарантировать, что к информации, требующей строгого разделения, не получают доступ неавторизованные пользователи. Более строгие меры доступа включают, например, AC-3(3) и AC-16. Когда классифицированная информация обрабатывается, хранится или передаётся в информационных системах, которые совместно принадлежат многим сущностям (например, партнеры по коалиции в военных союзах), могут требоваться более ограничительные меры безопасности для персонала поддержки, включая, например, MA-5(4).

Процессы для идентификации необходимых дополнительных мер безопасности

Организаций могут использовать подход *определения требований* или подход *гэп-анализа* при выборе мер безопасности и улучшений мер, чтобы дополнить начальные базовые наборы. В подходе определения требований организации имеют конкретную и вероятную информацию (или делают разумные предположения) о работах противников по угрозам[85]с некоторыми возможностями или атакующим потенциалом (например, уровни квалификации, экспертизы, доступные ресурсы). Чтобы эффективно противостоять кибератакам от противников с заявленными возможностями или атакующим потенциалом, организации стремятся достигнуть определенного уровня обороноспособности или кибер подготовленности. Организации могут выбрать дополнительные меры безопасности и улучшения мер из Приложения F, чтобы получить такую обороноспособность или уровень подготовленности. В отличие от подхода определения требований, подход гэп-анализа начинается с оценки организацией своей текущей обороноспособности или уровня кибер подготовленности. Исходя из этой начальной оценки возможностей, организации определяют типы угроз, которым они могут разумно противостоять. Если текущая обороноспособность или уровень кибер подготовленности организации недостаточны, гэп-анализ определяет требуемые возможности и уровни подготовленности. Организации впоследствии определяют меры безопасности и улучшения мер из Приложения F, чтобы достигнуть требуемых возможностей или уровней кибер подготовленности. Оба из подходов, описанных выше, требуют своевременной и точный информация об угрозах. Важно, что организации работают с соответствующим компонентом идентификации угрозы, чтобы получить такую информацию.

[84] Пример является только иллюстрацией. Инструкция 1253 CNSS обеспечивает конкретное руководство относительно мер безопасности, требуемых для систем национальной безопасности.

[85] Хотя этот пример сосредотачивается на угрозах информационным системам от целенаправленных атак, пространство значимых для организаций угроз также включает экологические разрушения и человеческие ошибки.

Во время процесса адаптации организации рассматривают переоценку приоритетных кодов для базовых меры безопасности, чтобы определить, являются ли какие-либо изменения к приоритетным кодам соответствующими. Это особенно важно при добавлении мер безопасности, которые не включены в любой из базовых наборов, потому что у этих мер безопасности есть приоритетные коды P0. Переоценка приоритетных кодов может быть основана на оценках организациями риска или решениях по проектированию/разработке, связанных с архитектурой безопасности или системными процессами и процессом обеспечения безопасности, которые могут потребовать некоторого упорядочивания в реализации мер безопасности.

Улучшение информационной безопасности без изменения выбора мер безопасности

Могут быть ситуации, в которых организации не могут применить достаточные меры безопасности в их информационных системах, чтобы соответственно уменьшить или смягчить риск (например, при использовании определенных типов информационных технологий или использовании некоторых вычислительных парадигм). Поэтому, необходимы альтернативные стратегии, чтобы препятствовать оказанию негативного влияния на функции предназначений/деятельности организаций - стратегии, которые рассматривают риски предназначение и деятельности, следующие из агрессивного использования информационных технологий. Ограничения на типы используемых технологий и на то, как используются информационные системы организаций, обеспечивают альтернативный метод, чтобы уменьшить или смягчить риск, который может быть использован в соединении с или вместо дополнительных мер безопасности. Ограничения на использование информационных систем и конкретных информационных технологий могут быть, в некоторых ситуациях, единственными практическими или разумными действиями, которые организации могут предпринять, чтобы иметь возможность выполнить установленные функции предназначения/деятельности перед лицом определенных противников. Примеры использования ограничений, включают:

- Ограничение информации, которую информационные системы могут обрабатывать, хранить или передавать или способ, которым автоматизируются функции предназначения/деятельности организаций;
- Запрещение внешнего доступа к информации организаций, путем удаления выбранных компонентов информационной системы из сетей (то есть, воздушный зазор); и
- Запрещение умеренно- или высоко-значимой информации в компонентах информационных систем организаций к которым есть публичный доступ, если явное определение риска не сделано, при санкционировании такого доступа.

Предоставление дополнительной конкретной информации для реализации мер безопасности

Так как меры безопасности - описание возможностей безопасности на верхних уровнях абстракции, меры безопасности могут испытывать недостаток в достаточной информации для успешной реализации. Поэтому, могут быть необходимы дополнительные детали, чтобы полностью определить назначение данной меры безопасности для целей реализации и гарантировать, что требования безопасности, связанные с этой мерой безопасности, удовлетворены. Например, дополнительная информация, может быть обеспечена как часть процесса движения от меры безопасности до спецификации требований и может включать *усовершенствование* деталей реализации, *усовершенствование* области или *итерацию*, чтобы применить эту же самую меру безопасности по-другому к различным областям. Организации гарантируют, что если существующая информация по мерам безопасности (например, операторы выбора и назначения) не достаточна, чтобы полностью определить применение по назначению мер безопасности, то такая информация предоставляется. У организаций есть гибкость, чтобы определить, включаются ли дополнительные детали как часть описания мер безопасности в дополнительном руководстве или в отдельном разделе приложения по мерам безопасности. Обеспечивая дополнительные детали, организации предостерегают от изменения назначения мер безопасности или языка оригинала в мере безопасности. Дополнительная информация реализации может быть задокументирована или в планы обеспечения безопасности или в планы системы и техники обеспечения безопасности. Типичные дополнительные детали, которые могут быть необходимы, чтобы полностью определить меры безопасности для назначений реализации, приведены в примере для SI-7(6) ниже:

SI-7 ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ВСТРОЕННОЕ МИКРОПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ

(6) *ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ВСТРОЕННОЕ МИКРОПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ | КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА*

Информационная система реализует криптографические механизмы, чтобы обнаружить несанкционированные изменения в программном обеспечении, встроенном микропрограммном обеспечении и информации.

Дополнительное Руководство: Криптографические механизмы, используемые для защиты целостности, включают, например, цифровые подписи и вычисление и приложение хешей, использование асимметричного шифрования, защиту конфиденциальности ключа, использование генерации хеша и использование открытого ключа, чтобы проверить информацию хеша. Связанная мера безопасности: SC-13.

Дополнительная деталь реализации для SI-7(6):

Цифровые подписи применяются ко всему трафику, для которого требуется неотказуемость, используя SHA 256 или другой одобренный NIST алгоритм имеющий, по крайней мере, ту же самую стойкость механизма.

3.3 СОЗДАНИЕ ОВЕРЛЕЕВ

Предыдущие разделы описали процесс адаптации базовых наборов мер безопасности для достижения более сфокусированных и соответствующих возможностей безопасности для организаций. В некоторых ситуациях для организаций может быть выгодным применить руководство адаптации к базовым наборам мер, чтобы разработать ряд мер для использования всем сообществом или определить специализированные требования, технологии или уникальные назначения/среды эксплуатации.[86] Например, федеральное правительство может решить установить общеправительственный набор мер и руководство реализации для: (i) систем инфраструктуры публичных ключей (PKI), которые могут быть универсально применимы ко всем системам PKI, реализованным в федеральных агентствах; (ii) информационных систем, базирующихся на облаках, которые универсально применимы ко всем федеральным агентствам, обеспечивающим или реализующим "облачные" службы; или (iii) промышленных систем управления (ICSs) в федеральных объектах, производящих электроэнергию или контролирующих экологические системы на федеральных объектах. Альтернативно, чтобы соотнести конкретные сообщества интересов со специализированными требованиями, Министерство обороны, например, может решить установить ряд мер безопасности и руководство реализации для их применения и сред, применяя руководство по адаптации к стандартным базовым наборам мер для систем национальной безопасности, чтобы достигнуть более специализированных решений. В каждом из вышеупомянутых примеров адаптированные базовые наборы мер могут быть разработаны для каждой области информационных технологий или для уникальных обстоятельств/сред и представлены многочисленным сообществам интересов – достигая, таким образом, стандартизированных возможностей безопасности, согласованности реализации и рентабельных решений по обеспечению безопасности.

Для учета потребности в разработке наборов мер безопасности для информационных систем и организаций, предназначенных для сообществ и специализированных, введена концепция *оверлея*. Оверлей - полностью определенный набор мер безопасности, улучшений мер и дополнительное руководство, полученных из приложения руководства адаптации из Раздела 3.2 к базовым наборам мер из Приложения D.[87] Оверлеи дополняют начальные базовые наборы мер безопасности: (i) обеспечивая возможность добавить или устранить меры безопасности; (ii) обеспечивая применимость мер безопасности и интерпретации для конкретных информационных технологий, вычислительных парадигм, сред эксплуатации, типов информационных систем, типов предназначений/деятельности, рабочих режимов, отраслевых секторов и законодательных/нормативных требований; (iii) устанавливая для сообществ значения параметров для операций назначения и/или выбора в мерах безопасности и улучшениях мер; и (iv) расширяя дополнительное руководство для мер безопасности, где необходимо. Организации, как правило, используют концепцию оверлея когда есть расхождение с основными предположениями, использованными при создании начальных базовых наборов мер безопасности (см. Раздел 3.1). Если организации не расходятся с основными предположениями для начальных базовых наборов

[86] Эти типы адаптации могут быть проведены на федеральном уровне или отдельными организациями.

[87] Инструкция 1253 CNSS обеспечивает руководство адаптации и базовые меры безопасности для систем национальной безопасности.

мер, то, вероятно, оверлей не должен создаваться. Альтернативно, базовые наборы могут не содержать ключевые предположения, которые выровнялись бы созданием оверлея с дополнительными предположениями.

Полный спектр работ по адаптации может быть использован организациями, чтобы обеспечить упорядоченный и структурированный подход для разработки адаптированных базовых наборов мер, поддерживающих области, описанные выше. Оверлеи обеспечивают возможность прийти к согласию через сообщества интересов и разработать планы обеспечения безопасности для информационных систем организаций, у которых есть всеобъемлющая поддержка для очень конкретных обстоятельств, ситуаций и/или условий. Категории оверлеев, которые могут быть полезными, включают, например:

- Сообщества интересов, отраслевые сектора или коалиции/партнерства (например, здравоохранение, обеспечение правопорядка, разведка, финансы, транспортировка, энергетика, союзническое сотрудничество/совместное использование);
- Парадигмы информационных технологий/вычислений (например, облака/мобильные устройства, PKI, Умные сети, кросс-доменные решения);
- Среды эксплуатации (например, пространственные, тактические);
- Типы информационных систем и режимов эксплуатации (например, промышленные системы/системы управления процессами, системы оружия, однопользовательские системы, автономные системы);
- Типы предназначений/эксплуатации (например, противодействие терроризму, оперативное реагирование, исследование, разработка, тестирование и оценка); и
- Законодательные/нормативные требования (например, Закон об иностранном разведывательном наблюдении, Закон о переносимости и подконтрольности медицинского страхования, Закон о неприкосновенности частной жизни).

Организации могут эффективно использовать концепции управления рисками, определенные в Специальной публикации NIST 800-39, разрабатывая оверлеи. Успешная разработка оверлеев требует участия: (i) профессионалов информационной безопасности, которые понимают конкретную предметную область, которая является фокусом усилий по разработке оверлея; и (ii) экспертов в предметной области оверлея, которые понимают меры безопасности из Приложения F и начальные базовые наборы мер из Приложения D. Формат и структура для разработки оверлеев представлены в Приложении I.

К одному базовому набору мер безопасности могут быть применены многие оверлеи. Адаптированные базовые наборы мер, которые являются результатом разработки оверлея, могут быть более или менее строгими, чем исходные базовые наборы мер. Оценки риска дают информацию, необходимую чтобы определить, находится ли риск реализации адаптированных базовых наборов в пределах допуска риска организаций или сообществ интересов, разрабатывающих оверлеи. Если используются многие оверлеи, возможен конфликт между ними. Если использование многих оверлеев приводит к конфликтам между приложением или удалением мер безопасности, конфликт может разрешить санкционирующее должностное лицо (или уполномоченный) в координации с владельцем назначения/деятельности и/или владельцем/управляющим информацией. Вообще, оверлеи предназначены, чтобы уменьшить потребность в оперативной адаптации организациями базовых наборов мер посредством выбора ряда мер и улучшений мер, которые более близко соответствуют общим обстоятельствам, ситуациям и/или условиям. Однако использование оверлеев не устраняет организации от выполнения дальнейшей адаптации, чтобы отразить специфичные для организации потребности, предположения или ограничения. Адаптация оверлеев выполняется в пределах ограничений, определенных в оверлее, и может требовать согласия/утверждения санкционирующих лиц или других определяемых организацией лиц. Например, оверлей, создаваемый для промышленной системы управления(ICS), может потребовать адаптации для применения к определенному типу ICS и её среды эксплуатации. Но ожидается, что применение оверлеев значительно сократило бы количество и степень специфичной для организаций оперативной адаптации.

3.4 ДОКУМЕНТИРОВАНИЕ ПРОЦЕССА ВЫБОРА МЕР БЕЗОПАСНОСТИ

Организации документируют соответствующие решения, принятые в процессе выбора мер безопасности, давая разумное обоснование этих решений. Эта документация важна, когда исследуются соображения безопасности для информационных систем организаций относительно потенциального влияния на их назначение/деятельность. Результирующий набор мер и поддерживающее обоснование для выбранных решений (включая любые используемые ограничения для информационных систем, требуемые организациями) документируются в планы обеспечения безопасности. Документирование существенных решений управления рисками в процессе выбора мер безопасности обязательно делать так, чтобы у санкционирующих должностных лиц мог быть доступ к необходимой информации, чтобы сделать осмысленные решения по санкционированию для информационных систем организации.[88] Без такой информации, понимание, предположений, ограничений и обоснования, поддерживающего эти решения управления рисками, по всей вероятности не будет доступно, когда состояние информационных систем или среды эксплуатации изменится, и исходные решения риска будут пересматриваться. Рисунок 4 суммирует процесс выбора мер безопасности, включая выбор начального базового набора мер безопасности и адаптацию базового набора, применяя руководство в Разделе 3.2.

РИСУНОК 4: ПРОЦЕСС ВЫБОРА МЕР БЕЗОПАСНОСТИ

Итеративный и динамический характер адаптации мер безопасности

У процесса адаптации мер безопасности, описанного выше, являющегося последовательным по сути, может также быть итеративный аспект. Организации могут хотеть выполнять шаги адаптации в любом порядке, основанном на потребностях организации и информации, полученной от оценок степени риска. Например, некоторые организации могут установить значения параметров для мер безопасности в начальных базовых наборах мер до выбора компенсирующих мер безопасности. Другие организации могут задержать завершение операций назначения и выбора в мерах безопасности, пока работы дополнения не будут завершены. Организации могут также обнаружить, что, когда полностью определены меры безопасности для намеченных сред эксплуатации, там могут возникнуть трудности, которые могут инициировать потребность в дополнительных (расширенных) мерах безопасности. Наконец, процесс адаптации мер безопасности не статичен - то есть, организации пересматривают шаг адаптации так часто как необходимо, основываясь на продолжающихся оценках риска организации.

[88] Процесс выбора мер безопасности также применяется к поставщикам общих мер безопасности и санкционирующим должностным лицам, представляющим решения по санкционированию для общих мер безопасности, развернутых в пределах организаций.

В дополнение к итеративному и динамическому характеру процесса адаптации мер безопасности, могут также быть побочные эффекты, поскольку меры добавляются и удаляются из базовых наборов. У мер безопасности в Приложении F может быть определенная степень зависимости и функционального перекрытия с другими мерами безопасности. Во многих случаях, меры безопасности сотрудничают, чтобы достичь возможности безопасности. Таким образом, у удаления определенной меры безопасности из базового набора во время процесса адаптации могут быть непредвиденные побочные эффекты (и потенциально неблагоприятные воздействия) на остающиеся мерах безопасности. Альтернативно, добавление новой меры безопасности к базовому набору во время процесса адаптации может устранить или уменьшить потребность в некоторых конкретных мерах, потому что новая мера обеспечивает лучшие возможности безопасности, чем возможности, обеспеченные другими мерами безопасности. Например, если организации реализуют SC-30(2), используя технологии виртуализации, чтобы произвольно/часто развертывать различные и изменяющиеся операционные системы и приложения, этот подход мог бы потенциально ограничить требование, чтобы обновлять конфигурации безопасности в CM-2(2). Поэтому, дополнение или удаление мер безопасности рассматриваются относительно всего объема потребностей информационной безопасности организации и её информационных систем, а не просто относительно добавляемых или удаленных мер безопасности.

Совет по реализации

Отклоняясь от базовых наборов мер безопасности во время процесса адаптации, организации рассматривают некоторые очень важные взаимосвязи между различными мерами безопасности и контролируют улучшения. Эти взаимосвязи зафиксированы в выборе мер безопасности и улучшений мер в базовых наборах и особенно существенны когда разрабатываются оверлеи (описанные в Разделе 3.3 и Приложении I). В некоторых случаях, взаимосвязи таковы, что это не значимо, чтобы включать меру безопасности или улучшение меры без некоторой другой меры или улучшения. Всё количество мер безопасности и улучшений обеспечивает требуемые *возможности безопасности*. Некоторые взаимосвязи очевидны, такие как взаимосвязь между улучшением Мандатного управления доступом (AC-3(3)) и Атрибутами безопасности (AC-16). Но другие взаимосвязи могут быть более тонкими. Это особенно видно в случае, где есть взаимосвязи между мерами, связанными с функциональностью безопасности и мерами, связанными с доверием к безопасности, как описано в Приложении E. Например, это не особенно значимо, чтобы реализовать AC-3(3), не реализуя также Монитор обращений (AC-25). Организациям предлагается обратить особое внимание на раздел *взаимосвязанных мер Дополнительного руководства* для мер безопасности, чтобы помочь в идентификации таких взаимосвязей.

Другие рассмотрения

Решения организаций по адаптации выполняются не в вакууме. В то время как такие решения справедливо фокусируются на рассмотрениях информационной безопасности, важно, чтобы решения были выровнены с другими факторами риска, которые организации обычно учитывают. Такие факторы риска, как стоимость, календарный план и исполнение рассматривают при определении в целом, какие меры безопасности использовать в информационных системах организации и средах эксплуатации. Например, в военных системах управления и контроля, в которых имеется угроза жизни, принятие мер безопасности балансируется с потребностью применения. Относительно системы авиадиспетчерской службы и консолей, используемых воздушными диспетчерами, потребность доступа к консоли в режиме реального времени, чтобы контролировать воздушное пространство, перевешивает потребность безопасности в AC-11, Блокировка сеанса. Короче говоря, процесс выбора мер безопасности (включая работы адаптации, описанные в Разделе 3.2), должен быть интегрирован в полный процесс управления рисками, как описано в Специальной публикации NIST 800-39.

Окончательно, организационный фактор распространяется на процесс выбора мер безопасности - то есть, меры безопасности масштабируемы относительно степени/строгости реализации. Расширяемость регламентируется категорированием безопасности в соответствии с FIPS Публикацией 199 и связанными уровнями воздействия на информационные системы из FIPS публикации 200, в зависимости от того, где меры безопасности должны применяться. Например, планы действий при непредвиденных обстоятельствах для информационных систем высокого уровня воздействия могут содержать существенное количество деталей реализации и быть довольно объемными. Напротив, планы действий при непредвиденных обстоятельствах

для систем низкого уровня воздействия могут содержать значительно меньше детали и быть довольно сжатыми. Организации используют осмотрительность в применении мер безопасности к информационным системам организаций, рассматривая факторы расширяемости в определенных эксплуатационных средах. Масштабирование мер безопасности для соответствующего системного уровня воздействия облегчает более рентабельный, основанный на риске подход к реализации мер безопасности - расходование только такого уровня ресурсов, который необходим, чтобы достигнуть достаточного снижения риска и адекватной безопасности.

Совет по реализации

Поддержка фиксации выбора мер безопасности и статуса мер безопасности может осуществляться в одном или нескольких документах или планах обеспечения безопасности. Используя многие документы, рассмотрите предоставление ссылок на необходимую информацию в соответствующих документах вместо того, чтобы требовать дублирования информации. Использование ссылок на соответствующее документирование уменьшает количество времени и ресурсов, необходимых организациям, чтобы генерировать такую информацию. Другие преимущества включают лучшее освоение безопасности и понимание возможностей информационной системы. Лучшее освоение/понимание безопасности поддерживает более эффективную интеграцию информационной безопасности в информационные системы организации.

3.5 НОВЫЕ РАЗРАБОТКИ И УНАСЛЕДОВАНИЕ СИСТЕМ

Процесс выбора мер безопасности, описанный в этом разделе, может быть применен к информационным системам организации с двух других точек зрения: (i) новые разработки; и (ii) наследование. Для систем новой разработки процесс выбора мер безопасности применяется с точки зрения *определения требований*, так как системы еще не существуют, и организации проводят начальное категорирование безопасности. Меры безопасности, включенные в планы обеспечения безопасности для информационных систем, служат спецификацией безопасности и, как ожидается, будут включены в системы во время фаз разработки и реализации жизненного цикла разработки систем. Напротив, для наследуемых информационных систем процесс выбора мер безопасности применяется с точки зрения *гэп-анализа*, когда организации ожидают существенные изменения в системах (например, во время главных обновлений, модификаций или аутсорсинга). Так как информационные системы уже существуют, организации, по всей вероятности, завершили процессы категорирования безопасности и выбора мер безопасности, заканчивающиеся включением ранее согласованных мер безопасности в соответствующие планы обеспечения безопасности и реализацией этих мер в информационных системах. Поэтому, гэп-анализ может быть применен следующим образом:

- Во-первых, *подтвердите* или *обновите* при необходимости, категорию безопасности и уровень воздействия для информационной системы, основанные на типах информации, которые в настоящий момент обрабатываются, хранятся или передаются системой.
- Во вторых, *проанализируйте* существующий план обеспечения безопасности, который описывает меры безопасности, которые в настоящий момент использованы, принимая во внимание любые обновления к категории безопасности и уровню воздействия информационной системы, а так же любым изменениям к организации, процессам назначения/деятельности, системе или эксплуатационной среде. Переоцените риск и пересмотрите план обеспечения безопасности по мере необходимости, включая документирование любых дополнительных мер безопасности, которые были бы необходимы системе, чтобы гарантировать, что риск для деятельности организации, активам организации, людям, другим организациям и Нации остается на допустимом уровне.
- В-третьих, *реализуйте* меры безопасности, описанные в обновленном плане обеспечения безопасности, задокументируйте в плане действий и вехах любые не реализованные меры безопасности и продолжайте остающиеся шаги Основ управления рисками таким же самым образом, как с системой новой разработки.

Применение гэп-анализа к внешним поставщикам услуг

Гэп-анализ также перспективен в применении, когда имеется взаимодействие с внешними поставщиками услуг. Как описано в Разделе 2.5, организации становятся все более и более уверенными во внешних поставщиках для сервисов информационной системы. Используя шаги в гэп-анализе, описанном выше, организации могут эффективно использовать процесс приобретения и соответствующие договорные механизмы, чтобы требовать от внешних поставщиков выполнения категорирования безопасности и шагов выбора мер безопасности в RMF. Результирующая информация может помочь определить, какие меры безопасности внешний поставщик или уже имеет или намеревается реализовать для услуг информационной системы, которые должны быть предоставлены. Если существует дефицит мер безопасности, ответственность за адекватное смягчение недопустимых рисков, являющихся результатом использования внешних сервисов информационной системы, остается за санкционирующими должностными лицами. В таких ситуациях организации могут уменьшить риск организации до допустимого уровня:

- Используя существующий договорный механизм, чтобы потребовать от внешнего поставщика удовлетворения дополнительных требований к мерам безопасности, установленных организацией;
- Согласуя с поставщиком дополнительные меры безопасности, если существующий договорный механизм не предусматривает такие дополнительные требования;
- Одобряя использование поставщиком компенсирующих мер безопасности; или
- Используя в информационной системе организации альтернативные действия по снижению риска,[89] когда контракт или не существует или контракт не предоставляет организациям необходимые рычаги, чтобы получить требуемые меры безопасности.

Совет по реализации

Много организаций управляют и сопровождают комплексные информационные системы, часто называемые системой систем. Архитектура предприятия играет ключевую роль в процессе выбора мер безопасности для этих типов информационных систем. Организации могут решать проблему комплексной системы, деля систему на две или больше подсистемы и применяя категорирование безопасности по FIPS 199 и определение уровня воздействия по FIPS 200 к каждой подсистеме. Применение отдельных уровней воздействия к каждой подсистеме не изменяет полный уровень воздействия информационной системы; скорее это позволяет составляющим подсистемам получать отдельное выделение мер безопасности вместо того, чтобы развертывать меры безопасности для более высокого воздействия в каждой подсистеме. Не допустимо рассматривать подсистемы как полностью независимые сущности, так как подсистемы являются взаимозависимыми и соединенными.

Организации разрабатывают архитектуры безопасности, чтобы выделить меры безопасности между подсистемами, включая мониторинг и контроль коммуникаций на ключевых внутренних границах в системе и обеспечение общесистемных мер безопасности, которые обеспечивают или превышают самый высокий уровень воздействия на информационную систему, для составляющих подсистем, наследующих возможности этих мер безопасности. Организации также полагают, что тиражированные подсистемы в сложных системах могут иметь общие уязвимости, которые могут быть использованы общими источниками угроз - таким образом, инвертирующими избыточность, на которую можно было бы положиться как меру по снижению риска. Воздействие, являющееся следствием инцидента безопасности в отношение одной составляющей подсистемы, может иметь лавинный процесс и воздействовать на много подсистем одновременно.

[89] Например, локальные политики, процедуры и/или компенсирующие меры безопасности могут быть установлены организациями, чтобы служить альтернативными действиями по снижению рисков, идентифицированных в гэп-анализе.

ПРИЛОЖЕНИЕ А

ССЫЛКИ

ЗАКОНЫ, ПОЛИТИКИ, ДИРЕКТИВЫ, НОРМАТИВНЫЕ АКТЫ, МЕМОРАНДУМЫ, СТАНДАРТЫ И РУКОВОДСТВА

ЗАКОНОДАТЕЛЬСТВО И ПРАВИТЕЛЬСТВЕННЫЕ РАСПОРЯЖЕНИЯ

1. Закон об электронном правительстве [включает FISMA] (P.L. 107-347), декабрь 2002.
2. Закон об управлении безопасностью федеральной информации (P.L. 107-347, Заголовок III), декабрь 2002.
3. Закон о сокращении документов (P.L. 104-13), май 1995.
4. ПАТРИОТИЧЕСКИЙ АКТ США (P.L. 107-56), октябрь 2001.
5. Закон о неприкосновенности частной жизни (приватности)1974 (P.L. 93-579), декабрь 1974.
6. Закон о свободе информации (FOIA), 5 U.S.C. § 552, с уточнениями закона №. 104-231, 110 Stat. 3048, Электронные поправки к Закону о свободе информации 1996.
7. Закон о переносимости и подконтрольности медицинского страхования и (P.L. 104-191), август 1996.
8. Закон об Атомной энергии 1954 (P.L. 83-703), август 1954.
9. Правительственное распоряжение 13556, Контролируемая неклассифицированная информация, ноябрь 2010.
10. Правительственное распоряжение 13587, Структурные реформы, чтобы улучшить безопасность классифицированных сетей и ответственное совместное использование и сохранность классифицированных данных, октябрь 2011.

ПОЛИТИКИ, ДИРЕКТИВЫ, ИНСТРУКЦИИ, НОРМАТИВНЫЕ АКТЫ И МЕМОРАНДУМЫ

1. Президентский меморандум, Национальная политика по инсайдерским угрозам а и минимальные стандарты для программ исполнительной власти по инсайдерским угрозам, ноябрь 2012.
2. Свод федеральных нормативных актов, Заголовок 5, *Административный персонал*, Раздел 731.106, *Обозначение публичных защищенных должностей и следственных требований* (5 C.F.R. 731.106).
3. Свод федеральных нормативных актов, Часть 5 Административный персонал, Подраздел C - Сотрудники, ответственные за управление или использование федеральных компьютерных систем, Раздел 930.301 до 930.305 (5 C.F.R. 930.301-305).
4. Комитет по политике систем национальной безопасности (CNSSP) № 11, *Национальная политика, регулирующая приобретение информационно-доверенных (IA) и связанных с IA продуктов информационных технологий (ИТ)*, июль 2003.
5. Комитет по политике систем национальной безопасности (CNSSP) № 12, *Национальная политика информационного доверия для космических систем, используемых для поддержки задач национальной безопасности,* март 2007.
6. Комитет по системам национальной безопасности (CNSS) Инструкция 4009, *Национальный глоссарий информационного доверия*, апрель 2010.
7. Комитет по системам национальной безопасности (CNSS) Инструкция 1253, Версия 2, *Категорирование безопасности и выбор мер безопасности для систем национальной безопасности*, март 2012.
8. Директивы комитета по системам национальной безопасности (CNSSD) № 504, *Директива по защите систем национальной безопасности от инсайдерских угроз*, январь 2012.
9. Департамент безопасности отечества, *Национальный план защиты инфраструктуры (NIPP)*, 2009.

10. Директива разведывательного ведомства (ICD) 705, *Чувствительные изолированные информационные фонды*, май 2010.

11. Федеральная директива по непрерывности деятельности 1 (FCD 1), *Национальная программа и требования по непрерывности деятельности исполнительной власти, февраль 2008.*

12. Исполнительное управление президента Соединенных Штатов и федеральный CIO Совет, *Путеводитель и руководство реализации по федеральным идентификационным данным, учетным данным и управлению доступом (FICAM)*, декабрь 2011.

13. Президентская директива по безопасности отечества 7, *Идентификация критической инфраструктуры, назначение приоритетов и защита*, декабрь 2003.

14. Президентская директива по безопасности отечества 12, *Политика по общему стандарту идентификации для федеральных сотрудников и подрядчиков*, август 2004.

15. Президентская директива по безопасности отечества 20 (Президентская директива по национальной безопасности 51), *Национальная политика непрерывности деятельности*, май 2007.

16. Директива разведывательного ведомства номер 704, *Стандарты обеспечения безопасности персонала и процедуры, регулирующие преемственность относительно доступа к чувствительной изолированной информации и другой информации программы контроля доступа*, октябрь 2008.

17. Директива по национальной коммуникационной системе (NCS) 3-10, *Минимальные требования для непрерывности коммуникационных возможностей*, июль 2007.

18. Инструкция по безопасности телекоммуникационных и информационных систем национальной безопасности (NSTISSI) 7003, *Защищенные распределенные систем (PDS)*, декабрь 1996.

19. Циркуляр Министерства управления и бюджета A-130, Приложение III, Переходящий Меморандум #4, *Управление федеральными информационными ресурсами*, ноябрь 2000.

20. Министерство управления и бюджета, Офис управления программой архитектуры федерального предприятия, *FEA Консолидированный документ эталонной модели*, Версия 2.3, октябрь 2007.

21. Министерство управления и бюджета, *Федеральная методология сегментной архитектуры (FSAM)*, январь 2009.

22. Меморандум 01-05 Министерства управления и бюджета, *Руководство по межведомственному совместному использованию персональных данных - защита неприкосновенность частной жизни*, декабрь 2000.

23. Меморандум 02-01 Министерства управления и бюджета, *Руководство по подготовке и представлению планов действий и вех по обеспечению безопасности*, октябрь 2001.

24. Меморандум 03-19 Министерства управления и бюджета, *Инструкция по отчетности для закона об управлении безопасностью федеральной информации и обновленное руководство по ежеквартальному созданию отчетов по безопасности IT-систем*, август 2003.

25. Меморандум 03-22 Министерства управления и бюджета, *Руководство OMB по реализации положений по приватности закона об электронном правительстве 2002,* сентябрь 2003.

26. Меморандум 04-04 Министерства управления и бюджета, *Руководство электронной аутентификации для федеральных агентств*, декабрь 2003.

27. Меморандум 04-26 Министерства управления и бюджета, Политики персонального использования и технология совместного использования файлов, сентябрь 2004.

28. Меморандум 05-08 Министерства управления и бюджета, *Обозначение высших должностных лиц агентства для приватности,* февраль 2005.

29. Меморандум 05-24 Министерства управления и бюджета, *Реализация Президентской директивы по безопасности отечества (HSPD), 12 - Политика по общему стандарту идентификации для федеральных сотрудников и подрядчиков*, август 2005.

30. Меморандум 06-15 Министерства управления и бюджета, *Сохранность персональной идентификационной информации*, май 2006.

31. Меморандум 06-16 Министерства управления и бюджета, *Защита чувствительной информации*, июнь 2006.

32. Меморандум 06-19 Министерства управления и бюджета, *Отчетность об инцидентах, затрагивающих личные данные, и учет стоимости безопасности в инвестициях агентства в информационные технологии,* июль 2006.

33. Меморандум Министерства управления и бюджета, *Рекомендации по руководству по уведомлению о хищениях идентификационных данных связанных с утечкой данных*, сентябрь 2006.

34. Меморандум 07-11 Министерства управления и бюджета, *Реализация принимаемых по-умолчанию конфигураций безопасности для операционных систем Windows*, март 2007.

35. Меморандум 07-16 Министерства управления и бюджета, *Предохранение от и ответственность за нарушение персональной идентификационной информации*, май 2007.

36. Меморандум 07-18 Министерства управления и бюджета, *Обеспечение новых приобретений, включающих конфигурации общей безопасности*, июнь 2007.

37. Меморандум 08-22 Министерства управления и бюджета, *Руководство по федеральной базовой конфигурации десктопов (FDCC)*, август 2008.

38. Меморандум 08-23 Министерства управления и бюджета, *Обеспечение безопасности инфраструктуры системы доменных имен Федерального правительства*, август 2008.

39. Белый дом, Офис Пресс-секретаря, *Обозначение и совместное использование контролируемой неклассифицированной информации (CUI)*, май 2008.

40. Белый дом, Офис Пресс-секретаря, *Классифицированная информация и контролируемая неклассифицированная информация*, май 2009.

41. Меморандум 11-11 Министерства управления и бюджета, *Продолжение реализации Президентской директивы по безопасности отечества (HSPD) 12 - Политика по общему стандарту идентификации для федеральных сотрудников и подрядчиков*, февраль 2011.

42. Меморандум Министерства управления и бюджета, *Требования для принятия вне-выпущенных идентификационных учетных данных*, октябрь 2011.

43. Меморандум 11-33 Министерства управления и бюджета, *Распоряжение FY 2011 об отчетности по закону об управлении безопасностью Федеральной информации и управлению приватностью агентства,* Сентябрь 2011.

СТАНДАРТЫ

1. Международная организация по Стандартизации/Международная электротехническая комиссия 27001:2005, *Технологии безопасности - Системы управления информационной безопасностью - Требования*.

2. Международная организация по Стандартизации/ Международная электротехническая комиссия 15408-1:2009, *Информационная технология – Методы и средства обеспечения безопасности - Критерии оценки безопасности информационных технологий - Часть 1: Введение и общая модель.*

3. Международная организация по Стандартизации/ Международная электротехническая комиссия 15408-1:2009, *Информационная технология – Методы и средства обеспечения безопасности - Критерии оценки безопасности информационных технологий - Часть 2: Функциональные требования безопасности.*

4. Международная организация по Стандартизации/ Международная электротехническая комиссия 15408-1:2009, *Информационная технология – Методы и средства обеспечения безопасности - Критерии оценки безопасности информационных технологий - Часть 3: Требования доверия к безопасности.*

5. Публикация 140-2 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Требования безопасности для Криптографических Модулей*, май 2001.
Публикация 140-3 Федеральных стандартов обработки информации Национального института стандартов и технологий (Проект), *Требования безопасности для Криптографических Модулей*, декабрь 2009.

6. Публикация 180-4 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Стандарт безопасности Хеш (SHS)*, март 2012.

7. Публикация 186-3 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Стандарт цифровой подписи (DSS)*, июнь 2009.

8. Публикация 188 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Стандартная метка безопасности для передачи информации*, сентябрь 1994.

9. Публикация 190 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Руководство по использованию альтернатив передовых аутентификационных технологий*, сентябрь 1994.

10. Публикация 197 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Усовершенствованный стандарт шифрования (AES)*, ноябрь 2001.

11. Публикация 198-1 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Код Хэширования по ключу аутентификации сообщений (HMAC)*, июль 2008.

12. Публикация 199 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Стандарты по категорированию безопасности федеральной информации и информационных систем*, февраль 2004.

13. Публикация 200 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Минимальные требования безопасности для Федеральной информации и информационных систем*, март 2006.

14. Публикация 201-1 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Проверка персональная идентификационных данных (PIV) федеральных сотрудников и подрядчиков*, март 2006.

РУКОВОДСТВА И МЕЖВЕДОМСТВЕННЫЕ ОТЧЕТЫ

1. Национальный институт стандартов и технологий Специальная публикация 800-12, *Введение в компьютерную безопасность: Справочник NIST*, октябрь 1995.

2. Национальный институт стандартов и технологий Специальная публикация 800-13, *Руководства по телекоммуникационной безопасности для сетевого управления телекоммуникациями*, октябрь 1995.

3. Национальный институт стандартов и технологий Специальная публикация 800-14, *Общепринятые принципы и методы для обеспечения безопасности систем информационных технологий*, сентябрь 1996.

4. Национальный институт стандартов и технологий Специальная публикация 800-15, *Минимальная спецификация функциональной совместимости для компонентов PKI (MISPC),* Версия 1, январь 1998.

5. Национальный институт стандартов и технологий Специальная публикация 800-16, *Требования по обучению информационной безопасности: Ролевая и основанная на выполнении модель*, апрель 1998.

6. Национальный институт стандартов и технологий Специальная публикация 800-17, *Система подтверждения соответствия режимов работы (MOVS): Требования и процедуры*, февраль 1998.

7. Национальный институт стандартов и технологий Специальная публикация 800-18, Пересмотр 1, *Руководство по разработке планов обеспечения безопасности для Федеральных информационных систем*, февраль 2006.

8. Национальный институт стандартов и технологий Специальная публикация 800-19, *Безопасность мобильных агентов*, октябрь 1999.

9. Национальный институт стандартов и технологий Специальная публикация 800-20, *Система подтверждения соответствия режимов работы для тройного алгоритма шифрования данных (TMOVS): Требования и процедуры,* октябрь 1999.

10. Национальный институт стандартов и технологий Специальная публикация 800-21-1, *Второй Выпуск, Руководство для реализации криптографии в Федеральном правительстве*, декабрь 2005.

11. Национальный институт стандартов и технологий Специальная публикация 800-22, Пересмотр 1a, *Статистический тестовый набор для генераторов случайных и псевдослучайных чисел криптографических приложений*, апрель 2010.

12. Национальный институт стандартов и технологий Специальная публикация 800-23, *Руководства для федеральных организаций по доверию к безопасности и приобретению/использованию проверенных/оценённых продуктов*, август 2000.

13. Национальный институт стандартов и технологий Специальная публикация 800-24, *Анализ уязвимости PBX: поиск дыр в вашем PBX прежде, чем кто-то еще сделает это,* август 2000.

14. Национальный институт стандартов и технологий Специальная публикация 800-25, *Использование Федеральными агентствами технологии публичных ключей для цифровых подписей и аутентификации,* октябрь 2000.

15. Национальный институт стандартов и технологий Специальная публикация 800-27, Пересмотр A, *Инженерные принципы для безопасности информационных технологий (Основа для достижения безопасности),* июнь 2004.

16. Национальный институт стандартов и технологий Специальная публикация 800-28, Пересмотр 2, *Руководства по активному контенту и мобильному коду*, март 2008.

17. Национальный институт стандартов и технологий Специальная публикация 800-29, *Сравнение требований безопасности для криптографических модулей в FIPS 140-1 и FIPS 140-2*, июнь 2001.

18. Национальный институт стандартов и технологий Специальная публикация 800-30, Пересмотр 1, *Руководство по проведению оценок риска*, сентябрь 2012.

19. Национальный институт стандартов и технологий Специальная публикация 800-32, *Введение в технологию публичных ключей и федеральную инфраструктуру PKI*, февраль 2001.

20. Национальный институт стандартов и технологий Специальная публикация 800-33, *Базовые технические модели для безопасности информационных технологий*, декабрь 2001.

21. Национальный институт стандартов и технологий Специальная публикация 800-34, Пересмотр 1, *Руководство по планированию на случай непредвиденных ситуаций для Федеральных информационных систем*, май 2010.

22. Национальный институт стандартов и технологий Специальная публикация 800-35, *Руководство по сервисам безопасности информационных технологий*, октябрь 2003.

23. Национальный институт стандартов и технологий Специальная публикация 800-36, *Руководство по выбору продуктов информационной безопасности*, октябрь 2003.

24. Национальный институт стандартов и технологий Специальная публикация 800-37, Пересмотр 1, *Руководство по применения основ управления рисками к Федеральным информационным системам: Подход безопасности жизненного цикла*, февраль 2010.

25. Национальный институт стандартов и технологий Специальная публикация 800-38A - Приложение, *Рекомендации по режимам работы блочного шифра: Три разновидности кражи шифрованного текста для режима CBC*, октябрь 2010.

26. Национальный институт стандартов и технологий Специальная публикация 800-38B, *Рекомендации по режимам работы блочного шифра: Режим CMAC для аутентификации*, май 2005.

27. Национальный институт стандартов и технологий Специальная публикация 800-38C, *Рекомендации по режимам работы блочного шифра: Режим CCM для аутентификации и конфиденциальности*, май 2004.

28. Национальный институт стандартов и технологий Специальная публикация 800-38D, *Рекомендации по режимам работы блочного шифра: Режим Galois/Counter (GCM) и GMAC*, ноябрь 2007.

29. Национальный институт стандартов и технологий Специальная публикация 800-38E, *Рекомендации по режимам работы блочного шифра: Режим XTS-AES для конфиденциальности на устройствах хранения информации,* январь 2010.

30. Национальный институт стандартов и технологий Специальная публикация 800-38F, *Рекомендации по режимам работы блочного шифра: Методы ключевого обертывания*, декабрь 2012.

31. Национальный институт стандартов и технологий Специальная публикация 800-39, *Управление риском информационной безопасности: Обзор организаций, предназначения и информационных систем,* март 2011.

32. Национальный институт стандартов и технологий Специальная публикация 800-40, Пересмотр 2, *Создание программы управления патчами и уязвимостями*, ноябрь 2005.

33. Национальный институт стандартов и технологий Специальная публикация 800-41, Пересмотр 1, *Руководства по межсетевым экранам и политике межсетевого экранирования*, сентябрь 2009.

34. Национальный институт стандартов и технологий Специальная публикация 800-43, *Руководство системного Администратора для Системы Windows 2000 Professional*, ноябрь 2002.

35. Национальный институт стандартов и технологий Специальная публикация 800-44, Пересмотр 2, *Руководства по обеспечению безопасности публичных веб серверов*, сентябрь 2007.

36. Национальный институт стандартов и технологий Специальная публикация 800-45, Пересмотр 2, *Руководства по безопасности электронной почты*, февраль 2007.

37. Национальный институт стандартов и технологий Специальная публикация 800-46, Пересмотр 1, *Руководство по корпоративной безопасности удаленной работы и удаленному доступу*, июнь 2009.

38. Национальный институт стандартов и технологий Специальная публикация 800-47, *Руководство по безопасности для взаимодействующих систем информационных технологий*, август 2002.

39. Национальный институт стандартов и технологий Специальная публикация 800-48, Пересмотр 1, *Руководство по обеспечению безопасности наследованных беспроводных сетей IEEE 802.11*, июль 2008.

40. Национальный институт стандартов и технологий Специальная публикация 800-49, *Федеральный S/MIME V3 клиентский профиль*, ноябрь 2002.

41. Национальный институт стандартов и технологий Специальная публикация 800-50, *Построение программы освоения и обучения безопасности информационных технологий*, октябрь 2003.

42. Национальный институт стандартов и технологий Специальная публикация 800-51, Пересмотр 1, *Руководство по использованию схем именования уязвимостей*, февраль 2011.

43. Национальный институт стандартов и технологий Специальная публикация 800-52, пересмотр 1 (проект), *Руководства по выбору, конфигурированию и использованию реализаций безопасности транспортного уровня (TLS)*, сентябрь 2013.

44. Национальный институт стандартов и технологий Специальная публикация 800-53A, Пересмотр 1, *Руководство по оценке мер безопасности в Федеральных информационных системах и организациях: Построение эффективных планов оценки безопасности,* июнь 2010.

45. Национальный институт стандартов и технологий Специальная публикация 800-54, *Безопасность протокола пограничного шлюза*, июль 2007.

46. Национальный институт стандартов и технологий Специальная публикация 800-55, Пересмотр 1, *Руководство по выполнению измерений информационной безопасности*, июль 2008.

47. Национальный институт стандартов и технологий Специальная публикация, 800-56A (Пересмотренная), *Рекомендация для ведомственных парных ключевых систем, использующих дискретную логарифмическую криптографию*, март 2007.

48. Национальный институт стандартов и технологий Специальная публикация 800-57 Пересмотр 3, *Рекомендации по управлению ключами*, июль 2012.

49. Национальный институт стандартов и технологий Специальная публикация 800-58, *Рассмотрения безопасности по Voice Over IP системам*, январь 2005.

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

51. Национальный институт стандартов и технологий Специальная публикация 800-60, Пересмотр 1, *Руководство по отображению типов информации и информационных систем к категориям безопасности*, август 2008.

52. Национальный институт стандартов и технологий Специальная публикация 800-61, Пересмотр 2, *Руководство по обработке инцидентов компьютерной безопасности*, август 2012.

53. Национальный институт стандартов и технологий Специальная публикация 800-63-1, *Руководство ПО электронной аутентификации*, декабрь 2011.

54. Национальный институт стандартов и технологий Специальная публикация 800-64, Пересмотр 2, *Рассмотрения безопасности в жизненном цикле разработки систем*, октябрь 2008.

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

56. Национальный институт стандартов и технологий Специальная публикация 800-66, Пересмотр 1, *Вводное ресурсное руководство по правилам безопасности для реализации закона о переносимости и подконтрольности медицинского страхования (HIPAA),* октябрь 2008.

57. Национальный институт стандартов и технологий Специальная публикация 800-67, Пересмотр 1, *Рекомендации по блочному шифру тройного алгоритма шифрования данных (TDEA)*, январь 2012.

58. Национальный институт стандартов и технологий Специальная публикация 800-68, Пересмотр 1, *Руководство по обеспечению безопасности систем Microsoft Windows XP для ИТ профессионалов: Контрольный список конфигурации безопасности NIST,* октябрь 2008.

59. Национальный институт стандартов и технологий Специальная публикация 800-69, *Руководство по обеспечению безопасности Microsoft Windows XP домашняя редакция: Контрольный список конфигурации безопасности NIST,* сентябрь 2006.

60. Национальный институт стандартов и технологий Специальная публикация 800-70, Пересмотр 2, *Национальная программа контрольных списков для продуктов ИТ - Руководства для пользователей и разработчиков контрольных списков*, февраль 2011.

61. Национальный институт стандартов и технологий Специальная публикация 800-72, *Руководства по судебным экспертизам PDA*, ноябрь 2004.

62. Национальный институт стандартов и технологий Специальная публикация 800-73-3, *Интерфейсы для проверки персональных идентификационных данных*, февраль 2010.

63. Национальный институт стандартов и технологий Специальная публикация 800-76-1, *Спецификация биометрических данных для проверки персональных идентификационных данных*, январь 2007.

64. Национальный институт стандартов и технологий Специальная публикация 800-77, *Руководство по IPsec VPN*, декабрь 2005.

65. Национальный институт стандартов и технологий Специальная публикация 800-78-3, *Криптографические алгоритмы и размеры ключей для проверки персональных идентификационных данных (PIV),* декабрь 2010.

66. Национальный институт стандартов и технологий Специальная публикация 800-79-1, *Руководства по аттестации выпускающих карты проверки персональных идентификационных данных*, июнь 2008.

67. Национальный институт стандартов и технологий Специальная публикация 800-81, *Руководство развертывания безопасной системы доменных имен (DNS)*, Пересмотр 1, апрель 2010.

68. Национальный институт стандартов и технологий Специальная публикация 800-82, Пересмотр 1, *Руководство по безопасности промышленных систем управления (ICS)*, апрель 2013.

69. Национальный институт стандартов и технологий Специальная публикация 800-83, *Руководство по предотвращению и обработке инцидентов с вредоносным программным обеспечением*, ноябрь 2005.

70. Национальный институт стандартов и технологий Специальная публикация 800-84, *Руководство по программам тестирования, обучения и подготовки для ИТ планов и возможностей*, сентябрь 2006.

71. Национальный институт стандартов и технологий Специальная публикация 800-85A-2, *Руководство по тестированию приложений PIV карт и интерфейса промежуточного программного обеспечения (соответствующее SP 800-73-3)*, июль 2010.

72. Национальный институт стандартов и технологий Специальная публикация 800-85B-1, (Проект) *Руководства по тестированию модели данных PIV*, сентябрь 2009.

73. Национальный институт стандартов и технологий Специальная публикация 800-86, *Руководство по интегрированию технологий расследования в реакцию на инциденты*, август 2006.

74. Национальный институт стандартов и технологий Специальная публикация 800-87, Пересмотр 1, *Коды для идентификации федеральных и сотрудничающих с федеральными организаций*, апрель 2008.

75. Национальный институт стандартов и технологий Специальная публикация 800-88, *Руководства по очистке носителей информации*, сентябрь 2006.

76. Национальный институт стандартов и технологий Специальная публикация 800-89, *Рекомендации по получению доверия для приложений цифровой подписи*, ноябрь 2006.

77. Национальный институт стандартов и технологий Специальная публикация 800-90A, *Рекомендации по генерации случайных чисел, используя детерминированные случайные двоичные генераторы*, январь 2012.

78. Национальный институт стандартов и технологий Специальная публикация 800-92, *Руководство по управлению журналом регистрации компьютерной безопасности*, сентябрь 2006.

79. Национальный институт стандартов и технологий Специальная публикация 800-94, *Руководство по системам обнаружения и предотвращения вторжений (IDPS)*, февраль 2007.

80. Национальный институт стандартов и технологий Специальная публикация 800-95, *Руководство по защищенным веб-сервисам*, август 2007.

81. Национальный институт стандартов и технологий Специальная публикация 800-96, *Руководства по функциональной совместимости PIV карт/ридеров*, сентябрь 2006.

82. Национальный институт стандартов и технологий Специальная публикация 800-97, *Создание робастных безопасных сетей: Руководство к IEEE 802.11i*, февраль 2007.

83. Национальный институт стандартов и технологий Специальная публикация 800-98, *Руководства для систем обеспечения безопасности радиочастотной идентификации (RFID)*, апрель 2007.

84. Национальный институт стандартов и технологий Специальная публикация 800-100, *Справочник по информационной безопасности: Руководство для менеджеров*, октябрь 2006.

85. Национальный институт стандартов и технологий Специальная публикация 800-101, *Руководства по судебным экспертизам сотовых телефонов*, май 2007.

86. Национальный институт стандартов и технологий Специальная публикация 800-103 (Проект), *Онтология идентификации учетных данных, Часть I: Основы и формулировки*, октябрь 2006.

87. Национальный институт стандартов и технологий Специальная публикация 800-104, *Система топографии визуальной PIV карты*, июнь 2007.

88. Национальный институт стандартов и технологий Специальная публикация 800-106, *Рандомизированные хешированные цифровые подписи*, февраль 2009.

89. Национальный институт стандартов и технологий Специальная публикация 800-107, *Рекомендация для приложений использующих одобренные хеш алгоритмы*, август 2012

90. Национальный институт стандартов и технологий Специальная публикация 800-108, *Рекомендация по формированию ключей, используя псевдослучайные функции*, октябрь 2009.

91. Национальный институт стандартов и технологий Специальная публикация 800-111, *Руководство по технологиям шифрования данных памяти для устройств конечного пользователя*, ноябрь 2007.

92. Национальный институт стандартов и технологий Специальная публикация 800-113, *Руководство по SSL VPN*, июль 2008.

93. Национальный институт стандартов и технологий Специальная публикация 800-114, *Руководство пользователя по обеспечению безопасности внешних устройств для удаленной работы и удаленного доступа,* ноябрь 2007.

94. Национальный институт стандартов и технологий Специальная публикация 800-115, *Техническое руководство по проверке и оценке информационной безопасности*, сентябрь 2008.

95. Национальный институт стандартов и технологий Специальная публикация 800-116, *Рекомендации по использованию учетных данных PIV в системах управления физическим доступом (PACS)*, ноябрь 2008.

96. Национальный институт стандартов и технологий Специальная публикация 800-117, Пересмотр 1.0, *Руководство по принятию и использованию протокол автоматизации контента безопасности (SCAP)*, июль 2010.

97. Национальный институт стандартов и технологий Специальная публикация 800-118 (Проект), *Руководство по корпоративному управлению паролями*, апрель 2009.

98. Национальный институт стандартов и технологий Специальная публикация 800-121, Пересмотр 1, *Руководство по безопасности Bluetooth*, июнь 2012.

99. Национальный институт стандартов и технологий Специальная публикация 800-122, *Руководство по защите конфиденциальности персональной идентификационной информации (PII)*, апрель 2010.

100. Национальный институт стандартов и технологий Специальная публикация 800-123, *Руководство по безопасности общих серверов*, июль 2008.

101. Национальный институт стандартов и технологий Специальная публикация 800-124, *Руководства по безопасности сотовых телефонов и PDA*, октябрь 2008.

102. Национальный институт стандартов и технологий Специальная публикация 800-125, *Руководство по безопасности технологий полной виртуализации*, январь 2011.

103. Национальный институт стандартов и технологий Специальная публикация 800-126, Пересмотр 2, *Техническая спецификация для протокола автоматизации контента безопасности (SCAP): SCAP Версия 1.2*, сентябрь 2011.

104. Национальный институт стандартов и технологий Специальная публикация 800-127, *Руководство по обеспечению безопасности радиосвязей WiMAX*, сентябрь 2010.

105. Национальный институт стандартов и технологий Специальная публикация 800-128, *Руководство по фокусируемому на безопасность управлению конфигурацией информационных систем*, август 2011.

106. Национальный институт стандартов и технологий Специальная публикация 800-133, *Рекомендация по генерации криптографических ключей*, декабрь 2012.

107. Национальный институт стандартов и технологий Специальная публикация 800-137, *Непрерывный мониторинг информационной безопасности для федеральных информационных систем и организаций,* сентябрь 2011.

108. Национальный институт стандартов и технологий Специальная публикация 800-142, *Практическое комбинаторное тестирование*, октябрь 2010.

109. Национальный институт стандартов и технологий Специальная публикация 800-144, *Руководства по безопасности и приватности в публичных облачных вычислениях*, декабрь 2011.

110. Национальный институт стандартов и технологий Специальная публикация 800-145, *Определение NIST облачных вычислений*, сентябрь 2011.

111. Национальный институт стандартов и технологий Специальная публикация 800-146, *Краткий обзор и рекомендации по облачным вычислениям*, май 2012.

112. Национальный институт стандартов и технологий Специальная публикация 800-147, *Руководства по защите базовой системы ввода-вывода (BIOS)*, апрель 2011.

113. Национальный институт стандартов и технологий Специальная публикация 800-153, *Руководства по обеспечению безопасности беспроводных локальных сетей (WLANs)*, сентябрь 2011.

114. Межведомственный отчет 7622 Национального института стандартов и технологий, *Отвлеченные методы управления рисками системы поставок для Федеральных информационных систем*, октябрь 2012.

ПРИЛОЖЕНИЕ B

ГЛОССАРИЙ

ОБЩИЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Приложение B обеспечивает определения для терминологии безопасности, используемой в Специальной публикации 800-53. Если специально не определено в этом глоссарии, все термины, использованные в этой публикации, непротиворечивы с определениями, содержавшимися в CNSS Инструкции 4009, *Национальном глоссарии информационного доверия*.

Adequate Security Адекватная Безопасность [Циркуляр OMB A-130, Приложение III, уточненный]	Безопасность, соразмерная с риском, следующим из потери, неправильного употребления или несанкционированного доступа к или модификации информации.
Advanced persistent threat Постоянная развивающаяся угроза	Противник, который обладает высоким уровнем компетентности и существенными ресурсами, которые позволяют ему создавать возможности для достижения его целей при использовании множественных векторов атаки (например, кибернетическая, физическая и радиолектронное подавление). Эти цели, как правило, включают формирование и расширение точек опоры в инфраструктуре информационных технологий намеченных организаций с целью экс-фильтрации информации, подрыва или воспрепятствования критическим аспектам предназначения, программ или структуры; или размещение их, чтобы выполнить эти цели в будущем. Постоянная развивающаяся угроза: (i) неоднократно преследует свои цели за длительный период времени; (ii) приспосабливается к усилиям защитников сопротивляться этому; и (iii) определяет, как поддерживать уровень взаимодействия, необходимый для выполнения её целей.
Agency Агентство	См. *Executive Agency.*
All Source Intelligence Все источники разведки [Министерство обороны, Совместная публикация 1-02]	Разведывательные продукты и/или организации и действия, которые включают все источники информации, наиболее часто включая разведку людскими ресурсами, разведку получением снимков, измерительную и сигнатурную разведку, сигнальную разведку и открытые источники данных продукции конечной разведки.
Assessment Оценка	См. *Security Control Assessment*.
Assessor Оценщик	См. *Security Control Assessor.*
Assurance Доверие [CNSSI 4009]	Мера уверенности, что средства защиты, методы, процедуры и архитектура информационной системы точно представляют и осуществляют политику безопасности.
Assurance Case Кейс доверия [Институт программной инженерии, университет Карнеги-Меллона]	Структурированный набор аргументов и состав свидетельств, показывающих, что информационная система удовлетворяет определенным утверждениям относительно заданного качественного показателя.
Audit Log Журнал аудита [CNSSI 4009]	Хронологическая запись действий информационной системы, включая записи доступа в систему и операций, выполнявшихся в установленный период.
Audit Record Запись аудита	Отдельная запись в журнале аудита регистрации, относящаяся к аудитируемому событию.

Audit Reduction Tools Инструменты сжатия аудита [CNSSI 4009]	Препроцессоры, разработанные, чтобы уменьшить объем записей аудита, чтобы облегчить ручной анализ. Перед анализом безопасности эти инструменты могут удалить много записей аудита, которые, как установлено, имеют малое значение для безопасности. Эти инструменты вообще удаляют записи, сгенерированные определенными классами событий такими, как записи, сгенерированные ночными резервными копиями.
Audit Trail След аудита [CNSSI 4009]	Хронологическая запись, которая позволяет восстанавливать и изучать последовательность действий сопутствующих или приводящих к конкретной операции, процедуре или событию в связанной с безопасностью транзакции, от начала до окончательного результата.
Authentication Аутентификация [FIPS 200]	Проверка идентификационных данных пользователя, процесса или устройства, обычно как предпосылка к предоставлению доступа к ресурсам в информационной системе.
Authenticator Аутентификатор	Средства для подтверждения идентификационных данных пользователя, процессора или устройства (например, пользовательский пароль или токен).
Authenticity Аутентичность	Свойство, определяющее подлинность и возможность проверять и доверять; уверенность в законности передачи, сообщения или автора сообщения. См. *Authentication.*
Authorization (to operate) Санкционирование (эксплуатировать)	Официальное управленческое решение, принимаемое высшим должностным лицом организации для того, чтобы разрешить эксплуатацию информационной системы и явно принять риск в отношении деятельности организации (включая предназначение, функции, имидж или репутацию), активов организации, людей, других организаций и Нации, основанное на реализации согласованного набора мер безопасности.
Authorization Boundary Граница санкционирования	Все компоненты информационной системы, которая санкционирована для эксплуатации санкционирующим должностным лицом, исключая отдельно санкционированные системы, с которыми соединена информационная система.
Authorize Processing Санкционирование обработки	См. *Authorization.*
Authorizing Official Санкционирующее должностное лицо	Высшее (федеральное) должностное лицо или руководитель с полномочием по формальному принятию на себя ответственности за эксплуатацию информационной системы на допустимом уровне риска в отношении деятельности организации (включая предназначение, функции, имидж или репутацию), активов организации, людей, других организаций и Нации.
Availability Доступность [44 U.S.C., Sec. 3542]	Обеспечение своевременного и надежного доступа к и использования информации.
Baseline Configuration Базовая Конфигурация	Задокументированный набор спецификаций информационной системы, или элемент конфигурации в системе, который был формально рассмотрен и согласован в данный момент времени и который может быть изменён только через процедуры контроля изменений.

Blacklisting Помещение в черный список	Процесс, используемый для идентификации: (i) программ, которые не уполномочены выполняться в информационной системе; или (ii) запрещенных Универсальных Локаторов Ресурсов (URL) / вебсайтов.
Boundary Protection Защита границ	Мониторинг и контроль коммуникаций на внешней границе информационной системы, чтобы предотвратить и обнаружить злонамеренные и другие несанкционированные соединения с помощью устройств защиты границ (например, шлюзов, маршрутизаторов, межсетевых экранов, сторожей, шифрованных туннелей).
Boundary Protection Device Устройство защиты границ	Устройство с соответствующими механизмами, которое: (i) облегчает рассмотрение политик безопасности различных взаимодействующих систем (например, контролируя поток информации в или из взаимодействующей системы); и/или (ii) обеспечивает защиту границ информационной системы.
Central Management Центральное управление	Управление и реализация выбранных мер безопасности и связанных процессов в целом в организации. Центральное управление включает планирование, реализацию, оценку, санкционирование и мониторинг определенных организацией, центрально управляемых мер и процессов безопасности.
Chief Information Officer Директор по информации [PL 104-106, Раздел 5125 (b)]	Должностное лицо агентства, ответственное за: (i) предоставление консультаций и другой помощи руководителю исполнительного агентства и другому персоналу высшего руководства агентства, чтобы гарантировать, что информационные технологии приобретаются и информационные ресурсы управляются в способе, который непротиворечив с законами, Правительственными распоряжениями, директивами, политиками, нормативными актами и приоритетами, установленными руководителем агентства; (ii) разработку, поддержание и облегчение реализации осмысленной и интегрированной архитектуры информационных технологий для агентства; и (iii) продвижение эффективного и рационального конструирования и использования всех основных информационных ресурсов процессов управления для агентства, включая улучшение процессов работы агентства. Примечание: Организации подчиненные федеральным агентствам могут использовать термин *Директор по информации*, чтобы обозначать людей, замещающих позиции с подобными обязанностями по безопасности как у Директораа по информации на уровне агентства.
Chief Information Security Officer Директор по информационной безопасности	См. *Senior Agency Information Security Officer.*
Chief Privacy Officer Директор по приватности	См. *Senior Agency Official for Privacy*.
Classified Information Классифицированная информация	Информация, которая была определена: (i) в соответствии с Правительственным распоряжением 12958 уточненным Правительственным распоряжением 13526, или любым предшествующим распоряжением, чтобы быть классифицированной информацией национальной безопасности; или (ii) в соответствии с законом об Атомной энергии 1954, с уточнениями, чтобы быть Ограниченными данными (RD).

Commodity Service Товарный сервис	Сервис информационной системы (например, телекоммуникационный сервис) поставляемый поставщиком коммерческих сервисов, как правило, большому и разнообразному набору потребителей. Организации, закупающие и/или получающие товарные сервисы, обладают ограниченной обозримостью структуры управления и эксплуатации поставщика, и хотя организация в состоянии согласовать соглашения об уровне обслуживания, организация, как правило, не имеет возможности требовать, чтобы поставщик реализовал конкретные меры безопасности.
Common Carrier Поставщик общих услуг связи	В телекоммуникационном контексте, телекоммуникационная компания, которая предлагает себя обществу для найма по предоставлению коммуникационных услуг связи. Примечание: В Соединенных Штатах такие компании являются обычно подчиненными регулированию через регулирующие комиссии федеральные и штатов.
Common Control Общая мера безопасности [NIST SP 800-37; CNSSI 4009]	Мера безопасности, которая является наследуемой одной или более информационными системами организации. См. *Security Control Inheritance*.
Common Control Provider Поставщик общих мер безопасности [NIST SP 800-37]	Должностное лицо организации, ответственное за разработку, реализацию, оценку и мониторинг общих мер безопасности (то есть, мер безопасности, наследуемых информационными системами).
Common Criteria Общие Критерии [CNSSI 4009]	Руководящий документ, который обеспечивает всесторонний, строгий метод для того, чтобы определить функциональные требования и требования доверия к безопасности для продуктов и систем.
Common Secure Configuration Общая безопасная конфигурация	Признанный стандартизированный и установленный эталон, который предусматривает конкретные безопасные установки конфигурации для данной платформы информационной технологии.
Compensating Security Controls Компенсирующие меры безопасности [CNSSI 4009, уточненный]	Меры безопасности, используемые вместо рекомендуемых мер в базовых наборах мер безопасности, описанных в Специальной публикации NIST 800-53 и CNSS Инструкции 1253, которые обеспечивают эквивалентную или сопоставимую защиту для информационной системы или организации.
Computer Matching Agreement Соглашение о компьютерном соответствии	Соглашение, заключаемое организацией в соответствии с программой компьютерного соответствия, в котором организация есть сторона, как требуется Законом о компьютерным соответствии и защите приватности 1988. С некоторыми исключениями программа компьютерного соответствия - любое компьютеризированное сравнение двух или более автоматизированных систем записей или системы записей с нефедеральными записями с целью установления или проверки пригодности к, или продолжения соответствия с, установленными законом и нормативными требованиями для, претендентами на, получателями или владельцами, участниками в, или поставщиками услуг относительно наличной или натуральной помощи или платежей в соответствии с программами федерального пособия, или компьютеризированное сравнение двух или более автоматизированных федеральных систем записей по персоналу или заработной плате или системы федеральных записей по персоналу или заработной плате с нефедеральными записями.

Confidentiality Конфиденциальность [44 U.S.C., Sec. 3542]	Сохранение установленных ограничений на доступ к и раскрытие информации, включая средства для защиты неприкосновенности частной жизни и конфиденциальной информации.
Configuration Control Контроль конфигурации [CNSSI 4009]	Процесс контроля модификации аппаратных средств, встроенного микропрограммного обеспечения, программного обеспечения и документации, чтобы защитить информационную систему от ненадлежащих модификаций до, во время и после реализации системы.
Configuration Item Элемент конфигурации	Объединение компонентов информационной системы, которое является назначенным для управления конфигурацией и рассматриваемое как отдельная сущность в процессе управления конфигурацией.
Configuration Management Управление конфигурацией	Набор работ направленных на то, чтобы определять и поддерживать целостность продуктов информационных технологий и информационных систем, посредством мер проведения инициализации, изменения и контроля конфигурации этих продуктов и систем всюду по жизненному циклу разработки систем.
Configuration Settings Установки конфигурации	Набор параметров, которые могут быть изменены в аппаратных средствах, программном обеспечении или встроенном микропрограммном обеспечении, влияющие на состояние безопасности и/или функциональность информационной системы.
Controlled Area Контролируемая зона	Любая область или пространство, для которого организация уверена, что обеспеченная физическая и процессуальная защита достаточна, чтобы удовлетворить требованиям, установленным для защиты информации и/или информационной системы.
Controlled Interface Контролируемый интерфейс [CNSSI 4009]	Граница с рядом механизмов, которые проводят в жизнь политику безопасности и контролируют поток информации между взаимодействующими информационными системами.
Controlled Unclassified Information Контролируемая неклассифицированная информация [E.O. 13556]	Обозначение категории, относящейся к неклассифицированной информации, в отношении которой не выполняются стандарты для классификации по национальной безопасности в соответствии с Правительственным распоряжением 12958, с уточнениями, но которая (i) имеет отношение к национальным интересам Соединенных Штатов или представляет важный интерес для сущностей вне федерального правительства, и (ii) в соответствии с законом или политикой требует защиты от несанкционированного раскрытия, специальных мер защиты при обработке или установленных ограничений на обмен или распространение.
Countermeasures Контрмеры [CNSSI 4009]	Действия, устройства, процедуры, технологии или другие меры, которые уменьшают уязвимость информационной системы. Синоним с мерами безопасности и мерами защиты.
Covert Channel Analysis Анализ скрытых каналов [CNSSI 4009]	Определение степени, с который модель политики безопасности и последующие низко-уровневые описания программы могут позволить несанкционированный доступ к информации.
Covert Storage Channel Скрытый канал памяти [CNSSI 4009]	Скрытый канал, включающий прямую или косвенную запись в область памяти одним процессом и прямое или косвенное чтение из области памяти другим процессом. Скрытые каналы хранения, как правило, включают конечный ресурс (например, секторы на диске), который совместно используется двумя субъектами с различными уровнями безопасности.

Covert Timing Channel Тайный канал синхронизации [CNSSI 4009]	Скрытый канал, в котором процесс сообщает информацию другому процессу, модулируя его собственное использование системных ресурсов (например, времени центрального процессора) таким способом, что это манипулирование влияет на реальное время отклика, наблюдаемое вторым процессом.
Cross Domain Solution Кросс-доменное решение [CNSSI 4009]	Форма контролируемого интерфейса, который обеспечивает возможность для ручного и/или автоматического доступа и/или передачи информации между различными доменами безопасности.
Cyber Attack Кибератака [CNSSI 4009]	Атака, через киберпространство, с целью инициативного использования киберпространства с целью разрушения, отключения, уничтожения или злонамеренного управления вычислительной средой/инфраструктурой; или нарушение целостности данных или кража контролируемой информации.
Cyber Security Кибербезопасность [CNSSI 4009]	Возможность защищать или оборонять использование киберпространства от кибератак.
Cyberspace Киберпространство [CNSSI 4009]	Глобальный домен в составе информационной среды, состоящий из взаимозависимой сети инфраструктур информационных систем включая Интернет, телекоммуникационные сети, компьютерные системы и встроенные процессоры и контроллеры.
Data Mining/Harvesting Интеллектуальный анализ данных / харвестинг	Аналитический процесс, который пытается найти корреляции или образцы в больших наборах данных с целью открытия знаний или данных.
Defense-in-Breadth Всесторонняя защита [CNSSI 4009]	Спланированный, систематизированный набор мультидисциплинарных действий, которые стремятся идентифицировать, управлять и уменьшать риск годных для использования уязвимостей в каждой стадии жизненного цикла системы, сети или субкомпонента (система, сеть или проект продукта и разработка; производство; упаковка; сборка; системная интеграция; поставка; эксплуатация; поддержка; и ликвидация).
Defense-in-Depth Эшелонированная защита	Стратегия информационной безопасности, интегрирующая возможности людей, технологий и эксплуатации по установке изменяемых барьеров на разнообразных уровнях и предназначениях организации.
Developer Разработчик	Общий термин, который включает: (i) разработчиков или производителей информационных систем, системных компонентов или сервисов информационной системы; (ii) системных интеграторов; (iii) поставщиков; и (iv) торговых посредников продукта. Разработка систем, компонентов или сервисов может происходить внутри в организации (то есть, внутренняя разработка) или через внешние сущности.
Digital Media Цифровые носители	Форма электронных носителей, где данные хранятся в цифровой (как противоположность аналоговой) форме.

Discretionary Access Control Дискреционный контроль доступа	Политика контроля доступа, которая определена для всех субъектов и объектов в информационной системе, когда политика определяет, что субъект, которому был предоставлен доступ к информации, может сделать одно или более следующего: (i) передать информацию к другим субъектам или объектам; (ii) предоставить свои полномочия другим субъектам; (iii) изменить атрибуты безопасности у субъектов, объектов, информационных систем или системных компонентов; (iv) выбрать атрибуты безопасности, которые будут связаны с недавно созданными или пересмотренными объектами; или (v) изменить правила установленного контроля доступа. Мандатный контроль доступа ограничивает эту возможность.
[CNSSI 4009]	Средства ограничения доступа к объектам (например, файлам, сущности данных) основанные на идентификации и ограничении осведомления субъектов (например, пользователей, процессов) и/или групп, к которым принадлежит объект. Меры обеспечения являются дискреционными в том смысле, что субъект с некоторым правом доступа способен передать это разрешение (возможно, косвенно) любому другому субъекту (если это не ограничено мандатным управлением доступом).
Domain Домен [CNSSI 4009]	Среда или контекст, который включает набор системных ресурсов и набор системных сущностей, которые имеют право на доступ к ресурсам как определено общей политикой безопасности, моделью обеспечения безопасности или архитектурой безопасности. См. *Security Domain*.
Enterprise Предприятие [CNSSI 4009]	Организация с определённым предназначением/целью и определёнными границами, использующая информационные системы для выполнения этого предназначения, и с ответственностью за управление его собственными рисками и деятельностью. Предприятие может включать все или некоторые из следующих аспектов деятельности: приобретение, программное управление, финансовый менеджмент (например, бюджеты), людские ресурсы, безопасность, и информационные системы, информацию и управление предназначением. См. *Организация*.
Enterprise Architecture Архитектура предприятия [44 U.S.C. Sec. 3601]	Стратегическая основа информационных активов, которая определяет предназначение; информация, необходимая чтобы выполнить предназначение; технологии, необходимые чтобы выполнить предназначение; и транзитные процессы для реализации новых технологий в ответ на изменяющиеся потребности предназначения; и включает базовую архитектуру; целевая архитектура; и план упорядочивания.
Environment of Operation Среда эксплуатации [NIST SP 800-37]	Физическое окружение, в котором информационная система обрабатывает, хранит и передаёт информацию.
Event Событие [CNSSI 4009, уточненный]	Любой, требующий внимания, случай в информационной системе.
Executive Agency Исполнительное агентство [41 U.S.C., Sec. 403]	Исполнительный департамент, определенный в 5 U.S.C., Раздел 101; военный департамент, определенный 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.
Exfiltration Экс-фильтрация	Несанкционированная передача информации из информационной системы.

External Information System (or Component) Внешняя информационная система (или компонент)	Информационная система или компонент информационной системы, которая находится за пределами границ санкционирования, установленных организацией, и для которой организация, как правило, не имеет прямого управления через приложение требуемых мер безопасности или оценки эффективности мер безопасности.
*External Information System Serv*ice Внешний сервис информационной системы	Сервис информационной системы, который реализован за пределами границ санкционирования информационной системы организации (то есть, сервис, который используется, но не является частью информационной системы организации), и для которого организация, как правило, не имеет прямого управления через приложение требуемых мер безопасности или оценки эффективности мер безопасности.
External Information System Service Provider Поставщик внешних услуг информационной системы	Поставщик внешних услуг информационной системы организации посредством различных отношений потребитель-производитель, включающих, но не ограничивающихся: совместные предприятия; коммерческие партнерства; соглашения аутсорсинга (то есть, через контракты, межведомственные соглашения, соглашения направлений деятельности); лицензионные соглашения; и/или простую цепочку поставок.
External Network Внешняя сеть	Сеть, не контролируемая организацией.
Failover Файловер	Возможность переключаться автоматически (как правило, без вмешательства или оповещения человека) к избыточной или резервной информационной системе после отказа или аварийного завершения ранее активной системы.
*Fair Information Practice Princip*les Принципы честной информационной практики	Принципы, которые широко приняты в Соединенных Штатах и на международном уровне как общие рамки для приватности и которые отражены в различных федеральных законах и нормах международного права и политиках. Во многих организациях принципы служат основанием для анализа рисков приватности и определения соответствующих стратегий их снижения.
Federal Agency Федеральное агентство	См. *Executive Agency.*
Federal Enterprise Architecture Архитектура федерального предприятия [Офис управления Программой FEA]	Базирующаяся на деятельности основа для общеправительственного усовершенствования, разработанная Министерством управления и бюджета, которая предназначена, чтобы облегчить усилия по преобразованию федерального правительства к тому, которое ориентируется на гражданина, ориентируется на результат и основывается на рынке.
Federal Information System Федеральная информационная система [40 U.S.C., Sec. 11331]	Информационная система, которая используется или управляется исполнительным агентством, подрядчиком исполнительного агентства или другой организацией от имени исполнительного агентства.
FIPS-Validated Cryptography Криптография, соответствующая FIPS	Криптографический модуль, проверенный посредством Программы подтверждения соответствия криптографических модулей (CMVP), чтобы удовлетворять требованиям, определенным в FIPS публикации 140-2 (с уточнениями). Как предпосылка к подтверждению соответствия CMVP, криптографический модуль обязан использовать реализацию криптографического алгоритма, которая успешно прошла тестирование подтверждения соответствия по Программе подтверждения соответствия криптографических алгоритмов (CAVP). См. *NSA-Approved Cryptography*.

Firmware Встроенное микропрограммное обеспечение [CNSSI 4009]	Компьютерные программы и данные, хранящиеся в аппаратных средствах - как правило, в постоянной памяти (ROM) или программируемом ПЗУ (PROM) - так, что программы и данные не могут быть динамически записаны или изменены во время выполнения программ.
Guard (System) Сторож (Системный) [CNSSI 4009, уточненный]	Механизм, ограничивающий обмен информацией между информационными системами или подсистемами.
Hardware Аппаратные средства [CNSSI 4009]	Физические компоненты информационной системы. См. *Software* и *Firmware.*
High-Impact System Система высокого воздействия [FIPS 200]	Информационная система, в которой, по крайней мере, одной цели безопасности (то есть, конфиденциальности, целостности или доступности) назначено, в соответствии с FIPS Публикацией 199, значение потенциала воздействия «высокий».
Hybrid Security Control Гибридная мера безопасности [CNSSI 4009]	Мера безопасности, которая реализована в информационной системе частично как общая мера безопасности и частично как специфичная для системы мера безопасности. См. *Common Control* и *System-Specific Security Control*.
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.
Impact Value Величина воздействия	Оцененное потенциальное воздействие, являющееся результатом компрометации конфиденциальности, целостности или доступности информации, выраженное в значениях низкое, умеренное или высокое.
Incident Инцидент [FIPS 200]	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.
Industrial Control System Промышленная система управления	Информационная система, используемая для контроля производственных процессов, таких как производство, обработка продукта, изготовление и распространение. Промышленные системы управления включают системы диспетчерского управления и сбора данных (SCADA), используемые для контроля географически распределённых активов, а так же распределенные системы управления (DCSs) и малые системы управления, использующие контроллеры с программируемой логикой, чтобы контролировать ограниченные процессы.
Information Информация [CNSSI 4009]	Любое сообщение или представление знаний, таких как факты, данные или мнения на любом носителе или в любой форме, включая текстовую, число-вую, графическую, картографическую, описательную или аудиовизуальную.
[FIPS 199]	Частный случай типа информации.
Information Leakage Утечка информации	Намеренный или неумышленный выпуск информации в недоверенную среду.
Information Owner Владелец информации [CNSSI 4009]	Должностное лицо с установленными законом или исполнительными полномочиями для указанной информации и ответственностью за установление мер безопасности по ее генерации, сбору, обработке, распространению и ликвидации.

Information Resources Информационные ресурсы [44 U.S.C., Sec. 3502]	Информация и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии.
Information Security Информационная безопасность [44 U.S.C., Sec. 3542]	Защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения, с целью обеспечения конфиденциальности, целостности и доступности.
Information Security Architecture Архитектура информационной безопасности	Встроенная, неотъемлемая часть архитектуры предприятия, которая описывает структуру и поведение для процессов безопасности предприятия, систем информационной безопасности, персонала и подразделений организации, демонстрируя их соответствие с предназначением предприятия и стратегическими планами.
Information Security Policy Политика информационной безопасности [CNSSI 4009]	Совокупность директив, нормативных актов, правил и методов, которые предписывают, как организации управлять, защищать и распределять информацию.
Information Security Program Plan План Программы информационной безопасности	Формальный документ, который содержит описание требований безопасности для программы информационной безопасности всей организации и описывает меры управления программой и имеющиеся или планируемые общие меры безопасности для удовлетворения этим требованиям.
Information Security Risk Риск информационной безопасности	Риск для деятельности организации (включая предназначение, функции, имидж, репутацию), активов организации, людей, других организаций и Нации вследствие наличия возможности для несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения информации и/или информационных систем.
Information Steward Управляющий информацией [CNSSI 4009]	Должностное лицо агентства с установленными законом или исполнительными полномочиями для указанной информации и ответственностью за установление мер безопасности для ее генерации, сбора, обработки, распространения и уничтожения.
Information System Информационная система [44 U.S.C., Sec. 3502]	Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или ликвидации информации. Примечание: Информационные системы также включают специализированные системы, такие как промышленные /производственные системы управления, телефонные коммутаторы и системы частных телефонных станций (PBX) и системы контроля за окружающей средой.
Information System Boundary Границы информационной системы	См. *Authorization Boundary*.
Information System Component Компонент информационной системы [NIST SP 800-128, уточненный]	Дискретный, идентифицируемый актив информационной технологии (например, аппаратные средства, программное обеспечение, встроенное микропрограммное обеспечение), который представляет конструктивный блок информационной системы. Компоненты информационной системы включают коммерческие продукты информационной технологии.
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.

Information System Resilience Устойчивость информационной системы	Возможность информационной системы продолжать: (i) работать при неблагоприятных условиях или воздействии, даже если находится в ухудшенном или ослабленном состоянии, поддерживая существенные эксплуатационные возможности; и (ii) восстанавливаться до эффективного эксплуатационного состояния в период времени, соотносимый с потребностями назначения.
Information System Security Officer Сотрудник безопасности информационной системы [CNSSI 4009]	Человек с возложенной ответственностью за поддержание соответствующего эксплуатационного состояния безопасности для информационной системы или программы.
Information System Service Сервис информационной системы	Возможность, обеспечиваемая информационной системой, которая облегчает обработку, хранение или передачу информации.
Information System-Related Security Risks Риски безопасности, связанные с информационной системой	Риски, которые возникают через потерю конфиденциальности, целостности, или доступность информации или информационных систем и которые учитывают воздействие на организацию (включая активы, предназначение, функции, имидж или репутацию), людей, другие организации и Нацию. См. *Риск*.
Information Technology Информационная технология [40 U.S.C., Sec. 1401]	Любое оборудование или взаимосвязанная система или подсистема оборудования, которое используется в автоматизированном получении, хранении, манипулировании, управлении, перемещении, контроле, показе, переключении, обмене, передаче или приеме данных или информации исполнительным агентством. Для целей предыдущего предложения, оборудование используется исполнительным агентством, если оборудование используется исполнительным агентством непосредственно или используется подрядчиком в соответствии с контрактом с исполнительным агентством который: (i) требует использования такого оборудования; или (ii) требует использования, до существенной степени, такого оборудования в исполнении сервиса или оснащении продукта. Термин информационная технология включает компьютеры, вспомогательное оборудование, программное обеспечение, встроенное микропрограммное обеспечение, и подобные процедуры, сервисы (включая службу поддержки) и связанные ресурсы.
Information Technology Product Продукт информационной технологии	См. *Information System Component*.
Information Type Тип информации [FIPS 199]	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 нормативному документу.
Insider Инсайдер [Президентский меморандум, Национальная политика в отношении инсайдерских угроз и минимальные стандарты для программ инсайдерских угроз исполнительной власти]	Любой человек с санкционированным доступом к любым ресурсам правительства США, которые включают персонал, средства, информацию, оборудование, сети или системы.

Insider Threat Инсайдерская угроза [Президентский меморандум, Национальная политика в отношении инсайдерских угроз и минимальные стандарты для программ инсайдерских угроз исполнительной власти]	Угроза, что инсайдер будет использовать её/его санкционированный доступ, умышленно или невольно, чтобы причинить вред безопасности Соединенных Штатов. Эта угроза может включать ущерб Соединенным Штатам через электронный шпионаж, терроризм, несанкционированное раскрытие информации национальной безопасности, или через потерю или нарушение ведомственных ресурсов или возможностей.
[CNSSI 4009]	Сущность с санкционированным доступом (то есть, в пределах домена безопасности), у которого есть возможность вредить информационной системе или предприятию посредством разрушения, раскрытия, модификации данных и/или отказа сервиса.
Insider Threat Program Программа в отношении инсайдерских угроз [Президентский меморандум, Национальная политика в отношении инсайдерских угроз и минимальные стандарты для программ инсайдерских угроз исполнительной власти]	Скоординированная группа возможностей под централизованным управление, которая организована, чтобы обнаружить и предотвратить несанкционированное раскрытие чувствительной информации. Как минимум, для департаментов и агентств, которые обрабатывают классифицированную информацию, программа в отношении инсайдерских угроз должна состоять из возможностей, которые обеспечивают доступ к информации; централизованную интеграцию, анализ информации и реакцию; обучение сотрудников в отношении инсайдерских угроз; и мониторинг работы пользователей на правительственных компьютерах. Для департаментов и агентств, которые не обрабатывают классифицированную информацию, они могут быть эффективно использованы для защиты информации, которая является не классифицированной, но чувствительной.
Integrity Целостность [44 U.S.C., Sec. 3542]	Защита против неправомерной модификации или уничтожения информации, включающая обеспечение неотказуемости и аутентичности информации.
Internal Network Внутренняя сеть	Сеть, где: (i) установление, поддержка и настройка мер безопасности находится под прямым управлением сотрудниками организации или подрядчиками; или (ii) криптографическая инкапсуляция или подобная технология безопасности, реализованная между контролируемыми организацией конечными точками, обеспечивает тот же самый эффект (по крайней мере, относительно конфиденциальности и целостности). Внутренняя сеть является, как правило, находящейся в собственности организации, однако может быть контролируемой организацией не будучи находящейся в собственности организации.
Label Метка	См. *Security Label.*
Line of Business Направление деятельности	Следующие OMB-определенные области деятельности, общие фактически ко всем федеральным агентствам: управление делами, финансовый менеджмент, управление субсидиями, управление людскими ресурсами, федеральная медицинская архитектура, безопасность информационных систем, формирование и исполнение бюджета, геопозиционирование и инфраструктура ИТ.
Local Access Локальный доступ	Доступ к информационной системе организации пользователем (или процессом, действующим от имени пользователя), взаимодействующим посредством прямой связи без использования сети.

Logical Access Control System Система контроля логического доступа [FICAM путеводитель и руководство реализации]	Автоматизированная система, которая контролирует возможность человека по доступу к одному или более ресурсам компьютерной системы, таким как рабочая станция, сеть, приложение или база данных. Система контроля логического доступа требует подтверждения соответствия идентификационных данных человека через некоторый механизм, такой как PIN, карта, биометрический или другой маркер. У неё есть возможность назначать различные права доступа различным людям в зависимости от их ролей и обязанностей в организации.
Low-Impact System Система низкого воздействия [FIPS 200]	Информационная система, в который всем трём целям безопасности (то есть, конфиденциальности, целостности и доступности) назначено, в соответствии с FIPS Публикацией 199, значение потенциала воздействия «низкий».
Malicious Code Вредоносный код	Программное обеспечение или встроенное микропрограммное обеспечение, предназначенные для выполнения несанкционированного процесса, который может оказать неблагоприятное влияние на конфиденциальность, целостность или доступность информационной системы. Вирус, червь, троянский конь или другая основанная на коде сущность, которая заражает узел. Шпионящее ПО и некоторые формы бесплатного ПО с размещенной в нем рекламой - также примеры вредоносного кода.
Malware Вредоносное ПО	См. *Malicious Code*.
Managed Interface Управляемый интерфейс	Интерфейс информационной системы, который обеспечивает возможность защиты границ, используя автоматизировала механизмы или устройства.
Mandatory Access Control Мандатный контроль доступа	Политика контроля доступа, которая единообразно определена для всех субъектов и объектов в границах информационной системы. Субъект, которому предоставлен доступом к информации, ограничен в отношении выполнения любого следующего: (i) передача информации к несанкционированным субъектам или объектам; (ii) предоставление его полномочий другим субъектам; (iii) изменение одного или более атрибутов безопасности на субъектах, объектах, информационной системе или системных компонентах; (iv) выбор атрибутов безопасности, которые будут связаны с недавно созданными или измененными объектами; или (v) изменение правил, определяющих контроль доступа. Определенным организацией субъектам можно явно предоставить установленные организацией полномочия (т.е., они доверенные субъекты) так, что, они не ограничены некоторыми или всеми вышеупомянутыми ограничениями.
[CNSSI 4009]	Средства ограничения доступа к объектам, основанные на чувствительности (как определено меткой безопасности) информации, содержавшейся в объектах, и формальном санкционировании (то есть, разрешение, формальное санкционирование доступа и «по-необходимости») доступа субъектов к информации такой чувствительности. Мандатный контроль доступа - тип не дискреционного контроля доступа.
Marking Маркирование	См., *Security Marking*.
Media Носитель информации [FIPS 200]	Физические устройства или записывающие поверхности включающие, но не ограничивающиеся, магнитные ленты, оптические диски, магнитные диски, микросхемы памяти высокого уровня интеграции (LSI) и распечатки (но не включающие дисплейные устройства), на которые делается запись, хранение или печать информации в информационной системе.

Metadata Метаданные	Информация, описывающая характеристики данных, включая, например, структурные метаданные, описывающие структуры данных (такие, как формат данных, синтаксис и семантика) и описательные метаданные, описывающие содержание данных (такие, как метки информационной безопасности).
Mobile Code Мобильный код	Программы или части программ, полученные из удаленных информационных систем, передающиеся через сеть и выполняемые в локальной информационной системе без явной установки или выполнения получателем.
Mobile Code Technologies Технологии мобильного кода	Разработки программного обеспечения, которые предоставляют механизмы для разработки и использования мобильного кода (например, Java, JavaScript, ActiveX, VBScript).
Mobile Device Мобильное устройство	Переносимое вычислительное устройство, которое: (i) имеет миниатюрный форм-фактор такой, что, его может легко перенести один человек; (ii) разработан, чтобы работать без физического соединения (например, с помощью беспроводных технологий передачи или получения информации); (iii) обладает локальным, несъемным или съемным устройством хранения данных; и (iv) включает автономный источник энергии. Мобильные устройства могут также включать возможности голосового сообщения, встроенные датчики, которые позволяют устройствам получать информацию, и/или встроенные функции синхронизации локальных данных с удаленными местоположениями. Примеры включают смартфоны, планшеты и электронные книги.
Moderate-Impact System Система умеренного воздействия [FIPS 200]	Информационная система, в которой, по крайней мере, одной цели безопасности (то есть, конфиденциальности, целостности или доступности) назначено в соответствии с FIPS Публикацией 199 значение потенциала воздействия «умеренный» и нет цели безопасности, которой назначено в соответствии с FIPS Публикацией 199 значение потенциала воздействия «высокий».
Multifactor Authentication Многофакторная аутентификация	Аутентификация, использующая два или более различных факторов, чтобы достичь аутентификации. Факторы включают: (i) нечто Вам известное (например, пароль/PIN); (ii) нечто, что Вы имеете (например, криптографическое устройство идентификации, токен); или (iii) что-то Ваше (например, биометрия). См. *Authenticator.*
Multilevel Security Многоуровневая безопасность [CNSSI 4009]	Концепция обработки информации с различными классами и категориями, которая одновременно разрешает доступ пользователями с различными уровнями допуска к информации и лишает доступа пользователей, которые имеют недостаточное санкционирование.
Multiple Security Levels Различные уровни безопасности [CNSSI 4009]	Возможности информационной системы, которая доверена, чтобы содержать, поддерживая разделение между, ресурсы (особенно по хранению данных) различных доменов безопасности.
*National Security Emergency Preparedness Telecommunications Service*s Телекоммуникационные Сервисы подготовленности к чрезвычайным ситуациям национальной безопасности [47 C.F.R., Часть 64, Приложение A]	Телекоммуникационные сервисы, которые используются, чтобы поддерживать состояние готовности или отвечать на и управлять любым событием или кризисом (локальным, национальным или международным), который вызывает или может вызвать повреждение или ущерб населению, ущерб или потерю собственности или ухудшить или угрожать национальной безопасности или подготовленности Соединенных Штатов к чрезвычайным ситуациям.

National Security System Система национальной безопасности [44 U.S.C., Sec. 3542]	Любая информационная система (включая любую телекоммуникационную систему) используемая или управляемая агентством или подрядчиком агентства, или другой организацией от имени агентства - (i) функция, деятельность или использование которой включает разведывательную деятельность; включает криптологические работы, связанные с национальной безопасностью; включает руководство и управление вооруженными силами; включает оборудование, которое является неотъемлемой частью оружия или системы оружия; или являются критическими по отношению к прямому выполнению военных задач или задач разведки (исключая систему, которая должна использоваться для стандартных административных и бизнес-приложений, например, платежей, финансов, логистики и приложений управления персоналом); или, (ii) постоянно защищена процедурами, установленными для информации, которая была специально определена критериями, установленными Правительственным распоряжением или законом конгресса, быть классифицированной в интересах национальной обороны или внешней политики.
Network Сеть [CNSSI 4009]	Информационная система (ы), реализованная с набором взаимосвязанных компонентов. Такие компоненты могут включать маршрутизаторы, концентраторы, кабельные соединения, телекоммуникационные контроллеры, центры распределения ключей и устройства технического контроля.
Network Access Сетевой доступ	Доступ к информационной системе пользователем (или процессом, действующим от имени пользователя), взаимодействующим через сеть (например, локальную сеть, глобальную сеть, Интернет).
Nondiscretionary Access Control Не дискреционный контроль доступа	См. *Mandatory Access Control*.
Nonlocal Maintenance Не локальная поддержка	Действия поддержки, проводимые людьми, взаимодействующими через сеть, включая внешнюю сеть (например, Интернет) или внутреннюю сеть.
Non-Organizational User Пользователь не из организации	Пользователь, который не является пользователем организации (включая общих пользователей).
Non-repudiation Неотказуемость	Защита, направленная против людей, ложно отрицающих выполнение определенных действий. Обеспечивает возможность определить, совершил ли данный человек определенные действия, такие как создание информации, отправка сообщения, одобрение информации и получение сообщения.
NSA-Approved Одобренное АНБ	Криптография, которая состоит из: (i) одобренного алгоритма; (ii) реализации криптографии, которая была одобрена для защиты классифицированной информации и/или контролируемой неклассифицированной информации в определенной среде; и (iii) поддерживающая инфраструктура управления ключами.
Object Объект	Пассивная сущность, связанная с информационной системой (например, устройства, файлы, записи, таблицы, процессы, программы, домены) содержащая или получающая информацию. Доступ к объекту (субъектом) подразумевает доступ к информации, которую он содержит. См. *Subject.*

Operations Security Эксплуатационная безопасность [CNSSI 4009]	Систематизированный и доказательный процесс, посредством которого потенциальным противникам можно не дать возможность получить информацию о возможностях и намерениях, идентифицируя, контролируя и защищая главным образом неклассифицированное свидетельство планирования и выполнения чувствительных работ. Процесс включает пять шагов: идентификация критической информации, анализ угроз, анализ уязвимостей, оценка рисков и приложение соответствующих контрмер.
Organization Организация [FIPS 200, уточненный]	Сущность любого размера, сложности или позиционирования в организационной структуре (например, федеральное агентство или, если соответствующе, любой из его операционных элементов).
Organizational User Пользователь организации	Сотрудник организации или человек, в отношение которого организация считает, что он имеет статус эквивалентный сотруднику, включая, например, подрядчик, приглашенный исследователь, человек, выделенный от другой организации. Политика и процедуры для того, чтобы предоставить людям статус эквивалентный сотруднику могут включать необходимые знания, отношение к организации и гражданство.
Overlay Оверлей	Спецификация мер безопасности, улучшений мер безопасности, дополнительного руководства и другой поддерживающей информации, используемых во время процесса адаптации, которые предназначены для дополнения (и дальнейшего совершенствования) базовых мер безопасности. Спецификация оверлея может быть более или менее строгой, чем исходная спецификация базового набора мер безопасности, и может быть применена ко многим информационным системам.
Penetration Testing Тестирование проникновения	Тестовая методология, в которой оценщики, работающие, как правило, с конкретными ограничениями, пытаются обойти или преодолеть средства защиты информационной системы.
Personally Identifiable Information Персональная идентификационная информация [Меморандум OMB 07-16]	Информация, которая может использоваться, чтобы отличить или проследить идентичность человека (например, имя, номер свидетельства социального страхования, биометрические данные и т.д.) самостоятельно или при объединении с другой персональной или идентификационной информацией, которая связана или связываема с конкретным человеком (например, дата и место рождения, девичья фамилия матери и т.д.).
Physical Access Control System Система контроля физического доступа [FICAM путеводитель и руководство реализации]	Автоматизированная система, которая управляет перемещением людей или активов через проход (ы) в безопасном периметре (ах), основываясь на наборе правил санкционирования.
Plan of Action and Milestones План действий и вехи [Меморандум OMB 02-01]	Документ, который определяет задачи, которые должны быть выполнены. Он детализирует ресурсы, требуемые для выполнения элементов плана, любые вехи, связанные с задачами, и намеченные даты завершения для вех.
Portable Storage Device Переносное устройство хранения данных	Компонент информационной системы, который может быть вставлен и удален из информационной системы и который используется, чтобы хранить данные или информацию (т.к., текст, видео, аудио и/или графические данные). Такие компоненты, обычно, реализуются в виде магнитных, оптических или полупроводниковых приборов (например, гибкие диски, компактные/-цифровые видеодиски, карты флэш-памяти, внешние жесткие диски и карты-/накопители флэш-памяти, которые содержат энергонезависимую память).

Potential Impact Потенциал воздействия [FIPS 199]	Потеря конфиденциальности, целостности или доступности, как ожидается, может иметь: (i) *ограниченное* отрицательное воздействие (FIPS публикация 199 «низкое»); (ii) *серьезное* отрицательное воздействие (FIPS публикация 199 «умеренное»); или (iii) *тяжелое* или *катастрофическое* отрицательное воздействие (FIPS публикация 199 «высокое») на деятельность организации, активы организации или людей.
Privacy Act Statement Заявление в отношении Закона о неприкосновенности частной жизни	Заявление раскрытия, требуемое Разделом (e) (3) Закона о неприкосновенности частной жизни 1974, с уточнениями, для представления на документах, используемых организациями для сбора от людей персональной идентифицирующей информации, которая будет сопровождаться в Системе записей Закона о неприкосновенности частной жизни (SORN).
Privacy Impact Assessment Оценка воздействия на приватность [Меморандум OMB 03-22]	Анализ того, как информация обрабатывается: (i), чтобы гарантировать обработку, соответствующую применимым законодательным, нормативным требованиям и требованиям политик относительно приватности; (ii), чтобы определить риски и результаты сбора, поддержания и распространения информации в соответствующей форме в электронной информационной системе; и (iii), чтобы исследовать и оценить соответствие защиты и альтернативных процессов обработки информации для смягчения потенциальных рисков приватности.
Privileged Account Привлегированная учетная запись	Учетная запись информационной системы с санкционированием привилегированного пользователя.
Privileged Command Привилегированная команда	Инициируемая человеком команда, выполняемая в информационной системе, затрагивающая контроль, мониторинг или администрирование системы, включая функции безопасности и связанную информацию, важную для безопасности.
Privileged User Привилегированный пользователь [CNSSI 4009]	Пользователь, который уполномочен (и поэтому, является доверенным) выполнять функции, связанные с безопасностью, которые обычные пользователи выполнять не уполномочены.
Protective Distribution System Система защищенного распространения	Проводная или оптоволоконная система, которая включает адекватные меры защиты и/или контрмеры (например, акустические, электрические, электромагнитные и физические), чтобы разрешить её использование для передачи незашифрованной информации.
Provenance Происхождение	Записи, описывающие владение и изменения к компонентам, компонентным процессам, информации, системам, организации и организационным процессам. Происхождение делает возможным все изменения к базовым компонентам, компонентным процессам, информации, системам, организациям и организационным процессам, будучи сообщенным конкретным агентам, функциям, местам или работам.
Public Key Infrastructure Инфраструктура Публичных Ключей [CNSSI 4009]	Основа и сервисы, которые предусматривают генерацию, изготовление, распределение, контроль, учет и ликвидацию сертификатов с открытым ключом. Компоненты, включающие персонал, политики, процессы, платформы сервера, программное обеспечение и рабочие станции, используются с целью администрирования сертификатов и пары публичный-закрытый ключ, включая возможности по выпуску, сопровождению, восстановлению и отмене сертификатов с открытым ключом.

Purge Уничтожение	Перевод санированных данных в состояние, обеспечивающее невосстанавление лабораторными методами.
Reciprocity Соглашение о взаимности [CNSSI 4009]	Совместное соглашение среди участвующих организаций, чтобы принять оценки безопасности другого участника с целью повторного использования ресурсов информационной системы и/или принять оцененное другим участником состояние с безопасностью, в качестве общей информации.
Records Записи	Записи (автоматизированные и/или ручные) свидетельства выполняемых действий или достигнутых результатов (например, формы, отчеты, результаты испытаний), которые служат основанием для того, чтобы проверить, что организация и информационная система используются как предназначено. Также используются, чтобы обратиться к элементам связанных полей данных (то есть, группы полей данных, к которым может получить доступ программа и которые содержат полный набор информации относительно определенных элементов).
Red Team Exercise Использование красной команды	Использование, отражающее реальные условия, которое проводится как моделируемая попытка соперника ставить под угрозу процессы предназначения и/или деятельности организации, чтобы обеспечить всестороннюю оценку возможностей безопасности информационной системы и организации.
Reference Monitor Монитор обращений	Набор проектных требований к механизму подтверждения обращений, который, как ключевой компонент операционной системы, проводит в жизнь политику контроля доступа по всем субъектам и объектам. Механизм подтверждения обращений должен быть: (i) всегда вызываемый (то есть, полностью посредничающй); (ii) неизменный; и (iii) достаточно маленький, чтобы быть подвергаемым анализу и тестам, законченность которых может быть гарантирована (то есть, поддающийся проверке).
Remote Access Удаленный доступ	Доступ к информационной системе организации пользователем (или процессом, действующий от имени пользователя), взаимодействующим через внешнюю сеть (например, Интернет).
Remote Maintenance Удаленная поддержка	Действия поддержки, проводимые людьми, связывающимися через внешнюю сеть (например, Интернет).
Resilience Устойчивость	См. *Information System Resilience*.
Restricted Data Данные ограниченного доступа [Закон об атомной энергии 1954]	Все данные относительно (i) проекта, изготовления или использования атомного оружия; (ii) производства специального ядерного материала; или (iii) использования специального ядерного материала в производстве энергии, но не включая данные рассекреченные или удаленные из категории «данные ограниченного доступа» в соответствии с Разделом 142 [Закона об атомной энергии 1954].

Risk Риск [FIPS 200, уточненный]	Мера степени, до которой сущности угрожают потенциальные обстоятельства или события и, как правило, функция: (i) неблагоприятных воздействий, которые возникли бы, если бы обстоятельства или события произошли; и (ii) вероятности возникновения. Риски безопасности, связанные с информационной системой - те риски, которые являются результатом потери конфиденциальности, целостности или доступности информации или информационных систем и отражают потенциальные неблагоприятные воздействия к деятельности организации (включая предназначение, функции, имидж или репутацию), активы организации, людей, другие организации и Нацию.
Risk Assessment Оценка риска	Процесс идентификации рисков к деятельности организации (включая предназначение, функции, имидж репутацию), активам организации, людям, другим организациям и Нации, следующих из эксплуатации информационной системы. Часть управления рисками, включающая анализ угроз и уязвимостей, и учитывающая их снижение, обеспечиваемое существующими или планируемыми мерами безопасности. Синоним с анализом рисков.
Risk Executive (Function) Ответственный за риски (функция) [CNSSI 4009]	Человек или группа в организации, который помогает обеспечивать, что: (i) связанные с риском рассмотрения безопасности для отдельных информационных систем, которые включают решения о санкционировании для этих систем, рассмотрены с точки зрения всей организации относительно полных стратегических целей и задач организации по выполнению её функций предназначения и деятельности; и (ii) управление риском отдельных информационных систем непротиворечиво с организацией, отражает допуск для риска организации и рассмотрен наряду с другими рисками организации, влияющими на успех в предназначении/деятельности.
Risk Management Управление рисками [CNSSI 4009, уточненный]	Программа и поддерживающие процессы по управлению рисками информационной безопасности для деятельности организации (включая предназначение, функции, имидж и репутацию), активов организации, людей, других организаций и Нации, включающие: (i) установление контекста для работ, связанных с риском; (ii) оценку риска; (iii) ответственность за однократное определение риска; и (iv) мониторинг риска в последующее время.
Risk Mitigation Снижение рисков [CNSSI 4009]	Расположение по приоритетам, оценка и реализуя соответствующих сокращающих риск мер безопасности/контрмер, рекомендованных процессом управления рисками.
Risk Monitoring Мониторинг рисков	Постоянное поддержание осведомленности о среде рисков организации, программе управления рисками и связанных действий по поддержанию решений относительно рисков.
Risk Response Реагирование на риски	Принятие, уклонение, смягчение, разделение или передача рисков для деятельности организации (то есть, предназначения, функций, имиджа или репутации), активов организации, людей, других организаций или Нации.

Role-Based Access Control Ролевый контроль доступа	Контроль доступа, основанный на ролях пользователей (то есть, наборе санкционирований контроля доступа, полученных пользователем, основанном на явном или неявном предположении о данном роль). Полномочия роли, могут быть наследованы через иерархию ролей и, как правило, отражают, полномочия, необходимые для выполнения определенных функций в организации. Предоставляемая роль может применяться к отдельному человеку или нескольким людям.
Safeguards Меры защиты [CNSSI 4009]	Защитные меры, предписанные для выполнения требований безопасности (то есть, конфиденциальности, целостности и доступности), определенных для информационной системы. Меры защиты могут включать средства защиты, ограничения управления, безопасность персонала и безопасность физических структур, областей и устройств. Синоним с мерами безопасности и контрмерами.
Sanitization Очистка	Меры, предпринимаемые, чтобы представить данные, записанные на носителе информации, в не восстанавливаемом виде, как для обычных, так и, для некоторых форм очистки, экстраординарных средств. Процесс по удалению информации с носителя информации таким образом, что восстановление данных не возможно. Это включает удаление всех классификационных меток, маркировок и журналов операций.
Scoping Considerations Объектовые особенности	Часть руководства по адаптации, обеспечиваемого организацией, с конкретными рассмотрениями по применимости и реализации мер безопасности в базовом наборе мер безопасности. Области рассмотрения включают политику/нормативные требования, технологию, физическую инфраструктуру, выделение системных компонент, эксплуатацию/среду, открытый доступ, расширяемость, общие меры безопасности и цели безопасности.
Security Безопасность [CNSSI 4009]	Состояние, которое следует из установления и поддержания мер защиты, которые дают возможность предприятию выполнять свое предназначение или критические функции, несмотря на риски, представляемые угрозами использования его информационных систем. Защитные меры могут включить комбинацию сдерживания, уклонения, предотвращения, обнаружения, восстановления и исправления, которые должны являться частью подхода управления рисками предприятия.
Security Assessment Оценка безопасности	См. *Security Control Assessment.*
Security Assessment Plan План оценки безопасности	Задачи по оценке мер безопасности и подробный путеводитель по тому, как провести такую оценку.
Security Assurance Доверие к безопасности	См. *Assurance.*
Security Attribute Атрибут безопасности	Абстракция, представляющая основные свойства или характеристики сущности относительно защиты информации; как правило, связанная с внутренними структурами данных (например, записи, буферы, файлы) в информационной системе и используемая, чтобы допустить реализацию контроля доступа и политик управления потоками, отражающих специальные инструкции распространения, обработки или распределения, или поддерживающих другие аспекты политики информационной безопасности.

Security Authorization Санкционирование безопасности	См. *Authorization.*
Security Authorization Boundary Граница санкционирования безопасности	См. *Authorization Boundary*.
Security Capability Возможности безопасности	Комбинация взаимно усиливающих мер безопасности (то есть, мер защиты и контрмер), реализованная техническими средствами (то есть, функциональностью в аппаратных средствах, программном обеспечении и встроенном микропрограммном обеспечении), физическими средствами (то есть, физическими устройствами и мерами защиты) и процедурными средствами (то есть, процедурами, выполняемыми людьми).
Security Categorization Категорирование безопасности	Процесс определения категории безопасности для информации или информационной системы. Методологии категорирования безопасности описаны в CNSS Инструкции 1253 для систем национальной безопасности и в FIPS публикации 199 для других кроме национальной безопасности систем. См. *Security Category*.
Security Category Категория безопасности [FIPS 199, уточненный; CNSSI 4009]	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.
Security Control Мера безопасности [FIPS 199, Уточненный]	Мера защиты или контрмера, предписанная для информационной системы или организации, разработанная, чтобы защитить конфиденциальность, целостность и доступность ее информации и выполнить ряд определенных требований безопасности.
Security Control Assessment Оценка мер безопасности [CNSSI 4009, Уточненный]	Проверка или оценка мер безопасности для определения степени, до которой меры безопасности реализованы правильно, применяются как пред-назначено и производят желаемый результат относительно удовлетворения требований безопасности для информационной системы или организации.
Security Control Assessor Оценщик мер безопасности	Человек, группа или организация, ответственные за проведение оценки мер безопасности.
Security Control Baseline Базовый набор мер безопасности [FIPS 200, Уточненный]	Набор минимальных мер безопасности, определенный для информационной системы низкого воздействия, умеренного воздействия или высокого воздействия, который обеспечивает начальную точку для процесса адаптации.
Security Control Enhancement Улучшение мер безопасности	Усиление мер безопасности с целью: (i) создания дополнительной, но связанной, функциональности мер безопасности; (ii) увеличение стойкости мер безопасности; или (iii) добавление доверия к мерам безопасности.
Security Control Inheritance Наследование мер безопасности [CNSSI 4009]	Ситуация, в которой информационная система или приложение получают защиту от мер безопасности (или части мер безопасности), которые разработаны, реализованы, оценены, санкционированы и контролируются другими сущностями, чем ответственные за систему или приложение; сущностями, или внутренними или внешними к организации, где система или приложение находятся. См. *Common Control*.
Security Control Overlay Оверлей мер безопасности	См. *Overlay.*

Security Domain Домен безопасности [CNSSI 4009]	Домен, который реализует политику безопасности и администрируется отдельным должностным лицом.
Security Functionality Функциональность безопасности	Связанные с безопасностью особенности, функции, механизмы, сервисы, процедуры и архитектуры, реализованные в информационных системах или средах организаций, в которых работают эти системы.
Security Functions Функции безопасности	Аппаратные средства, программное обеспечение и/или встроенное микропрограммное обеспечение информационной системы, ответственные за осуществление политики безопасности системы и поддержание изоляции кода и данных, на которых базируется защита.
Security Impact Analysis Анализ воздействия на безопасность [CNSSI 4009]	Анализ, проводимый должностным лицом организации, чтобы определить степень, до которой изменения в информационной системе влияют на состояние безопасности системы.
Security Incident Инцидент безопасности	См. *Incident.*
Security Kernel Ядро безопасности [CNSSI 4009]	Аппаратные средства, встроенное микропрограммное обеспечение и программные элементы доверенной вычислительной базы, реализующие концепцию монитора обращений. Ядро безопасности должно быть посредником всего доступа, быть защищено от модификации и быть поддающимся проверке на корректность.
Security Label Метка безопасности	Средства, используемые чтобы связать ряд атрибутов безопасности с конкретным информационным объектом, как часть структуры данных для этого объекта.
Security Marking Маркирование безопасности	Средства, используемые чтобы связать ряд атрибутов безопасности с объектами в удобочитаемой форме, чтобы позволить организации основанное на процессе осуществление политик информационной безопасности.
Security Objective Цель безопасности, [FIPS 199]	Конфиденциальность, целостность или доступность.
Security Plan План обеспечения безопасности	Формальный документ, который представляет описание требований безопасности для информационной системы или программы информационной безопасности и описывает реализованные или планируемые меры безопасности для удовлетворения этим требованиям. См. *System Security Plan* или *Information Security Program Plan.*
Security Policy Политика безопасности [CNSSI 4009]	Набор критериев для обеспечения сервисами безопасности.
Security Policy Filter Фильтр политики безопасности	Аппаратный и/или программный компонент, который выполняет одну или более следующих функций: (i) проверка контента, чтобы гарантировать тип данных представленного контента; (ii) контроль контента, анализирующий представленный контент, чтобы проверить выполнение им определенной политики (например, разрешенный по сравнению с запрещенными конструкциями файлов и частями контента); (iii) средство проверки злонамеренного контента, которое оценивает контент вредоносного кода; (iv) средство проверки подозрительной активности, которое оценивает или выполняет контент безопасным способом, такой как песочница/взрывная камера и мониторы подозрительной активности; или (v) обеззараживание, очистка и преобразование контента, которое изменяет представленный контент, чтобы выполнить определенную политику.

Security Requirement Требование безопасности [FIPS 200, уточненный]	Требование, предъявленное к информационной системе или организации, которое получено из применимых законов, Правительственных распоряжений, директив, политик, стандартов, инструкций, нормативных актов, процедур и/или потребностей предназначения/деятельности, чтобы гарантировать конфиденциальность, целостность и доступность информации, которая обрабатывается, хранится или передается. Примечание: Требования безопасности могут использоваться в различных контекстах от высокоуровневых действий, связанных с политикой, до низкоуровневых действий, связанных с реализацией, в разработке систем и технических дисциплинах.
Security Service Сервис безопасности [CNSSI 4009]	Возможность, которая поддерживает одно или более требований безопасности (конфиденциальность, целостность, доступность). Примеры сервисов безопасности - ключевой менеджмент, контроль доступа и аутентификация.
Security-Relevant Information Информация, связанная с безопасностью	Любая информация в информационной системе, которая может потенциально влиять на применение функций безопасности или обеспечение сервисов безопасности таким образом, что это может иметь результат в отказе проведения в жизнь политики безопасности системы или поддержки изоляции кода и данных.
Senior Agency Information Security Officer Высшее должностное лицо агентства по информационной безопасности, [44 U.S.C., Sec. 3544]	Должностное лицо, ответственное за выполнение обязанностей Директора по информации в отношение FISMA и служащее основной связью Директора по информации с санкционирующими должностными лицами агентства, владельцами информационной системы и сотрудниками безопасности информационной системы. Примечание: организации, подчиненные федеральным агентствам, могут использовать термин Высшее должностное лицо по информационной безопасности или Директор по информационной безопасности, чтобы обозначить людей, занимающих позиции с обязанностями, подобными Высшему должностному лицу агентства по информационной безопасности.
Senior Agency Official for Privacy Высшее должностное лицо агентства по приватности	Высшее должностное лицо организации с полной ответственностью во всей организации за проблемы приватности информации.
Senior Information Security Officer Высшее должностное лицо по информационной безопасности	См. *Senior Agency Information Security Officer* .
Sensitive Information Чувствительная информация [CNSSI 4009, уточненный]	Информация, потеря, неправильное употребление или несанкционированный доступ или модификация которой могут оказать негативное воздействие на национальные интересы или проведение федеральных программ или приватность, на которую люди наделены правом в соответствии с 5 U.S.C. Раздел 552a (Закон о неприкосновенности частной жизни); она может не соответствовать специально определеным критериями, установленным Правительственным распоряжением или законом конгресса, чтобы являться классифицированной в интересах национальной обороны или внешней политики.
Sensitive Compartmented Information Чувствительная изолированная информация [CNSSI 4009]	Чувствительные данные относительно или полученные из источников, методов или аналитических процессов разведки, которые требуется обрабатывать в рамках формальных систем управления доступом, установленных Директором национальной разведки.
Service-Oriented Architecture Сервис-ориентированная архитектура	Набор принципов и методологий проектирования и разработки программного обеспечения в форме взаимодействующих сервисов. Эти сервисы - четко определенные бизнес-функции, которые созданы как компоненты программного обеспечения (то есть, дискретные части кода и/или структур данных), которые могут быть снова использованы для различного назначения.

Software Программное обеспечение [CNSSI 4009]	Компьютерные программы и связанные с ними данные, которые могут быть динамически записанными или измененными во время выполнения.
Spam Спам	Злоупотребление электронными системами обмена сообщениями, чтобы без разбора отправлять незапрашиваемые объемные сообщения.
Special Access Program Программа специального доступа [CNSSI 4009]	Программа, установленная для конкретного класса классифицированных данных, которая налагает требования защиты и доступа, которые превышают обычно требуемые для информации на таком уровне классификации.
Spyware Шпионящее программное обеспечение	Программное обеспечение, которое тайно или скрытно установлено в информационную систему, чтобы собирать информацию о людях или организациях без их ведома; тип вредоносного кода.
Subject Субъект	Человек, процесс или устройство, порождающие информацию, для передачи между объектами или изменения состояния системы. См. *Объект*.
Subsystem Подсистема	Основное подразделение или компонент информационной системы, состоящее из информации, информационных технологий и персонала, которое выполняет одну или более конкретные функции.
Supplemental Guidance Дополнительное руководство	Описания, используемые для предоставления дополнительной разъясняющей информации для мер безопасности или улучшений мер безопасности.
Supplementation Дополнение	Процесс добавления мер безопасности или улучшений мер безопасности в отношение базового набора мер безопасности, как часть процесса адаптации (во время выбора мер безопасности), чтобы соответственно удовлетворить потребности управления рисками организации.
Supply Chain Цепочка поставок [ISO 28001, уточненный]	Связанный набор ресурсов и процессов между множественными уровнями разработчиков, который начинается с определения источника продуктов и услуг и расширяется через проектирование, разработку, производство, обработку, отгрузку и поставку продуктов и услуг к получателю.
Supply Chain Element Элемент цепочки поставок	Продукт информационной технологии или компонент продукта, который содержит программируемую логику и который критически важен для функционирования информационной системы.
System Система	См. *Information System*.
System of Records Notice Уведомление о системе записей	Официальное публичное уведомление о системе (ах) записей организации, как требуется Законом о неприкосновенности частной жизни 1974, которое идентифицирует: (i) назначение системы записей; (ii) люди, охваченные информацией в системе записей; (iii) категории поддерживаемых записей о людях; и (iv) пути, по которым распределяется информация.
System Security Plan План обеспечения безопасности системы [NIST SP 800-18]	Формальный документ, который представляет описание требований безопасности для информационной системы и описывает реализованные или планируемые меры безопасности для удовлетворения этим требованиям.

System-Specific Security Control Мера безопасности, специфичная для системы	Мера безопасности для информационной системы, которая не определялась как общая мера безопасности или часть гибридной меры безопасности, которые должны быть реализованы в информационной системе.
Tailored Security Control Baseline Адаптированный базовый набор мер безопасности	Набор мер безопасности, являющийся результатом применения руководства адаптации к базовому набору мер безопасности. См. *Tailoring*.
Tailoring Адаптация	Процесс, посредством которого базовые наборы мер безопасности изменяются путем: (i) идентификации и определения общих мер безопасности; (ii) приложения объектовых особенностей при применении и реализации базовых мер безопасности; (iii) выбора компенсирующих мер безопасности; (iv) назначения конкретных значений к определенным организацией параметрам мер безопасности; (v) дополнения базовых наборов дополнительными мерами безопасности или улучшениями мер безопасности; и (vi) предоставления дополнительной уточняющей информации для реализации мер безопасности.
Threat Угроза [CNSSI 4009, уточненный]	Любое обстоятельство или событие с потенциалом к неблагоприятному воздействию на деятельность организации (включая предназначение, функции, имидж или репутацию), активы организации, людей, другие организации или Нацию через информационную систему посредством несанкционированного доступа, разрушения, раскрытия, модификации информации и/или отказа сервиса.
Threat Assessment Оценка угрозы [CNSSI 4009]	Формальное описание и оценка угрозы информационной системе.
Threat Source Источник угрозы [FIPS 200]	Намерение и метод, имеющие целью намеренное использование уязвимости или ситуации, и метод, который может случайно инициировать уязвимость. Синоним с агентом угрозы.
Trusted Path Доверенный путь	Механизм, посредством которого пользователь (через устройство ввода данных) может связаться непосредственно с функциями безопасности информационной системы с необходимой доверительностью, чтобы поддержать политику безопасности системы. Этот механизм может быть активирован только пользователем или функциями безопасности информационной системы и не может быть имитирован недоверенным программным обеспечением.
Trustworthiness Доверительность [CNSSI 4009]	Свойство человека или предприятия, которое предоставляет другим уверенность через квалификацию, возможности и надежность этой сущности, чтобы выполнить конкретные задачи и исполнить возложенные обязанности.
Trustworthiness Доверительность (Информационная система)	Степень, до которой информационная система (включая компоненты информационной технологии, которые используются, чтобы создать систему), как можно ожидать, сохранит конфиденциальность, целостность и доступность обрабатываемой, хранимой или передаваемой системой информации через полный спектр угроз. Доверенная информационная система - система, которая способна к действию в границах определенных уровней риска, несмотря на экологические разрушения, человеческие ошибки, структурные отказы и целеустремленные атаки, которые, как ожидается, могут произойти в среде её эксплуатации.

User Пользователь [CNSSI 4009, уточненный]	Человек, или (системный) процесс, действующий от имени человека, уполномоченный на доступ к информационной системе. См. *Organizational User* и *Non-Organizational User*.
Virtual Private Network Виртуальная частная сеть [CNSSI 4009]	Защищенное соединение информационной системы, использующее туннелирование, меры безопасности и преобразование адресов конечных точек, производящее впечатление выделенной линии.
Vulnerability Уязвимость [CNSSI 4009]	Недостаток в информационной системе, процедурах безопасности системы, внутренних мерах безопасности или реализации, который может быть использован или инициирован источником угрозы.
Vulnerability Analysis Анализ уязвимостей	См. *Vulnerability Assessment*.
Vulnerability Assessment Оценка уязвимостей [CNSSI 4009]	Систематизированное исследование информационной системы или продукта, позволяющее определить соответствие мер безопасности, идентифицировать недостатки безопасности, обеспечить данные, по которым можно предсказать эффективность предложенных мер безопасности, и подтвердить соответствие таких мер после реализации.
Whitelisting Белый лист	Процесс, используемый для идентификации: (i) программ, которые санкционированы для выполнения в информационной системе; или (ii) санкционированных Универсальных локаторов ресурсов (URL) /вебсайтов.

ПРИЛОЖЕНИЕ C

АКРОНИМЫ

ОБЩИЕ СОКРАЩЕНИЯ

APT	Advanced Persistent Threat - Постоянная развивающаяся угроза
CFR	Code of Federal Regulations - Свод федеральных нормативных актов
CIO	Chief Information Officer - Директор по информации
CISO	Chief Information Security Officer – Директор по информационной безопасности
CAVP	Cryptographic Algorithm Validation Program - Программа подтверждения соответствия криптографических алгоритмов
CMVP	Cryptographic Module Validation Program - Программа подтверждения соответствия криптографических модулей
CNSS	Committee on National Security Systems - Комитет по системам национальной безопасности
CPO	Chief Privacy Officer – Директор по приватности
CUI	Controlled Unclassified Information - Контролируемая некласифицированная информация
DCS	Distributed Control System - Распределенная система управления
DNS	Domain Name System – Система доменных имен
DoD	Department of Defense - Министерство обороны
FAR	Federal Acquisition Regulation - Федеральное регулирование приобретения
FEA	Federal Enterprise Architecture - Архитектура федерального предприятия
FICAM	Federal Identity, Credential and Access Management - Федеральные идентификационные данные, учетные данные и управление доступом
FIPP	Fair Information Practice Principles - Принципы честной информационной практики
FIPS	Federal Information Processing Standards - Федеральные стандарты обработки информации
FISMA	Federal Information Security Management Act - Закон об управлении безопасностью федеральной информации
HSPD	Homeland Security Presidential Directive - Президентская директива по безопасность отечества
ICS	Industrial Control System – Промышленная система управления
IEEE	Institute of Electrical and Electronics Engineers - Институт инженеров по электронике и радиотехнике
IPsec	Internet Protocol Security - Безопасность интернет протокола
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission - Международная организация по стандартизации/Международная электротехническая комиссия
ITL	Information Technology Laboratory - Лаборатория информационной технологии
LACS	Logical Access Control System - Система управления логическим доступом
LSI	Large-Scale Integration - Интеграция высокого уровня
NIST	National Institute of Standards and Technology - Национальный институт стандартов и технологий

NISTIR	National Institute of Standards and Technology Interagency or Internal Report - Межведомственный или внутренний отчет национального института стандартов и технологий
NSA	National Security Agency - Агентство национальной безопасности
NSTISSI	National Security Telecommunications and Information System Security Instruction - Инструкция по безопасности телекоммуникационных и информационных систем национальной безопасности
ODNI	Office of the Director of National Intelligence - Офис Директора национальной разведки
OMB	Office of Management and Budget - Министерство управления и бюджета
OPSEC	Operations Security – Эксплуатационная безопасность
PBX	Private Branch Exchange - Частная телефонная станция
PACS	Physical Access Control System - Система управления физическим доступом
PIA	Privacy Impact Assessment - Оценка воздействия на приватность
PII	Personally Identifiable Information – Персональная идентификационная информация
PIV	Personal Identity Verification – Подтверждение соответствия персональных идентификационных данных
PKI	Public Key Infrastructure - Инфраструктура публичных ключей
RBAC	Role-Based Access Control - Ролевой контроль доступа
RD	Restricted Data – Данные ограниченного доступа
RMF	Risk Management Framework - Основы управления риском
SAISO	Senior Agency Information Security Officer - Высший сотрудник агентства по информационной безопасности
SAMI	Sources And Methods Information - Информационные источники и методы
SAOP	Senior Agency Official for Privacy – Высшее должностное лицо агентства по приватности
SAP	Special Access Program - Программа специального доступа
SC	Security Category - Категория безопасности
SCADA	Supervisory Control and Data Acquisition - Диспетчерское управление и сбор данных
SCI	Sensitive Compartmented Information - Чувствительная изолированная Информация
SOA	Service-Oriented Architecture – Сервис-ориентированная архитектура
SORN	System of Records Notice - Уведомление системы записей
SP	Special Publication - Специальная публикация
TCP/IP	Transmission Control Protocol/Internet Protocol - Протокол управления передачей / интернет-протокол
USB	Universal Serial Bus - Универсальная последовательная шина
VoIP	Voice over Internet Protocol - Голосовой интернет-протокол
VPN	Virtual Private Network - Виртуальная частная сеть

ПРИЛОЖЕНИЕ D

БАЗОВЫЕ МЕРЫ БЕЗОПАСНОСТИ - СВОДКА

ИНФОРМАЦИОННЫЕ СИСТЕМЫ НИЗКОГО ВОЗДЕЙСТВИЯ, УМЕРЕННОГО ВОЗДЕЙСТВИЯ И ВЫСОКОГО ВОЗДЕЙСТВИЯ

Это приложение содержит базовые меры безопасности, которые представляют начальную точку в определении мер безопасности для информационных систем низкого воздействия, умеренного воздействия и высокого воздействия.[90] Три базовых набора мер безопасности являются по сути иерархическими относительно мер безопасности, используемых в этих базовых наборах.[91] Если мера безопасности выбрана для одного из базовых наборов, идентификатор семейства и номер меры безопасности перечислены в соответствующем столбце. Если мера безопасности не используется в определенном базовом наборе, она отмечается как «*Not Selected (не выбрана*)». Улучшения мер безопасности, когда используется дополнение мер, обозначены номером улучшения. Например, запись IR-2 (1) (2) в высоком базовом наборе для IR-2 указывает, что вторая мера безопасности из семейства «Реагирование на инциденты» была выбрана одновременно с улучшением мер безопасности (1) и (2). Некоторые меры безопасности и улучшения не используются ни в одном из базовых наборов мер в этом приложении, но доступны для использования организациями при необходимости. Эта ситуация возникает, например, когда результаты оценки степени риска указывают на потребность в дополнительных мерах безопасности или улучшениях мер, чтобы соответственно смягчить риск к деятельности и активам организации, людям, другим организациям и Нации.

Организации могут использовать рекомендуемое значение приоритетного кода, связанное с каждой мерой безопасности в базовых наборах, чтобы помочь в принятии упорядоченных решений по реализации мер безопасности (то есть, мера безопасности с Приоритетным кодом 1 [P1], имеет более высокий приоритет для реализации, чем мера безопасности с Приоритетным кодом 2 [P2]; мера безопасности с Приоритетным кодом 2 [P2] имеет более высокий приоритет для реализации, чем мера безопасности с Приоритетным кодом 3 [P3], а Приоритетный код 0 [P0] указывает, что мера безопасности нет выбрана ни в одном из базовых наборов). Это рекомендованное упорядочивание приоритетов помогает гарантировать, что меры безопасности, от которых зависят другие меры безопасности, реализуются вначале, таким образом, давая возможность организациям развернуть меры безопасности в более структурированном и упорядоченном способе в соответствии с доступными ресурсами. Реализация мер безопасности в последовательности приоритетных кодов не подразумевает какой-либо определенный уровень снижения риска, пока все меры безопасности в плане обеспечения безопасности не будут реализованы. Приоритетные коды используются только для упорядочивания реализации, а не для того, чтобы принять решения по выбору мер безопасности. Таблица D-1 резюмирует последовательности приоритетные кодов для мер безопасности базового уровня безопасности в Таблице D-2.

ТАБЛИЦА D-1: ПРИОРИТЕТНЫЕ КОДЫ МЕР БЕЗОПАСНОСТИ

Приоритетный код	Последовательность	Действие
Приоритетный код 1 **(P1)**	ПЕРВАЯ	P1 Мера безопасности реализуется первой.
Приоритетный код 2 **(P2)**	СЛЕДУЮЩАЯ	P2 Мера безопасности реализуется после реализации меры P1.
Приоритетный код 3 **(P3)**	ПОСЛЕДНЯЯ	P3 Мера безопасности реализуется после реализации мер P1 и P2.
Неустановленный Приоритетный код **(P0)**	НЕТ	Мера безопасности не выбрана ни в одном из базовых наборов мер.

[90] Полное описание всех мер безопасности представлено в Приложениях F и G. Кроме того, некоторые документы для отдельных базовых наборов мер безопасности (перечисленных в Приложениях 1, 2, и 3) доступны в http://csrc.nist.gov/publications. Сетевая версия каталога мер безопасности также доступна в http://web.nvd.nist.gov/view/800-53/home.

[91] Иерархическая природа применяется к требованиям безопасности каждой меры безопасности (то есть, основной меры безопасности плюс всех ее улучшений) в низком, умеренном и высоком уровне воздействия в том, что требования к мере безопасности для конкретного уровня воздействия (например, CP-4 *Проверка Плана действий при непредвиденных обстоятельствах* - Умеренно: CP 4 (1)) определяют более строгий набор требований безопасности для этой меры безопасности, чем следующий более низкий уровень воздействия той же самой меры безопасности (например, CP-4 *Проверка Плана действий при непредвиденных обстоятельствах* - Низко: CP 4).

Таблица D-2 представляет сводку мер безопасности и улучшений мер из Приложения F, которые были назначены начальным базовым наборам мер (то есть, низкому, умеренному и высокому). Последовательности приоритетных кодов для реализации мер безопасности и тех мер безопасности, которые были выбраны из Приложения F, также приведены в Таблице D-2. В дополнение к Таблице D-2, последовательности приоритетных кодов и базовые наборы мер безопасности аннотируются в секции «Приоритет и базовые наборы» сводного раздела, расположенного ниже каждой меры безопасности в Приложении F.

ТАБЛИЦА D-2: БАЗОВЫЕ НАБОРЫ МЕР БЕЗОПАСНОСТИ[92]

№ МЕРЫ	НАЗВАНИЕ МЕРЫ	ПРИОРИТЕТ	НАЧАЛЬНЫЙ БАЗОВЫЙ НАБОР МЕР		
			НИЗКИЙ	УМЕРЕННЫЙ	ВЫСОКИЙ
Контроль доступа					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Information Sharing	P2	Not Selected	AC-21	AC-21
AC-22	Publicly Accessible Content	P3	AC-22	AC-22	AC-22
AC-23	Data Mining Protection	P0	Not Selected	Not Selected	Not Selected
AC-24	Access Control Decisions	P0	Not Selected	Not Selected	Not Selected
AC-25	Reference Monitor	P0	Not Selected	Not Selected	Not Selected

[92] Базовые наборы мер безопасности в Таблице D-2 являются начальными базовыми наборами, выбираемыми организациями до проведения работ адаптации, описанных в Разделе 3.2. Базовые наборы мер обеспечения и приоритетные коды применимы только к системам, не относящимся к национальной безопасности. Базовые наборы мер безопасности для систем национальной безопасности включены в Инструкцию 1253 CNSS.

№ МЕРЫ	НАЗВАНИЕ МЕРЫ	ПРИОРИТЕТ	НАЧАЛЬНЫЙ БАЗОВЫЙ НАБОР МЕР		
			НИЗКИЙ	УМЕРЕННЫЙ	ВЫСОКИЙ
Освоение и подготовка					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness Training	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Role-Based Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	**Withdrawn**	---	---	---	---
Аудит и подконтрольность					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Audit Events	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	P2	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
AU-15	Alternate Audit Capability	P0	Not Selected	Not Selected	Not Selected
AU-16	Cross-Organizational Auditing	P0	Not Selected	Not Selected	Not Selected
Оценка и санкционирование безопасности					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	System Interconnections	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	**Withdrawn**	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P2	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Penetration Testing	P2	Not Selected	Not Selected	CA-8
CA-9	Internal System Connections	P2	CA-9	CA-9	CA-9
Управление конфигурацией					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)

№ МЕРЫ	НАЗВАНИЕ МЕРЫ	ПРИОРИТЕТ	НАЧАЛЬНЫЙ БАЗОВЫЙ НАБОР МЕР		
			НИЗКИЙ	УМЕРЕННЫЙ	ВЫСОКИЙ
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11
	Планирование действий в чрезвычайных ситуациях				
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	**Withdrawn**	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-11	Alternate Communications Protocols	P0	Not Selected	Not Selected	Not Selected
CP-12	Safe Mode	P0	Not Selected	Not Selected	Not Selected
CP-13	Alternative Security Mechanisms	P0	Not Selected	Not Selected	Not Selected
	Идентификация и аутентификация				
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IA-9	Service Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-10	Adaptive Identification and Authentication	P0	Not Selected	Not Selected	Not Selected
IA-11	Re-authentication	P0	Not Selected	Not Selected	Not Selected
	Реагирование на инциденты				
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)

№ МЕРЫ	НАЗВАНИЕ МЕРЫ	ПРИОРИТЕТ	НАЧАЛЬНЫЙ БАЗОВЫЙ НАБОР МЕР		
			НИЗКИЙ	УМЕРЕННЫЙ	ВЫСОКИЙ
IR-3	Incident Response Testing	P2	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	P3	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8	IR-8
IR-9	Information Spillage Response	P0	Not Selected	Not Selected	Not Selected
IR-10	Integrated Information Security Analysis Team	P0	Not Selected	Not Selected	Not Selected
	Поддержка				
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	P2	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	P3	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	P2	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	Maintenance Personnel	P2	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	P2	Not Selected	MA-6	MA-6
	Защита носителей				
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	MP-1
MP-2	Media Access	P1	MP-2	MP-2	MP-2
MP-3	Media Marking	P2	Not Selected	MP-3	MP-3
MP-4	Media Storage	P1	Not Selected	MP-4	MP-4
MP-5	Media Transport	P1	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	P1	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Media Use	P1	MP-7	MP-7 (1)	MP-7 (1)
MP-8	Media Downgrading	P0	Not Selected	Not Selected	Not Selected
	Физическая защита и защита окружения				
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2	PE-2	PE-2
PE-3	Physical Access Control	P1	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	P2	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-7	**Withdrawn**	---	---	---	---
PE-8	Visitor Access Records	P3	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	P1	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	P1	Not Selected	PE-10	PE-10
PE-11	Emergency Power	P1	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	P1	PE-12	PE-12	PE-12
PE-13	Fire Protection	P1	PE-13	PE-13 (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	P1	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	P2	PE-16	PE-16	PE-16

№ МЕРЫ	НАЗВАНИЕ МЕРЫ	ПРИОРИТЕТ	НАЧАЛЬНЫЙ БАЗОВЫЙ НАБОР МЕР		
			НИЗКИЙ	УМЕРЕННЫЙ	ВЫСОКИЙ
PE-17	Alternate Work Site	P2	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P3	Not Selected	Not Selected	PE-18
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
PE-20	Asset Monitoring and Tracking	P0	Not Selected	Not Selected	Not Selected
	Планирование				
PL-1	Security Planning Policy and Procedures	P1	PL-1	PL-1	PL-1
PL-2	System Security Plan	P1	PL-2	PL-2 (3)	PL-2 (3)
PL-3	**Withdrawn**	---	---	---	---
PL-4	Rules of Behavior	P2	PL-4	PL-4 (1)	PL-4 (1)
PL-5	**Withdrawn**	---	---	---	---
PL-6	**Withdrawn**	---	---	---	---
PL-7	Security Concept of Operations	P0	Not Selected	Not Selected	Not Selected
PL-8	Information Security Architecture	P1	Not Selected	PL-8	PL-8
PL-9	Central Management	P0	Not Selected	Not Selected	Not Selected
	Безопасность персонала				
PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
PS-2	Position Risk Designation	P1	PS-2	PS-2	PS-2
PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
PS-4	Personnel Termination	P1	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	P2	PS-5	PS-5	PS-5
PS-6	Access Agreements	P3	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	P1	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	P3	PS-8	PS-8	PS-8
	Оценка риска				
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	**Withdrawn**	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	Technical Surveillance Countermeasures Survey	P0	Not Selected	Not Selected	Not Selected
	Закупки систем и сервисов				
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	P1	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	P1	SA-3	SA-3	SA-3
SA-4	Acquisition Process	P1	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)
SA-5	Information System Documentation	P2	SA-5	SA-5	SA-5
SA-6	**Withdrawn**	---	---	---	---
SA-7	**Withdrawn**	---	---	---	---
SA-8	Security Engineering Principles	P1	Not Selected	SA-8	SA-8
SA-9	External Information System Services	P1	SA-9	SA-9 (2)	SA-9 (2)

№ МЕРЫ	НАЗВАНИЕ МЕРЫ	ПРИОРИТЕТ	НАЧАЛЬНЫЙ БАЗОВЫЙ НАБОР МЕР		
			НИЗКИЙ	УМЕРЕННЫЙ	ВЫСОКИЙ
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	P1	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P0	Not Selected	Not Selected	Not Selected
SA-14	Criticality Analysis	P0	Not Selected	Not Selected	Not Selected
SA-15	Development Process, Standards, and Tools	P2	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	P2	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	P1	Not Selected	Not Selected	SA-17
SA-18	Tamper Resistance and Detection	P0	Not Selected	Not Selected	Not Selected
SA-19	Component Authenticity	P0	Not Selected	Not Selected	Not Selected
SA-20	Customized Development of Critical Components	P0	Not Selected	Not Selected	Not Selected
SA-21	Developer Screening	P0	Not Selected	Not Selected	Not Selected
SA-22	Unsupported System Components	P0	Not Selected	Not Selected	Not Selected
	Защита систем и коммуникаций				
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Availability	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Transmission Confidentiality and Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	**Withdrawn**	---	---	---	---
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Cryptographic Protection	P1	SC-13	SC-13	SC-13
SC-14	**Withdrawn**	---	---	---	---
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P2	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	SC-21	SC-21	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	SC-22	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24

№ МЕРЫ	НАЗВАНИЕ МЕРЫ	ПРИОРИТЕТ	НАЧАЛЬНЫЙ БАЗОВЫЙ НАБОР МЕР		
			НИЗКИЙ	УМЕРЕННЫЙ	ВЫСОКИЙ
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Platform-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Concealment and Misdirection	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P0	Not Selected	Not Selected	Not Selected
SC-33	**Withdrawn**	---	---	---	---
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
SC-35	Honeyclients	P0	Not Selected	Not Selected	Not Selected
SC-36	Distributed Processing and Storage	P0	Not Selected	Not Selected	Not Selected
SC-37	Out-of-Band Channels	P0	Not Selected	Not Selected	Not Selected
SC-38	Operations Security	P0	Not Selected	Not Selected	Not Selected
SC-39	Process Isolation	P1	SC-39	SC-39	SC-39
SC-40	Wireless Link Protection	P0	Not Selected	Not Selected	Not Selected
SC-41	Port and I/O Device Access	P0	Not Selected	Not Selected	Not Selected
SC-42	Sensor Capability and Data	P0	Not Selected	Not Selected	Not Selected
SC-43	Usage Restrictions	P0	Not Selected	Not Selected	Not Selected
SC-44	Detonation Chambers	P0	Not Selected	Not Selected	Not Selected
	Целостность систем и информации				
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	P2	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	**Withdrawn**	---	---	---	---
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
SI-14	Non-Persistence	P0	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	P0	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	P1	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	P0	Not Selected	Not Selected	Not Selected

Таблицы от D-3 до D-19 представляют более подробную сводку мер безопасности и улучшений мер из Приложения F. Каждая таблица сосредотачивается на отдельном семействе мер безопасности. Следует учитывать, что Таблица D-2 включает только те меры безопасности и улучшения мер, которые определены для трёх базовых наборов мер безопасности, а Таблицы от D-3 до D-19 содержат все меры безопасности и улучшения мер для соответствующих семейств мер безопасности. Таблицы включают следующую информацию: (i) меры безопасности и улучшения мер, которые были выбраны для базовых наборов мер безопасности, обозначены как "x" в столбце для выбранного базового набора;[93] (ii) меры безопасности и улучшения мер, которые не были выбраны ни для одного базового набора мер безопасности (то есть, меры безопасности и улучшения мер, доступные для выбора, чтобы достчь большей защиты) обозначены пустыми ячейками в столбцах базовых наборов; (iii) меры безопасности и улучшения мер, которые были выбраны из Приложения F, обозначены как "x" в столбце «WITHDRAWN (изъята)»; и (iv) меры безопасности и улучшения мер, у которых есть связанные с доверием характеристики или свойства (то есть, связанные с доверием меры безопасности) обозначены как "x" в столбце «ASSURANCE (доверие)». Меры безопасности, связанные с доверием, обсуждены более подробно в Приложении E, включая назначение этих мер безопасности базовым наборам мер безопасности (см. Таблицы E-1 через E-3).

[93] Базовые меры безопасности в Таблицах от D-3 до D-19 применимы только к системам, не относящимся к национальной безопасности. Базовые меры безопасности для систем национальной безопасности включены в Инструкцию 1253 CNSS.

ТАБЛИЦА D-3: МЕРЫ БЕЗОПАСНОСТИ КОНТРОЛЯ ДОСТУПА – СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-1	**Access Control Policy and Procedures**		x	x	x	x
AC-2	**Account Management**			x	x	x
AC-2(1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*				x	x
AC-2(2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*				x	x
AC-2(3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*				x	x
AC-2(4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*				x	x
AC-2(5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*					x
AC-2(6)	*ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT*					
AC-2(7)	*ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES*					
AC-2(8)	*ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION*					
AC-2(9)	*ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED / GROUPS ACCOUNTS*					
AC-2(10)	*ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*					
AC-2(11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*					x
AC-2(12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*					x
AC-2(13)	*ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS*					x
AC-3	**Access Enforcement**			x	x	x
AC-3(1)	*ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS*	x	Incorporated into AC-6.			
AC-3(2)	*ACCESS ENFORCEMENT | DUAL AUTHORIZATION*					
AC-3(3)	*ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL*					
AC-3(4)	*ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL*					
AC-3(5)	*ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION*					
AC-3(6)	*ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION*	x	Incorporated into MP-4 and SC-28.			
AC-3(7)	*ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL*					
AC-3(8)	*ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*					
AC-3(9)	*ACCESS ENFORCEMENT | CONTROLLED RELEASE*					
AC-3(10)	*ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS*					
AC-4	**Information Flow Enforcement**				x	x
AC-4(1)	*INFORMATION FLOW ENFORCEMENT | OBJECT SECURITY ATTRIBUTES*					
AC-4(2)	*INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS*					
AC-4(3)	*INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL*					
AC-4(4)	*INFORMATION FLOW ENFORCEMENT | CONTENT CHECK ENCRYPTED INFORMATION*					
AC-4(5)	*INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES*					
AC-4(6)	*INFORMATION FLOW ENFORCEMENT | METADATA*					
AC-4(7)	*INFORMATION FLOW ENFORCEMENT | ONE-WAY FLOW MECHANISMS*					
AC-4(8)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTERS*					
AC-4(9)	*INFORMATION FLOW ENFORCEMENT | HUMAN REVIEWS*					
AC-4(10)	*INFORMATION FLOW ENFORCEMENT | ENABLE / DISABLE SECURITY POLICY FILTERS*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-4(11)	*INFORMATION FLOW ENFORCEMENT | CONFIGURATION OF SECURITY POLICY FILTERS*					
AC-4(12)	*INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS*					
AC-4(13)	*INFORMATION FLOW ENFORCEMENT | DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS*					
AC-4(14)	*INFORMATION FLOW ENFORCEMENT | SECURITY POLICY FILTER CONSTRAINTS*					
AC-4(15)	*INFORMATION FLOW ENFORCEMENT | DETECTION OF UNSANCTIONED INFORMATION*					
AC-4(16)	*INFORMATION FLOW ENFORCEMENT | INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS*	x	Incorporated into AC-4.			
AC-4(17)	*INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*					
AC-4(18)	*INFORMATION FLOW ENFORCEMENT | SECURITY ATTRIBUTE BINDING*					
AC-4(19)	*INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA*					
AC-4(20)	*INFORMATION FLOW ENFORCEMENT | APPROVED SOLUTIONS*					
AC-4(21)	*INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*					
AC-4(22)	*INFORMATION FLOW ENFORCEMENT | ACCESS ONLY*					
AC-5	**Separation of Duties**				x	x
AC-6	**Least Privilege**				x	x
AC-6(1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*				x	x
AC-6(2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*				x	x
AC-6(3)	*LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*					x
AC-6(4)	*LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*					
AC-6(5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*				x	x
AC-6(6)	*LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*					
AC-6(7)	*LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*					
AC-6(8)	*LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*					
AC-6(9)	*LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*				x	x
AC-6(10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*				x	x
AC-7	**Unsuccessful Logon Attempts**			x	x	x
AC-7(1)	*UNSUCCESSFUL LOGON ATTEMPTS | AUTOMATIC ACCOUNT LOCK*	x	Incorporated into AC-7.			
AC-7(2)	*UNSUCCESSFUL LOGON ATTEMPTS | PURGE / WIPE MOBILE DEVICE*					
AC-8	**System Use Notification**			x	x	x
AC-9	**Previous Logon (Access) Notification**					
AC-9(1)	*PREVIOUS LOGON NOTIFICATION | UNSUCCESSFUL LOGONS*					
AC-9(2)	*PREVIOUS LOGON NOTIFICATION | SUCCESSFUL / UNSUCCESSFUL LOGONS*					
AC-9(3)	*PREVIOUS LOGON NOTIFICATION | NOTIFICATION OF ACCOUNT CHANGES*					
AC-9(4)	*PREVIOUS LOGON NOTIFICATION | ADDITIONAL LOGON INFORMATION*					
AC-10	**Concurrent Session Control**					x
AC-11	**Session Lock**				x	x
AC-11(1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*				x	x
AC-12	**Session Termination**				x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-12(1)	*SESSION TERMINATION | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*					
AC-13	**Supervision and Review — Access Control**	x	Incorporated into AC-2 and AU-6.			
AC-14	**Permitted Actions without Identification or Authentication**			x	x	x
AC-14(1)	*PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | NECESSARY USES*	x	Incorporated into AC-14.			
AC-15	**Automated Marking**	x	Incorporated into MP-3.			
AC-16	**Security Attributes**					
AC-16(1)	*SECURITY ATTRIBUTES | DYNAMIC ATTRIBUTE ASSOCIATION*					
AC-16(2)	*SECURITY ATTRIBUTES | ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS*					
AC-16(3)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY INFORMATION SYSTEM*					
AC-16(4)	*SECURITY ATTRIBUTES | ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS*					
AC-16(5)	*SECURITY ATTRIBUTES | ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES*					
AC-16(6)	*SECURITY ATTRIBUTES | MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION*					
AC-16(7)	*SECURITY ATTRIBUTES | CONSISTENT ATTRIBUTE INTERPRETATION*					
AC-16(8)	*SECURITY ATTRIBUTES | ASSOCIATION TECHNIQUES / TECHNOLOGIES*					
AC-16(9)	*SECURITY ATTRIBUTES | ATTRIBUTE REASSIGNMENT*					
AC-16(10)	*SECURITY ATTRIBUTES | ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS*					
AC-17	**Remote Access**			x	x	x
AC-17(1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*				x	x
AC-17(2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*				x	x
AC-17(3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*				x	x
AC-17(4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*				x	x
AC-17(5)	*REMOTE ACCESS | MONITORING FOR UNAUTHORIZED CONNECTIONS*	x	Incorporated into SI-4.			
AC-17(6)	*REMOTE ACCESS | PROTECTION OF INFORMATION*					
AC-17(7)	*REMOTE ACCESS | ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS*	x	Incorporated into AC-3(10).			
AC-17(8)	*REMOTE ACCESS | DISABLE NONSECURE NETWORK PROTOCOLS*	x	Incorporated into CM-7.			
AC-17(9)	*REMOTE ACCESS | DISCONNECT / DISABLE ACCESS*					
AC-18	**Wireless Access**			x	x	x
AC-18(1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*				x	x
AC-18(2)	*WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS*	x	Incorporated into SI-4.			
AC-18(3)	*WIRELESS ACCESS | DISABLE WIRELESS NETWORKING*					
AC-18(4)	*WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*					x
AC-18(5)	*WIRELESS ACCESS | ANTENNAS / TRANSMISSION POWER LEVELS*					x
AC-19	**Access Control for Mobile Devices**			x	x	x
AC-19(1)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF WRITABLE / PORTABLE STORAGE DEVICES*	x	Incorporated into MP-7.			
AC-19(2)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES*	x	Incorporated into MP-7.			
AC-19(3)	*ACCESS CONTROL FOR MOBILE DEVICES | USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER*	x	Incorporated into MP-7.			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AC-19(4)	*ACCESS CONTROL FOR MOBILE DEVICES* | *RESTRICTIONS FOR CLASSIFIED INFORMATION*					
AC-19(5)	*ACCESS CONTROL FOR MOBILE DEVICES* | *FULL DEVICE / CONTAINER-BASED ENCRYPTION*				x	x
AC-20	**Use of External Information Systems**			x	x	x
AC-20(1)	*USE OF EXTERNAL INFORMATION SYSTEMS* | *LIMITS ON AUTHORIZED USE*				x	x
AC-20(2)	*USE OF EXTERNAL INFORMATION SYSTEMS* | *PORTABLE STORAGE DEVICES*				x	x
AC-20(3)	*USE OF EXTERNAL INFORMATION SYSTEMS* | *NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES*					
AC-20(4)	*USE OF EXTERNAL INFORMATION SYSTEMS* | *NETWORK ACCESSIBLE STORAGE DEVICES*					
AC-21	**Information Sharing**				x	x
AC-21(1)	*INFORMATION SHARING* | *AUTOMATED DECISION SUPPORT*					
AC-21(2)	*INFORMATION SHARING* | *INFORMATION SEARCH AND RETRIEVAL*					
AC-22	**Publicly Accessible Content**			x	x	x
AC-23	**Data Mining Protection**					
AC-24	**Access Control Decisions**					
AC-24(1)	*ACCESS CONTROL DECISIONS* | *TRANSMIT ACCESS AUTHORIZATION INFORMATION*					
AC-24(2)	*ACCESS CONTROL DECISIONS* | *NO USER OR PROCESS IDENTITY*					
AC-25	**Reference Monitor**		x			

ТАБЛИЦА D-4: МЕРЫ БЕЗОПАСНОСТИ ОСВОЕНИЯ И ПОДГОТОВКИ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AT-1	**Security Awareness and Training Policy and Procedures**		x	x	x	x
AT-2	**Security Awareness Training**		x	x	x	x
AT-2(1)	*SECURITY AWARENESS | PRACTICAL EXERCISES*		x			
AT-2(2)	*SECURITY AWARENESS | INSIDER THREAT*		x		x	x
AT-3	**Role-Based Security Training**		x	x	x	x
AT-3(1)	*ROLE-BASED SECURITY TRAINING | ENVIRONMENTAL CONTROLS*		x			
AT-3(2)	*ROLE-BASED SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*		x			
AT-3(3)	*ROLE-BASED SECURITY TRAINING | PRACTICAL EXERCISES*		x			
AT-3(4)	*ROLE-BASED SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR*		x			
AT-4	**Security Training Records**		x	x	x	x
AT-5	**Contacts with Security Groups and Associations**	x	Incorporated into PM-15.			

ТАБЛИЦА D-5: МЕРЫ БЕЗОПАСНОСТИ АУДИТА И ПОДКОНТРОЛЬНОСТИ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AU-1	**Audit and Accountability Policy and Procedures**		x	x	x	x
AU-2	**Audit Events**			x	x	x
AU-2(1)	*AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES*	x	Incorporated into AU-12.			
AU-2(2)	*AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT*	x	Incorporated into AU-12.			
AU-2(3)	*AUDIT EVENTS | REVIEWS AND UPDATES*				x	x
AU-2(4)	*AUDIT EVENTS | PRIVILEGED FUNCTIONS*	x	Incorporated into AC-6(9).			
AU-3	**Content of Audit Records**			x	x	x
AU-3(1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*				x	x
AU-3(2)	*CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*					x
AU-4	**Audit Storage Capacity**			x	x	x
AU-4(1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*					
AU-5	**Response to Audit Processing Failures**			x	x	x
AU-5(1)	*RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY*					x
AU-5(2)	*RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS*					x
AU-5(3)	*RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS*					
AU-5(4)	*RESPONSE TO AUDIT PROCESSING FAILURES | SHUTDOWN ON FAILURE*					
AU-6	**Audit Review, Analysis, and Reporting**		x	x	x	x
AU-6(1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*		x		x	x
AU-6(2)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUTOMATED SECURITY ALERTS*	x	Incorporated into SI-4.			
AU-6(3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*		x		x	x
AU-6(4)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CENTRAL REVIEW AND ANALYSIS*		x			
AU-6(5)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*		x			x
AU-6(6)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*		x			x
AU-6(7)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PERMITTED ACTIONS*		x			
AU-6(8)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS*		x			
AU-6(9)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES*		x			
AU-6(10)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | AUDIT LEVEL ADJUSTMENT*		x			
AU-7	**Audit Reduction and Report Generation**		x		x	x
AU-7(1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*		x		x	x
AU-7(2)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC SORT AND SEARCH*					
AU-8	**Time Stamps**			x	x	x
AU-8(1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*				x	x
AU-8(2)	*TIME STAMPS | SECONDARY AUTHORITATIVE TIME SOURCE*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
AU-9	**Protection of Audit Information**			x	x	x
AU-9(1)	*PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE* MEDIA					
AU-9(2)	*PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*					x
AU-9(3)	*PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*					x
AU-9(4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*				x	x
AU-9(5)	*PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION*					
AU-9(6)	*PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS*					
AU-10	**Non-repudiation**		x			x
AU-10(1)	*NON-REPUDIATION | ASSOCIATION OF IDENTITIES*		x			
AU-10(2)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY*		x			
AU-10(3)	*NON-REPUDIATION | CHAIN OF CUSTODY*		x			
AU-10(4)	*NON-REPUDIATION | VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY*		x			
AU-10(5)	*NON-REPUDIATION | DIGITAL SIGNATURES*	x	Incorporated into SI-7.			
AU-11	**Audit Record Retention**			x	x	x
AU-11(1)	*AUDIT RECORD RETENTION | LONG-TERM RETRIEVAL CAPABILITY*		x			
AU-12	**Audit Generation**			x	x	x
AU-12(1)	*AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL*					x
AU-12(2)	*AUDIT GENERATION | STANDARDIZED FORMATS*					
AU-12(3)	*AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*					x
AU-13	**Monitoring for Information Disclosure**		x			
AU-13(1)	*MONITORING FOR INFORMATION DISCLOSURE | USE OF AUTOMATED TOOLS*		x			
AU-13(2)	*MONITORING FOR INFORMATION DISCLOSURE | REVIEW OF MONITORED SITES*		x			
AU-14	**Session Audit**		x			
AU-14(1)	*SESSION AUDIT | SYSTEM START-UP*		x			
AU-14(2)	*SESSION AUDIT | CAPTURE/RECORD AND LOG CONTENT*		x			
AU-14(3)	*SESSION AUDIT | REMOTE VIEWING / LISTENING*		x			
AU-15	**Alternate Audit Capability**					
AU-16	**Cross-Organizational Auditing**					
AU-16(1)	*CROSS-ORGANIZATIONAL AUDITING | IDENTITY PRESERVATION*					
AU-16(2)	*CROSS-ORGANIZATIONAL AUDITING | SHARING OF AUDIT INFORMATION*					

ТАБЛИЦА D-6: МЕРЫ БЕЗОПАСНОСТИ ОЦЕНКИ И САНКЦИОНИРОВАНИЯ БЕЗОПАСНОСТИ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CA-1	**Security Assessment and Authorization Policies and Procedures**		x	x	x	x
CA-2	**Security Assessments**		x	x	x	x
CA-2(1)	*SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*		x		x	x
CA-2(2)	*SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*		x			x
CA-2(3)	*SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS*		x			
CA-3	**System Interconnections**		x	x	x	x
CA-3(1)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3(2)	*SYSTEM INTERCONNECTIONS | CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3(3)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS*					
CA-3(4)	*SYSTEM INTERCONNECTIONS | CONNECTIONS TO PUBLIC NETWORKS*					
CA-3(5)	*SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*				x	x
CA-4	**Security Certification**	x	Incorporated into CA-2.			
CA-5	**Plan of Action and Milestones**		x	x	x	x
CA-5(1)	*PLAN OF ACTION AND MILESTONES | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*		x			
CA-6	**Security Authorization**		x	x	x	x
CA-7	**Continuous Monitoring**		x	x	x	x
CA-7(1)	*CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*		x		x	x
CA-7(2)	*CONTINUOUS MONITORING | TYPES OF ASSESSMENTS*	x	Incorporated into CA-2.			
CA-7(3)	*CONTINUOUS MONITORING | TREND ANALYSES*		x			
CA-8	**Penetration Testing**		x			x
CA-8(1)	*PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM*		x			
CA-8(2)	*PENETRATION TESTING | RED TEAM EXERCISES*		x			
CA-9	**Internal System Connections**		x	x	x	x
CA-9(1)	*INTERNAL SYSTEM CONNECTIONS | SECURITY COMPLIANCE CHECKS*		x			

ТАБЛИЦА D-7: МЕРЫ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CM-1	**Configuration Management Policy and Procedures**		x	x	x	x
CM-2	**Baseline Configuration**		x	x	x	x
CM-2(1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*		x		x	x
CM-2(2)	*BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*		x			x
CM-2(3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*		x		x	x
CM-2(4)	*BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE*	x	Incorporated into CM-7.			
CM-2(5)	*BASELINE CONFIGURATION | AUTHORIZED SOFTWARE*	x	Incorporated into CM-7.			
CM-2(6)	*BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS*		x			
CM-2(7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*		x		x	x
CM-3	**Configuration Change Control**		x		x	x
CM-3(1)	*CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*		x			x
CM-3(2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*		x		x	x
CM-3(3)	*CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION*					
CM-3(4)	*CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE*					
CM-3(5)	*CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE*					
CM-3(6)	*CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHY MANAGEMENT*					
CM-4	**Security Impact Analysis**		x	x	x	x
CM-4(1)	*SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*		x			x
CM-4(2)	*SECURITY IMPACT ANALYSIS | VERIFICATION OF SECURITY FUNCTIONS*		x			
CM-5	**Access Restrictions for Change**				x	x
CM-5(1)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*					x
CM-5(2)	*ACCESS RESTRICTIONS FOR CHANGE | REVIEW SYSTEM CHANGES*					x
CM-5(3)	*ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*					x
CM-5(4)	*ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION*					
CM-5(5)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES*					
CM-5(6)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES*					
CM-5(7)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS*	x	Incorporated into SI-7.			
CM-6	**Configuration Settings**			x	x	x
CM-6(1)	*CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*					x
CM-6(2)	*CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*					x
CM-6(3)	*CONFIGURATION SETTINGS | UNAUTHORIZED CHANGE DETECTION*	x	Incorporated into SI-7.			
CM-6(4)	*CONFIGURATION SETTINGS | CONFORMANCE DEMONSTRATION*	x	Incorporated into CM-4.			
CM-7	**Least Functionality**			x	x	x
CM-7(1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*				x	x
CM-7(2)	*LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*				x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CM-7(3)	*LEAST FUNCTIONALITY | REGISTRATION COMPLIANCE*					
CM-7(4)	*LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE / BLACKLISTING*				X	
CM-7(5)	*LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING*					X
CM-8	**Information System Component Inventory**		X	X	X	X
CM-8(1)	*INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*		X		X	X
CM-8(2)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*		X			X
CM-8(3)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*		X		X	X
CM-8(4)	*INFORMATION SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*		X			X
CM-8(5)	*INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS*		X		X	X
CM-8(6)	*INFORMATION SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS / APPROVED DEVIATIONS*		X			
CM-8(7)	*INFORMATION SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY*		X			
CM-8(8)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING*		X			
CM-8(9)	*INFORMATION SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS*		X			
CM-9	**Configuration Management Plan**				X	X
CM-9(1)	*CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY*					
CM-10	**Software Usage Restrictions**			X	X	X
CM-10(1)	*SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE*					
CM-11	**User-Installed Software**			X	X	X
CM-11(1)	*USER-INSTALLED SOFTWARE | ALERTS FOR UNAUTHORIZED INSTALLATIONS*					
CM-11(2)	*USER-INSTALLED SOFTWARE | PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS*					

ТАБЛИЦА D-8: МЕРЫ БЕЗОПАСНОСТИ ПЛАНИРОВАНИЯ ДЕЙСТВИЙ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**		x	x	x	x
CP-2	**Contingency Plan**			x	x	x
CP-2(1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*				x	x
CP-2(2)	*CONTINGENCY PLAN | CAPACITY PLANNING*					x
CP-2(3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*				x	x
CP-2(4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					x
CP-2(6)	*CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE*					
CP-2(7)	*CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS*					
CP-2(8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*				x	x
CP-3	**Contingency Training**		x	x	x	x
CP-3(1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*		x			x
CP-3(2)	*CONTINGENCY TRAINING | AUTOMATED TRAINING ENVIRONMENTS*		x			
CP-4	**Contingency Plan Testing**		x	x	x	x
CP-4(1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		x		x	x
CP-4(2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*		x			x
CP-4(3)	*CONTINGENCY PLAN TESTING | AUTOMATED TESTING*		x			
CP-4(4)	*CONTINGENCY PLAN TESTING | FULL RECOVERY / RECONSTITUTION*		x			
CP-5	**Contingency Plan Update**	x	Incorporated into CP-2.			
CP-6	**Alternate Storage Site**				x	x
CP-6(1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-6(2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*					x
CP-6(3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*				x	x
CP-7	**Alternate Processing Site**				x	x
CP-7(1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*				x	x
CP-7(2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*				x	x
CP-7(3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*				x	x
CP-7(4)	*ALTERNATE PROCESSING SITE | PREPARATION FOR USE*					x
CP-7(5)	*ALTERNATE PROCESSING SITE | EQUIVALENT INFORMATION SECURITY SAFEGUARDS*	x	Incorporated into CP-7.			
CP-7(6)	*ALTERNATE PROCESSING SITE | INABILITY TO RETURN TO PRIMARY SITE*					
CP-8	**Telecommunications Services**				x	x
CP-8(1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*				x	x
CP-8(2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*				x	x
CP-8(3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*					x
CP-8(4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*					x
CP-8(5)	*TELECOMMUNICATIONS SERVICES | ALTERNATE TELECOMMUNICATION SERVICE TESTING*					
CP-9	**Information System Backup**			x	x	x
CP-9(1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*				x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
CP-9(2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*					X
CP-9(3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*					X
CP-9(4)	*INFORMATION SYSTEM BACKUP | PROTECTION FROM UNAUTHORIZED MODIFICATION*	X	Incorporated into CP-9.			
CP-9(5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE STORAGE SITE*					X
CP-9(6)	*INFORMATION SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM*					
CP-9(7)	*INFORMATION SYSTEM BACKUP | DUAL AUTHORIZATION*					
CP-10	**Information System Recovery and Reconstitution**			X	X	X
CP-10(1)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | CONTINGENCY PLAN TESTING*	X	Incorporated into CP-4.			
CP-10(2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*				X	X
CP-10(3)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPENSATING SECURITY CONTROLS*	X	Addressed by tailoring procedures.			
CP-10(4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*					X
CP-10(5)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | FAILOVER CAPABILITY*	X	Incorporated into SI-13.			
CP-10(6)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | COMPONENT PROTECTION*					
CP-11	**Alternate Communications Protocols**					
CP-12	**Safe Mode**		X			
CP-13	**Alternative Security Mechanisms**					

ТАБЛИЦА D-9: МЕРЫ БЕЗОПАСНОСТИ ИДЕНТИФИКАЦЦИИ И АУТЕНТИФИКАЦИИ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IA-1	**Identification and Authentication Policy and Procedures**		x	x	x	x
IA-2	**Identification and Authentication(Organizational Users)**			x	x	x
IA-2(1)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*			x	x	x
IA-2(2)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*				x	x
IA-2(3)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*				x	x
IA-2(4)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*					x
IA-2(5)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | GROUP AUTHENTICATION*					
IA-2(6)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE*					
IA-2(7)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE*					
IA-2(8)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*				x	x
IA-2(9)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*					x
IA-2(10)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON*					
IA-2(11)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS - SEPARATE DEVICE*				x	x
IA-2(12)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS*			x	x	x
IA-2(13)	*IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION*					
IA-3	**Device Identification and Authentication**				x	x
IA-3(1)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*					
IA-3(2)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION*	x	Incorporated into IA-3(1).			
IA-3(3)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION*					
IA-3(4)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*					
IA-4	**Identifier Management**			x	x	x
IA-4(1)	*IDENTIFIER MANAGEMENT | PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS*					
IA-4(2)	*IDENTIFIER MANAGEMENT | SUPERVISOR AUTHORIZATION*					
IA-4(3)	*IDENTIFIER MANAGEMENT | MULTIPLE FORMS OF CERTIFICATION*					
IA-4(4)	*IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*					
IA-4(5)	*IDENTIFIER MANAGEMENT | DYNAMIC MANAGEMENT*					
IA-4(6)	*IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT*					
IA-4(7)	*IDENTIFIER MANAGEMENT | IN-PERSON REGISTRATION*					
IA-5	**Authenticator Management**			x	x	x

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IA-5(1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*			x	x	x
IA-5(2)	*AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*				x	x
IA-5(3)	*AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*				x	x
IA-5(4)	*AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION*					
IA-5(5)	*AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY*					
IA-5(6)	*AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS*					
IA-5(7)	*AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS*					
IA-5(8)	*AUTHENTICATOR MANAGEMENT | MULTIPLE INFORMATION SYSTEM ACCOUNTS*					
IA-5(9)	*AUTHENTICATOR MANAGEMENT | CROSS-ORGANIZATION CREDENTIAL MANAGEMENT*					
IA-5(10)	*AUTHENTICATOR MANAGEMENT | DYNAMIC CREDENTIAL ASSOCIATION*					
IA-5(11)	*AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*			x	x	x
IA-5(12)	*AUTHENTICATOR MANAGEMENT | BIOMETRIC-DASED AUTHENTICATION*					
IA-5(13)	*AUTHENTICATOR MANAGEMENT | EXPIRATION OF CACHED AUTHENTICATORS*					
IA-5(14)	*AUTHENTICATOR MANAGEMENT | MANAGING CONTENT OF PKI TRUST STORES*					
IA-5(15)	*AUTHENTICATOR MANAGEMENT | FICAM-APPROVED PRODUCTS AND SERVICES*					
IA-6	**Authenticator Feedback**			x	x	x
IA-7	**Cryptographic Module Authentication**			x	x	x
IA-8	**Identification and Authentication (Non-Organizational Users)**			x	x	x
IA-8(1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*			x	x	x
IA-8(2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*			x	x	x
IA-8(3)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS*			x	x	x
IA-8(4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-ISSUED PROFILES*			x	x	x
IA-8(5)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV-I CREDENTIALS*					
IA-9	**Service Identification and Authentication**					
IA-9(1)	*SERVICE IDENTIFICATION AND AUTHENTICATION | INFORMATION EXCHANGE*					
IA-9(2)	*SERVICE IDENTIFICATION AND AUTHENTICATION | TRANSMISSION OF DECISIONS*					
IA-10	**Adaptive Identification and Authentication**					
IA-11	**Re-authentication**					

ТАБЛИЦА D-10: МЕРЫ БЕЗОПАСНОСТИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
IR-1	**Incident Response Policy and Procedures**		x	x	x	x
IR-2	**Incident Response Training**		x	x	x	x
IR-2(1)	*INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*		x			x
IR-2(2)	*INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*		x			x
IR-3	**Incident Response Testing**		x		x	x
IR-3(1)	*INCIDENT RESPONSE TESTING | AUTOMATED TESTING*		x			
IR-3(2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*		x		x	x
IR-4	**Incident Handling**			x	x	x
IR-4(1)	*INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*				x	x
IR-4(2)	*INCIDENT HANDLING | DYNAMIC RECONFIGURATION*					
IR-4(3)	*INCIDENT HANDLING | CONTINUITY OF OPERATIONS*					
IR-4(4)	*INCIDENT HANDLING | INFORMATION CORRELATION*					x
IR-4(5)	*INCIDENT HANDLING | AUTOMATIC DISABLING OF INFORMATION SYSTEM*					
IR-4(6)	*INCIDENT HANDLING | INSIDER THREATS - SPECIFIC CAPABILITIES*					
IR-4(7)	*INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION COORDINATION*					
IR-4(8)	*INCIDENT HANDLING | CORRELATION WITH EXTERNAL ORGANIZATIONS*					
IR-4(9)	*INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY*					
IR-4(10)	*INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*					
IR-5	**Incident Monitoring**		x	x	x	x
IR-5(1)	*INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*		x			x
IR-6	**Incident Reporting**			x	x	x
IR-6(1)	*INCIDENT REPORTING | AUTOMATED REPORTING*				x	x
IR-6(2)	*INCIDENT REPORTING | VULNERABILITIES RELATED TO INCIDENTS*					
IR-6(3)	*INCIDENT REPORTING | COORDINATION WITH SUPPLY CHAIN*					
IR-7	**Incident Response Assistance**			x	x	x
IR-7(1)	*INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*				x	x
IR-7(2)	*INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*					
IR-8	**Incident Response Plan**			x	x	x
IR-9	**Information Spillage Response**					
IR-9(1)	*INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL*					
IR-9(2)	*INFORMATION SPILLAGE RESPONSE | TRAINING*					
IR-9(3)	*INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS*					
IR-9(4)	*INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL*					
IR-10	**Integrated Information Security Analysis Team**					

ТАБЛИЦА D-11: МЕРЫ БЕЗОПАСНОСТИ ПОДДЕРЖКИ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MA-1	**System Maintenance Policy and Procedures**		x	x	x	x
MA-2	**Controlled Maintenance**			x	x	x
MA-2(1)	*CONTROLLED MAINTENANCE | RECORD CONTENT*	x	Incorporated into MA-2.			
MA-2(2)	*CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*					x
MA-3	**Maintenance Tools**				x	x
MA-3(1)	*MAINTENANCE TOOLS | INSPECT TOOLS*				x	x
MA-3(2)	*MAINTENANCE TOOLS | INSPECT MEDIA*				x	x
MA-3(3)	*MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*					x
MA-3(4)	*MAINTENANCE TOOLS | RESTRICTED TOOL USE*					
MA-4	**Nonlocal Maintenance**			x	x	x
MA-4(1)	*NONLOCAL MAINTENANCE | AUDITING AND REVIEW*					
MA-4(2)	*NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*				x	x
MA-4(3)	*NONLOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*					x
MA-4(4)	*NONLOCAL MAINTENANCE | AUTHENTICATION / SEPARATION OF MAINTENANCE SESSIONS*					
MA-4(5)	*NONLOCAL MAINTENANCE | APPROVALS AND NOTIFICATIONS*					
MA-4(6)	*NONLOCAL MAINTENANCE | CRYPTOGRAPHIC PROTECTION*					
MA-4(7)	*NONLOCAL MAINTENANCE | REMOTE DISCONNECT VERIFICATION*					
MA-5	**Maintenance Personnel**			x	x	x
MA-5(1)	*MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*					x
MA-5(2)	*MAINTENANCE PERSONNEL | SECURITY CLEARANCES FOR CLASSIFIED SYSTEMS*					
MA-5(3)	*MAINTENANCE PERSONNEL | CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS*					
MA-5(4)	*MAINTENANCE PERSONNEL | FOREIGN NATIONALS*					
MA-5(5)	*MAINTENANCE PERSONNEL | NON-SYSTEM-RELATED MAINTENANCE*					
MA-6	**Timely Maintenance**				x	x
MA-6(1)	*TIMELY MAINTENANCE | PREVENTIVE MAINTENANCE*					
MA-6(2)	*TIMELY MAINTENANCE | PREDICTIVE MAINTENANCE*					
MA-6(3)	*TIMELY MAINTENANCE | AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE*					

ТАБЛИЦА D-12: МЕРЫ БЕЗОПАСНОСТИ ЗАЩИТЫ НОСИТЕЛЕЙ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MP-1	**Media Protection Policy and Procedures**		x	x	x	x
MP-2	**Media Access**			x	x	x
MP-2(1)	*MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS*	x	Incorporated into MP-4(2).			
MP-2(2)	*MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28(1).			
MP-3	**Media Marking**				x	x
MP-4	**Media Storage**				x	x
MP-4(1)	*MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28(1).			
MP-4(2)	*MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS*					
MP-5	**Media Transport**				x	x
MP-5(1)	*MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS*	x	Incorporated into MP-5.			
MP-5(2)	*MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES*	x	Incorporated into MP-5.			
MP-5(3)	*MEDIA TRANSPORT | CUSTODIANS*					
MP-5(4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*				x	x
MP-6	**Media Sanitization**			x	x	x
MP-6(1)	*MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*					x
MP-6(2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*					x
MP-6(3)	*MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*					x
MP-6(4)	*MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6(5)	*MEDIA SANITIZATION | CLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6(6)	*MEDIA SANITIZATION | MEDIA DESTRUCTION*	x	Incorporated into MP-6.			
MP-6(7)	*MEDIA SANITIZATION | DUAL AUTHORIZATION*					
MP-6(8)	*MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION*					
MP-7	**Media Use**			x	x	x
MP-7(1)	*MEDIA USE | PROHIBIT USE WITHOUT OWNER*				x	x
MP-7(2)	*MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA*					
MP-8	**Media Downgrading**					
MP-8(1)	*MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS*					
MP-8(2)	*MEDIA DOWNGRADING | EQUIPMENT TESTING*					
MP-8(3)	*MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION*					
MP-8(4)	*MEDIA DOWNGRADING | CLASSIFIED INFORMATION*					

ТАБЛИЦА D-13: МЕРЫ БЕЗОПАСНОСТИ ФИЗИЧЕСКАЯ ЗАЩИТА И ЗАЩИТА ОКРУЖЕНИЯ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-1	**Physical and Environmental Protection Policy and Procedures**		x	x	x	x
PE-2	**Physical Access Authorizations**			x	x	x
PE-2(1)	*PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE*					
PE-2(2)	*PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION*					
PE-2(3)	*PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS*					
PE-3	**Physical Access Control**			x	x	x
PE-3(1)	*PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*					x
PE-3(2)	*PHYSICAL ACCESS CONTROL | FACILITY / INFORMATION SYSTEM BOUNDARIES*					
PE-3(3)	*PHYSICAL ACCESS CONTROL | CONTINUOUS GUARDS / ALARMS / MONITORING*					
PE-3(4)	*PHYSICAL ACCESS CONTROL | LOCKABLE CASINGS*					
PE-3(5)	*PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*					
PE-3(6)	*PHYSICAL ACCESS CONTROL | FACILITY PENETRATION TESTING*					
PE-4	**Access Control for Transmission Medium**				x	x
PE-5	**Access Control for Output Devices**				x	x
PE-5(1)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS*					
PE-5(2)	*ACCESS CONTROL FOR OUTPUT DEVICES | ACCESS TO OUTPUT BY INDIVIDUAL IDENTITY*					
PE-5(3)	*ACCESS CONTROL FOR OUTPUT DEVICES | MARKING OUTPUT DEVICES*					
PE-6	**Monitoring Physical Access**		x	x	x	x
PE-6(1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*		x		x	x
PE-6(2)	*MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*		x			
PE-6(3)	*MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE*		x			
PE-6(4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*		x			x
PE-7	**Visitor Control**	x	Incorporated into PE-2 and PE-3.			
PE-8	**Visitor Access Records**		x	x	x	x
PE-8(1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*					x
PE-8(2)	*VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS*	x	Incorporated into PE-2.			
PE-9	**Power Equipment and Cabling**				x	x
PE-9(1)	*POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*					
PE-9(2)	*POWER EQUIPMENT AND CABLING | AUTOMATIC VOLTAGE CONTROLS*					
PE-10	**Emergency Shutoff**				x	x
PE-10(1)	*EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION*	x	Incorporated into PE-10.			
PE-11	**Emergency Power**				x	x
PE-11(1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*					x
PE-11(2)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-12	**Emergency Lighting**			x	x	x
PE-12(1)	*EMERGENCY LIGHTING | ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*					
PE-13	**Fire Protection**			x	x	x
PE-13(1)	*FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*					x
PE-13(2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*					x
PE-13(3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*				x	x
PE-13(4)	*FIRE PROTECTION | INSPECTIONS*					
PE-14	**Temperature and Humidity Controls**			x	x	x
PE-14(1)	*TEMPERATURE AND HUMIDITY CONTROLS | AUTOMATIC CONTROLS*					
PE-14(2)	*TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS*					
PE-15	**Water Damage Protection**			x	x	x
PE-15(1)	*WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*					x
PE-16	**Delivery and Removal**			x	x	x
PE-17	**Alternate Work Site**				x	x
PE-18	**Location of Information System Components**					x
PE-18(1)	*LOCATION OF INFORMATION SYSTEM COMPONENTS | FACILITY SITE*					
PE-19	**Information Leakage**					
PE-19(1)	*INFORMATION LEAKAGE | NATIONAL EMISSIONS / TEMPEST POLICIES AND PROCEDURES*					
PE-20	**Asset Monitoring and Tracking**					

ТАБЛИЦА D-14: МЕРЫ БЕЗОПАСНОСТИ ПЛАНИРОВАНИЯ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PL-1	**Security Planning Policy and Procedures**		x	x	x	x
PL-2	**System Security Plan**		x	x	x	x
PL-2(1)	*SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS*	x	Incorporated into PL-7.			
PL-2(2)	*SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE*	x	Incorporated into PL-8.			
PL-2(3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*		x		x	x
PL-3	**System Security Plan Update**	x	Incorporated into PL-2.			
PL-4	**Rules of Behavior**		x	x	x	x
PL-4(1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*		x		x	x
PL-5	**Privacy Impact Assessment**	x	Incorporated into Appendix J, AR-2.			
PL-6	**Security-Related Activity Planning**	x	Incorporated into PL-2.			
PL-7	**Security Concept of Operations**					
PL-8	**Information Security Architecture**		x		x	x
PL-8(1)	*INFORMATION SECURITY ARCHITECTURE | DEFENSE-IN-DEPTH*		x			
PL-8(2)	*INFORMATION SECURITY ARCHITECTURE | SUPPLIER DIVERSITY*		x			
PL-9	**Central Management**		x			

ТАБЛИЦА D-15: МЕРЫ БЕЗОПАСНОСТИ ПЕРСОНАЛА - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PS-1	**Personnel Security Policy and Procedures**		x	x	x	x
PS-2	**Position Risk Designation**			x	x	x
PS-3	**Personnel Screening**			x	x	x
PS-3(1)	*PERSONNEL SCREENING | CLASSIFIED INFORMATION*					
PS-3(2)	*PERSONNEL SCREENING | FORMAL INDOCTRINATION*					
PS-3(3)	*PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES*					
PS-4	**Personnel Termination**			x	x	x
PS-4(1)	*PERSONNEL TERMINATION | POST-EMPLOYMENT REQUIREMENTS*					
PS-4(2)	*PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*					x
PS-5	**Personnel Transfer**			x	x	x
PS-6	**Access Agreements**		x	x	x	x
PS-6(1)	*ACCESS AGREEMENTS | INFORMATION REQUIRING SPECIAL PROTECTION*	x	Incorporated into PS-3.			
PS-6(2)	*ACCESS AGREEMENTS | CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION*		x			
PS-6(3)	*ACCESS AGREEMENTS | POST-EMPLOYMENT REQUIREMENTS*		x			
PS-7	**Third-Party Personnel Security**		x	x	x	x
PS-8	**Personnel Sanctions**			x	x	x

ТАБЛИЦА D-16: МЕРЫ БЕЗОПАСНОСТИ ОЦЕНКИ РИСКА - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
RA-1	**Risk Assessment Policy and Procedures**		x	x	x	x
RA-2	**Security Categorization**			x	x	x
RA-3	**Risk Assessment**		x	x	x	x
RA-4	**Risk Assessment Update**	x	Incorporated into RA-3.			
RA-5	**Vulnerability Scanning**		x	x	x	x
RA-5(1)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*		x		x	x
RA-5(2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*		x		x	x
RA-5(3)	*VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE*		x			
RA-5(4)	*VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*		x			x
RA-5(5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*		x		x	x
RA-5(6)	*VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*		x			
RA-5(7)	*VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS*	x	Incorporated into CM-8.			
RA-5(8)	*VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS*		x			
RA-5(9)	*VULNERABILITY SCANNING | PENETRATION TESTING AND ANALYSES*	x	Incorporated into CA-8.			
RA-5(10)	*VULNERABILITY SCANNING | CORRELATE SCANNING INFORMATION*		x			
RA-6	**Technical Surveillance Countermeasures Survey**		x			

ТАБЛИЦА D-17: МЕРЫ БЕЗОПАСНОСТИ ЗАКУПКИ СИСТЕМ И СЕРВИСОВ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-1	**System and Services Acquisition Policy and Procedures**		x	x	x	x
SA-2	**Allocation of Resources**		x	x	x	x
SA-3	**System Development Life Cycle**		x	x	x	x
SA-4	**Acquisition Process**		x	x	x	x
SA-4(1)	*ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*		x		x	x
SA-4(2)	*ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*		x		x	x
SA-4(3)	*ACQUISITION PROCESS | DEVELOPMENT METHODS / TECHNIQUES / PRACTICES*		x			
SA-4(4)	*ACQUISITION PROCESS | ASSIGNMENT OF COMPONENTS TO SYSTEMS*	x	Incorporated into CM-8(9).			
SA-4(5)	*ACQUISITION PROCESS | SYSTEM / COMPONENT / SERVICE CONFIGURATIONS*		x			
SA-4(6)	*ACQUISITION PROCESS | USE OF INFORMATION ASSURANCE PRODUCTS*		x			
SA-4(7)	*ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*		x			
SA-4(8)	*ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN*		x			
SA-4(9)	*ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*		x		x	x
SA-4(10)	*ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*		x	x	x	x
SA-5	**Information System Documentation**		x	x	x	x
SA-5(1)	*INFORMATION SYSTEM DOCUMENTATION | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*	x	Incorporated into SA-4(1).			
SA-5(2)	*INFORMATION SYSTEM DOCUMENTATION | SECURITY-RELEVANT EXTERNAL SYSTEM INTERFACES*	x	Incorporated into SA-4(2).			
SA-5(3)	*INFORMATION SYSTEM DOCUMENTATION | HIGH-LEVEL DESIGN*	x	Incorporated into SA-4(2).			
SA-5(4)	*INFORMATION SYSTEM DOCUMENTATION | LOW-LEVEL DESIGN*	x	Incorporated into SA-4(2).			
SA-5(5)	*INFORMATION SYSTEM DOCUMENTATION | SOURCE CODE*	x	Incorporated into SA-4(2).			
SA-6	**Software Usage Restrictions**	x	Incorporated into CM-10 and SI-7.			
SA-7	**User-Installed Software**	x	Incorporated into CM-11 and SI-7.			
SA-8	**Security Engineering Principles**		x		x	x
SA-9	**External Information System Services**		x	x	x	x
SA-9(1)	*EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS*		x			
SA-9(2)	*EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*		x		x	x
SA-9(3)	*EXTERNAL INFORMATION SYSTEMS | ESTABLISH / MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*		x			
SA-9(4)	*EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*		x			
SA-9(5)	*EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*		x			
SA-10	**Developer Configuration Management**		x		x	x
SA-10(1)	*DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION*		x			
SA-10(2)	*DEVELOPER CONFIGURATION MANAGEMENT | ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES*		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-10(3)	*DEVELOPER CONFIGURATION MANAGEMENT | HARDWARE INTEGRITY VERIFICATION*		X			
SA-10(4)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED GENERATION*		X			
SA-10(5)	*DEVELOPER CONFIGURATION MANAGEMENT | MAPPING INTEGRITY FOR VERSION CONTROL*		X			
SA-10(6)	*DEVELOPER CONFIGURATION MANAGEMENT | TRUSTED DISTRIBUTION*		X			
SA-11	**Developer Security Testing and Evaluation**		X		X	X
SA-11(1)	*DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS*		X			
SA-11(2)	*DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES*		X			
SA-11(3)	*DEVELOPER SECURITY TESTING AND EVALUATION | INDEPENDENT VERIFICATION OF ASSESSMENT PLANS / EVIDENCE*		X			
SA-11(4)	*DEVELOPER SECURITY TESTING AND EVALUATION | MANUAL CODE REVIEWS*		X			
SA-11(5)	*DEVELOPER SECURITY TESTING AND EVALUATION | PENETRATION TESTING*		X			
SA-11(6)	*DEVELOPER SECURITY TESTING AND EVALUATION | ATTACK SURFACE REVIEWS*		X			
SA-11(7)	*DEVELOPER SECURITY TESTING AND EVALUATION | VERIFY SCOPE OF TESTING / EVALUATION*		X			
SA-11(8)	*DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS*		X			
SA-12	**Supply Chain Protection**		X			X
SA-12(1)	*SUPPLY CHAIN PROTECTION | ACQUISITION STRATEGIES / TOOLS / METHODS*		X			
SA-12(2)	*SUPPLY CHAIN PROTECTION | SUPPLIER REVIEWS*		X			
SA-12(3)	*SUPPLY CHAIN PROTECTION | TRUSTED SHIPPING AND WAREHOUSING*	X	Incorporated into SA-12(1).			
SA-12(4)	*SUPPLY CHAIN PROTECTION | DIVERSITY OF SUPPLIERS*	X	Incorporated into SA-12(13).			
SA-12(5)	*SUPPLY CHAIN PROTECTION | LIMITATION OF HARM*		X			
SA-12(6)	*SUPPLY CHAIN PROTECTION | MINIMIZING PROCUREMENT TIME*	X	Incorporated into SA-12(1).			
SA-12(7)	*SUPPLY CHAIN PROTECTION | ASSESSMENTS PRIOR TO SELECTION / ACCEPTANCE / UPDATE*		X			
SA-12(8)	*SUPPLY CHAIN PROTECTION | USE OF ALL-SOURCE INTELLIGENCE*		X			
SA-12(9)	*SUPPLY CHAIN PROTECTION | OPERATIONS SECURITY*		X			
SA-12(10)	*SUPPLY CHAIN PROTECTION | VALIDATE AS GENUINE AND NOT ALTERED*		X			
SA-12(11)	*SUPPLY CHAIN PROTECTION | PENETRATION TESTING / ANALYSIS OF ELEMENTS, PROCESSES, AND ACTORS*		X			
SA-12(12)	*SUPPLY CHAIN PROTECTION | INTER-ORGANIZATIONAL AGREEMENTS*		X			
SA-12(13)	*SUPPLY CHAIN PROTECTION | CRITICAL INFORMATION SYSTEM COMPONENTS*		X			
SA-12(14)	*SUPPLY CHAIN PROTECTION | IDENTITY AND TRACEABILITY*		X			
SA-12(15)	*SUPPLY CHAIN PROTECTION | PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES*		X			
SA-13	**Trustworthiness**		X			
SA-14	**Criticality Analysis**		X			
SA-14(1)	*CRITICALITY ANALYSIS | CRITICAL COMPONENTS WITH NO VIABLE ALTERNATIVE SOURCING*	X	Incorporated into SA-20.			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-15	**Development Process, Standards, and Tools**		x			x
SA-15(1)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | QUALITY METRICS*		x			
SA-15(2)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | SECURITY TRACKING TOOLS*		x			
SA-15(3)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*		x			
SA-15(4)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING / VULNERABILITY ANALYSIS*		x			
SA-15(5)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION*		x			
SA-15(6)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CONTINUOUS IMPROVEMENT*		x			
SA-15(7)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | AUTOMATED VULNERABILITY ANALYSIS*		x			
SA-15(8)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT / VULNERABILITY INFORMATION*		x			
SA-15(9)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | USE OF LIVE DATA*		x			
SA-15(10)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | INCIDENT RESPONSE PLAN*		x			
SA-15(11)	*DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ARCHIVE INFORMATION SYSTEM / COMPONENT*		x			
SA-16	**Developer-Provided Training**		x			x
SA-17	**Developer Security Architecture and Design**		x			x
SA-17(1)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL POLICY MODEL*		x			
SA-17(2)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | SECURITY-RELEVANT COMPONENTS*		x			
SA-17(3)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | FORMAL CORRESPONDENCE*		x			
SA-17(4)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | INFORMAL CORRESPONDENCE*		x			
SA-17(5)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | CONCEPTUALLY SIMPLE DESIGN*		x			
SA-17(6)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING*		x			
SA-17(7)	*DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR LEAST PRIVILEGE*		x			
SA-18	**Tamper Resistance and Detection**		x			
SA-18(1)	*TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC*		x			
SA-18(2)	*TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES*		x			
SA-19	**Component Authenticity**		x			
SA-19(1)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*		x			
SA-19(2)	*COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE / REPAIR*		x			
SA-19(3)	*COMPONENT AUTHENTICITY | COMPONENT DISPOSAL*		x			
SA-19(4)	*COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING*		x			
SA-20	**Customized Development of Critical Components**		x			
SA-21	**Developer Screening**		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SA-21(1)	*DEVELOPER SCREENING | VALIDATION OF SCREENING*		X			
SA-22	**Unsupported System Components**		X			
SA-22(1)	*UNSUPPORTED SYSTEM COMPONENTS | ALTERNATIVE SOURCES FOR CONTINUED SUPPORT*		X			

ТАБЛИЦА D-18: МЕРЫ БЕЗОПАСНОСТИ ЗАЩИТЫ СИСТЕМ И КОММУНИКАЦИЙ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-1	**System and Communications Protection Policy and Procedures**		x	x	x	x
SC-2	**Application Partitioning**		x		x	x
SC-2(1)	*APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS*		x			
SC-3	**Security Function Isolation**		x			x
SC-3(1)	*SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION*		x			
SC-3(2)	*SECURITY FUNCTION ISOLATION | ACCESS / FLOW CONTROL FUNCTIONS*		x			
SC-3(3)	*SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY*		x			
SC-3(4)	*SECURITY FUNCTION ISOLATION | MODULE COUPLING AND COHESIVENESS*		x			
SC-3(5)	*SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES*		x			
SC-4	**Information in Shared Resources**				x	x
SC-4(1)	*INFORMATION IN SHARED RESOURCES | SECURITY LEVELS*	x	Incorporated into SC-4.			
SC-4(2)	*INFORMATION IN SHARED RESOURCES | PERIODS PROCESSING*					
SC-5	**Denial of Service Protection**			x	x	x
SC-5(1)	*DENIAL OF SERVICE PROTECTION | RESTRICT INTERNAL USERS*					
SC-5(2)	*DENIAL OF SERVICE PROTECTION | EXCESS CAPACITY / BANDWIDTH / REDUNDANCY*					
SC-5(3)	*DENIAL OF SERVICE PROTECTION | DETECTION / MONITORING*					
SC-6	**Resource Availability**		x			
SC-7	**Boundary Protection**			x	x	x
SC-7(1)	*BOUNDARY PROTECTION | PHYSICALLY SEPARATED SUBNETWORKS*	x	Incorporated into SC-7.			
SC-7(2)	*BOUNDARY PROTECTION | PUBLIC ACCESS*	x	Incorporated into SC-7.			
SC-7(3)	*BOUNDARY PROTECTION | ACCESS POINTS*				x	x
SC-7(4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*				x	x
SC-7(5)	*BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*				x	x
SC-7(6)	*BOUNDARY PROTECTION | RESPONSE TO RECOGNIZED FAILURES*	x	Incorporated into SC-7(18).			
SC-7(7)	*BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*				x	x
SC-7(8)	*BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*					x
SC-7(9)	*BOUNDARY PROTECTION | RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC*					
SC-7(10)	*BOUNDARY PROTECTION | PREVENT UNAUTHORIZED EXFILTRATION*					
SC-7(11)	*BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC*					
SC-7(12)	*BOUNDARY PROTECTION | HOST-BASED PROTECTION*					
SC-7(13)	*BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*					
SC-7(14)	*BOUNDARY PROTECTION | PROTECTS AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS*					
SC-7(15)	*BOUNDARY PROTECTION | ROUTE PRIVILEGED NETWORK ACCESSES*					
SC-7(16)	*BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS / DEVICES*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-7(17)	*BOUNDARY PROTECTION | AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS*					
SC-7(18)	*BOUNDARY PROTECTION | FAIL SECURE*		x			x
SC-7(19)	*BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS*					
SC-7(20)	*BOUNDARY PROTECTION | DYNAMIC ISOLATION / SEGREGATION*					
SC-7(21)	*BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*		x			x
SC-7(22)	*BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS*		x			
SC-7(23)	*BOUNDARY PROTECTION | DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE*					
SC-8	**Transmission Confidentiality and Integrity**				x	x
SC-8(1)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*				x	x
SC-8(2)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PRE / POST TRANSMISSION HANDLING*					
SC-8(3)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS*					
SC-8(4)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL / RANDOMIZE COMMUNICATIONS*					
SC-9	**Transmission Confidentiality**	x	Incorporated into SC-8.			
SC-10	**Network Disconnect**				x	x
SC-11	**Trusted Path**		x			
SC-11(1)	*TRUSTED PATH | LOGICAL ISOLATION*		x			
SC-12	**Cryptographic Key Establishment and Management**			x	x	x
SC-12(1)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*					x
SC-12(2)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*					
SC-12(3)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*					
SC-12(4)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES*	x	Incorporated into SC-12.			
SC-12(5)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | PKI CERTIFICATES / HARDWARE TOKENS*	x	Incorporated into SC-12.			
SC-13	**Cryptographic Protection**			x	x	x
SC-13(1)	*CRYPTOGRAPHIC PROTECTION | FIPS-VALIDATED CRYPTOGRAPHY*	x	Incorporated into SC-13.			
SC-13(2)	*CRYPTOGRAPHIC PROTECTION | NSA-APPROVED CRYPTOGRAPHY*	x	Incorporated into SC-13.			
SC-13(3)	*CRYPTOGRAPHIC PROTECTION | INDIVIDUALS WITHOUT FORMAL ACCESS APPROVALS*	x	Incorporated into SC-13.			
SC-13(4)	*CRYPTOGRAPHIC PROTECTION | DIGITAL SIGNATURES*	**x**	Incorporated into SC-13.			
SC-14	**Public Access Protections**	**x**	Capability provided by AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10.			
SC-15	**Collaborative Computing Devices**			x	x	x
SC-15(1)	*COLLABORATIVE COMPUTING DEVICES | PHYSICAL DISCONNECT*					
SC-15(2)	*COLLABORATIVE COMPUTING DEVICES | BLOCKING INBOUND / OUTBOUND COMMUNICATIONS TRAFFIC*	x	Incorporated into SC-7.			
SC-15(3)	*COLLABORATIVE COMPUTING DEVICES | DISABLING / REMOVAL IN SECURE WORK AREAS*					

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-15(4)	*COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS*					
SC-16	**Transmission of Security Attributes**					
SC-16(1)	*TRANSMISSION OF SECURITY ATTRIBUTES | INTEGRITY VALIDATION*					
SC-17	**Public Key Infrastructure Certificates**				x	x
SC-18	**Mobile Code**				x	x
SC-18(1)	*MOBILE CODE | IDENTIFY UNACCEPTABLE CODE / TAKE CORRECTIVE ACTIONS*					
SC-18(2)	*MOBILE CODE | ACQUISITION / DEVELOPMENT / USE*					
SC-18(3)	*MOBILE CODE | PREVENT DOWNLOADING / EXECUTION*					
SC-18(4)	*MOBILE CODE | PREVENT AUTOMATIC EXECUTION*					
SC-18(5)	*MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS*					
SC-19	**Voice Over Internet Protocol**				x	x
SC-20	**Secure Name /Address Resolution Service (Authoritative Source)**			x	x	x
SC-20(1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | CHILD SUBSPACES*	x	Incorporated into SC-20.			
SC-20(2)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | DATA ORIGIN / INTEGRITY*					
SC-21	**Secure Name /Address Resolution Service (Recursive or Caching Resolver)**			x	x	x
SC-21(1)	*SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | DATA ORIGIN / INTEGRITY*	x	Incorporated into SC-21.			
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**			x	x	x
SC-23	**Session Authenticity**				x	x
SC-23(1)	*SESSION AUTHENTICITY | INVALIDATE SESSION IDENTIFIERS AT LOGOUT*					
SC-23(2)	*SESSION AUTHENTICITY | USER-INITIATED LOGOUTS / MESSAGE DISPLAYS*	x	Incorporated into AC-12(1).			
SC-23(3)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*					
SC-23(4)	*SESSION AUTHENTICITY | UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION*	x	Incorporated into SC-23(3).			
SC-23(5)	*SESSION AUTHENTICITY | ALLOWED CERTIFICATE AUTHORITIES*					
SC-24	**Fail in Known State**		x			x
SC-25	**Thin Nodes**					
SC-26	**Honeypots**					
SC-26(1)	*HONEYPOTS | DETECTION OF MALICIOUS CODE*	x	Incorporated into SC-35.			
SC-27	**Platform-Independent Applications**					
SC-28	**Protection of Information at Rest**				x	x
SC-28(1)	*PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION*					
SC-28(2)	*PROTECTION OF INFORMATION AT REST | OFF-LINE STORAGE*					
SC-29	**Heterogeneity**		x			
SC-29(1)	*HETEROGENEITY | VIRTUALIZATION TECHNIQUES*		x			
SC-30	**Concealment and Misdirection**		x			
SC-30(1)	*CONCEALMENT AND MISDIRECTION | VIRTUALIZATION TECHNIQUES*	x	Incorporated into SC-29(1).			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SC-30(2)	*CONCEALMENT AND MISDIRECTION | RANDOMNESS*		x			
SC-30(3)	*CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING / STORAGE LOCATIONS*		x			
SC-30(4)	*CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*		x			
SC-30(5)	*CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*		x			
SC-31	**Covert Channel Analysis**		x			
SC-31(1)	*COVERT CHANNEL ANALYSIS | TEST COVERT CHANNELS FOR EXPLOITABILITY*		x			
SC-31(2)	*COVERT CHANNEL ANALYSIS | MAXIMUM BANDWIDTH*		x			
SC-31(3)	*COVERT CHANNEL ANALYSIS | MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS*		x			
SC-32	**Information System Partitioning**		x			
SC-33	**Transmission Preparation Integrity**	x	Incorporated into SC-8.			
SC-34	**Non-Modifiable Executable Programs**		x			
SC-34(1)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE*		x			
SC-34(2)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION / READ-ONLY MEDIA*		x			
SC-34(3)	*NON-MODIFIABLE EXECUTABLE PROGRAMS | HARDWARE-BASED PROTECTION*		x			
SC-35	**Honeyclients**					
SC-36	**Distributed Processing and Storage**		x			
SC-36(1)	*DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES*		x			
SC-37	**Out-of-Band Channels**		x			
SC-37(1)	*OUT-OF-BAND CHANNELS | ENSURE DELIVERY / TRANSMISSION*		x			
SC-38	**Operations Security**		x			
SC-39	**Process Isolation**		x	x	x	x
SC-39(1)	*PROCESS ISOLATION | HARDWARE SEPARATION*		x			
SC-39(2)	*PROCESS ISOLATION | THREAD ISOLATION*		x			
SC-40	**Wireless Link Protection**					
SC-40(1)	*WIRELESS LINK PROTECTION | ELECTROMAGNETIC INTERFERENCE*					
SC-40(2)	*WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL*					
SC-40(3)	*WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION*					
SC-40(4)	*WIRELESS LINK PROTECTION | SIGNAL PARAMETER IDENTIFICATION*					
SC-41	**Port and I/O Device Access**					
SC-42	**Sensor Capability and Data**					
SC-42(1)	*SENSOR CAPABILITY AND DATA | REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES*					
SC-42(2)	*SENSOR CAPABILITY AND DATA | AUTHORIZED USE*					
SC-42(3)	*SENSOR CAPABILITY AND DATA | PROHIBIT USE OF DEVICES*					
SC-43	**Usage Restrictions**					
SC-44	**Detonation Chambers**					

ТАБЛИЦА D-19: МЕРЫ БЕЗОПАСНОСТИ ЦЕЛОСТНОСТИ СИСТЕМ И ИНФОРМАЦИИ - СВОДКА

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-1	**System and Information Integrity Policy and Procedures**		x	x	x	x
SI-2	**Flaw Remediation**			x	x	x
SI-2(1)	*FLAW REMEDIATION | CENTRAL MANAGEMENT*					x
SI-2(2)	*FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*				x	x
SI-2(3)	*FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS*					
SI-2(4)	*FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS*	x	Incorporated into SI-2.			
SI-2(5)	*FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES*					
SI-2(6)	*FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE*					
SI-3	**Malicious Code Protection**			x	x	x
SI-3(1)	*MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*				x	x
SI-3(2)	*MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*				x	x
SI-3(3)	*MALICIOUS CODE PROTECTION | NON-PRIVILEGED USERS*	x	Incorporated into AC-6(10).			
SI-3(4)	*MALICIOUS CODE PROTECTION | UPDATES ONLY BY PRIVILEGED USERS*					
SI-3(5)	*MALICIOUS CODE PROTECTION | PORTABLE STORAGE DEVICES*	x	Incorporated into MP-7.			
SI-3(6)	*MALICIOUS CODE PROTECTION | TESTING / VERIFICATION*					
SI-3(7)	*MALICIOUS CODE PROTECTION | NONSIGNATURE-BASED DETECTION*					
SI-3(8)	*MALICIOUS CODE PROTECTION | DETECT UNAUTHORIZED COMMANDS*					
SI-3(9)	*MALICIOUS CODE PROTECTION | AUTHENTICATE REMOTE COMMANDS*					
SI-3(10)	*MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS*					
SI-4	**Information System Monitoring**		x	x	x	x
SI-4(1)	*INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM*		x			
SI-4(2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*		x		x	x
SI-4(3)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOL INTEGRATION*		x			
SI-4(4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*		x		x	x
SI-4(5)	*INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*		x		x	x
SI-4(6)	*INFORMATION SYSTEM MONITORING | RESTRICT NON-PRIVILEGED USERS*	x	Incorporated into AC-6(10).			
SI-4(7)	*INFORMATION SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS*		x			
SI-4(8)	*INFORMATION SYSTEM MONITORING | PROTECTION OF MONITORING INFORMATION*	x	Incorporated into SI-4.			
SI-4(9)	*INFORMATION SYSTEM MONITORING | TESTING OF MONITORING TOOLS*		x			
SI-4(10)	*INFORMATION SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS*		x			
SI-4(11)	*INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES*		x			
SI-4(12)	*INFORMATION SYSTEM MONITORING | AUTOMATED ALERTS*		x			
SI-4(13)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS*		x			
SI-4(14)	*INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION*		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-4(15)	*INFORMATION SYSTEM MONITORING | WIRELESS TO WIRELINE COMMUNICATIONS*		x			
SI-4(16)	*INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION*		x			
SI-4(17)	*INFORMATION SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*		x			
SI-4(18)	*INFORMATION SYSTEM MONITORING | ANALYZE TRAFFIC / COVERT EXFILTRATION*		x			
SI-4(19)	*INFORMATION SYSTEM MONITORING | INDIVIDUALS POSING GREATER RISK*		x			
SI-4(20)	*INFORMATION SYSTEM MONITORING | PRIVILEGED USER*		x			
SI-4(21)	*INFORMATION SYSTEM MONITORING | PROBATIONARY PERIODS*		x			
SI-4(22)	*INFORMATION SYSTEM MONITORING | UNAUTHORIZED NETWORK SERVICES*		x			
SI-4(23)	*INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES*		x			
SI-4(24)	*INFORMATION SYSTEM MONITORING | INDICATORS OF COMPROMISE*		x			
SI-5	**Security Alerts, Advisories, and Directives**		x	x	x	x
SI-5(1)	*SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*		x			x
SI-6	**Security Function Verification**		x			x
SI-6(1)	*SECURITY FUNCTION VERIFICATION | NOTIFICATION OF FAILED SECURITY TESTS*	x	Incorporated into SI-6.			
SI-6(2)	*SECURITY FUNCTION VERIFICATION | AUTOMATION SUPPORT FOR DISTRIBUTED TESTING*					
SI-6(3)	*SECURITY FUNCTION VERIFICATION | REPORT VERIFICATION RESULTS*					
SI-7	**Software, Firmware, and Information Integrity**		x		x	x
SI-7(1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*		x		x	x
SI-7(2)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*		x			x
SI-7(3)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CENTRALLY MANAGED INTEGRITY TOOLS*		x			
SI-7(4)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TAMPER-EVIDENT PACKAGING*	x	Incorporated into SA-12.			
SI-7(5)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*		x			x
SI-7(6)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION*		x			
SI-7(7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*		x		x	x
SI-7(8)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUDITING CAPABILITY FOR SIGNIFICANT EVENTS*		x			
SI-7(9)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS*		x			
SI-7(10)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE*		x			
SI-7(11)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*		x			
SI-7(12)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION*		x			

CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
SI-7(13)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*		x			
SI-7(14)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*		x			x
SI-7(15)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*		x			
SI-7(16)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*		x			
SI-8	**Spam Protection**				x	x
SI-8(1)	*SPAM PROTECTION | CENTRAL MANAGEMENT*				x	x
SI-8(2)	*SPAM PROTECTION | AUTOMATIC UPDATES*				x	x
SI-8(3)	*SPAM PROTECTION | CONTINUOUS LEARNING CAPABILITY*					
SI-9	**Information Input Restrictions**	x	Incorporated into AC-2, AC-3, AC-5, AC-6.			
SI-10	**Information Input Validation**		x		x	x
SI-10(1)	*INFORMATION INPUT VALIDATION | MANUAL OVERRIDE CAPABILITY*		x			
SI-10(2)	*INFORMATION INPUT VALIDATION | REVIEW / RESOLUTION OF ERRORS*		x			
SI-10(3)	*INFORMATION INPUT VALIDATION | PREDICTABLE BEHAVIOR*		x			
SI-10(4)	*INFORMATION INPUT VALIDATION | REVIEW / TIMING INTERACTIONS*		x			
SI-10(5)	*INFORMATION INPUT VALIDATION | REVIEW / RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS*		x			
SI-11	**Error Handling**				x	x
SI-12	**Information Handling and Retention**			x	x	x
SI-13	**Predictable Failure Prevention**		x			
SI-13(1)	*PREDICTABLE FAILURE PREVENTION | TRANSFERRING COMPONENT RESPONSIBILITIES*		x			
SI-13(2)	*PREDICTABLE FAILURE PREVENTION | TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION*	x	Incorporated into SI-7(16).			
SI-13(3)	*PREDICTABLE FAILURE PREVENTION | MANUAL TRANSFER BETWEEN COMPONENTS*		x			
SI-13(4)	*PREDICTABLE FAILURE PREVENTION | STANDBY COMPONENT INSTALLATION / NOTIFICATION*		x			
SI-13(5)	*PREDICTABLE FAILURE PREVENTION | FAILOVER CAPABILITY*		x			
SI-14	**Non-Persistence**		x			
SI-14(1)	*NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES*		x			
SI-15	**Information Output Filtering**		x			
SI-16	**Memory Protection**		x		x	x
SI-17	**Fail-Safe Procedures**		x			

КОРРЕКТИРОВКА БАЗОВЫХ НАБОРОВ МЕР БЕЗОПАСНОСТИ

РАЗМЕЩЕНИЕ МЕР БЕЗОПАСНОСТИ И ПРИСВОЕНИЕ ПРИОРИТЕТНЫХ КОДОВ УПОРЯДОЧИВАНИЯ

С каждой версией SP 800-53, с базовыми мерами безопасности могут происходить незначительные корректировки, включая, например, размещение дополнительных мер безопасности и/или улучшений мер безопасности, устранение выбранных меры безопасности/улучшений и изменение приоритетных кодов упорядочивания (P-кодов). Эти изменения отражают: (i) продолжающееся получение и анализ информации об угрозах; (ii) периодическая перепроверка начальных предположений, которые генерировали базовые наборы мер безопасности; (iii) стремление обобщить начальные базовые наборы мер безопасности для систем национальной безопасности и не относящихся к национальной безопасности, чтобы достигнуть сходимости для всего сообщества (полагаясь впоследствии на частные оверлеи, чтобы описать любые корректировки от общих начальных наборов); и (iv) периодическая переоценка приоритетных кодов, чтобы соответственно сбалансировать рабочую нагрузку по реализации мер безопасности. Со временем, поскольку каталог меры безопасности расширяется, чтобы соответствовать продолжающимся вызовам со стороны динамичного и растущего пространства угрозы, которое становится все более и более сложным, организации придут к тому, чтобы полагаться в намного большей степени на оверлеи, для обеспечения необходимой специализации их планов обеспечения безопасности.

ПРИЛОЖЕНИЕ E

ДОВЕРИЕ И ДОВЕРЕННОСТЬ

МЕРЫ УВЕРЕННОСТИ В БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Доверие к безопасности - критический аспект в определении доверенности информационных систем. Доверие - мера уверенности в том, что функции безопасности, возможности, методы, политики, процедуры, механизмы и архитектура информационных систем организации точно интерпретируют и проводят в жизнь установленные политики безопасности.[94] Цель этого приложения:

- Поощрять организации включать требования доверия в приобретение информационных систем, системных компонентов и сервисов;
- Поощрять разработчиков аппаратных средств, программного обеспечения и встроенного микропрограммного обеспечения использовать такие методы разработки, результат которых выражался бы в более доверенных продуктах и системах информационных технологий;
- Поощрять организации идентифицировать, выбирать и использовать продукты информационных технологий, которые были созданы с соответствующими уровнями доверия и использовать правильные системы и инженерные технологии и методы обеспечения безопасности в течение процесса жизненного цикла разработки систем;
- Уменьшать риск информационной безопасности, развертывая более доверенные продукты информационных технологий в критических информационных системах или системных компонентах; и
- Поощрять разработчиков и организации получать на непрерывной основе свидетельства доверия для того, чтобы поддерживать доверенность информационных систем.

Минимальные требования безопасности для федеральной информации и информационных систем определены в FIPS публикации 200. Эти требования могут быть удовлетворены путем выбора, адаптации, реализации и получения свидетельств доверия для мер безопасности в низком, умеренном или высоком базовых наборах мер в Приложении D.[95] Базовые наборы включают также связанные с доверием меры безопасности для минимальных требований доверия, которые применимы в общем к федеральной информации и информационным системам.[96] Однако, рассматривая текущее пространство угроз и увеличивающийся риск к деятельности и активам организаций, людям, другим организациям и Нации, которую несут постоянные совершенствующиеся угрозы (APT), организации могут хотеть реализовать дополнительные, связанные с доверием, меры безопасности из Приложения F. Эти дополнительные меры безопасности могут быть выбраны, основываясь на руководстве по адаптации, представленном в Разделе 3.2. Организации могут также рассмотреть разработку оверлеев высокого доверия для критических функций предназначения/деятельности, специализированных сред эксплуатации и/или информационных технологий (см. Раздел 3.3 и Приложение I). Когда связанные с доверием меры безопасности не могут быть удовлетворены, организации могут предложить компенсирующие мер безопасности (например, процедурные/эксплуатационные решения,

[94] Раздел 2.6 обеспечивают введение в концепции доверия и доверенности и связь между этими двумя концепциями. Модель доверенности иллюстрирована на рисунке 3.

[95] CNSS Инструкция 1253 определяет базовые наборы мер безопасности для систем национальной безопасности. Поэтому, связанные с доверием меры безопасности в базовых наборах, установленных для сообщества национальной безопасности, если такие назначены, могут отличаться от мер безопасности, которые определены в Таблицах от E-1 до E-3.

[96] Трудно определить, обеспечивает ли данный базовый набор мер безопасности из Приложения D доверие, необходимое для всех информационных технологий, пользователей, платформ и организаций. Например, в то время как использование формальных методов могло бы быть соответствующим в междоменном продукте, для сложной системы авиадиспетчерской службы или для веб-сервера, предоставляющего информацию о подготовленности к чрезвычайным ситуациям от Департамента безопасности отечества, могли бы быть подходящими другие технологии доверия. Тем не менее, в существующих базовых наборах есть аспекты доверия, которые отражают минимальное доверие, которое, как ожидается, является общим для всех технологий, пользователей, платформ и организаций.

компенсирующие недостаточные решения, основанные на технологиях) или принять больший уровень риска относительно фактически достигнутых возможностей безопасности.

Новый взгляд на доверие

Несмотря на то, что предыдущие версии Специальной публикации 800-53 содержали минимальные требования доверия, фокус был на высокоуровневых, более абстрактных требованиях, применяемых к низкому, умеренному и высокому базовым наборам мер. Этот пересмотр использует фундаментально отличный подход к доверию, определяя конкретные, связанные с доверием меры безопасности в Приложении F, которые могут быть реализованы организациями, основываясь на категорировании безопасности их информационных систем - создавая требования доверия более *практичные* и обеспечивающие возможности для повышения уровней доверия, основываясь на потребностях предназначения и деятельности, текущих/перспективных угрозах, конкретных средах эксплуатации или использовании новых технологий. Идентификация конкретных связанных с доверием мер обеспечения в низком, умеренном и высоком базовых наборах мер в легко читаемых таблицах (Таблицы E-1, E-2, E-3) помогает организациям быстро определить меры безопасности, необходимые, чтобы удовлетворить минимальные требования доверия. Дополнительные связанные с доверием меры безопасности в Таблице E-4 предоставляют организациям специфический язык для использования в приобретениях, нацеленный на разработчиков информационных систем, системных компонентов и сервисов информационных систем. Меры безопасности определяют конкретные методологии, технологии, проектные и архитектурные соображения, а так же проверенные системные и инженерные принципы обеспечения безопасности, чтобы существенно улучшить качество компонентов аппаратных средств, программного обеспечения и встроенного микропрограммного обеспечения, которые будут интегрированы в информационные системы организаций или критическую инфраструктуру. Выделение связанных с доверием мер безопасности не предназначено, чтобы подразумевать более важный уровень для таких мер безопасности. Достижение адекватной безопасности для информационных систем организаций требует корректной комбинации и функциональных и связанных с доверием мер безопасности. Только понимая важность концепции доверия и распознавая то, какие меры безопасности более ориентированы на доверие относительно более ориентированных на функциональность, организации смогут выбирать самую соответствующую комбинацию мер безопасности, чтобы защитить их деятельность и активы, людей, другие организации и Нацию.

Следующие разделы обеспечивают описание связанных с доверием мер безопасности, которые включены в каждый из базовых наборов мер безопасности в Приложении D. Критерии для определения того, связана ли мера безопасности с доверием или связана с функциональностью, основаны на полных характеристиках меры безопасности. В общем, связанные с доверием меры безопасности, это меры, которые: (i) определяют процессы, процедуры, технологии или методологии проектирования и разработки информационных систем и системных компонентов (то есть, аппаратных средств, программного обеспечения, встроенного микропрограммного обеспечения); (ii) обеспечивают процессы, поддерживающие деятельность, включая улучшение качества систем/компонентов/процессов; (iii) предоставляют свидетельство безопасности действий, связанных с разработкой или эксплуатацией; (iv) определяют эффективность мер безопасности или риски (например, аудит, тестирование, оценка, анализ, определение, проверка, подтверждение соответствия, мониторинг); или (v) улучшают квалификацию, знания и понимание персонала (например, освоение/обучение безопасности, обучение реакции на инциденты, обучение действиям в чрезвычайных ситуациях).

Меры безопасности могут быть определены как меры связанные с доверием, даже когда меры безопасности выражают некоторые функциональные характеристики или свойства (например, SI-4, Мониторинг информационной системы). Различие между функциональностью и доверием менее важно, когда описываются связанные с доверием меры безопасности в базовых наборах - прежде всего, потому что меры безопасности в трех базовых наборах после применения процесса адаптации становятся частью планов обеспечения безопасности для информационных систем и для организаций.[97] Однако различие становится более важным, когда организации используют вариант выбора дополнительных мер безопасности, чтобы увеличить уровень доверия (или степень уверенности) в функциональности безопасности и возможностях безопасности.

[97] Организации должны знать, что необходимо тщательно анализировать связанные с доверием меры безопасности в базовых наборах во время процесса адаптации, включая разработку оверлеев, чтобы гарантировать, что меры безопасности, которые обеспечивают меры уверенности в функциональности безопасности, необходимой для защиты предназначения/деятельности, не будут непреднамеренно устранены.

Минимальные требования доверия - Системы низкого уровня воздействия

Требование доверия: Организация, базируясь на ее требования безопасности, политику безопасности и необходимые возможности безопасности, ожидает: (i) **ограниченную** стойкость функциональности безопасности; и (ii) **ограниченный** уровень уверенности, поддержанный глубиной и покрытием соответствующего свидетельства безопасности, что функциональность безопасности полна, непротиворечива и корректна.

Дополнительное руководство: Функциональность и доверие к безопасности для систем низкого уровня воздействия достигаются реализацией мер безопасности адаптированного базового набора мер низкого уровня из Приложении D. Требования доверия для систем низкого воздействия (включая компоненты информационной технологии, которые являются частью этих систем), соответствуют тому, что легко достижимо с не модифицируемыми, коммерческими серийными (COTS) продуктами и услугами. Вследствие ограниченной стойкости функциональности, ожидаемой для систем низкого воздействия, глубина/покрытие свидетельства безопасности[98] является минимальной и не ожидается, что будет больше чем то, что обычно обеспечивается производителями, поставщиками и торговыми посредниками COTS. Свидетельство глубины/покрытия далее дополняется результатами оценок мер безопасности и постоянным мониторингом информационных систем организации и сред, в которых работают системы. Помимо основанной на технологии функциональности, акцент делается на ограниченный уровень уверенности в законченности, корректности и согласованности процедурной и/или эксплуатационной функциональности безопасности (например, политик, процедур, физической безопасности и безопасности персонала). Требования доверия, определенные в форме связанных с разработкой и эксплуатационных мер обеспечения доверия для систем низкого уровня воздействия, перечислены в Таблице E-1. Организации, посредством процесса адаптации (включая оценку риска организации), могут добавлять другие связанные с доверием меры безопасности и/или улучшения мер безопасности к набору, включенному в Таблицу E-1.

ТАБЛИЦА E-1: СВЯЗАННЫЕ С ДОВЕРИЕМ МЕРЫ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМ НИЗКОГО УРОВНЯ ВОЗДЕЙСТВИЯ[99]

ID	МЕРЫ БЕЗОПАСНОСТИ	ID	МЕРЫ БЕЗОПАСНОСТИ
AC	AC-1	**MP**	MP-1
AT	AT-1, AT-2, AT-3, AT-4	**PE**	PE-1, PE-6, PE-8
AU	AU-1, AU-6	**PL**	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9	**PS**	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-4, CM-8	**RA**	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	**SA**	SA-1, SA-2, SA-3, SA-4, SA-4(10), SA-5, SA-9
IA	IA-1	**SC**	SC-1, SC-39
IR	IR-1, IR-2, IR-5	**SI**	SI-1, SI-4, SI-5
MA	MA-1		

[98] Специальная публикация NIST 800-53A обеспечивает дополнительную информацию о глубине и покрытии при оценках мер безопасности.

[99] Связанные с доверием меры безопасности в Таблице E-1 являются *подмножеством* мер безопасности, содержавшихся в базовом наборе мер безопасности для систем низкого уровня воздействия в Приложении D. Реализация связанных с доверием мер безопасности в Таблице E-1 (включая глубину/покрытие свидетельства безопасности из Специальной публикации NIST 800-53A) удовлетворит минимальные требования доверия для систем низкого уровня воздействия, установленные FIPS Публикацией 200.

Минимальные требования доверия - Системы умеренного уровня воздействия

Требование доверия: Организация, базируясь на ее требования безопасности, политику безопасности и необходимые возможности безопасности, ожидает: (i) **умеренную** стойкость функциональности безопасности; и (ii) **умеренный** уровень уверенности, поддержанный глубиной и покрытием соответствующего свидетельства безопасности, что функциональность безопасности полна, непротиворечива и корректна.

Дополнительное руководство: Функциональность и доверие безопасности для систем умеренного уровня воздействия достигаются реализацией мер безопасности адаптированного базового набора мер умеренного уровня из Приложении D. Требования доверия для систем умеренного воздействия (включая компоненты информационной технологии, которые являются частью этих систем), добавляют к ожиданиям в низком уровне доверия: (i) включение функциональности безопасности COTS с большей стойкостью механизмов и возможностями чем стойкость механизмов и возможности, достигнутые в системах низкого воздействия; (ii) требование, возможно, некоторых специальных разработок; (iii) установление более безопасных параметров конфигурации; и (iv) требование некоторой дополнительной оценки реализованных возможностей. Вследствие умеренной стойкости функциональности, ожидаемой для систем умеренного воздействия, глубина/покрытие свидетельства безопасности[100] является более существенной, чем минимального свидетельства, произведенного для систем низкого воздействия, но тем не менее в масштабе того, что обеспечивается производителями, поставщиками и торговыми посредниками COTS. Свидетельство глубины/покрытия далее дополняется результатами дополнительных оценок мер безопасности и постоянным мониторингом информационных систем организации и сред, в которых работают системы. Помимо основанной на технологии функциональности, акцент делается на умеренный уровень уверенности в законченности, корректности и согласованности процедурной и/или эксплуатационной функциональности безопасности (например, политик, процедур, физической безопасности и безопасности персонала). Требования доверия, определенные в форме связанных с разработкой и эксплуатационных мер доверия для систем умеренного уровня воздействия, перечислены в Таблице E-2. Организации, посредством процесса адаптации (включая оценку риска организации), могут добавлять другие связанные с доверием меры безопасности и/или улучшения мер к набору, включенному в Таблицу E-2.

ТАБЛИЦА E-2: СВЯЗАННЫЕ С ДОВЕРИЕМ МЕРЫ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМ УМЕРЕННОГО УРОВНЯ ВОЗДЕЙСТВИЯ[101]

ID	МЕРЫ БЕЗОПАСНОСТИ	ID	МЕРЫ БЕЗОПАСНОСТИ
AC	AC-1	**MP**	MP-1
AT	AT-1, AT-2, **AT-2(2)**, AT-3, AT-4	**PE**	PE-1, PE-6, **PE-6(1)**, PE-8
AU	AU-1, AU-6, **AU-6(1)**, **AU-6(3)**, **AU-7**, **AU-7(1)**	**PL**	PL-1, PL-2, **PL-2(3)**, PL-4, **PL-4(1)**, **PL-8**
CA	CA-1, CA-2, **CA-2(1)**, CA-3, CA-5, CA-6, CA-7, **CA-7(1)**, CA-9	**PS**	PS-1, PS-6, PS-7
CM	CM-1, CM-2, **CM-2(1)**, **CM-2(3)**, **CM-2(7)**, **CM-3**, **CM-3(2)**, CM-4, CM-8, **CM-8(1)**, **CM-8(3), CM-8(5)**	**RA**	RA-1, RA-3, RA-5, **RA-5(1), RA-5(2), RA-5(5)**
CP	CP-1, CP-3, CP-4, **CP-4(1)**	**SA**	SA-1, SA-2, SA-3, SA-4, **SA-4(1)**, **SA-4(2)**, **SA-4(9)**, SA-4(10), SA-5, **SA-8**, SA-9, **SA-9(2)**, **SA-10**, **SA-11**
IA	IA-1	**SC**	SC-1, **SC-2**, SC-39
IR	IR-1, IR-2, **IR-3**, **IR-3(2)**, IR-5	**SI**	SI-1, SI-4, **SI-4(2)**, **SI-4(4)**, **SI-4(5)**, SI-5, **SI-7**, **SI-7(1)**, **SI-7(7)**, **SI-10**, **SI-16**
MA	MA-1		

[100] Специальная публикация NIST 800-53A обеспечивает дополнительную информацию о глубине и покрытии при оценках мер безопасности.

[101] Связанные с доверием меры безопасности в Таблице E-2 являются *подмножеством* мер безопасности, содержавшихся в базовом наборе мер безопасности для систем умеренного уровня воздействия в Приложении D. Реализация связанных с доверием мер безопасности в Таблице E-2 (включая глубину/покрытие свидетельства безопасности из Специальной публикации NIST 800-53A) удовлетворит минимальные требования доверия для систем умеренного уровня воздействия, установленные FIPS Публикацией 200. **Полужирный** текст указывает на *дополнение* относительно базового набора низкого уровня (то есть, меры безопасности, связанные с доверием, добавляются к базовому набору низкого уровня, чтобы получить увеличенный уровень доверия в базовом наборе умеренного уровня).

Минимальные требования доверия - Системы высокого уровня воздействия

Требование доверия: Организация, базируясь на ее требования безопасности, политику безопасности и необходимые возможности безопасности, ожидает: (i) **высокую** стойкость функциональности безопасности; и (ii) **высокий** уровень уверенности, поддержанный глубиной и покрытием соответствующего свидетельства безопасности, что функциональность безопасности полна, непротиворечива и корректна.

Дополнительное руководство: Функциональность и доверие безопасности для систем высокого уровня воздействия достигаются реализацией мер безопасности адаптированного базового набора мер высокого уровня из Приложения D. Требования доверия для систем высокого воздействия (включая компоненты информационной технологии, которые являются частью этих систем), добавляют к ожиданиям в умеренном уровне доверия: (i) включение самого высокого уровня возможностей безопасности COTS, которые следуют из приложения обычно принимаемых лучших коммерческих методов разработки для того, чтобы уменьшить уровень скрытых дефектов, некоторые специальные разработки и дополнительную оценку реализованных возможностей. Вследствие высокой стойкости функциональности, ожидаемой для систем высокого воздействия, глубина/покрытие свидетельства безопасности[102] является более всесторонней, чем свидетельства, произведенного для систем умеренного воздействия. Хотя свидетельство, может быть в масштабе того, что обеспечивается производителями, поставщиками и торговыми посредниками COTS, тем не менее, может требоваться большее доверие от независимых поставщиков оценки. Свидетельство глубины/покрытия дополняется результатами дополнительных оценок мер безопасности и постоянным мониторингом информационных систем организации/сред эксплуатации. Помимо основанной на технологии функциональности, имеется высокий уровень уверенности в законченности, корректности и согласованности процедурной и/или эксплуатационной функциональности безопасности (например, политик, процедур, физической безопасности и безопасности персонала). Требования доверия, определенные в форме связанных с разработкой и эксплуатационных мер обеспечения доверия для систем высокого уровня воздействия, перечислены в Таблице E-3. Организации, посредством процесса адаптации (включая оценку риска организации), могут добавлять другие, связанные с доверием меры безопасности и/или улучшения мер безопасности к набору, включенному в Таблицу E-3.

ТАБЛИЦА E-3: СВЯЗАННЫЕ С ДОВЕРИЕМ МЕРЫ БЕЗОПАСНОСТИ ДЛЯ СИСТЕМ ВЫСОКОГО УРОВНЯ ВОЗДЕЙСТВИЯ[103]

ID	МЕРЫ БЕЗОПАСНОСТИ	ID	МЕРЫ БЕЗОПАСНОСТИ
AC	AC-1	**MP**	MP-1
AT	AT-1, AT-2, AT-2(2), AT-3, AT-4	**PE**	PE-1, PE-6, PE-6(1), **PE-6(4)**, PE-8
AU	AU-1, AU-6, AU-6(1), AU-6(3), **AU-6(5)**, **AU-6(6)**, AU-7, AU-7(1), **AU-10**	**PL**	PL-1, PL-2, PL-2(3), PL-4, PL-4(1), PL-8
CA	CA-1, CA-2, CA-2(1), **CA-2(2)**, CA-3, CA-5, CA-6, CA-7, CA-7(1), **CA-8**, CA-9	**PS**	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-2(1), **CM-2(2)**, CM-2(3), CM-2(7), CM-3, **CM-3(1)**, CM-3(2), CM-4, **CM-4(1)**, CM-8, CM-8(1), **CM-8(2)**, CM-8(3), **CM-8(4)**, CM-8(5)	**RA**	RA-1, RA-3, RA-5, RA-5(1), RA-5(2), **RA-5(4)**, RA-5(5)
CP	CP-1, CP-3, **CP-3(1)**, CP-4, CP-4(1), **CP-4(2)**	**SA**	SA-1, SA-2, SA-3, SA-4, SA-4(1), SA-4(2), SA-4(9), SA-4(10), SA-5, SA-8, SA-9, SA-9(2), SA-10, SA-11, **SA-12**, **SA-15**, **SA-16**, **SA-17**
IA	IA-1	**SC**	SC-1, SC-2, **SC-3**, **SC-7(18)**, **SC-7(21)**, **SC-24**, SC-39
IR	IR-1, IR-2, **IR-2(1)**, **IR-2(2)**, IR-3, IR-3(2), IR-5, **IR-5(1)**	**SI**	SI-1, SI-4, SI-4(2), SI-4(4), SI-4(5), SI-5, **SI-5(1)**, **SI-6**, SI-7, SI-7(1), **SI-7(2)**, **SI-7(5)**, SI-7(7), **SI-7(14)**, SI-10, SI-16
MA	MA-1		

[102] Специальная публикация NIST 800-53A обеспечивает дополнительную информацию о глубине и покрытии при оценках мер безопасности.

[103] Связанные с доверием меры безопасности в Таблице E-2 являются *подмножеством* мер безопасности, содержавшихся в базовом наборе мер безопасности для систем высокого уровня воздействия в Приложении D. Реализация связанных с доверием мер безопасности в Таблице E-2 (включая глубину/покрытие свидетельства безопасности из Специальной публикации NIST 800-53A) удовлетворит минимальные требования доверия для систем высокого уровня воздействия, установленные FIPS Публикацией 200. **Полужирный** текст указывает на *дополнение* относительно базового набора умеренного уровня (то есть, меры безопасности, связанные с доверием, добавляются к базовому набору умеренного уровня, чтобы получить увеличенный уровень доверия в базовом наборе высокого уровня).

Меры безопасности для достижения повышенного доверия

Хотя связанные с доверием меры безопасности, представленные в предыдущих разделах для низкого, умеренного и высокого базовых наборов мер, обеспечивают минимальные требования доверия, организации могут, с течением времени, захотеть повысить уровень доверия в своих информационных системах - увеличивая уровень доверенности соответственно. Это выполняется путем добавления связанных с доверием мер безопасности к мерам в базовых наборах, чтобы увеличить и стойкость функциональности безопасности и степень уверенности, что функциональность корректна, полна и непротиворечиво - создавая функциональность, очень стойкую к проникновению, фальсификации или обходу. Функциональность безопасности, которая является очень стойкой к проникновению, фальсификации и обходу требует существенного объема работ со стороны противников, чтобы поставить под угрозу конфиденциальность, целостность или доступность информационной системы или системных компонентов, где эта функциональность используется.

Так как высоко-доверенные продукты информационных технологий могут быть более дорогостоящими и труднодостижимыми, организации могут хотеть разделять свои информационные системы на отдельные подсистемы, чтобы изолировать критические компоненты и сфокусировать усилия по высокому доверию на более узко определенном подмножестве информационных ресурсов. Организациям, которые считают решения по информационным технологиям высокого доверия труднодостижимыми, вероятно, придется положиться в большей степени на процедурные или эксплуатационные меры защиты, чтобы гарантировать успех в предназначении и деятельности. Это включает, например, реинжиниринг критических процессов предназначения и деятельности, чтобы быть менее восприимчивым к угрозам высокого уровня. Таблица E-4 представляет дополнительные, связанные с разработкой и эксплуатационные действия (например, в семействах мер безопасности SA, SI и CM), которые организации могут выбрать, чтобы достигнуть повышенного уровня доверия (включительно до высокого уровня доверия). Список связанных с доверием мер безопасности не является исчерпывающим. Организации, во время процесса адаптации, могут определять другие меры безопасности, как связанные с доверием, и добавлять к набору мер в Таблице E-4.

ТАБЛИЦА E-4: МЕРЫ БЕЗОПАСНОСТИ ДЛЯ ПОВЫШЕННОГО ДОВЕРИЯ[104]

ID	МЕРЫ БЕЗОПАСНОСТИ	ID	МЕРЫ БЕЗОПАСНОСТИ
AC	**AC-25**	**MP**	Нет дополнительных мер
AT	**AT-2(1)**, **AT-3(**все улучшения)	**PE**	**PE-6(2)**, **PE-6(3)**
AU	**AU-6(4)**, **AU-6(7)**, **AU-6(8)**, **AU-6(9)**, **AU-6(10)**, **AU-10(**все улучшения), **AU-11(1)**, **AU-13(**плюс улучшения), **AU-14(**плюс улучшения)	**PL**	**PL-8(**все улучшения), **PL-9**
CA	**CA-2(3)**, **CA-5(1)**, **CA-7(3)**, **CA-8(**все улучшения), **CA-9(1)**	**PS**	**PS-6(2), PS-6(3)**
CM	**CM-2(6)**, **CM-4(2)**, **CM-8(6)**, **CM-8(7)**, **CM-8(8), CM-8(9)**	**RA**	**RA-5(3), RA-5(6)**, **RA-5(8)**, **RA-5(10)**, **RA-6**
CP	**CP-3(2)**, **CP-4(3)**, **CP-4(4), CP-12**	**SA**	**SA-4(3)**, **SA-4(5)**, **SA-4(6)**, **SA-4(7)**, **SA-4(8)**, **SA-9(1)**, **SA-9(3)**, **SA-9(4)**, **SA-9(5)**, **SA-10(**все улучшения), **SA-11(**все улучшения), **SA-12(**все улучшения), **SA-13**, **SA-14**, **SA-15(**все улучшения), **SA-17(**все улучшения), **SA-18(**плюс улучшения), **SA-19(**плюс улучшения), **SA-20**, **SA-21(**плюс улучшение), **SA-22(**плюс улучшение)
IA	Нет дополнительных мер	**SC**	**SC-2(1)**, **SC-3(**все улучшения), **SC-6**, **SC-7(22), SC-11(**плюс улучшение), SC**-29(**плюс улучшение), **SC-30(**плюс улучшения), **SC-31(**плюс улучшения), **SC-32**, **SC-34(**плюс улучшения), **SC-36(**плюс улучшение), **SC-37(**плюс улучшение), **SC-38**, **SC-39(**все улучшения)
IR	**IR-3(1)**	**SI**	**SI-4(1)**, **SI-4(3)**, **SI-4(7)**, **SI-4(9)**, **SI-4(10)**, **SI-4(11)**, **SI-4(12)**, **SI-4(13)**, **SI-4(14)**, **SI-4(15)**, **SI-4(16)**, **SI-4(17)**, **SI-4(18)**, **SI-4(19)**, **SI-4(20)**, **SI-4(21)**, **SI-4(22)**, **SI-4(23)**, **SI-4(24)**, **SI-7(3)**, **SI-7(6)**, **SI-7(8)**, **SI-7(9)**, **SI-7(10)**, **SI-7(11)**, **SI-7(12)**, **SI-7(13)**, **SI-7(15)**, **SI-7(16)**, **SI-10(**все улучшения), **SI-13(**плюс улучшения), **SI-14(**плюс улучшение), **SI-15**, **SI-17**
MA	Нет дополнительных мер		

[104] Связанные с доверием меры безопасности в Таблице E-4 представляют дополнительные меры безопасности, необходимые для достижения повышенных уровней доверия (то есть, меры безопасности, которые должны идти сверх мер минимальных уровней доверия, которые представлены связанными с доверием мерами безопасности в Таблицах E-1, E-2 и E-3). Когда связанная с доверием мера безопасности назначена базовому набору (то есть, перечислена в Таблицах E-1, E-2 или E-3), но все её улучшения находятся в Таблице E-4, то это определяется в таблице как **Мера безопасности** (*все улучшения*). Когда связанная с доверием мера безопасности и все ее улучшения не назначены базовым наборам, то это определяется в таблице как **Мера безопасности** (*плюс улучшения*). Когда связанные с доверием улучшения для определенной меры безопасности выделены одному из базовых наборов, остающиеся невыбранные улучшения меры перечислены индивидуально в Таблице E-4.

ПРИЛОЖЕНИЕ F

КАТАЛОГ МЕР БЕЗОПАСНОСТИ

МЕРЫ БЕЗОПАСНОСТИ, УЛУЧШЕНИЯ И ДОПОЛНИТЕЛЬНЫЕ РУКОВОДСТВА

Каталог мер безопасности в этом приложении содержит совокупность мер защиты и контрмер для организаций и информационных систем.[105] Меры безопасности были разработаны, чтобы облегчить соответствие с применимыми федеральными законами, правительственными распоряжениями, директивами, политиками, нормативными актами, стандартами и руководствами.[106] Организация каталога мер безопасности, структура мер и концепция назначения мер безопасности и улучшений мер безопасности в начальные базовые наборы мер безопасности в Приложении D описана в Главе Два. Меры безопасности в каталоге, за редким исключением, были разработаны так, чтобы быть нейтральными относительно политики и технологий. Это означает, что меры безопасности и улучшения мер сосредотачиваются на фундаментальных мерах защиты и контрмерах, необходимых, чтобы защитить информацию во время обработки, в период хранения и во время передачи. Поэтому, представление о приложении мер безопасности к конкретным технологиям, сообществам интересов, средам эксплуатации или функциям предназначений/деятельности выходит за рамки этой публикации. Эти области определяются при помощи процесса адаптации, описанного в Главе Три и разработки оверлеев, описанных в Приложении I.

В немногих случаях, когда конкретные технологии указаны в мерах безопасности (например, мобильные устройства, PKI, беспроводная связь, VOIP), организации должны учитывать, что необходимость обеспечить адекватную безопасность находится за пределами требований к единственной мере безопасности, связанной с определенной технологией. Многие из необходимых мер защиты/контрмер получены из других мер безопасности в каталоге, назначенных начальным базовым наборам мер безопасности как начальной точке для разработки планов обеспечения безопасности и оверлеев, используя процесс адаптации. В дополнение к управляемой организацией разработке специализированных планов обеспечения безопасности и оверлеев, Специальные публикации и Межведомственные отчеты NIST могут дать представление о рекомендуемых мерах безопасности для конкретных технологий и приложений, специфичных для конкретной области (например, умные сети, здравоохранение, промышленные системы управления и мобильные устройства).

Использование каталога мер безопасности нейтрального относительно политики и технологий обладает следующими преимуществами:

• Это поощряет организации сосредотачиваться на возможностях безопасности, требуемых для успеха в предназначении/деятельности и защите информации, независимо от информационных технологий, которые использованы в информационных системах организации;

• Это поощряет организации анализировать каждую меру безопасности по ее применимости для конкретных технологий, сред эксплуатации, функций предназначения/деятельности и сообществ интересов; и

[105] Сетевая версия каталога мер безопасности также доступна в http://web.nvd.nist.gov/view/800-53/home.

[106] Соответствие требует от организаций проявлять должную старательность относительно управления информационной безопасностью и управления рисками. Должная старательность в информационной безопасности включает использование всей соответствующей информации как часть программы управления рисками всей организации, чтобы эффективно использовать руководство по адаптации и присущую публикациям NIST гибкость так, чтобы выбранные меры безопасности, задокументированные в планы обеспечения безопасности организаций, соответствовали конкретным требования предназначения и деятельности организаций. В разработке, реализации и поддержании мер защиты и контрмер с необходимой и достаточной стойкостью механизмов важно использовать инструменты управления рисками и технологии, которые доступны организациям, чтобы противодействовать текущие угрозы деятельности и активам организаций, людям, другим организациям и Нации. Использование эффективных, основанные на риске, процессов, процедур и технологий поможет гарантировать, что у всех федеральных информационных систем и организаций есть необходимая устойчивость, чтобы поддержать долговременные федеральные обязанности, критические приложения инфраструктуры и непрерывность деятельности правительства.

• Это поощряет организации уточнять политику безопасности как часть процесса адаптации для мер безопасности, у которых есть переменные параметры.

Например, организации, использующие смартфоны, планшеты или другие типы мобильных устройств, запустили бы процесс адаптации, предполагая, что все меры безопасности и улучшения мер в соответствующем базовом наборе (низком, умеренном или высоком) необходимы. Процесс адаптации может иметь результат в исключении некоторых мер безопасности по ряду причин, включая, например, неспособность технологии поддержать реализацию мер безопасности. Однако устранение таких мер безопасности, без понимания потенциально неблагоприятного воздействия на функции предназначения и деятельности организаций, может значительно увеличить риск информационной безопасности и должно быть тщательно проанализировано. Этот тип анализа важен для организаций, чтобы принять эффективные, основанные на риске решения, включая выбор соответствующих компенсирующих мер безопасности, когда рассматривается использование этих появляющихся мобильных устройств и технологий. Конкретизация планов обеспечения безопасности с использованием руководства по адаптации и оверлеев вместе с исчерпывающим набором мер безопасности нейтральных относительно политики и технологий, способствует рентабельной, основанной на риске информационной безопасности для организаций - в любом секторе, для любой технологии и в любой среде эксплуатации.

Меры безопасности в каталоге, как ожидается, будут изменяться с течением времени, поскольку меры будут исключаться, пересматриваться и добавляться. Чтобы поддерживать устойчивость в планах обеспечения безопасности и автоматизированных инструментах, поддерживающих реализацию Специальной публикации 800-53, меры безопасности не будут перенумеровываться каждый раз, когда мера безопасности исключена. Скорее нотации мер безопасности, которые были исключены, будут поддерживаться в каталоге для исторического назначения. Меры безопасности исключаются по множеству причин, включая, например: возможности безопасности, обеспечиваемые изъятой мерой безопасности, были включены в другую меру безопасности; возможности безопасности, обеспечиваемые изъятой мерой, избыточны по отношению к существующей мере безопасности; или мера безопасности, как считается, больше не является необходимой.

Иногда могут быть повторы в требованиях, содержащихся в мерах безопасности и улучшениях мер, которые являются частью каталога мер безопасности. Эти повторы в требованиях предназначены, чтобы усилить требования с точки зрения разнообразных мер безопасности и/или улучшений. Например, требование для строгой идентификации и аутентификации при проведении удаленных работ поддержки, появляется в семействе MA в конкретном контексте работ поддержки систем, проводимых организациями. Требование идентификации и аутентификации также появляется в более общем контексте в семействе IA. Хотя эти требования кажутся избыточными (то есть, накладываются), они, фактически, взаимно укрепляют и не предназначены, чтобы требовать дополнительных усилий от организаций в разработке и реализации программ обеспечения безопасности.

Совет по реализации

Новые меры безопасности и улучшения мер безопасности будут разрабатываться на регулярной основе, используя практическую информацию от угроз национального уровня и баз данных уязвимостей, а так же информацию относительно тактики, технологий и процедур, используемых противниками в проведении кибератак. Предложенные модификации к мерам безопасности и базовым наборам мер безопасности будут тщательно взвешены во время каждого цикла пересмотра, учитывая требование устойчивости каталога мер безопасности и потребности ответить на изменяющиеся угрозы, уязвимости, методы атак и информационные технологии. Главная цель состоит в том, чтобы повышать базовый уровень информационной безопасности в течение долгого времени. Организации могут разрабатывать новые меры безопасности, когда требуются конкретные возможности безопасности и соответствующие меры безопасности отсутствуют в Приложениях F или G.

ХАРАКТЕРИСТИКИ КЛАССОВ МЕР БЕЗОПАСНОСТИ

ХАРАКТЕРИСТИКА УПРАВЛЕНЧЕСКИХ, ЭКСПЛУАТАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

Поскольку у многих мер безопасности в семействах мер безопасности в Приложении F есть различные комбинации *управленческих*, *эксплуатационных* и *технических* свойств, конкретные характеристики классов были удалены из семейств мер безопасности. Организации могут, однако, счесть полезным применять такие характеристики к отдельным мерам безопасности и улучшениям мер безопасности или к отдельным разделам определенной меры безопасности/улучшения. Организации могут счесть выгодным, чтобы использовать характеристики классов, как способ сгруппировать или сослаться на меры безопасности. Характеристики классов могут также помочь организации в процессе выделения мер безопасности и улучшений мер в случае: (i) ответственных частей или информационных систем (например, общих или гибридных мер безопасности); (ii) конкретных ролей; и/или (iii) конкретных компонентов систем. Например, организации могут решить, что ответственность за специфичные для систем меры безопасности, которые они поместили в класс управленческих, принадлежат владельцу информационной системы, меры безопасности, помещенные в эксплуатационный класс, принадлежат сотруднику безопасности информационной системы (ISSO), и меры безопасности, помещенные в технический класс, принадлежат одному или более системным администраторам. Этот пример предназначен, чтобы иллюстрировать потенциальное использование обозначения классов для мер безопасности и/или улучшений мер; он не предназначен, чтобы предложить или потребовать дополнительных задач для организаций.

ПРЕДОСТЕРЕЖЕНИЕ

РАЗРАБОТКА СИСТЕМ, КОМПОНЕНТОВ И СЕРВИСОВ

С возобновлением акцента на доверенность информационных систем и безопасность цепочки поставок, важно, что у организаций есть возможность определить их требования информационной безопасности с ясностью и спецификой, чтобы затронуть отрасль информационной технологии и получить системы, компоненты, и сервисы, необходимые для предназначения и успеха в бизнесе. Чтобы гарантировать, что у организаций есть такая возможность, Специальная публикация 800-53 содержит ряд мер безопасности в семействе «Закупки систем и сервисов» (то есть, в семействе SA), определяющих требования для разработки информационных систем, продуктов информационных технологий и сервисов информационных систем. Поэтому, многие из мер безопасности в семействе SA адресованы разработчикам этих систем, компонентов и сервисов. Для организаций важно понимать, что область мер безопасности в семействе SA включает разработку всех систем/компонентов/сервисов и разработчиков, связанных с такой разработкой, независимо от того, проводится ли разработка внутренним персоналом организации или внешними разработчиками посредством процессов заключения контракта/приобретения. Затрагиваемые меры безопасности включают SA-8, SA-10, SA-11, SA-15, SA-16, SA-17, SA-20, и SA-21.

Основные принципы каталога

Меры безопасности и улучшения мер в Приложениях F и G в целом разработаны, чтобы быть нейтральными в отношении к политике и независимыми от технологий/реализация. Организации конкретизируют информацию о мерах безопасности и улучшениях мер двумя способами:

• Определяя детали реализации мер безопасности (например, зависимость от платформы) в соответствующем плане обеспечения безопасности для информационной системы или плане программы обеспечения безопасности организации; и

• Устанавливая конкретные значения в переменных разделах выбранных мер безопасности с помощью операций назначения и выбора.

Операции присвоения и выбора предоставляют организациям возможность специализировать меры безопасности и улучшения мер, основанные на требованиях безопасности организации или требованиях, вытекающих из федеральных законов, правительственных распоряжений, директив, политик, нормативных актов, стандартов или руководств. Определенные организацией параметры, используемые в операциях назначения и выбора в основных мерах безопасности, применяются также ко всем улучшениям мер безопасности, связанных с этими мерами безопасности. Улучшения мер безопасности усиливают фундаментальную возможность безопасности в основной мере безопасности, но не являются заменой тому, чтобы использовать операции назначения или выбора для обеспечения большей специфики мер безопасности. Операции назначения для мер безопасности и улучшений мер безопасности не содержат минимальные или максимальные значения (например, проверка планов действий при непредвиденных обстоятельствах, по крайней мере, ежегодно). Организации должны сверяться с конкретными федеральными законами, правительственными распоряжениями, директивами, нормативными актами, политиками, стандартами или руководствами как первичными источниками такой информации. Отсутствие минимальных и максимальных значений мер безопасности и улучшений мер не устраняет для организаций необходимость выполнения требований исходных публикаций мер безопасности.

Первая мера безопасности в каждом семействе (то есть, мера безопасности - 1) определяет требования для конкретных политик и процедур, которые необходимы для эффективной реализации других мер безопасности в семействе. Поэтому, отдельные меры безопасности и улучшения мер в конкретном семействе не говорят о разработке таких политик и процедур. Дополнительные разделы руководства мер безопасности и улучшений мер не содержат каких-либо требований или ссылок на FIPS или Специальные публикации NIST. Публикации NIST, однако, включены в раздел ссылок для каждой меры безопасности.

В поддержку инициативы Объединенной экспертной группы разработать единую основу информационной безопасности для федерального правительства, в это приложение включены меры безопасности и улучшения мер для систем национальной безопасности. Включение таких мер безопасности и улучшений не предназначено, чтобы предъявить требования безопасности к организациям, которые управляют системами национальной безопасности. Скорее организации могут использовать меры безопасности и улучшения мер на добровольной основе с одобрения федеральных должностных лиц, имеющих полномочия санкционирования по системам национальной безопасности. Кроме того, приоритеты мер безопасности и базовые наборы мер безопасности, перечисленные в Приложении D и в сводных блоках приоритетов и базовых наборов, находящихся ниже каждой меры безопасности в Приложении F, применяются к системам, не относящимся к национальной безопасности, *только* если иное не предписано федеральными должностными лицами с полномочиями по политике национальной безопасности.

Использование каталога

Организации используют меры безопасности[107] в федеральных информационных системах и средах, в которых эти системы работают, в соответствии с FIPS Публикацией 199, FIPS Публикацией 200 и Специальными публикациями NIST 800-37 и 800-39. Категорирование безопасности федеральной информации и информационных систем, как требуется FIPS Публикацией 199, является первым шагом в RMF.[108] Затем, организации выбирают соответствующий набор мер безопасности для их информационных систем, удовлетворяя минимальные требования безопасности, сформулированные в FIPS публикации 200. Приложение D включает три базовых набора мер безопасности, которые связаны с определяемыми уровнями воздействия информационные системы, как определено во время процесса категорирования безопасности.[109] После выбора базового набора мер, организации адаптируют базовые наборы путем: (i) идентификации/ определения общих мер безопасности; (ii) применения объектовых особенностей; (iii) выбора, если необходимо, компенсирующих мер безопасности; (iv) назначения величин параметров мер безопасности в операциях выбора и назначения; (v) дополнения базовых наборов мер безопасности дополнительными мерами безопасности и улучшениями мер из каталога мер безопасности; и (vi) предоставления дополнительной информации для реализации мер безопасности. Организации могут также использовать процесс адаптации базовых наборов мер совместно с концепцией оверлеев, которая описана в Разделе 3.2 и Приложении I. Оценки степени риска, как описано в Специальной публикации NIST 800-30, являются руководством и информацией к процессу выбора мер безопасности.[110]

ПРЕДОСТЕРЕЖЕНИЕ

ИСПОЛЬЗОВАНИЕ КРИПТОГРАФИИ

Если для защиты информации, основанной на выборе мер безопасности в Приложении F и последующей реализации информационными системами организации, требуется криптография, криптографические механизмы должны соответствовать применимым федеральным законам, правительственным распоряжениям, директивам, политике, нормативным актам, стандартам и руководствам. Это включает, одобренную NSA криптографию для защиты классифицированной информации, оценённую на соответствие FIPS криптографию для защиты неклассифицированной информации и одобренные NSA и совместимые с FIPS технологии и процессы управления ключами. Меры безопасности SC-12 и SC-13 предоставляют конкретную информацию о выборе соответствующих криптографических механизмов, включая стойкость таких механизмов.

[107] Меры безопасности из Специальной публикации 800-53 доступны онлайн и могут быть загружены в различных форматах с веб-сайта NIST: http://web.nvd.nist.gov/view/800-53/home.

[108] CNSS Инструкция 1253 даёт представление по категорированию безопасности систем национальной безопасности.

[109] CNSS Инструкция 1253 даёт представление о базовых наборах мер безопасности для систем национальной безопасности и конкретных требованиях по адаптации, связанных с такими системами.

[110] Есть дополнительные меры безопасности и улучшения мер, имеющиеся в каталоге, которые не используются ни в одном из начальных базовых наборов мер. Эти дополнительные меры безопасности и улучшения мер доступны организациям и могут использоваться в процессе адаптации, чтобы достигнуть необходимого уровня защиты в соответствии с оценками степени риска организаций.

Каталог мер безопасности представлен на страницах F-7…F-233 NIST Special Publication 800-53 Revision 4.

ПРИЛОЖЕНИЕ G

ПРОГРАММЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕРЫ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ ОБЩИМИ ДЛЯ ОРГАНИЗАЦИИ ПРОГРАММАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Закон об управлении безопасностью Федеральной информации (FISMA) требует, чтобы организации разработали и реализовали программу информационной безопасности всей организации, направленную на обеспечение информационной безопасности для информации и информационных систем, которые поддерживают деятельность и активы организации, включая предоставляемые или управляемые другой организацией, подрядчиком или другим источником. Меры безопасности управления программой информационной безопасности (PM), описанные в этом приложении реализуется, как правило, на уровне организации и не ориентированы на отдельные информационные системы организаций. Меры безопасности по управлению программами были разработаны, чтобы облегчить согласие с применимыми федеральными законами, правительственными распоряжениями, директивами, политиками, нормативными актами и стандартами. Меры безопасности не связаны с какими-либо уровнями воздействия из FIPS публикации 200 и поэтому, непосредственно не связаны с каким- либо из базовых наборов мер безопасности, описанных в Приложении D. Меры управления программами являются, однако, дополнением мер безопасности из Приложения F и сосредотачиваются на программных, общих для всей организации требованиях информационной безопасности, которые независимы от любой конкретной информационной системы и важны для управления программами информационной безопасности. Руководство по адаптации может быть применено к мерам управления программами таким же способом, как применяется к мерам безопасности в Приложении F. Организации определяют человека или людей, подотчетных и ответственных за разработку, реализацию, оценку, санкционирование и мониторинг мер управления программами. Организации документируют меры управления программами в *плане программы информационной безопасности*. Общий для организации план программы информационной безопасности дополняет отдельные планы обеспечения безопасности, разрабатываемые для каждой информационной системы организации. Вместе, планы обеспечения безопасности для отдельных информационных систем и программа информационной безопасности закрывают все количество мер безопасности, используемых организацией.

В дополнение к документированию мер управления программой информационной безопасности, план программы обеспечения безопасности предоставляет организации механизм, в центральном репозитории, чтобы задокументировать все меры безопасности из Приложения F, которые были определены, как *общие меры безопасности* (т.е. меры безопасности, наследуемые информационными системами организации).[111] Меры управления программой информационной безопасности и общие меры безопасности, содержавшиеся в плане программы информационной безопасности, реализуются, оцениваются по эффективности[112] и авторизуются высшим должностным лицом организации, с тем же самыми или подобными полномочиями и ответственностью за управление рисками, как у должностных лиц санкционирования для информационных систем. План действий и вехи разрабатываются и сопровождаются для мер управления программой и общих мер безопасности, которые, как полагают из оценки, менее чем эффективны. Меры управления программой информационной безопасности и общие меры безопасности являются также подчиненными тем же самым требованиям непрерывного мониторинга, как меры безопасности, используемые в отдельных информационных системах организации.

Таблица G-1 представляет сводку мер безопасности семейства управления программой из Приложения G. Организации могут использовать рекомендуемые *приоритетные коды*, связанные с каждой мерой управления программой, для помощи в принятии решений по упорядочиванию для реализации (то есть, у

[111] Общие меры безопасности - те меры безопасности, которые являются наследуемыми одной или более информационными системами организации и, таким образом, являются отдельными и отличными от мер управления программой информационной безопасности.

[112] Процедуры оценки по мерам управления программой и общим мерам безопасности могут быть найдены в Специальной публикации NIST 800-53A.

меры безопасности с Приоритетным Кодом 1 [P1], есть более высокий приоритет для реализации чем у меры безопасности с Приоритетным Кодом 2 [P2]; и у меры безопасности с Приоритетным Кодом 2 [P2] есть более высокий приоритет для реализации чем у меры безопасности с Приоритетным Кодом 3 [P3].

TABLE G-1: МЕРЫ БЕЗОПАСНОСТИ УПРАВЛЕНИЯ ПРОГРАММОЙ

№ МЕРЫ	НАЗВАНИЕ МЕРЫ	ПРИОРИТЕТ	НАЧАЛЬНЫЙ БАЗОВЫЙ НАБОР МЕР		
			НИЗКИЙ	СРЕДНИЙ	ВЫСОКИЙ
PM-1	План программы информационной безопасности	P1	**Вводятся в действие для всей организации Поддерживают программу информационной безопасности. Не связаны с базовыми мерами безопасности. Независимы от любого уровня воздействия на систему.**		
PM-2	Высший сотрудник по информационной безопасности	P1			
PM-3	Ресурсы информационной безопасности	P1			
PM-4	Формирование плана действий и вех	P1			
PM-5	Реестр информационных систем	P1			
PM-6	Меры по соблюдению информационной безопасности	P1			
PM-7	Архитектура предприятия	P1			
PM-8	План критической инфраструктуры	P1			
PM-9	Стратегия управления рисками	P1			
PM-10	Процесс санкционирования безопасности	P1			
PM-11	Определение процесса предназначения/деятельности	P1			
PM-12	Программа инсайдерских угроз	P1			
PM-13	Трудовые ресурсы информационной безопасности	P1			
PM-14	Проверка, обучение и мониторинг	P1			
PM-15	Контакты с группами и ассоциациями по безопасности	P3			
PM-16	Программа освоения угроз	P1			

ПРЕДОСТЕРЕЖЕНИЕ

Организациям требуется реализовать меры управления программой безопасности, чтобы обеспечить основу для программы информационной безопасности организации. Успешная реализация мер безопасности для информационных систем организации зависит от успешной реализации общих для организации мер управления программой. Однако, способ, в котором организации реализуют меры управления программой, зависит от конкретных характеристик организаций, включая, например, размер, сложность и требования предназначение/деятельности соответствующих организаций.

PM-1 ПЛАН ПРОГРАММЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мера безопасности: Организация:

a. Разрабатывает и распространяет общий для организации план программы информационной безопасности, который:

1. Обеспечивает обзор требований для программы обеспечения безопасности и описание мер управления программой обеспечения безопасности и существующих или планируемых общих мер безопасности для удовлетворения этим требованиям;

2. Включает идентификацию и назначение ролей, ответственности, обязанностей по управлению, координации среди сущностей организации и выполнению;

3. Отражает координацию среди сущностей организации, ответственных за различные аспекты информационной безопасности (то есть, технический, физический, персонала, кибер-физический); и

4. Является одобренным высшим должностным лицом с ответственностью и подконтрольностью в отношении рисков, относящимся к деятельности организации (включая предназначение, функции, имидж и репутацию), активам организации, людям, другим организациям и Нации;

b. Рассматривает план программы информационной безопасности общий для организации [Присвоение: определенная организацией частота];

c. Обновляет план, определяя изменения и проблемы организации, идентифицированные во время реализации плана или оценок мер безопасности; и

d. Защищает план программы информационной безопасности от несанкционированного раскрытия и модификации.

Дополнительное руководство: планы программы информационной безопасности могут быть на усмотрение организаций представлены в отдельных документах или в совокупности документов. Планы документируют меры управления программой и определенные организацией общие меры безопасности. Планы программы информационной безопасности предоставляют достаточную информацию о мерах безопасности/общих мерах безопасности управления программой (включая спецификацию параметров для любой операции *назначения* и *выбора* явно или ссылкой), чтобы определить реализации, которые однозначно совместимы с замыслом планов и определенным риском, который будет понесен, если планы будут реализованы как предназначено.

Планы обеспечения безопасности для отдельных информационных систем и план программы информационной безопасности общий для организации совместно, обеспечивают полный охват всех мер безопасности, используемых в организации. Общие меры безопасности документируются в приложении к плану программы информационной безопасности организации, если меры безопасности не включены в отдельный план обеспечения безопасности для информационной системы (например, меры безопасности, примененные как часть системы обнаружения вторжений, обеспечивающей защиту границ всей организации, наследуются одной или более информационными системами организации). Общий для организации план программы информационной безопасности должен указывать, какие отдельные планы обеспечения безопасности содержат описания общих мер безопасности.

У организаций есть возможность описать общие меры безопасности в отдельном документе или в нескольких документах. В случае нескольких документов, документы, описывающие общие меры безопасности, включаются как приложения к плану программы информационной безопасности. Если план программы информационной безопасности содержит несколько документов, организация определяет в каждом документе должностное лицо или должностные лица организации, ответственные за разработку, реализацию, оценку, санкционирование и мониторинг соответствующих общих мер безопасности. Например, организация может потребовать, чтобы Отдел управления средствами разработал, реализовал, оценил, санкционировал и непрерывно контролировал общие меры обеспечения физической защиты и защиты окружения из семейства PE, когда такие меры безопасности не связаны с определенной информационной системой, но при этом, поддерживают различные информационные системы. Связанная мера безопасности: PM-8.

Улучшения меры безопасности: Нет.

Ссылки: Нет.

PM-2 ВЫСШИЙ СОТРУДНИК ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мера безопасности: Организация назначает высшего сотрудника по информационной безопасности с задачей и ресурсами по координации, разработке, реализации и сопровождению общей для организации программы информационной безопасности.

Дополнительное руководство: сотрудник безопасности, описанный в этой мере безопасности, является должностным лицом организации. Для федерального агентства (как определено в применимых федеральных законах, правительственных распоряжениях, директивах, политиках или нормативных актах) это должностное лицо - Высший сотрудник информационной безопасности агентства. Организации могут также именовать это должностное лицо как Высший сотрудник информационной безопасности или Директор по информационной безопасности.

Улучшения меры безопасности: Нет.

Ссылки: нет.

PM-3 РЕСУРСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мера безопасности: Организация:

a. Гарантирует, что все основное планирование и инвестиционные запросы включают ресурсы, необходимые для реализации программы информационной безопасности и документируют все исключения к этому требованию;

b. Использует экономическую модель /Exhibit 300/Exhibit 53 для учета требуемых ресурсов; и

c. Гарантирует, что ресурсы информационной безопасности доступны для расходования, как запланировано.

Дополнительное руководство: Организации рассматривают установление приоритетов для усилий по информационной безопасности и, как части, необходимых ресурсов, назначают специализированную экспертизу и ресурсы по необходимости. Организации могут назначить и уполномочить Наблюдательный Совет по инвестициям (или подобную группу) для управления и обеспечения надзора за аспектами основного планирования, связанными с информационной безопасностью, и процесса контроля инвестиций. Связанные меры безопасности: PM-4, SA 2.

Улучшения меры безопасности: Нет.

Ссылки: Специальная публикация NIST 800-65.

PM-4 ФОРМИРОВАНИЕ ПЛАНА ДЕЙСТВИЙ И ВЕХ

Мера безопасности: Организация:

a. Реализует процесс для того, чтобы гарантировать, что план действий и вехи для программы обеспечения безопасности и соответствующих информационных систем организации:

1. Разработаны и поддерживаются;

2. Документируют корректирующие действия по информационной безопасности по соответствующему реагированию на риски к деятельности и активам организации, людям, другим организациям и Нации; и

3. Представляют отчеты в соответствии с требованиями FISMA OMB к отчетности.

b. Пересматривает план действий и вехи для согласованности со стратегией управления рисками организации и общими для организации приоритетами по ответным действиям на риски.

Дополнительное руководство: План действий и вехи - ключевой документ в программе информационной безопасности, подчиненный федеральным требованиям к отчетности, установленным OMB. С возрастанием акцента на общее для организации управление рисками на всех трех уровнях в иерархии управления рисками (т.е. организации, процессов предназначения/деятельности и информационных систем), организации рассматривают план действий и вехи с точки зрения организации, располагая по приоритетам действия по реакции на риски и гарантируя согласованность целями и задачам организации. Обновления плана действий и вех основываются на результатах оценок мер безопасности и действиях по постоянному мониторингу. Руководство OMB по отчетности FISMA, содержит инструкции относительно плана действий и вех организации. Связанная мера безопасности: CA-5.

Улучшения меры безопасности: Нет.

Ссылки: Меморандум 02-01 OMB; Специальная публикация NIST 800-37.

PM-5 РЕЕСТР ИНФОРМАЦИОННЫХ СИСТЕМ

Мера безопасности: Организация разрабатывает и сопровождает реестр своих информационных систем.

Дополнительное руководство: Эта мера безопасности определяется требованиями FISMA в отношении реестров. OMB предоставляет руководство по разработке реестров информационных систем и соответствующие требования к отчетности. По конкретным требованиям к отчетности по реестрам информационных систем организации консультируются с ежегодным руководством OMB по отчетности FISMA.

Улучшения меры безопасности: Нет.

Ссылки: Web: www.omb.gov.

PM-6 МЕРЫ ПО СОБЛЮДЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мера безопасности: Организация разрабатывает, мониторит и отчитывается относительно результатов мер по соблюдению информационной безопасности.

Дополнительное руководство: Меры по соблюдению - основанные на результатах выполнения метрики, используемые организацией, чтобы измерить эффективность или действенность программы информационной безопасности и мер безопасности, использованных в поддержку программы.

Улучшения меры безопасности: Нет.

Ссылки: Специальная публикация NIST 800-55.

PM-7 АРХИТЕКТУРА ПРЕДПРИЯТИЯ

Мера безопасности: организация разрабатывает архитектуру предприятия с соображениями в части информационной безопасности и результирующего риска к деятельности организации, активам организации, людям, другим организациям и Нации.

Дополнительное руководство: архитектура предприятия, разработанная организацией, должна ориентироваться на архитектуру федерального предприятия. Интеграция требований информационной безопасности и связанных мер безопасности в архитектуру предприятия организации помогает гарантировать, что рассмотрения безопасности осуществляются организациями с начала жизненного цикла разработки систем и непосредственно и явно связаны с процессами предназначения/ деятельности организации. Этот процесс интеграции требований безопасности также встраивается в архитектуру предприятия, интегральная *архитектура информационной безопасности* согласуется с управлением рисками организации и стратегиями информационной безопасности. Для PM-7, архитектура информационной безопасности разрабатывается на уровне системы систем (в целом для организации), представляя все информационные системы организации. Для PL-8 архитектура информационной безопасности разрабатывается на уровне, представляющем отдельную информационную систему, но при этом согласуется с архитектурой информационной безопасности, определенной для организации. Требования безопасности и интеграция мер безопасности наиболее эффективно достигаются через приложение Основ управления рисками и поддерживающие стандарты и руководства по обеспечению безопасности. Федеральная Методология архитектуры сегментов дает представление об интегрировании требований информационной безопасности и мер безопасности в архитектуру предприятия. Связанные меры безопасности: PL-2, PL-8, PM-11, RA-2, SA-3.

Улучшения меры безопасности: Нет.

Ссылки: Специальная публикация NIST 800-39; Web: www.fsam.gov.

PM-8 ПЛАН КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Мера безопасности: Организация определяет проблемы информационной безопасности при разработке, документировании и обновлении плана защиты критической инфраструктуры и ключевых ресурсов.

Дополнительное руководство: Стратегии защиты основаны на назначении приоритетов критическим активам и ресурсам. Требования и руководство по определению критической инфраструктуры и ключевых ресурсов и для подготовки соответствующего план защиты критической инфраструктуры содержатся в применимых федеральных законах, правительственных распоряжениях, директивах, политиках, нормативных актах, стандартах и руководствах. Связанные меры безопасности: PM-1, PM-9, PM-11, RA-3.

Улучшения меры безопасности: Нет.

Ссылки: HSPD 7; Национальный план защиты инфраструктуры.

PM-9 СТРАТЕГИЯ УПРАВЛЕНИЯ РИСКАМИ

Мера безопасности: Организация:

a. Разрабатывает всеобъемлющую стратегию управления рисками к деятельности и активам организации, людям, другим организациям и Нации, связанную с деятельностью и используемыми информационными системами;

b. Последовательно реализует стратегию управления рисками организации; и

c. Пересматривает и обновляет стратегию управления рисками [Назначение: определенная организацией частота] или по мере необходимости, чтобы соответствовать изменениям в организации.

Дополнительное руководство: Общая для организации стратегия управления рисками включает, например, однозначное определение допустимого риска для организации, приемлемых методологий оценки степени риска, стратегий снижения риска, процесса последовательной оценки риска в организации относительно допустимого риска организации и подходов к контролю риска в течение долгого времени. Использование функции ответственного за риски может облегчить соответствующее, общее для организации, приложение стратегии управления рисками. Общая для организации стратегия управления рисками может использовать связанную с риском информацию из других источников, и внутренних и внешних к организации, чтобы гарантировать, что стратегия является и всеобъемлющей и всесторонней. Связанная мера безопасности: RA-3.

Улучшения меры безопасности: Нет.

Ссылки: NIST Специальные публикации 800-30, 800-39.

PM-10 ПРОЦЕСС САНКЦИОНИРОВАНИЯ БЕЗОПАСНОСТИ

Мера безопасности: Организация:

a. Управляет (то есть, документирует, отслеживает и отчитывается) состоянием безопасности информационных систем организации и сред, в которых эти системы работают посредством процессов санкционирования безопасности;

b. Назначает людей выполнять конкретные роли и обязанности в рамках процесса управления рисками организации; и

c. Полностью интегрирует процессы санкционирования безопасности в общую для организации программу управления рисками.

Дополнительное руководство: Процессы санкционирования безопасности для информационных систем и сред эксплуатации требуют реализации общего для организации процесса управления рисками, Основ управления рисками и соответствующих стандартов и руководств по обеспечению безопасности. Конкретные роли в процессе управления рисками включают ответственного в организации за риски (функция) и назначенных для каждой информационной системы организации должностных лиц санкционирования и поставщика общих мер безопасности. Процессы санкционирования безопасности интегрируются с процессами постоянного мониторинга организации, чтобы облегчить постоянное понимание и принятие рисков к деятельности и активам организации, людям, другим организациям и Нации. Связанная мера безопасности: CA-6.

Улучшения меры безопасности: Нет.

Ссылки: Специальные публикации NIST 800-37, 800-39.

PM-11 ОПРЕДЕЛЕНИЕ ПРОЦЕССА ПРЕДНАЗНАЧЕНИЯ/ДЕЯТЕЛЬНОСТИ

Мера безопасности: Организация:

a. Устанавливает процессы предназначения/деятельности с соображениями в отношении информационной безопасности и результирующего риска к деятельности организации, активам организации, людям, другим организациям и Нации; и

b. Определяет потребности в защите информации, являющиеся результатом установления процессов предназначения/деятельности, и пересматривает процессы по мере необходимости, пока достигаемые потребности защиты не получены.

Дополнительное руководство: Потребности в защите информации являются независимыми от технологий, требуют возможностей по противостоянию угрозам организациям, людям или Нации через компрометацию информации (то есть, потерю конфиденциальности, целостности или доступности). Потребности в защите информации происходят из потребностей предназначения/деятельности, определенных организацией, процессов предназначения/деятельности, выбранных, чтобы удовлетворить заявленные потребности, и стратегии управления рисками организации. Потребности в защите информации определяют требуемые меры безопасности для организации и соответствующих информационных систем, поддерживающих процессы предназначения/деятельности. Неотъемлемым в определении потребностей организации в защите информации является понимание уровня неблагоприятного воздействия, которое может быть результатом, если происходит компрометация информации. Чтобы сделать такое определение потенциального воздействия, используется процесс категорирования безопасности. Определение процесса предназначения/деятельности и соответствующих требований по защите информации документируются организацией в соответствии с политикой и процедурами организации. Связанные меры безопасности: PM-7, PM-8, RA-2.

Улучшения меры безопасности: Нет.

Ссылки: FIPS публикация 199; Специальная публикация NIST 800-60.

PM-12 ПРОГРАММА ИНСАЙДЕРСКИХ УГРОЗ

Мера безопасности: Организация реализует программу инсайдерских угроз, которая включает группу кросс-дисциплинарной обработки инцидентов инсайдерских угроз.

Дополнительное руководство: Организациям, обрабатывающим классифицированную информацию, требуется, в соответствии с Правительственным распоряжением 13587 и Национальной политикой по инсайдерским угрозам, подготовить программы инсайдерских угроз. Стандарты и руководства, которые применяются к программам инсайдерских угроз в классифицированных средах, могут также быть эффективно использованы, чтобы улучшить безопасность Контролируемой неклассифицированной информации в системах, не относящихся к национальной безопасности. Программы инсайдерских угроз включают меры безопасности по обнаружению и предотвращению злонамеренной инсайдерской деятельности через централизованную интеграцию и анализ технической и нетехнической информации, чтобы идентифицировать потенциальные интересы инсайдерских угроз. Руководителем департамента/агентства назначается высшее должностное лицо организации, как ответственный человек по реализации и обеспечению надзора за программой. В дополнение к возможностям централизованной интеграции и анализа программ инсайдерских угроз, как минимум, готовятся политики и планы реализации департамента/агентства в отношении инсайдерских угроз, проводится централизованный мониторинг деятельности отдельных сотрудников на принадлежащих правительству классифицированных компьютерах, осуществляется обучение по инсайдерским угрозам сотрудников, получающим доступ к информации из всех офисов департамента/агентства (такой, как людские ресурсы, юридическая, физическая безопасность, безопасность персонала, информационные технологии, безопасность информационных систем и обеспечение правопорядка) для анализа инсайдерских угроз, и проводятся самооценки состояния департамента/агентства в отношении инсайдерских угроз.

Программы инсайдерских угроз могут усилить существующие группы организаций по обработке инцидентов, которые уже могут иметься на местах, такие, как группы реагирования на инциденты компьютерной безопасности. В этих усилиях особенно важны записи по людским ресурсам, поскольку

они являются убедительным свидетельством, показывающим, что некоторым типам преступлений инсайдеров часто предшествует нетехническое поведение на рабочем месте (например, повторяющиеся примеры раздраженного поведения и конфликтов с сослуживцами и другими коллегами). Эти предвестники могут лучше информировать и являться руководством для должностных лиц организации в более сфокусированных, целенаправленных контролирующих усилиях. Участие юридической группы важно, чтобы гарантировать, что все работы мониторинга выполнены в соответствии с соответствующим законодательством, директивами, нормативными актами, политиками, стандартами и руководствами. Связанные меры безопасности: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4, PM-1, PM-14.

Улучшения меры безопасности: Нет.

Ссылки: Правительственное распоряжение 13587.

PM-13 ТРУДОВЫЕ РЕСУРСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мера безопасности: Организация осуществляет разработку и совершенствование программы трудовых ресурсов информационной безопасности.

Дополнительное руководство: Разработка и развитие программы трудовых ресурсов информационной безопасности включает, например: (i) определение уровней знаний и умений, необходимых для выполнения обязанностей и задач по информационной безопасности; (ii) разработка основанной на ролях программы обучения для людей, которым назначили роли и обязанности по информационной безопасности; и (iii) предоставление стандартов для определения и создания индивидуальных квалификационных требований для должностных лиц и претендентов на должности, связанные с информационной безопасностью. Такие программы трудовых ресурсов могут также включать карьерный рост, связанный с информационной безопасностью, чтобы поощрить: (i) профессионалов информационной безопасности, по продвижению в области деятельности и заполнению позиций с большей ответственностью; и (ii) организации по заполнению должностей, связанных с информационной безопасностью, квалифицированным персоналом. Разработка и развитие программы трудовых ресурсов информационной безопасности осуществляется в дополнение к программам организации по освоению и обучению безопасности. Разработка и развитие программы трудовых ресурсов информационной безопасности сосредотачивается на разработке и учреждении базовых возможностей информационной безопасности выбранного персонала, требуемых для защиты деятельности, активов и людей организации. Связанные меры безопасности: AT-2, AT-3.

Улучшения меры безопасности: Нет.

Ссылки: Нет.

PM-14 ПРОВЕРКА, ОБУЧЕНИЕ И МОНИТОРИНГ

Мера безопасности: Организация:

a. Реализует процесс для гарантии того, что планы действий организации по проверке, обучению и мониторингу безопасности, связанные с информационными системами организации:

1. Разработаны и поддерживаются; и
2. Продолжают выполняться своевременно;

b. Пересматривает планы проверки, обучения и мониторинга для согласования со стратегией управления рисками и общими для организации приоритетами действий по реагированию на риски.

Дополнительное руководство: Эта мера гарантирует, что организации обеспечивают надзор действий по проверке, обучению и мониторингу безопасности, проводимых для всей организации, и что эти работы координируются. Ввиду важности непрерывного мониторинга программ, реализующих информационную безопасность на всех трех уровнях иерархии управления рисками, и широкого использования общих мер безопасности, организации координируют и консолидируют проверку и мониторинг работ, которые обычно проводятся как часть текущих оценок организации, поддерживающих множество мер безопасности. Работы по обучению безопасности, которые, как правило, сосредотачивался на отдельных информационных системах и конкретных ролях, также необходимо координировать для всех элементов организации. Планы и работы по проверке, обучению и мониторингу получают информацию из текущих угроза и оценок уязвимостей. Связакнные меры безопасности: AT-3, CA-7, CP-4, IR-3, SI-4.

Улучшения меры безопасности: Нет.

Ссылки: Специальные публикации NIST 800-16, 800-37, 800-53A, 800-137.

PM-15 КОНТАКТЫ С ГРУППАМИ И АССОЦИАЦИЯМИ ПО БЕЗОПАСНОСТИ

Мера безопасности: Организация устанавливает и оформляет контакт с выбранными группами и ассоциациями в рамках сообщества безопасности:

a. Чтобы облегчить постоянное образование и обучение безопасности для персонала организации;

b. Чтобы поддерживать соответствие с рекомендованными практиками, методами и технологиями безопасности; и

c. Чтобы делиться текущей связанной с безопасностью информацией включая угрозы, уязвимости и инциденты.

Дополнительное руководство: Постоянный контакт с группами и ассоциациями безопасности имеет первостепенную важность в среде быстро изменяющихся технологий и угроз. Группы и ассоциации безопасности включают, например, специальные группы, комиссии, профессиональные ассоциации, группы новостей и/или аналогичные группы профессионалов безопасности в подобных организациях. Организации выбирают группы и ассоциации, основываясь на функциях предназначения/деятельности организации. Организации совместно используют информацию об угрозах, уязвимостях и инцидентах, не противореча с применимыми федеральными законами, Правительственными распоряжениями, директивами, политиками, нормативными актами, стандартами и руководствами. Связанная мера безопасности: SI-5.

Улучшения меры безопасности: Нет.

Ссылки: Нет.

PM-16 ПРОГРАММА ОСВОЕНИЯ УГРОЗ

Мера безопасности: Организация реализует программу освоения угроз, которая включает возможность совместного использования информации между организациями.

Дополнительное руководство: Из-за постоянного изменения и повышения изощренности противников, особенно в части постоянных развивающихся угроз (APT), становится более вероятно, что противники могут успешно нарушать или ставить под угрозу информационные системы организаций. Один из лучших методов, чтобы довести эту озабоченность до организаций - делиться информацией об угрозах. Это может включать, например, совместное использование событий угроз (то есть, тактики, технологий и процедур), которые организации испытали, способы противодействия, которые организации нашли эффективными против определенных типов угроз, разведку угроз (то есть, выявление и предупреждение об угрозах, которые возможно реализуются). Совместное использование информации об угрозах может быть двусторонним (например, правительственно-коммерческие кооперации, правительственно-правительственные кооперации), или многосторонним (например, принятие организациями участия в консорциумах по совместно использованию информации об угрозах). Информация об угрозах может быть очень чувствительной, требующей специальных соглашений и защиты, или менее чувствительной и свободно совместно используемой. Связанные меры безопасности: PM-12, PM-16.

Улучшения меры безопасности: Нет.

Ссылки: Нет.

ПРИЛОЖЕНИЕ H

МЕЖДУНАРОДНЫЕ СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОТОБРАЖЕНИЯ МЕР БЕЗОПАСНОСТИ НА ISO/IEC 27001 И 15408

Таблицы отображения в этом приложении предоставляют организациям общую индикацию покрытия мер безопасности относительно ISO/IEC 27001, *Информационные технологии - Методы безопасности - Системы управления информационной безопасностью - Требования*[113] и ISO/IEC 15408, *Информационные технологии - Методы безопасности - Критерии оценки безопасности ИТ.*[114] ISO/IEC 27001 применяется ко всем типам организаций и определяет требования для того, чтобы установить, реализовать, управлять, контролировать, пересматривать, сопровождать и улучшать задокументированную систему управления информационной безопасностью (ISMS) в контексте коммерческих рисков. Специальная публикация NIST 800-39 включает руководство по управлению риском на уровне организации, уровне процесса предназначения/деятельности и уровне информационной системы, непротиворечивое с ISO/IEC 27001, и предоставляет дополнительные детали реализации федеральному правительству и его подрядчикам. ISO/IEC 15408 (также известный как Общие Критерии) обеспечивает функциональные требования и требования доверия для разработчиков информационных систем и компонентов информационных систем (то есть, продуктов информационных технологий). Так как многие из технических мер безопасности, определенных в Приложении F, реализованы в аппаратных средствах, программном обеспечении и компонентах встроенного микропрограммного обеспечения информационных систем, организации могут получить существенную выгоду из приобретения и применения продуктов информационных технологий, оцененных в соответствии с требованиями ISO/IEC 15408. Использование таких продуктов может представить свидетельства, что некоторые меры безопасности реализованы правильно, работают как предназначено и дают требуемый эффект в удовлетворении заявленным требованиям безопасности.

Ранее, отображение ISO/IEC 27001 было создано путём связывания основной темы безопасности, идентифицированной в каждой из базовых мер безопасности Специальной публикации 800-53 к подобной теме безопасности в стандарт ISO/IEC. Эта методология привела к отображению отношений мер безопасности, а не к отображению эквивалентных требований меры безопасности. Обновление ISO/IEC 27001:2013 обеспечило возможность переоценить, удовлетворила ли реализация мер безопасности из Специальной публикации 800-53 намерение отображенных мер безопасности из ISO/IEC 27001 и наоборот, удовлетворила ли реализация мер безопасности из ISO/IEC 27001 намерение отображенных мер безопасности из Специальной публикации 800-53. Чтобы успешно соответствовать критериям отображения, реализация отображенных мер безопасности должна иметь результат в эквивалентном состоянии информационной безопасности. Однако, это не означает, что эквивалентность мер безопасности, основанная исключительно на приведенных здесь таблицах отображения, должна быть предположена организациями. Несмотря на то, что пересмотренные отображения мер безопасности более точны, есть кроме того определенная степень субъективности в анализе отображения, потому что отображения являются не всегда однозначными и могут не быть абсолютно эквивалентными. Следующие примеры иллюстрируют некоторые из проблем отображения:

- **Пример 1:** Планирование на случай непредвиденных ситуаций Специальной публикации 800-53 и управление бесперебойной деятельностью ISO/IEC 27001, как считается, имеют подобную, но не ту же самую функциональность.
- **Пример 2:** В некоторых случаях, подобные темы учитываются в двух наборах мер безопасности, но имеют различный контекст, ракурс или область. Специальная публикация 800-53 адресует меру безопасности

[113] ISO/IEC 27001 был опубликован в октябре 2005 Международной организацией по стандартизации (ISO) и Международная электротехническая комиссия (IEC).

[114] ISO/IEC 15408 был опубликован в сентябре 2012 Международной организацией по стандартизации (ISO) и Международная электротехническая комиссия (IEC).

потока информации широко с точки зрения одобренного санкционирования для того, чтобы контролировать доступ между исходными и целевыми объектами, тогда как ISO/IEC 27001 учитывает информационный поток более узко, поскольку он применяется к взаимодействующим сетевым доменам.

- **Пример 3:** Мера безопасности A.6.1.1, Роли и обязанности по информационной безопасности, в ISO/IEC 27001 утверждает, что “все обязанности по информационной безопасности должны быть определены и выделены”, в то время как мера безопасности PM-10, в Процессе санкционирования безопасности, в Специальной публикации 800-53, которая отображена на A.6.1.1, имеет три различных части. Первая часть утверждает, что организация “назначает людей выполнять конкретные роли и обязанности …” Если A.6.1.1 отображен на PM-10, не обеспечивая дополнительной информации, организации могли бы предположить, что, если они реализуют A.6.1.1 (то есть, все обязанности определены и выделены), то намерение PM-10 было бы также полностью удовлетворено. Однако, это не имело бы место, так как другие две части PM-10 не будут учтены. Чтобы разрешить и разъяснить отображения мер безопасности, когда мера безопасности в правом столбце Таблиц H-1 и H-2 не полностью удовлетворяет намерение меры безопасности в левом столбце таблиц, мера безопасности в правом столбце определяется со звездочкой (*).

В нескольких случаях мера безопасности ISO/IEC 27001 может быть непосредственно отображены только на улучшение меры безопасности Специальной публикации 800-53. В таких случаях соответствующее улучшение определяется в Таблице H-2 указанием, что соответствующая мера безопасности ISO/IEC 27001 удовлетворяет только намерение указанного улучшения и не соответствует связанной основной мере безопасности из Специальной публикации 800-53 или любым другим улучшениям той основной меры безопансости. Там где улучшения не определены, мера безопасности ISO/IEC 27001 соответствует только базовой мере безопансости Специальной публикации 800-53.

И наконец, меры безопасности из ISO/IEC 27002 не рассмотрены в анализе отображения, так как стандарт является информативным, а не нормативеным.

Таблица H-1 обеспечивает отображение от мер безопасности в Специальной публикации NIST 800-53 к мерам безопасности в ISO/IEC 27001. Пожалуйста, рассмотрите вводный текст в начале Приложения H прежде, чем использовать отображения в Таблице H-1.

ТАБЛИЦА H-1: ОТОБРАЖЕНИЕ NIST SP 800-53 В ISO/IEC 27001

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AC-2	Account Management	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
AC-3	Access Enforcement	A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3
AC-4	Information Flow Enforcement	A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
AC-5	Separation of Duties	A.6.1.2
AC-6	Least Privilege	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
AC-7	Unsuccessful Logon Attempts	A.9.4.2
AC-8	System Use Notification	A.9.4.2
AC-9	Previous Logon (Access) Notification	A.9.4.2
AC-10	Concurrent Session Control	None
AC-11	Session Lock	A.11.2.8, A.11.2.9
AC-12	Session Termination	None
AC-13	**Withdrawn**	---
AC-14	Permitted Actions without Identification or Authentication	None
AC-15	**Withdrawn**	---
AC-16	Security Attributes	None
AC-17	Remote Access	A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2
AC-18	Wireless Access	A.6.2.1, A.13.1.1, A.13.2.1
AC-19	Access Control for Mobile Devices	A.6.2.1, A.11.2.6, A.13.2.1
AC-20	Use of External Information Systems	A.11.2.6, A.13.1.1, A.13.2.1
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	None
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	A.9.4.1*
AC-25	Reference Monitor	None
AT-1	Security Awareness and Training Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AT-2	Security Awareness Training	A.7.2.2, A.12.2.1
AT-3	Role-Based Security Training	A.7.2.2*
AT-4	Security Training Records	None
AT-5	**Withdrawn**	---
AU-1	Audit and Accountability Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
AU-2	Audit Events	None
AU-3	Content of Audit Records	A.12.4.1*
AU-4	Audit Storage Capacity	A.12.1.3
AU-5	Response to Audit Processing Failures	None
AU-6	Audit Review, Analysis, and Reporting	A.12.4.1, A.16.1.2, A.16.1.4
AU-7	Audit Reduction and Report Generation	None
AU-8	Time Stamps	A.12.4.4
AU-9	Protection of Audit Information	A.12.4.2, A.12.4.3, A.18.1.3
AU-10	Non-repudiation	None
AU-11	Audit Record Retention	A.12.4.1, A.16.1.7
AU-12	Audit Generation	A.12.4.1, A.12.4.3

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
AU-13	Monitoring for Information Disclosure	None
AU-14	Session Audit	A.12.4.1*
AU-15	Alternate Audit Capability	None
AU-16	Cross-Organizational Auditing	None
CA-1	Security Assessment and Authorization Policies and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CA-2	Security Assessments	A.14.2.8, A.18.2.2, A.18.2.3
CA-3	System Interconnections	A.13.1.2, A.13.2.1, A.13.2.2
CA-4	**Withdrawn**	---
CA-5	Plan of Action and Milestones	None
CA-6	Security Authorization	None
CA-7	Continuous Monitoring	None
CA-8	Penetration Testing	None
CA-9	Internal System Connections	None
CM-1	Configuration Management Policy and	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CM-2	Baseline Configuration	None
CM-3	Configuration Change Control	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
CM-4	Security Impact Analysis	A.14.2.3
CM-5	Access Restrictions for Change	A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1
CM-6	Configuration Settings	None
CM-7	Least Functionality	A.12.5.1*
CM-8	Information System Component Inventory	A.8.1.1, A.8.1.2
CM-9	Configuration Management Plan	A.6.1.1*
CM-10	Software Usage Restrictions	A.18.1.2
CM-11	User-Installed Software	A.12.5.1, A.12.6.2
CP-1	Contingency Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
CP-2	Contingency Plan	A.6.1.1, A.17.1.1, A.17.2.1
CP-3	Contingency Training	A.7.2.2*
CP-4	Contingency Plan Testing	A.17.1.3
CP-5	**Withdrawn**	---
CP-6	Alternate Storage Site	A.11.1.4, A.17.1.2, A.17.2.1
CP-7	Alternate Processing Site	A.11.1.4, A.17.1.2, A.17.2.1
CP-8	Telecommunications Services	A.11.2.2, A.17.1.2
CP-9	Information System Backup	A.12.3.1, A.17.1.2, A.18.1.3
CP-10	Information System Recovery and	A.17.1.2
CP-11	Alternate Communications Protocols	A.17.1.2*
CP-12	Safe Mode	None
CP-13	Alternative Security Mechanisms	A.17.1.2*
IA-1	Identification and Authentication Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
IA-2	Identification and Authentication (Organizational Users)	A.9.2.1
IA-3	Device Identification and Authentication	None
IA-4	Identifier Management	A.9.2.1
IA-5	Authenticator Management	A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3
IA-6	Authenticator Feedback	A.9.4.2
IA-7	Cryptographic Module Authentication	A.18.1.5
IA-8	Identification and Authentication (Non-Organizational Users)	A.9.2.1
IA-9	Service Identification and Authentication	None

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
IA-10	Adaptive Identification and Authentication	None
IA-11	Re-authentication	None
IR-1	Incident Response Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2
IR-2	Incident Response Training	A.7.2.2*
IR-3	Incident Response Testing	None
IR-4	Incident Handling	A.16.1.4, A.16.1.5, A.16.1.6
IR-5	Incident Monitoring	None
IR-6	Incident Reporting	A.6.1.3, A.16.1.2
IR-7	Incident Response Assistance	None
IR-8	Incident Response Plan	A.16.1.1
IR-9	Information Spillage Response	None
IR-10	Integrated Information Security Analysis Team	None
MA-1	System Maintenance Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MA-2	Controlled Maintenance	A.11.2.4*, A.11.2.5*
MA-3	Maintenance Tools	None
MA-4	Nonlocal Maintenance	None
MA-5	Maintenance Personnel	None
MA-6	Timely Maintenance	A.11.2.4
MP-1	Media Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
MP-2	Media Access	A.8.2.3, A.8.3.1, A.11.2.9
MP-3	Media Marking	A.8.2.2
MP-4	Media Storage	A.8.2.3, A.8.3.1, A.11.2.9
MP-5	Media Transport	A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6
MP-6	Media Sanitization	A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
MP-7	Media Use	A.8.2.3, A.8.3.1
MP-8	Media Downgrading	None
PE-1	Physical and Environmental Protection Policy	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PE-2	Physical Access Authorizations	A.11.1.2*
PE-3	Physical Access Control	A.11.1.1, A.11.1.2, A.11.1.3
PE-4	Access Control for Transmission Medium	A.11.1.2, A.11.2.3
PE-5	Access Control for Output Devices	A.11.1.2, A.11.1.3
PE-6	Monitoring Physical Access	None
PE-7	**Withdrawn**	---
PE-8	Visitor Access Records	None
PE-9	Power Equipment and Cabling	A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
PE-10	Emergency Shutoff	A.11.2.2*
PE-11	Emergency Power	A.11.2.2
PE-12	Emergency Lighting	A.11.2.2*
PE-13	Fire Protection	A.11.1.4, A.11.2.1
PE-14	Temperature and Humidity Controls	A.11.1.4, A.11.2.1, A.11.2.2
PE-15	Water Damage Protection	A.11.1.4, A.11.2.1, A.11.2.2
PE-16	Delivery and Removal	A.8.2.3, A.11.1.6, A.11.2.5
PE-17	Alternate Work Site	A.6.2.2, A.11.2.6, A.13.2.1
PE-18	Location of Information System Components	A.8.2.3, A.11.1.4, A.11.2.1
PE-19	Information Leakage	A.11.1.4, A.11.2.1
PE-20	Asset Monitoring and Tracking	A.8.2.3*
PL-1	Security Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PL-2	System Security Plan	A.14.1.1
PL-3	**Withdrawn**	---
PL-4	Rules of Behavior	A.7.1.2, A.7.2.1, A.8.1.3

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
PL-5	**Withdrawn**	---
PL-6	**Withdrawn**	---
PL-7	Security Concept of Operations	A.14.1.1*
PL-8	Information Security Architecture	A.14.1.1*
PL-9	Central Management	None
PS-1	Personnel Security Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
PS-2	Position Risk Designation	None
PS-3	Personnel Screening	A.7.1.1
PS-4	Personnel Termination	A.7.3.1, A.8.1.4
PS-5	Personnel Transfer	A.7.3.1, A.8.1.4
PS-6	Access Agreements	A.7.1.2, A.7.2.1, A.13.2.4
PS-7	Third-Party Personnel Security	A.6.1.1*, A.7.2.1*
PS-8	Personnel Sanctions	A.7.2.3
RA-1	Risk Assessment Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
RA-2	Security Categorization	A.8.2.1
RA-3	Risk Assessment	A.12.6.1*
RA-4	**Withdrawn**	---
RA-5	Vulnerability Scanning	A.12.6.1*
RA-6	Technical Surveillance Countermeasures Survey	None
SA-1	System and Services Acquisition Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SA-2	Allocation of Resources	None
SA-3	System Development Life Cycle	A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6
SA-4	Acquisition Process	A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2
SA-5	Information System Documentation	A.12.1.1*
SA-6	**Withdrawn**	---
SA-7	**Withdrawn**	---
SA-8	Security Engineering Principles	A.14.2.5
SA-9	External Information System Services	A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2
SA-10	Developer Configuration Management	A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7
SA-11	Developer Security Testing and Evaluation	A.14.2.7, A.14.2.8
SA-12	Supply Chain Protections	A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3
SA-13	Trustworthiness	None
SA-14	Criticality Analysis	None
SA-15	Development Process, Standards, and Tools	A.6.1.5, A.14.2.1,
SA-16	Developer-Provided Training	None
SA-17	Developer Security Architecture and Design	A.14.2.1, A.14.2.5
SA-18	Tamper Resistance and Detection	None
SA-19	Component Authenticity	None
SA-20	Customized Development of Critical Components	None
SA-21	Developer Screening	A.7.1.1
SA-22	Unsupported System Components	None
SC-1	System and Communications Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SC-2	Application Partitioning	None
SC-3	Security Function Isolation	None
SC-4	Information In Shared Resources	None
SC-5	Denial of Service Protection	None
SC-6	Resource Availability	None

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
SC-7	Boundary Protection	A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3
SC-8	Transmission Confidentiality and Integrity	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
SC-9	**Withdrawn**	---
SC-10	Network Disconnect	A.13.1.1
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.10.1.2
SC-13	Cryptographic Protection	A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5
SC-14	**Withdrawn**	---
SC-15	Collaborative Computing Devices	A.13.2.1*
SC-16	Transmission of Security Attributes	None
SC-17	Public Key Infrastructure Certificates	A.10.1.2
SC-18	Mobile Code	None
SC-19	Voice Over Internet Protocol	None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	None
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	None
SC-22	Architecture and Provisioning for Name/Address Resolution Service	None
SC-23	Session Authenticity	None
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Honeypots	None
SC-27	Platform-Independent Applications	None
SC-28	Protection of Information at Rest	A.8.2.3*
SC-29	Heterogeneity	None
SC-30	Concealment and Misdirection	None
SC-31	Covert Channel Analysis	None
SC-32	Information System Partitioning	None
SC-33	**Withdrawn**	---
SC-34	Non-Modifiable Executable Programs	None
SC-35	Honeyclients	None
SC-36	Distributed Processing and Storage	None
SC-37	Out-of-Band Channels	None
SC-38	Operations Security	A.12.x
SC-39	Process Isolation	None
SC-40	Wireless Link Protection	None
SC-41	Port and I/O Device Access	None
SC-42	Sensor Capability and Data	None
SC-43	Usage Restrictions	None
SC-44	Detonation Chambers	None
SI-1	System and Information Integrity Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2
SI-2	Flaw Remediation	A.12.6.1, A.14.2.2, A.14.2.3, A.16.1.3
SI-3	Malicious Code Protection	A.12.2.1
SI-4	Information System Monitoring	None
SI-5	Security Alerts, Advisories, and Directives	A.6.1.4*
SI-6	Security Function Verification	None
SI-7	Software, Firmware, and Information Integrity	None
SI-8	Spam Protection	None
SI-9	**Withdrawn**	---

NIST SP 800-53 CONTROLS		ISO/IEC 27001 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
SI-10	Information Input Validation	None
SI-11	Error Handling	None
SI-12	Information Handling and Retention	None
SI-13	Predictable Failure Prevention	None
SI-14	Non-Persistence	None
SI-15	Information Output Filtering	None
SI-16	Memory Protection	None
SI-17	Fail-Safe Procedures	None
PM-1	Information Security Program Plan	A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2
PM-2	Senior Information Security Officer	A.6.1.1*
PM-3	Information Security Resources	None
PM-4	Plan of Action and Milestones Process	None
PM-5	Information System Inventory	None
PM-6	Information Security Measures of Performance	None
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	None
PM-10	Security Authorization Process	A.6.1.1*
PM-11	Mission/Business Process Definition	None
PM-12	Insider Threat Program	None
PM-13	Information Security Workforce	A.7.2.2*
PM-14	Testing, Training, and Monitoring	None
PM-15	Contacts with Security Groups and Associations	A.6.1.4
PM-16	Threat Awareness Program	None

Таблица H-2 обеспечивает отображение от мер безопасности в ISO/IEC 27001 к мерам безопасности в Специальной публикации 800-53.[115] Пожалуйста, рассмотрите вводный текст в начале Приложения H прежде, чем использовать отображения в Таблице H-2.

ТАБЛИЦА H-2: ОТОБРАЖЕНИЕ ISO/IEC 27001 В NIST SP 800-53

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.5 Information Security Policies	
A.5.1 Management direction for information security	
A.5.1.1 Policies for information security	All XX-1 controls
A.5.1.2 Review of the policies for information security	All XX-1 controls
A.6 Organization of information security	
A.6.1 Internal organization	
A.6.1.1 Information security roles and responsibilities	All XX-1 controls, CM-9, CP-2,PS-7, SA-3, SA-9, PM- 2, PM-10
A.6.1.2 Segregation of duties	AC-5
A.6.1.3 Contact with authorities	IR-6
A.6.1.4 Contact with special interest groups	SI-5, PM-15
A.6.1.5 Information security in project management	SA-3, SA-9, SA-15
A.6.2 Mobile devices and teleworking	
A.6.2.1 Mobile device policy	AC-17, AC-18, AC-19
A.6.2.2 Teleworking	AC-3, AC-17, PE-17
A.7 Human Resources Security	
A.7.1 Prior to Employment	
A.7.1.1 Screening	PS-3, SA-21
A.7.1.2 Terms and conditions of employment	PL-4, PS-6
A.7.2 During employment	
A.7.2.1 Management responsibilities	PL-4, PS-6, PS-7, SA-9
A.7.2.2 Information security awareness, education, and training	AT-2, AT-3, CP-3, IR-2, PM-13
A.7.2.3 Disciplinary process	PS-8
A.7.3 Termination and change of employment	
A.7.3.1 Termination or change of employment responsibilities	PS-4, PS-5
A.8 Asset Management	
A.8.1 Responsibility for assets	
A.8.1.1 Inventory of assets	CM-8
A.8.1.2 Ownership of assets	CM-8
A.8.1.3 Acceptable use of assets	PL-4
A.8.1.4 Return of assets	PS-4, PS-5
A.8.2 Information Classification	
A.8.2.1 Classification of information	RA-2
A.8.2.2 Labelling of Information	MP-3
A.8.2.3 Handling of Assets	MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-18, PE- 20, SC-8, SC-28
A.8.3 Media Handling	
A.8.3.1 Management of removable media	MP-2, MP-4, MP-5, MP-6, MP-7
A.8.3.2 Disposal of media	MP-6
A.8.3.3 Physical media transfer	MP-5
A.9 Access Control	

[115] Использование обозначения, *мера безопасности XX-1* в отображении Таблицы H-2 отсылает к набору мер безопасности, представленных первой мерой безопасности в каждом семействе в Приложении F, где *XX* заполнитель для двухбуквенного идентификатора семейства.

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.9.1 Business requirement of access control	
A.9.1.1 Access control policy	AC-1
A.9.1.2 Access to networks and network services	AC-3, AC-6
A.9.2 User access management	
A.9.2.1 User registration and de-registration	AC-2, IA-2, IA-4, IA-5, IA-8
A.9.2.2 User access provisioning	AC-2
A.9.2.3 Management of privileged access rights	AC-2, AC-3, AC-6, CM-5
A.9.2.4 Management of secret authentication information of users	IA-5
A.9.2.5 Review of user access rights	AC-2
A.9.2.6 Removal or adjustment of access rights	AC-2
A.9.3 User responsibilities	
A.9.3.1 Use of secret authentication information	IA-5
A.9.4 System and application access control	
A.9.4.1 Information access restriction	AC-3, AC-24
A.9.4.2 Secure logon procedures	AC-7, AC-8, AC-9, IA-6
A.9.4.3 Password management system	IA-5
A.9.4.4 Use of privileged utility programs	AC-3, AC-6
A.9.4.5 Access control to program source code	AC-3, AC-6, CM-5
A.10 Cryptography	
A.10.1 Cryptographic controls	
A.10.1.1 Policy on the use of cryptographic controls	SC-13
A.10.1.2 Key Management	SC-12, SC-17
A.11 Physical and environmental security	
A.11.1 Secure areas	
A.11.1.1 Physical security perimeter	PE-3*
A.11.1.2 Physical entry controls	PE-2, PE-3, PE-4, PE-5
A.11.1.3 Securing offices, rooms and facilities	PE-3, PE-5
A.11.1.4 Protecting against external and environmental threats	CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE- 19
A.11.1.5 Working in secure areas	SC-42(3)*
A.11.1.6 Delivery and loading areas	PE-16
A.11.2 Equipment	
A.11.2.1 Equipment siting and protection	PE-9, PE-13, PE-14, PE-15, PE-18, PE-19
A.11.2.2 Supporting utilities	CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15
A.11.2.3 Cabling security	PE-4, PE-9
A.11.2.4 Equipment maintenance	MA-2, MA-6
A.11.2.5 Removal of assets	MA-2, MP-5, PE-16
A.11.2.6 Security of equipment and assets off-premises	AC-19, AC-20, MP-5, PE-17
A.11.2.7 Secure disposal or reuse of equipment	MP-6
A.11.2.8 Unattended user equipment	AC-11
A.11.2.9 Clear desk and clear screen policy	AC-11, MP-2, MP-4
A.12 Operations security	
A.12.1 Operational procedures and responsibilities	
A.12.1.1 Documented operating procedures	All XX-1 controls, SA-5
A.12.1.2 Change management	CM-3, CM-5, SA-10
A.12.1.3 Capacity management	AU-4, CP-2(2), SC-5(2)
A.12.1.4 Separation of development, testing, and operational environments	CM-4(1)*, CM-5*
A.12.2 Protection from malware	
A.12.2.1 Controls against malware	AT-2, SI-3

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.12.3 Backup	
A.12.3.1 Information backup	CP-9
A.12.4 Logging and monitoring	
A.12.4.1 Event logging	AU-3, AU-6, AU-11, AU-12, AU-14
A.12.4.2 Protection of log information	AU-9
A.12.4.3 Administrator and operator logs	AU-9, AU-12
A.12.4.4 Clock synchronization	AU-8
A.12.5 Control of operational software	
A.12.5.1 Installation of software on operational systems	CM-5, CM-7(4), CM-7(5), CM-11
A.12.6 Technical vulnerability management	
A.12.6.1 Management of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
A.12.6.2 Restrictions on software installation	CM-11
A.12.7 Information systems audit considerations	
A.12.7.1 Information systems audit controls	AU-5*
A.13 Communications security	
A.13.1 Network security management	
A.13.1.1 Network controls	AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10
A.13.1.2 Security of network services	CA-3, SA-9
A.13.1.3 Segregation in networks	AC-4, SC-7
A.13.2 Information transfer	
A.13.2.1 Information transfer policies and procedures	AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, SC-7, SC-8, SC-15
A.13.2.2 Agreements on information transfer	CA-3, PS-6, SA-9
A.13.2.3 Electronic messaging	SC-8
A.13.2.4 Confidentiality or nondisclosure agreements	PS-6
A.14 System acquisition, development and maintenance	
A.14.1 Security requirements of information systems	
A.14.1.1 Information security requirements analysis and specification	PL-2, PL-7, PL-8, SA-3, SA-4
A.14.1.2 Securing application services on public networks	AC-3, AC-4, AC-17, SC-8, SC-13
A.14.1.3 Protecting application services transactions	AC-3, AC-4, SC-7, SC-8, SC-13
A.14.2 Security in development and support processes	
A.14.2.1 Secure development policy	SA-3, SA-15, SA-17
A.14.2.2 System change control procedures	CM-3, SA-10, SI-2
A.14.2.3 Technical review of applications after operating platform changes	CM-3, CM-4, SI-2
A.14.2.4 Restrictions on changes to software packages	CM-3, SA-10
A.14.2.5 Secure system engineering principles	SA-8
A.14.2.6 Secure development environment	SA-3*
A.14.2.7 Outsourced development	SA-4, SA-10, SA-11, SA-12, SA-15
A.14.2.8 System security testing	CA-2, SA-11
A.14.2.9 System acceptance testing	SA-4, SA-12(7)
A.14.3 Test data	
A.14.3.1 Protection of test data	SA-15(9)*
A.15 Supplier Relationships	
A.15.1 Information security in supplier relationships	
A.15.1.1 Information security policy for supplier relationships	SA-12
A.15.1.2 Address security within supplier agreements	SA-4, SA-12

ISO/IEC 27001 CONTROLS	NIST SP 800-53 CONTROLS *Note: An asterisk (*) indicates that the ISO/IEC control does not fully satisfy the intent of the NIST control.*
A.15.1.3 Information and communication technology supply chain	SA-12
A.15.2 Supplier service delivery management	
A.15.2.1 Monitoring and review of supplier services	SA-9
A.15.2.2 Managing changes to supplier services	SA-9
A.16 Information security incident management	
A.16.1 Managing of information security incidents and improvements	
A.16.1.1 Responsibilities and procedures	IR-8
A.16.1.2 Reporting information security events	AU-6, IR-6
A.16.1.3 Reporting information security weaknesses	SI-2
A.16.1.4 Assessment of and decision on information security events	AU-6, IR-4
A.16.1.5 Response to information security incidents	IR-4
A.16.1.6 Learning from information security incidents	IR-4
A.16.1.7 Collection of evidence	AU-4*, AU-9*, AU-10(3)*, AU-11*
A.17 Information security aspects of business continuity management	
A.17.1 Information security continuity	
A.17.1.1 Planning information security continuity	CP-2
A.17.1.2 Implementing information security continuity	CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13
A.17.1.3 Verify, review, and evaluate information security continuity	CP-4
A.17.2 Redundancies	
A.17.2.1 Availability of information processing facilities	CP-2,CP-6, CP-7
A.18 Compliance	
A.18.1 Compliance with legal and contractual requirements	
A.18.1.1 Identification of applicable legislation and contractual requirements	All XX-1 controls
A.18.1.2 Intellectual property rights	CM-10
A.18.1.3 Protection of records	AC-3, AC-23, AU-9, AU-10, CP-9, SC-8, SC-8(1), SC-13, SC-28, SC-28(1)
A.18.1.4 Privacy and protection of personal information	Appendix J Privacy controls
A.18.1.5 Regulation of cryptographic controls	IA-7, SC-12, SC-13, SC-17
A.18.2 **Information security reviews**	
A.18.2.1 Independent review of information security	CA-2(1), SA-11(3)
A.18.2.2 Compliance with security policies and standards	All XX-1 controls, CA-2
A.18.2.3 Technical compliance review	CA-2

Примечание: контент Таблицы H-3, отображение от функциональных требований и требований доверия в ISO/IEC 15408 (Общие Критерии) к мерам безопасности в Специальной публикации 800-53, не затронут изменениями выше.

Таблица H-3 обеспечивает обобщенное отображение функциональных требований и требований доверия из ISO/IEC 15408 (Общие Критерии) к мерам безопасности в Специальной публикации 800-53. Таблица представляет *неформальное* соответствие между требованиями безопасности и мерами безопасности (то есть, таблица не предназначена, чтобы определить, является ли требования безопасности ISO/IEC 15408 полностью, частично или не удовлетворяющими соответствующим мерам безопасности). Однако таблица может служить выгодной начальной точкой для дальнейшего анализа соответствия. Организации предостерегают, что, удовлетворение требованиям безопасности ISO/IEC 15408 для определенного оцененного и подтвердившего соответствие продукта информационных технологий, что представлено присутствием некоторых мер безопасности из Приложения F, не подразумевает, что такие требования будут удовлетворены всюду по всей информационной системе (которая может состоять из многих, интегрированных отдельных компонентов продуктов). Дополнительная информация, объясняющая конкретные отображения, которые представлены в Таблице H-3, доступна в вебсайте Национального партнерства информационного доверия (NIAP): http://www.niap-cce vs.org.

ТАБЛИЦА H-3: ОТОБРАЖЕНИЕ ISO/IEC 15408 В NIST SP 800-53

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
Functional Requirements			
FAU_ARP.1	**Security Audit Automatic Response** Security Alarms	AU-5	**Response to Audit Processing Failures**
		AU-5(1)	**Response to Audit Processing Failures** *Audit Storage Capacity*
		AU-5(2)	**Response to Audit Processing Failures** *Real-Time Alerts*
		AU-5(3)	**Response to Audit Processing Failures** *Configurable Traffic Volume Thresholds*
		AU-5(4)	**Response to Audit Processing Failures** *Shutdown on Failure*
		PE-6(2)	**Monitoring Physical Access** *Automated Intrusion Recognition / Responses*
		SI-3	**Malicious Code Protection**
		SI-3(8)	**Malicious Code Protection** *Detect Unauthorized Commands*
		SI-4(5)	**Information System Monitoring** *System-Generated Alerts*
		SI-4(7)	**Information Systems Monitoring** *Automated Response to Suspicious Events*
		SI-4(22)	**Information Systems Monitoring** *Unauthorized Network Services*
		SI-7(2)	**Software, Firmware, and Information Integrity** *Automated Notifications of Integrity Violations*
		SI-7(5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*
		SI-7(8)	**Software, Firmware, and Information Integrity** *Auditing Capability for Significant Events*
FAU_GEN.1	**Security Audit Data Generation** Audit Data Generation	AU-2	**Audit Events**
		AU-3	**Content of Audit Records**
		AU-3(1)	**Content of Audit Records** *Additional Audit Information*
		AU-12	**Audit Generation**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FAU_GEN.2	**Security Audit Data Generation** User Identity Association	AU-3	**Content of Audit Records**
FAU_SAA.1	**Security Audit Analysis** Potential Violation Analysis	SI-4	**Information System Monitoring**
FAU_SAA.2	**Security Audit Analysis** Profile-Based Anomaly Detection	AC-2(12)	**Account Management** *Account Monitoring / Atypical Usage*
		SI-4	**Information System Monitoring**
FAU_SAA.3	**Security Audit Analysis** Simple Attack Heuristics	SI-3(7)	**Malicious Code Protection** *Non Signature-Based Protection*
		SI-4	**Information System Monitoring**
FAU_SAA.4	**Security Audit Analysis** Complex Attack Heuristics	SI-3(7)	**Malicious Code Protection** *Non Signature-Based Protection*
		SI-4	**Information System Monitoring**
FAU_SAR.1	**Security Audit Review** Audit Review	AU-7	**Audit Reduction and Report Generation**
FAU_SAR.2	**Security Audit Review** Restricted Audit Review	AU-9(6)	**Protection of Audit Information** *Read Only Access*
FAU_SAR.3	**Security Audit Review** Selectable Audit Review	AU-7	**Audit Reduction and Report Generation**
		AU-7(1)	**Audit Reduction and Report Generation** *Automatic Processing*
		AU-7(2)	**Audit Reduction and Report Generation** *Automatic Sort and Search*
FAU_SEL.1	**Security Audit Event Selection** Selective Audit	AU-12	**Audit Generation**
FAU_STG.1	**Security Audit Event Storage** Protected Audit Trail Storage	AU-9	**Protection of Audit Information**
FAU_STG.2	**Security Audit Event Storage** Guarantees of Audit Data Availability	AU-9	**Protection of Audit Information** *Alternate audit capability*
FAU_STG.3	**Security Audit Event Storage** Action In Case of Possible Audit Data Loss	AU-5	**Response to Audit Processing Failures**
		AU-5(1)	**Response to Audit Processing Failures** *Audit Storage Capacity*
		AU-5(2)	**Response To Audit Processing Failures** *Real-Time Alerts*
		AU-5(4)	**Response To Audit Processing Failures** *Shutdown on Failure*
FAU_STG.4	**Security Audit Event Storage** Prevention of Audit Data Loss	AU-4	**Audit Storage Capacity**
		AU-5	**Response to Audit Processing Failures**
		AU-5(2)	**Response To Audit Processing Failures** *Real-Time Alerts*
		AU-5(4)	**Response To Audit Processing Failures** *Shutdown on Failure*
FCO_NRO.1	**Non-Repudiation of Origin** Selective Proof of Origin	AU-10	**Non-Repudiation**
		AU-10(1)	**Non-Repudiation** *Association Of Identities*
		AU-10(2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FCO_NRO.2	**Non-Repudiation of Origin** Enforced Proof of Origin	AU-10	**Non-Repudiation**
		AU-10(1)	**Non-Repudiation** *Association Of Identities*
		AU-10(2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*
FCO_NRR.1	**Non-Repudiation of Receipt** Selective Proof of Receipt	AU-10	**Non-Repudiation**
		AU-10(1)	**Non-Repudiation** *Association Of Identities*
		AU-10(2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*
FCO_NRR.2	**Non-Repudiation of Receipt** Enforced Proof of Receipt	AU-10	**Non-Repudiation**
		AU-10(1)	**Non-Repudiation** *Association Of Identities*
		AU-10(2)	**Non-Repudiation** *Validate Binding of Information Producer Identity*
FCS_CKM.1	**Cryptographic Key Management** Cryptographic Key Generation	SC-12	**Cryptographic Key Establishment and Management**
FCS_CKM.2	**Cryptographic Key Management** Cryptographic Key Distribution	SC-12	**Cryptographic Key Establishment and Management**
FCS_CKM.3	**Cryptographic Key Management** Cryptographic Key Access	SC-12	**Cryptographic Key Establishment and Management**
FCS_CKM.4	**Cryptographic Key Management** Cryptographic Key Destruction	SC-12	**Cryptographic Key Establishment and Management**
FCS_COP.1	**Cryptographic Operation** Cryptographic Operation	SC-13	**Cryptographic Protection**
FDP_ACC.1	**Access Control Policy** Subset Access Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-3(4)	**Access Enforcement** *Discretionary Access Control*
		AC-3(7)	**Access Enforcement** *Role-Based Access Control*
FDP_ACC.2	**Access Control Policy** Complete Access Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-3(4)	**Access Enforcement** *Discretionary Access Control*
		AC-3(7)	**Access Enforcement** *Role-Based Access Control*
FDP_ACF.1	**Access Control Functions** Security Attribute Based Access Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-3(4)	**Access Enforcement** *Discretionary Access Control*
		AC-3(7)	**Access Enforcement** *Role-Based Access Control*
		AC-16	**Security Attributes**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SC-16	**Transmission of Security Attributes**
FDP_DAU.1	**Data Authentication** Basic Data Authentication	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SI-7(6)	**Software, Firmware, And Information Integrity** *Cryptographic Protection*
		SI-10	**Information Input Validation**
FDP_DAU.2	**Data Authentication** Data Authentication With Identity of Guarantor	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SI-7(6)	**Software, Firmware, And Information Integrity** *Cryptographic Protection*
		SI-10	**Information Input Validation**
FDP_ETC.1	**Export from the TOE** Export of User Data without Security Attributes	No Mapping.	
FDP_ETC.2	**Export from the TOE** Export of User Data with Security Attributes	AC-4(18)	**Information Flow Enforcement** *Security Attribute Binding*
		AC-16	**Security Attributes**
		AC-16(5)	**Security Attributes** *Attribute Displays for Output Devices*
		SC-16	**Transmission of Security Attributes**
FDP_IFC.1	**Information Flow Control Policy** Subset Information Flow Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-4	**Information Flow Enforcement**
		AC-4(1)	**Information Flow Enforcement** *Object Security Attributes*
FDP_IFC.2	**Information Flow Control Policy** Complete Information Flow Control	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-4	**Information Flow Enforcement**
FDP_IFF.1	**Information Flow Control Functions** Simple Security Attributes	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-4	**Information Flow Enforcement**
		AC-4(1)	**Information Flow Enforcement** *Object Security Attributes*
		AC-4(2)	**Information Flow Enforcement** *Processing Domains*
		AC-4(7)	**Information Flow Enforcement** *One-Way Flow Mechanisms*
		AC-16	**Security Attributes**
		SC-7	**Boundary Protection**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FDP_IFF.2	**Information Flow Control Functions** Hierarchical Security Attributes	AC-3	**Access Enforcement**
		AC-3(3)	**Access Enforcement** *Mandatory Access Control*
		AC-4(1)	**Information Flow Enforcement** *Object Security Attributes*
		AC-16	**Security Attributes**
FDP_IFF.3	**Information Flow Control Functions** Limited Illicit Information Flows	SC-31	**Covert Channel Analysis**
		SC-31(2)	**Covert Channel Analysis** *Maximum Bandwidth*
FDP_IFF.4	**Information Flow Control Functions** Partial Elimination of Illicit Information Flows	SC-31	**Covert Channel Analysis**
		SC-31(2)	**Covert Channel Analysis** *Maximum Bandwidth*
FDP_IFF.5	**Information Flow Control Functions** No Illicit Information Flows	SC-31	**Covert Channel Analysis**
		SC-31(2)	**Covert Channel Analysis** *Maximum Bandwidth*
FDP_IFF.6	**Information Flow Control Functions** Illicit Information Flow Monitoring	SC-31	**Covert Channel Analysis**
		SI-4(18)	**Information System Monitoring** *Analyze Traffic / Covert Exfiltration*
FDP_ITC.1	**Import from Outside of the TOE** Import of User Data without Security Attributes	AC-4(9)	**Information Flow Enforcement** *Human Reviews*
		AC-4(12)	**Information Flow Enforcement** *Data Type Identifiers*
FDP_ITC.2	**Import from Outside of the TOE** Import of User Data with Security Attributes	AC-4(18)	**Information Flow Enforcement** *Security Attribute Binding*
		AC-16	**Security Attributes**
		SC-16	**Transmission of Security Attributes**
FDP_ITT.1	**Internal TOE Transfer** Basic Internal Transfer Protection	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
		SC-5	**Denial of Service Protection**
FDP_ITT.2	**Internal TOE Transfer** Transmission Separation by Attribute	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
		SC-5	**Denial of Service Protection**
		AC-4(21)	**Information Flow Enforcement** *Physical / Logical Separation of Information Flows*
FDP_ITT.3	**Internal TOE Transfer** Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SC-8(1)	**Transmission Integrity** *Cryptographic or Alternate Physical Protection*
		SI-7(5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FDP_ITT.4	**Internal TOE Transfer** Attribute-Based Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Checks*
		SC-8(1)	**Transmission Integrity** *Cryptographic or Alternate Physical Protection*
		AC-4(21)	**Information Flow Enforcement** *Physical / Logical Separation of Information Flows*
		SI-7(5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*
FDP_RIP.1	**Residual Information Protection** Subset Residual Information Protection	SC-4	**Information in Shared Resources**
FDP_RIP.2	**Residual Information Protection** Full Residual Information Protection	SC-4	**Information in Shared Resources**
FDP_ROL.1	**Rollback** Basic Rollback	CP-10(2)	**Information System Recovery and Reconstitution** *Transaction Recovery*
FDP_ROL.2	**Rollback** Advanced Rollback	CP-10(2)	**Information System Recovery and Reconstitution** *Transaction Recovery*
FDP_SDI.1	**Stored Data Integrity** Stored Data Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Scans*
FDP_SDI.2	**Stored Data Integrity** Stored Data Integrity Monitoring and Action	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** *Integrity Scans*
		SI-7(5)	**Software, Firmware, and Information Integrity** *Automated Response to Integrity Violations*
FDP_UCT.1	**Inter-TSF User Data Confidentiality Transfer Protection** Basic Data Exchange Confidentiality	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
FDP_UIT.1	**Inter-TSF User Data Integrity Transfer Protection** Data Exchange Integrity	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** *Cryptographic or Alternate Physical Protection*
		SI-7	**Software, Firmware, and Information Integrity**
		SI-7(6)	**Software, Firmware, and Information Integrity** *Cryptographic Protection*
FDP_UIT.2	**Inter-TSF User Data Integrity Transfer Protection** Source Data Exchange Recovery	No Mapping.	

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FDP_UIT.3	**Inter-TSF User Data Integrity Transfer Protection** Destination Data Exchange Recovery	No Mapping.	
FIA_AFL.1	**Authentication Failure** Authentication Failure Handling	AC-7	**Unsuccessful Logon Attempts**
FIA_ATD.1	**User Attribute Definition** User Attribute Definition	AC-2	**Account Management**
		IA-2	**Identification and Authentication (Organizational Users)**
FIA_SOS.1	**Specification of Secrets** Verification of Secrets	IA-5	**Authenticator Management**
		IA-5(1)	**Authenticator Management** Password-Based Authentication
		IA-5(12)	**Authenticator Management** Biometric Authentication
FIA_SOS.2	**Specification of Secrets** TSF Generation of Secrets	IA-5	**Authenticator Management**
		IA-5(1)	**Authenticator Management** Password-Based Authentication
		IA-5(12)	**Authenticator Management** Biometric Authentication
FIA_UAU.1	**User Authentication** Timing of Authentication	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_UAU.2	**User Authentication** User Authentication Before Any Action	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_UAU.3	**User Authentication** Unforgeable Authentication	IA-2(8)	**Identification and Authentication (Organizational Users)** *Network Access To Privileged Accounts - Replay Resistant*
		IA-2(9)	**Identification and Authentication (Organizational Users)** *Network Access To Non-Privileged Accounts - Replay Resistant*
FIA_UAU.4	**User Authentication** Single-Use Authentication Mechanisms	IA-2(8)	**Identification and Authentication (Organizational Users)** *Network Access To Privileged Accounts - Replay Resistant*
		IA-2(9)	**Identification and Authentication (Organizational Users)** *Network Access To Non-Privileged Accounts - Replay Resistant*
FIA_UAU.5	**User Authentication** Multiple Authentication Mechanisms	IA-2(1)	**Identification and Authentication (Organizational Users)** Network Access To Privileged Accounts
		IA-2(2)	**Identification and Authentication (Organizational Users)** Network Access To Non-Privileged Accounts

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		IA-2(3)	**Identification and Authentication (Organizational Users)** Local Access To Privileged Accounts
		IA-2(4)	**Identification and Authentication (Organizational Users)** Local Access To Non-Privileged Accounts
		IA-2(6)	**Identification and Authentication (Organizational Users)** Network Access To Privileged Accounts - Separate Device
		IA-2(7)	**Identification and Authentication (Organizational Users)** Network Access To Non-Privileged Accounts - Separate Device
		IA-2(11)	**Identification and Authentication (Organizational Users)** Remote Access - Separate Device
FIA_UAU.6	**User Authentication** Re-Authenticating	IA-11	**Re-authentication**
FIA_UAU.7	**User Authentication** Protected Authentication Feedback	IA-6	**Authenticator Feedback**
FIA_UID.1	**User Identification** Timing of Identification	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_UID.2	**User Identification** User Identification Before Any Action	AC-14	**Permitted Actions without Identification or Authentication**
		IA-2	**Identification and Authentication (Organizational Users)**
		IA-8	**Identification and Authentication (Non-Organizational Users)**
FIA_USB.1	**User-Subject Binding** User-Subject Binding	AC-16(3)	**Security Attributes** Maintenance Of Attribute Associations By Information System
FMT_MOF.1	**Management of Functions in TSF** Management of Security Functions Behavior	AC-3(7)	**Access Enforcement** Role-Based Access Control
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
FMT_MSA.1	**Management of Security Attributes** Management of Security Attributes	AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
		AC-16(2)	**Security Attributes** Attribute Value Changes By Authorized Individuals
		AC-16(4)	**Security Attributes** Association of Attributes By Authorized Individuals
		AC-16(10)	**Security Attributes** Attribute Configuration By Authorized Individuals

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FMT_MSA.2	**Management of Security Attributes** Secure Security Attributes	AC-16	**Security Attributes**
		CM-6	**Configuration Settings**
		SI-10	**Information Input Validation**
FMT_MSA.3	**Management of Security Attributes** Static Attribute Initialization	No Mapping.	
FMT_MSA.4	**Management of Security Attributes** Security Attribute Value Inheritance	No Mapping.	
FMT_MTD.1	**Management of TSF Data** Management of TSF Data	AC-3(7)	**Access Enforcement** Role-Based Access Control
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
		AU-6(7)	**Audit Review, Analysis, and Reporting** Permitted Actions
		AU-9(4)	**Protection of Audit Information** Access By Subset of Privileged Users
FMT_MTD.2	**Management of TSF Data** Management of Limits on TSF Data	AC-3(7)	**Access Enforcement** Role-based Access Control
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
FMT_MTD.3	**Management of TSF Data** Secure TSF Data	SI-10	**Information Input Validation**
FMT_REV.1	**Revocation** Revocation	AC-3(7)	**Access Enforcement** Rose-based Access Control
		AC-3(8)	**Access Enforcement** Revocation Of Access Authorizations
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
FMT_SAE.1	**Security Attribute Expiration** Time-Limited Authorization	AC-3(7)	**Access Enforcement** Role-based Access Control
		AC-6	**Least Privilege**
		AC-6(1)	**Least Privilege** Authorize Access To Security Functions
FMT_SMF.1	**Specification of Management Functions** Specification of Management Functions	No Mapping.	
FMT_SMR.1	**Security Management Roles** Security Roles	AC-2(7)	**Account Management** Role-based schemes
		AC-3(7)	**Access Enforcement** Role-Based Access Control
		AC-5	**Separation of Duties**
		AC-6	**Least Privilege**
FMT_SMR.2	**Security Management Roles** Restrictions on Security Roles	AC-2(7)	**Account Management** Role-based schemes
		AC-3(7)	**Access Enforcement** Role-Based Access Control
		AC-5	**Separation of Duties**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		AC-6	**Least Privilege**
FMT_SMR.3	**Security Management Roles** Assuming Roles	AC-6(1)	**Least Privilege** Authorized Access to Security Functions
		AC-6(2)	**Least Privilege** Non-Privileged Access For Nonsecurity Functions
FPR_ANO.1	**Anonymity** Anonymity	No Mapping.	
FPR_ANO.2	**Anonymity** Anonymity Without Soliciting Information	No Mapping.	
FPR_PSE.1	**Pseudonymity** Pseudonymity	No Mapping.	
FPR_PSE.2	**Pseudonymity** Reversible Pseudonymity	No Mapping.	
FPR_PSE.3	**Pseudonymity** Alias Pseudonymity	No Mapping.	
FPR_UNL.1	**Unlinkability** Unlinkability	No Mapping.	
FPR_UNO.1	**Unobservability** Unobservability	No Mapping.	
FPR_UNO.2	**Unobservability** Allocation of Information Impacting Unobservability	No Mapping.	
FPR_UNO.3	**Unobservability** Unobservability Without Soliciting Information	No Mapping.	
FPR_UNO.4	**Unobservability** Authorized User Observability	No Mapping.	
FPT_FLS.1	**Fail Secure** Failure with Preservation of Secure State	SC-7(18)	**Boundary Protection** Fail Secure
		SC-24	**Fail in Known State**
FPT_ITA.1	**Availability of Exported TSF Data** Inter-TSF Availability within a Defined Availability Metric	CP-10	**Information System Recovery And Reconstitution** Restore Within Time Period
		SC-5	**Denial of Service Protection**
		SC-5(2)	**Denial of Service Protection** Excess Capacity/Bandwidth/Redundancy
		SC-5(3)	**Denial of Service Protection** Detection/Monitoring
FPT_ITC.1	**Confidentiality of Exported TSF Data** Inter-TSF Confidentiality During Transmission	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
FPT_ITI.1	**Integrity of Exported TSF Data** Inter-TSF Detection of Modification	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
		SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** Integrity Scans

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SI-7(5)	**Software, Firmware, and Information Integrity** Automated Response to Integrity Violations
		SI-7(6)	**Software, Firmware, and Information Integrity** Cryptographic Protection
FPT_ITI.2	**Integrity of Exported TSF Data** Inter-TSF Detection and Correction of Modification	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
		SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** Integrity Scans
		SI-7(5)	**Software, Firmware, and Information Integrity** Automated Response to Integrity Violations
		SI-7(6)	**Software, Firmware, and Information Integrity** Cryptographic Protection
FPT_ITT.1	**Internal TOE TSF Data Transfer** Basic Internal TSF Data Transfer Protection	SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
FPT_ITT.2	**Internal TOE TSF Data Transfer** TSF Data Transfer Separation	AC-4(21)	**Information Flow Enforcement** Physical / Logical Separation Of Information Flows
		SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic Or Alternate Physical Protection
FPT_ITT.3	**Internal TOE TSF Data Transfer** TSF Data Integrity Monitoring	SI-7	**Software, Firmware, and Information Integrity**
		SI-7(1)	**Software, Firmware, and Information Integrity** Integrity Scans
		SI-7(5)	**Software, Firmware, and Information Integrity** Automated Response to Integrity Violations
		SI-7(6)	**Software, Firmware, and Information Integrity** Cryptographic Protection
FPT_PHP.1	**TSF Physical Protection** Passive Detection of Physical Attack	PE-3(5)	**Physical Access Control** Tamper Protection
		PE-6(2)	**Monitoring Physical Access** Automated Intrusion Recognition / Responses
		SA-18	**Tamper Resistance and Detection**
FPT_PHP.2	**TSF Physical Protection** Notification of Physical Attack	PE-3(5)	**Physical Access Control** Tamper Protection
		PE-6(2)	**Monitoring Physical Access** Automated Intrusion Recognition / Responses
		SA-18	**Tamper Resistance and Detection**
FPT_PHP.3	**TSF Physical Protection** Resistance to Physical Attack	PE-3(5)	**Physical Access Control** Tamper Protection

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-18	**Tamper Resistance and Detection**
FPT_RCV.1	**Trusted Recovery** Manual Recovery	CP-10	**Information System Recovery and Reconstitution**
		CP-12	**Safe Mode**
FPT_RCV.2	**Trusted Recovery** Automated Recovery	CP-10	**Information System Recovery and Reconstitution**
		CP-12	**Safe Mode**
FPT_RCV.3	**Trusted Recovery** Automated Recovery Without Undue Loss	CP-10	**Information System Recovery and Reconstitution**
		CP-12	**Safe Mode**
FPT_RCV.4	**Trusted Recovery** Function Recovery	SI-6	**Security Function Verification**
		SI-10(3)	**Information Input Validation** Predictable Behavior
		SC-24	**Fail in Known State**
FPT_RPL.1	**Replay Detection** Replay Detection	IA-2(8)	**Identification and Authentication (Organizational Users)** Network Access To Privileged Accounts - Replay Resistant
		IA-2(9)	**Identification and Authentication (Organizational Users)** Network Access To Non-Privileged Accounts - Replay Resistant
		SC-23	**Session Authenticity**
		SI-3(9)	**Malicious Code Protection** Authenticate Remote Commands
FPT_SSP.1	**State Synchrony Protocol** Simple Trusted Acknowledgement	No Mapping.	
FPT_SSP.2	**State Synchrony Protocol** Mutual Trusted Acknowledgement	No Mapping.	
FPT_STM.1	**Time Stamps** Reliable Time Stamps	AU-8	**Time Stamps**
FPT_TDC.1	**Inter-TSF TSF Data Consistency** Inter-TSF Basic Data Consistency	AC-16(7)	**Security Attributes** | Consistent Attribute Interpretation
		AC-16(8)	**Security Attributes** Association Techniques/Technologies
FPT_TEE.1	**Testing of External Entities** Testing of External Entities	SI-6	**Security Functionality Verification**
FPT_TRC.1	**Internal TOE TSF Data Replication Consistency** Internal TSF Consistency	SI-7	**Software, Firmware, and Information Integrity**
FPT_TST.1	**TSF Self Test** TSF Testing	SI-6	**Security Functionality Verification**
		SI-7	**Software, Firmware, and Information Integrity**
FRU_FLT.1	**Fault Tolerance** Degraded Fault Tolerance	AU-15	**Alternate Audit Capability**
		CP-11	**Alternate Communications Protocols**
		SC-24	**Fail in Known State**
		SI-13	**Predictable Failure Prevention**
		SI-13(1)	**Predictable Failure Prevention** Transferring Component Responsibilities

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SI-13(2)	**Predictable Failure Prevention** Time Limit on Process Execution Without Supervision
		SI-13(3)	**Predictable Failure Prevention** Manual Transfer Between Components
		SI-13(4)	**Predictable Failure Prevention** Standby Component Installation/Notification
		SI-13(5)	**Predictable Failure Prevention** Failover Capability
FRU_FLT.2	**Fault Tolerance** Limited Fault Tolerance	AU-15	**Alternate Audit Capability**
		CP-11	**Alternate Communications Protocols**
		SC-24	**Fail in Known State**
		SI-13	**Predictable Failure Prevention**
		SI-13(1)	**Predictable Failure Prevention** Transferring Component Responsibilities
		SI-13(2)	**Predictable Failure Prevention** Time Limit on Process Execution Without Supervision
		SI-13(3)	**Predictable Failure Prevention** Manual Transfer Between Components
		SI-13(4)	**Predictable Failure Prevention** Standby Component Installation/Notification
		SI-13(5)	**Predictable Failure Prevention** Failover Capability
FRU_PRS.1	**Priority of Service** Limited Priority of Service	SC-6	**Resource Availability**
FRU_PRS.2	**Priority of Service** Full Priority of Service	SC-6	**Resource Availability**
FRU_RSA.1	**Resource Allocation** Maximum Quotas	SC-6	**Resource Availability**
FRU_RSA.2	**Resource Allocation** Minimum and Maximum Quotas	SC-6	**Resource Availability**
FTA_LSA.1	**Limitation on Scope of Selectable Attributes** Limitation on Scope of Selectable Attributes	AC-2(6)	**Account Management** Dynamic Privilege Management
		AC-2(11)	**Account Management** Usage Conditions
FTA_MCS.1	**Limitation on Multiple Concurrent Sessions** Basic Limitation on Multiple Concurrent Sessions	AC-10	**Concurrent Session Control**
FTA_MCS.2	**Limitation on Multiple Concurrent Sessions** Per-User Limitation on Multiple Concurrent Sessions	AC-10	**Concurrent Session Control**
FTA_SSL.1	**Session Locking and Termination** TSF-Initiated Session Locking	AC-11	**Session Lock**
		AC-11(1)	**Session Lock** Pattern-Hiding Displays
FTA_SSL.2	**Session Locking and Termination** User-Initiated Locking	AC-11	**Session Lock**
		AC-11(1)	**Session Lock** Pattern-Hiding Displays

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
FTA_SSL.3	**Session Locking and Termination** TSF-Initiated Termination	AC-12	**Session Termination**
		SC-10	**Network Disconnect**
FTA_SSL.4	**Session Locking and Termination** User-Initiated Termination	AC-12(1)	**Session Termination** User-Initiated Logouts / Message Displays
FTA_TAB.1	**TOE Access Banners** Default TOE Access Banners	AC-8	**System Use Notification**
FTA_TAH.1	**TOE Access History** TOE Access History	AC-9	**Previous Login (Access) Notification**
		AC-9(1)	**Previous Login (Access) Notification** Unsuccessful Logons
FTA_TSE.1	**TOE Session Establishment** TOE Session Establishment	AC-2(11)	**Account Management** Usage Conditions
FTP_ITC.1	**Inter-TSF Trusted Channel** Inter-TSF Trusted Channel	IA-3(1)	**Device Identification and Authentication** Cryptographic Bidirectional Authentication
		SC-8	**Transmission Confidentiality and Integrity**
		SC-8(1)	**Transmission Confidentiality and Integrity** Cryptographic or Alternate Physical Protection
FTP_TRP.1	**Trusted Path** Trusted Path	SC-11	**Trusted Path**
Assurance Requirements			
ASE_INT.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**ST Introduction** ST Introduction	SA-4	**Acquisition Process**
ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Conformance Claims** Conformance Claims	PL-2	**System Security Plan**
		SA-4(7)	**Acquisition Process** NIAP-Approved Protection Profiles
ASE_SPD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Problem Definition** Security Problem Definition	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_OBJ.1 EAL1	**Security Objectives** Security Objectives for the Operational Environment	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_OBJ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Objectives** Security Objectives	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ASE_ECD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Extended Components Definition** Extended Components Definition	No Mapping.	
ASE_REQ.1 EAL1	**Security Requirements** Stated Security Requirements	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_REQ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Requirements** Derived Security Requirements	PL-2	**System Security Plan**
		SA-4	**Acquisition Process**
ASE_TSS.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**TOE Summary Specification** TOE Summary Specification	PL-2	**System Security Plan**
		SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
ASE_TSS.2	**TOE Summary Specification** TOE Summary Specification with Architectural Design Summary	PL-2	**System Security Plan**
		SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information For Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_ARC.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Architecture** Security Architecture Description	AC-25	**Reference Monitor**
		SA-17	**Developer Security Architecture and Design**
		SA-18	**Tamper Resistance and Detection**
		SC-3	**Security Function Isolation**
		SC-3(1)	**Security Function Isolation** Hardware Separation
		SC-3(2)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-41	**Process Isolation**
ADV_FSP.1 EAL1	**Functional Specification** Basic Functional Specification	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
ADV_FSP.2 EAL2	**Functional Specification** Security-Enforcing Functional Specification	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.3 EAL3	**Functional Specification** Functional Specification With Complete Summary	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.4 EAL4	**Functional Specification** Complete Functional Specification	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.5 EAL5 EAL6	**Functional Specification** Complete Semi-Formal Functional Specification with Additional Error Information	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_FSP.6 EAL7	**Functional Specification** Complete Semi-Formal Functional Specification with Additional Formal Specification	SA-4(1)	**Acquisition Process** Functional Properties of Security Controls
		SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(3)	**Developer Security Architecture and Design** Formal Correspondence
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_IMP.1 EAL4 EAL5	**Implementation Representation** Implementation Representation of the TSF	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
ADV_IMP.2 EAL6 EAL7	**Implementation Representation** Complete Mapping of the Implementation Representation of the TSF	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17(3)	**Developer Security Architecture and Design** Formal Correspondence
ADV_INT.1	**TSF Internals** Well-Structured Subset of TSF Internals	SA-8	**Security Engineering Principles**
		SC-3(3)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-3(4)	**Security Function Isolation** Module Coupling and Cohesiveness
		SC-3(5)	**Security Function Isolation** Layered Structures

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ADV_INT.2 EAL5	**TSF Internals** Well-Structured Internals	SA-8	**Security Engineering Principles**
		SC-3(3)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-3(4)	**Security Function Isolation** Module Coupling and Cohesiveness
		SC-3(5)	**Security Function Isolation** Layered Structures
ADV_INT.3 EAL6 EAL7	**TSF Internals** Minimally Complex Internals	SA-8	**Security Engineering Principles**
		SA-17(5)	**Developer Security Architecture and Design** Conceptually Simple Design
		SC-3(3)	**Security Function Isolation** Minimize Nonsecurity Functionality
		SC-3(4)	**Security Function Isolation** Module Coupling and Cohesiveness
		SC-3(5)	**Security Function Isolation** Layered Structures
		AC-25	**Reference Monitor**
ADV_SPM.1 EAL6 EAL7	**Security Policy Modeling** Formal TOE Security Policy Model	SA-17(1)	**Developer Security Architecture and Design** Formal Policy Model
		SA-17(3)	**Developer Security Architecture and Design** Formal Correspondence
ADV_TDS.1 EAL2	**TOE Design** Basic Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_TDS.2 EAL3	**TOE Design** Architectural Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_TDS.3 EAL4	**TOE Design** Basic Modular Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
ADV_TDS.4 EAL5	**TOE Design** Semiformal Modular Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
		SA-17(2)	**Developer Security Architecture and Design** Security Relevant Components
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ADV_TDS.5 EAL6	**TOE Design** Complete Semiformal Modular Design	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
		SA-17(2)	**Developer Security Architecture and Design** Security Relevant Components
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
ADV_TDS.6 EAL7	**TOE Design** Complete Semiformal Modular Design with Formal High-Level Design Presentation	SA-4(2)	**Acquisition Process** Design / Implementation Information for Security Controls
		SA-17	**Developer Security Architecture and Design**
		SA-17(2)	**Developer Security Architecture and Design** Security Relevant Components
		SA-17(3)	**Developer Security Architecture and Design** Formal Correspondence
		SA-17(4)	**Developer Security Architecture and Design** Informal Correspondence
AGD_OPE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Operational User Guidance** Operational User Guidance	SA-5	**Information System Documentation**
AGD_PRE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Preparative Procedures** Preparative Procedures	SA-5	**Information System Documentation**
ALC_CMC.1 EAL1	**CM Capabilities** Labeling of the TOE	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMC.2 EAL2	**CM Capabilities** Use of a CM System	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMC.3 EAL3	**CM Capabilities** Authorization Controls	CM-3	**Configuration Change Control**
		CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMC.4 EAL4 EAL5	**CM Capabilities** Production Support, Acceptance Procedures, and Automation	CM-3	**Configuration Change Control**
		CM-3(1)	**Configuration Change Control** Automated Document / Notification / Prohibition of Changes
		CM-3(3)	**Configuration Change Control** Automated Change Implementation
		CM-9	**Configuration Management Plan**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-10	**Developer Configuration Management**
ALC_CMC.5 EAL6 EAL7	**CM Capabilities** Advanced Support	CM-3	**Configuration Change Control**
		CM-3(1)	**Configuration Change Control** Automated Document / Notification / Prohibition of Changes
		CM-3(2)	**Configuration Change Control** Test / Validate / Document Changes
		CM-3(3)	**Configuration Change Control** Automated mechanisms to field and deploy
		CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.1 EAL1	**CM Scope** TOE CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.2 EAL2	**CM Scope** Parts of the TOE CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.3 EAL3	**CM Scope** Implementation Representation CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.4 EAL4	**CM Scope** Problem Tracking CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_CMS.5 EAL5 EAL6 EAL7	**CM Scope** Development Tools CM Coverage	CM-9	**Configuration Management Plan**
		SA-10	**Developer Configuration Management**
ALC_DEL.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Delivery** Delivery Procedures	MP-5	**Media Transport**
		SA-10(1)	**Developer Configuration Management** Software / Firmware Integrity Verification
		SA-10(6)	**Developer Configuration Management** Trusted Distribution
		SA-18	**Tamper Resistance and Detection**
		SA-19	**Component Authenticity**
ALC_DVS.1 EAL3 EAL4 EAL5	**Development Security** Identification of Security Measures	SA-1	**System and Services Acquisition Policy and Procedures**
		SA-3	**System Development Lifecycle**
		SA-12	**Supply Chain Protection**
ALC_DVS.2 EAL6 EAL7	**Development Security** Sufficiency of Security Measures	CM-5	**Access Restrictions for Change**
		SA-3	**System Development Lifecycle**
		SA-12	**Supply Chain Protection**
ALC_FLR.1	**Flaw Remediation** Basic Flaw Remediation	SA-10	**Developer Configuration Management**
		SA-11	**Developer Security Testing / Evaluation**
		SI-2	**Flaw Remediation**
ALC_FLR.2	**Flaw Remediation** Flaw Reporting Procedures	SA-10	**Developer Configuration Management**
		SA-11	**Developer Security Testing / Evaluation**
		SI-2	**Flaw Remediation**
ALC_FLR.3	**Flaw Remediation** Systematic Flaw Remediation	SA-10	**Developer Configuration Management**
		SA-11	**Developer Security Testing / Evaluation**
		SI-2	**Flaw Remediation**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ALC_LCD.1 EAL3 EAL4 EAL5 EAL6	**Life-Cycle Definition** Developer Defined Life-Cycle Model	SA-3	**System Development Life Cycle**
		SA-15	**Development Process, Standards, and Tools**
ALC_LCD.2 EAL7	**Life-Cycle Definition** Measurable Life-Cycle Model	SA-3	**System Development Life Cycle**
		SA-15	**Development Process, Standards, and Tools**
ALC_TAT.1 EAL4	**Tools and Techniques** Well-Defined Development Tools	SA-15	**Development Process, Standards, and Tools**
ALC_TAT.2 EAL5	**Tools and Techniques** Compliance with Implementation Standards	SA-15	**Development Process, Standards, and Tools**
ALC_TAT.3 EAL6 EAL7	**Tools and Techniques** Compliance with Implementation Standards – All Parts	SA-15	**Development Process, Standards, and Tools**
ATE_COV.1 EAL2	**Coverage** Evidence of Coverage	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_COV.2 EAL3 EAL4 EAL5	**Coverage** Analysis of Coverage	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_COV.3 EAL6 EAL7	**Coverage** Rigorous Analysis of Coverage	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.1 EAL3	**Depth** Testing: Basic Design	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.2 EAL4	**Depth** Testing: Security Enforcing Modules	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.3 EAL5 EAL6	**Depth** Testing: Modular Design	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_DPT.4 EAL7	**Depth** Testing: Implementation Representation	SA-11	**Developer Security Testing and Evaluation**
		SA-11(7)	**Developer Security Testing and Evaluation** *Verify Scope of Testing / Evaluation*
ATE_FUN.1 EAL2 EAL3 EAL4 EAL5	**Functional Tests** Functional Testing	SA-11	**Developer Security Testing and Evaluation**
ATE_FUN.2 EAL6 EAL7	**Functional Tests** Ordered Functional Testing	SA-11	**Developer Security Testing and Evaluation**
ATE_IND.1 EAL1	**Independent Testing** Independent Testing – Conformance	CA-2	**Security Assessments**
		CA-2(1)	**Security Assessments** *Independent Assessors*
		SA-11(3)	**Developer Security Testing and Evaluation** *Independent Verification of Assessment Plans / Evidence*

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
ATE_IND.2 EAL2 EAL3 EAL4 EAL5 EAL6	**Independent Testing** Independent Testing – Sample	CA-2	**Security Assessments**
		CA-2(1)	**Security Assessments** *Independent Assessors*
		SA-11(3)	**Developer Security Testing and Evaluation** *Independent Verification of Assessment Plans / Evidence*
ATE_IND.3 EAL7	**Independent Testing** Independent Testing – Complete	CA-2	**Security Assessments**
		CA-2(1)	**Security Assessments** *Independent Assessors*
		SA-11(3)	**Developer Security Testing and Evaluation** *Independent Verification of Assessment Plans / Evidence*
AVA_VAN.1 EAL1	**Vulnerability Analysis** Vulnerability Survey	CA-2(2)	**Security Assessments** *Specialized Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.2 EAL2 EAL3	**Vulnerability Analysis** Vulnerability Analysis	CA-2(2)	**Security Assessments** *Specialized Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.3 EAL4	**Vulnerability Analysis** Focused Vulnerability Analysis	CA-2(2)	**Security Assessments** *Specialized Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.4 EAL5	**Vulnerability Analysis** Methodical Vulnerability Analysis	CA-2(2)	**Security Assessments** *Types of Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
AVA_VAN.5 EAL6 EAL7	**Vulnerability Analysis** Advanced Methodical Vulnerability Analysis	CA-2(2)	**Security Assessments** *Types of Assessments*
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**

ISO/IEC 15408 REQUIREMENTS		NIST SP 800-53 CONTROLS	
		SA-11(2)	**Developer Security Testing and Evaluation** *Threat And Vulnerability Analyses / Flaw Remediation*
		SA-11(5)	**Developer Security Testing and Evaluation** *Penetration Testing*
ACO_COR.1	**Composition Rationale** Composition Rationale	SA-17	**Developer Security Architecture and Design**
ACO_DEV.1	**Development Evidence** Functional Description	SA-17	**Developer Security Architecture and Design**
ACO_DEV.2	**Development Evidence** Basic Evidence of Design	SA-17	**Developer Security Architecture and Design**
ACO_DEV.3	**Development Evidence** Detailed Evidence of Design	SA-17	**Developer Security Architecture and Design**
ACO_REL.1	**Reliance on Dependent Component** Basic Reliance Information	SA-17	**Developer Security Architecture and Design**
ACO_REL.2	**Reliance on Dependent Component** Reliance Information	SA-17	**Developer Security Architecture and Design**
ACO_CTT.1	**Composed TOE Testing** Interface Testing	SA-11	**Developer Security Testing and Evaluation**
ACO_CTT.2	**Composed TOE Testing** Rigorous Interface Testing	SA-11	**Developer Security Testing and Evaluation**
ACO_VUL.1	**Composition Vulnerability Analysis** Composition Vulnerability Review	CA-2	**Security Assessments**
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11	**Developer Security Testing and Evaluation**
ACO_VUL.2	**Composition Vulnerability Analysis** Composition Vulnerability Analysis	CA-2	**Security Assessments**
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11	**Developer Security Testing and Evaluation**
ACO_VUL.3	**Composition Vulnerability Analysis** Enhanced-Basic Composition Vulnerability Review	CA-2	**Security Assessments**
		CA-8	**Penetration Testing**
		RA-3	**Risk Assessment**
		SA-11	**Developer Security Testing and Evaluation**

ПРИЛОЖЕНИЕ I

ШАБЛОН ОВЕРЛЕЯ

ПРИМЕНЕНИЕ РУКОВОДСТВА ПО АДАПТАЦИИ ДЛЯ СПЕЦИАЛЬНЫХ УСЛОВИЙ ИЛИ ИСПОЛЬЗОВАНИЯ В ИНТЕРЕСАХ ВСЕГО СООБЩЕСТВА[116]

Организации могут использовать следующий шаблон, когда разрабатывают адаптированные базовые наборы мер безопасности, используя концепцию оверлеев.[117] Шаблон представлен как пример, конкретные организации могут использовать другие форматы или изменять формат в этом приложении, основаясь на потребностях организации и типе разрабатываемого оверлея. Уровень детализации оверлея выбирается на усмотрение организации, инициирующей оверлей, но должен быть достаточного покрытия и глубины, чтобы обеспечить соответствующее обоснование и подтверждение для разработанного результирующего адаптированного базового набора мер, включая любые основанные на риске решения, принятые во время процесса разработки оверлея. Меры безопасности базового набора, адаптируемого с использованием концепции оверлея, отражаются в планах обеспечения безопасности, которые подлежат одобрению уполномоченными должностными лицами. Пример шаблона состоит из восьми разделов:

- Идентификация;
- Характеристики оверлея;
- Применимость;
- Сводка оверлея;
- Детальные спецификации мер безопасности оверлея;
- Рассмотрения по адаптации;
- Определения; и
- Дополнительная информация или инструкции.

Как могут использоваться оверлеи

В рамках Основ управления рисками (RMF) оверлеи реализуются как часть процесса адаптации после завершения начального процесса категорирования безопасности, описанного в Разделе 3.1 и любом специфичном для организации руководстве. Результаты процесса категорирования безопасности заключаются в определении *уровня воздействия* на информационную систему, и впоследствии используются для выбора начального набора мер безопасности из базовыхнаборов мер безопасности в Приложении D.[118] После того, как начальный набор мер безопасности идентифицирован, организации инициируют процесс адаптации, чтобы модифицировать и согласовать более тщательно меры безопасности с особыми условиями организации. Оверлеи обеспечивают руководство по адаптации в ракурсе всего сообщества, определяя специализированные требования, функции предназначения/деятельности, технологии или среды эксплуатации. Оверлеи обеспечивают владельцам информационной системы, ответственным за реализацию и

[116] Адаптированные базовые наборы мер безопасности, подготовленные с использованием концепции *оверлеев*, могут быть представлены независимо во многих местах и публикациях, включая, например, политики OMB, Инструкции CNSS, Специальные публикации NIST, промышленные стандарты и специфичных для секторов руководствах. Как часть инициативы оверлеев, Приложение I предыдущего руководства, относящееся к безопасности систем управления производственными и технологическими процессами, было перенесено в Специальную публикацию NIST 800-82.

[117] Хотя организации поощрены использовать оверлейную концепцию, чтобы адаптировать базовые мер безопасности, генерирация широко распространяемых оверлеев по дному и тому же предмету может оказаться контрпродуктивна. Оверлейная концепция является самой эффективной, когда сообщества интересов сотрудничают, чтобы создать основанные на согласии оверлеи которые не являются повторяющимися.

[118] CNSS Инструкция 1253 обеспечивают руководство по категорированию безопасности и базовые наборы мер безопасности для систем национальной безопасности.

поддержание таких систем, однородность и эффективность мер безопасности, выбранных посредством предоставленных параметров адаптации, разработанных специалистами по безопасности и другими экспертами в предметной области.

Есть значительный ряд параметров, которые могут использоваться, чтобы строить оверлеи в зависимости от специфики, требуемой разработчиками оверлеев. Некоторые оверлеи могут быть очень связаны с аппаратными средствами, встроенным микропрограммным обеспечением и программным обеспечением, которые формируют ключевые компоненты информационной системы, и средой, в которой работает система. Другие оверлеи могут быть более абстрактны в отношении применимости к большому классу информационных систем, которые могут быть развернуты в различных средах. Пример шаблона, описанный ниже, может использоваться для любого уровня специфики на этом континууме потенциальных параметров оверлеев.

Оверлеи, которые обеспечивают *большую специфику*, как правило, разрабатываются организациями с полномочиями владельцев информационных систем и сред эксплуатации. Организации выбирают соответствующие действия адаптации для выбранных мер базового уровня безопасности, как описано в Разделе 3.2. Многие из переменных и условий, которые квалифицируют оверлей для использования на конкретной информационной системе, сделаны явными, чтобы гарантировать согласованность при применении оверлея. Оверлеи, которые обеспечивают *меншую специфику*, могут быть также разработаны экспертами по безопасности и в предметной области для приложения к больш**и**м классам информационных систем или в ситуациях, где имеются не полные знания о конкретных деталях реализации, связанных с системой. Менее конкретные оверлеи могут требовать дополнительной адаптации по настройке набора мер безопасности для конкретной информационной системы. Эти оверлеи разрешают многие из операций назначения и выбора в мерах безопасности (то есть, переменных частей мер безопасности), для выполнения организациями, которые владеют и управляют информационными системами. Восемь разделов, входящих в оверлей, описаны ниже.

Идентификация

Организации идентифицируют оверлей, предоставляя: (i) уникальное имя для оверлея; (ii) номер версии и дату; (iii) версию Специальной публикации NIST 800-53, использованной для создания оверлея; (iv) другую документацию, использованную для создания оверлея; (v) автора или авторскую группу и адрес контакта; и (vi) тип полученного организацией санкционирования. Организации определяют, как долго оверлей должен быть в действии и любые события, которые могут инициировать обновление оверлея кроме изменений Специальной публикация NIST 800-53 или специфичного для организации руководства по безопасности. Если нет уникальных событий, которые могут инициировать обновление оверлея, этот раздел содержит указанную нотацию.

Характеристики оверлея

Организации описывают характеристики, которые определяют намеченное использование оверлея, чтобы помочь потенциальным пользователям выбрать самый соответствующий оверлей для своих функций предназначений/деятельности. Это может включать, например, описание: (i) среды, в которой будет использоваться информационная система (например, в защищенном здании в пределах континентальных Соединенных Штатов, в беспилотном космическом корабле, во время перемещения для деятельности в зарубежную страну, которая известна тем, что она попыталась получить доступ к чувствительной информации или классифицированной информации, или в мобильном агрегате, который находится в непосредственной близости от враждебных сущностей); (ii) тип информации, которая будет обрабатываться, храниться или передаваться (например, персональные идентификационные данные и опознавательная информация, информация финансового менеджмента, средства, парк и информация управления оборудованием, информация оборонная и национальной безопасности, информация разработки систем); (iii) функциональность информационной системы или типа систем (например, автономные системы, системы управления производственным/технологическим процессом, или междоменные системы); и (iv) другие характеристики, имеющие отношение к оверлею, которые помогают защищать функции предназначения/ деятельности

организации, информационные системы, информацию или людей от конкретного набора угроз, которые не могут быть определены предположениями, описанными в Главе Три.

Применимость

Организации предоставляют критерии, чтобы помочь потенциальным пользователям оверлея в определении, применим ли оверлей к определенной информационной системе или среде эксплуатации. Типичные форматы включают, например, список вопросов или дерева решений, основанных на описании характеристик информационной системы (включая связанные приложения) и среды её эксплуатации на уровне специфики, соответствующей оверлею.

Сводка оверлея

Организации предоставляют краткую сводку существенных характеристик оверлея. Эта сводка может включать, например: (i) меры безопасности и улучшения мер безопасности, на которые влияет оверлей; (ii)индикацию того, какие меры безопасности/улучшения выбраны или не выбраны, основываясь на характеристиках и предположениях оверлея, руководстве по адаптации, представленном в Разделе 3.2, или любом специфичном для организации руководстве; (iii) выбранные меры безопасности/улучшения, включая обзор нового дополнительного руководства и значений параметров; и (iv) ссылки на действующие законы, Правительственные распоряжения, директивы, инструкции, нормативные акты, политики или стандарты.

Детальные спецификации мер безопасности оверлея

Организации предоставляют всестороннее представление мер безопасности /улучшений мер безопасности в оверлее как часть процесса адаптации. Это может включать, например: (i) подтверждение выбора или не выбора конкретной меры безопасности /улучшения меры безопасности; (ii) модификации к дополнительному руководству или добавление нового дополнительного руководства для мер безопасности и улучшений мер безопасности, чтобы определить характеристики оверлея и сред, в которых оверлей предназначен для использования; (iii) уникальные значения параметров для операций выбор или назначения мер безопасности; (iv) конкретные установленные законом и/или нормативные требования (сверх и вне FISMA), которые выполняются мерой безопасности или улучшением меры безопасности; (v) рекомендации по компенсации мер безопасности, если соответствующе; и (vi) руководство по расширению основных возможностей мер безопасности/улучшений мер посредством определения дополнительной функциональности, изменения стойкости механизмов или добавления или ограничения параметров реализации.

Рассмотрения по адаптации

Организации предоставляют информацию владельцам информационной системы и санкционирующим должностным лицам по тому, что нужно рассмотреть во время процесса адаптации, когда определяется набор мер безопасности, применимый к их конкретным информационным системам. Это особенно важно для оверлеев, которые используются в среде эксплуатации, отличной от предполагаемой базовыми наборами мер безопасности (как определено в Разделе 3.1). Кроме того, организации могут представить руководство по использованию множественных оверлеев применительно к базовым наборам мер безопасности и определяющее любые потенциальные конфликты, которые могут возникнуть между спецификациями оверлеев и базовыми мерами безопасности.

Определения

Организации предоставляют те термины и соответствующие определения, которые уникальны и имеют отношение к оверлею. Термины и определения перечисляются в алфавитном порядке. Если нет уникальных терминов или определений для оверлея, это указывается в этом разделе.

Дополнительная информация или инструкции

Организации предоставляют любую дополнительную информацию или инструкции, имеющие отношение к оверлею, не охваченные в предыдущих разделах.

ПРИЛОЖЕНИЕ J

КАТАЛОГ МЕР ПРИВАТНОСТИ

МЕРЫ ПРИВАТНОСТИ, УЛУЧШЕНИЯ И ДОПОЛНИТЕЛЬНОЕ РУКОВОДСТВО

Потребность защитить приватность человека столь же важна сегодня, как это было в 1974, когда Закон о неприкосновенности частной жизни первоначально стремился сбалансировать потребность правительства собирать информацию о людях с правом гражданина быть уведомленным относительно того, как эта информация используется, собирается, поддерживается и уничтожается после требуемого периода использования. Эти интересы также совмещаются в частном секторе, где здравоохранение, финансовые и другие сервисы продолжают поставляться через сети со всё более и более высокими уровнями персонализации. Распространение социальных сетей, Умных сетей, мобильных устройств и облачных вычислений, а так же переход от структурированных к неструктурированным данным и средам метаданных, добавили существенные сложности и проблемы для федеральных организаций в сохранении приватности. Эти проблемы значительно выходят за пределы традиционного представления безопасности информационных технологий по защите приватности, которое фокусировалось, прежде всего, на обеспечении конфиденциальности. Теперь имеются гораздо более значимые последствия в отношении контроля целостности персональных данных и гарантии того, что персональные данные доступны по требованию. Побуждающий фон вынуждает федеральные организации расширить свое представление о приватности, чтобы оправдать надежды гражданина о приватности, которые идут помимо информационной безопасности.

Приватность, по отношению к персональной идентификационной информации (PII),[119] имеет базовое значение, которое может быть достигнуто только с учетом соответствующего законодательства, политик, процедур и соответствующих мер безопасности, чтобы гарантировать соответствие с требованиями. Защита приватности людей и их PII, которые собираются, используются, поддерживаются, находятся в общем доступе и удаляются программами и информационными системами, является фундаментальной ответственностью федеральных организаций. Приватность также включает право каждого человека решать, предоставлять ли и когда персональные данные в общий доступ, сколько информации предоставлять в общий доступ и конкретные обстоятельства, при которых информация может предоставляться в общий доступ. В сегодняшнем мире цифровых технологий эффективная приватность для людей зависит от мер защиты, используемых в информационных системах, которые обрабатывают, хранят и передают PII, и сред, в которых работают эти системы. Организации не могут иметь эффективной приватности без базового фундамента информационной безопасности. Приватность, однако, шире чем безопасность и включает, например, принципы открытости, уведомления и избирательности.

Это приложение обеспечивает структурированный набор мер безопасности для того, чтобы защитить приватность и служит путеводителем для организаций по использованию в идентификации и реализации мер обеспечения приватности относительно всего жизненного цикла PII в печатной или электронной форме. Меры безопасности сосредотачиваются на приватности информации как на характеристике, отличной от, но очень связанной с безопасностью информации. Меры приватности - административные, технические и физические меры защиты, используемые организациями, чтобы защитить и гарантировать надлежащую обработку PII

[119] Меморандумов OMB 07-16 определяют PII как информацию, которая может использоваться, чтобы отличить или проследить идентификационные данные человека, такие как имя, номер социального страхования, биометрические сведения и т.п., отдельно или в совокупности с другой персональной или идентифицирующей информацией, которая связана или связываема с конкретным человеком, такой как дата и место рождения, девичья фамилия родителя и т.п. Меморандум OMB 10-22 далее уточняет, что “определение PII не привязано к любой отдельной категории информации или технологии. Скорее он требует индивидуальной оценки конкретного риска, что человек может быть идентифицирован, путем исследования контекста использования и комбинации элементов данных. При выполнении этой оценки агентствам важно понимать, что не-PII может стать PII всякий раз, когда дополнительная информация стала публично доступной на любом носителе и из любого источника, которая, если объединить с другой доступной информацией, может использоваться, чтобы идентифицировать человека.” NIST Специальная публикация 800-122 также содержит определение PII, которое отличается от этого приложения, потому что оно фокусируется на цели безопасности конфиденциальности а не приватности в широком смысле. Определения PII организациями могут изменяться, основываясь на рассмотрении дополнительных нормативных требований. Меры приватности в этом приложении применяются независимо от определения PII организациями.

организацией.[120] Организации могут также участвовать в работах, которые не включают сбор и использование PII, но могут, тем не менее, поднимать вопросы приватности и связанного риска. Меры приватности также применимы к этим работам и могут использоваться, чтобы проанализировать риск приватности и смягчить такой риск, когда необходимо.

Меры приватности в этом приложении основаны на Принципах честной информационной практики (FIPPs),[121] воплощенных в Законе о неприкосновенности частной жизни 1974 г., Разделе 208 из закона об Электронном правительстве 2002 г. и политиках Министерства управления и бюджета (OMB). FIPPs разработаны, чтобы создать общественное доверие к методам приватности организаций и помочь организациям избежать материальных потерь и нематериального ущерба от инцидентов приватности. Есть восемь семейств мер приватности, каждое из которых связано с одним из FIPPs. Семейства приватности могут быть реализованы в организации, департаменте, агентстве, подразделении, офисе, программе или на уровне информационной системы, под руководством и надзором Высшего должностного лица агентства по приватности (SAOP) / Директора по приватности (CPO)[122] и в координации с Директором по информационной безопасности, Директором по информации, должностными лицами программы, юрисконсультом и другими, как соответствующе. Таблица J-1 представляет сводку мер приватности по семействам в каталоге мер обеспечения приватности.

ТАБЛИЦА J-1: СВОДКА МЕР ПРИВАТНОСТИ ПО СЕМЕЙСТВАМ

ID	МЕРЫ ПРИВАТНОСТИ
AP	**Полномочия и назначение**
AP-1	Полномочия по сбору
AP-2	Спецификация назначения
AR	**Подконтрольность, аудит, и управление рисками**
AR-1	Управление и программа приватности
AR-2	Воздействие приватности и оценка степени риска
AR-3	Требования приватности для подрядчиков и поставщиков услуг
AR-4	Мониторинг и аудит приватности
AR-5	Освоение и обучение приватности
AR-6	Отчетность по приватности
AR-7	Проектирование и разработка систем с улучшенной приватностью
AR-8	Учет раскрытий
DI	**Качество и целостность данных**
DI-1	Качество данных
DI-2	Целостность данных и Совет по целостности данных
DM	**Минимизация и хранение данных**
DM-1	Минимизация персональной идентификационной информации
DM-2	Хранение и ликвидация данных

[120] В 2010 году Комитет по приватности Федерального совета CIO выпустил основу для проектирования и реализации программы приватности под названием *Лучшие практики: Элементы федеральной программы приватности (Белые страницы элементов).* Меры приватности в этом приложении отражают много элементов, включенных в этот документ. Организации могут использовать меры приватности и руководство в указанном документе, чтобы разработать программу приватности всей организации или улучшить уже существующую программу.

[121] FIPPs широко используются в Соединенных Штатах и на международном уровне, как общие рамки для приватности, и отражены в других федеральных законах и нормах международного права и политиках. Во многих организациях FIPPs служат основанием для того, чтобы анализировать риски приватности и определять соответствующие стратегии их снижения. Федеральный Профиль безопасности и приватности архитектуры предприятия (FEA-SPP) также содержит информацию и материалы по разработке мер приватности.

[122] Все федеральные агентства и департаменты определяют SAOP/CPO как старшее должностное лицо организации с полной ответственностью в организации за проблемы приватности информации. Меморандум OMB 05-08 предоставляет руководство для определения SAOPs/CPOs. Термины SAOP/CPO, используемые в этом приложении, означает высшего руководителя организации по приватности, титул которого может измениться от организации к организации.

ID	МЕРЫ ПРИВАТНОСТИ
DM-3	Минимизация PII, используемых в проверках, обучении и исследованиях
IP	**Персональлное участие и восстановление**
IP-1	Согласие
IP-2	Персональный доступ
IP-3	Восстановление
IP-4	Управление жалобами
SE	**Безопасность**
SE-1	Реестр персональной идентификационной информации
SE-2	Реакция на инциденты приватности
TR	**Открытость**
TR-1	Уведомление о приватности
TR-2	Система уведомительных записей и положения Закона о неприкосновенности частной жизни
TR-3	Распространение информации Программы приватности
UL	**Ограничение на использование**
UL-1	Внутреннее использование
UL-2	Совместное использование информации с третьими сторонами

Есть большое сходство между структурой мер приватности в этом приложении и структурой мер безопасности в Приложениях F и G. Например, мера AR-1 (Управление и Программа приватности) требует, чтобы организации разработали планы обеспеченич приватности, которые могут быть реализованы на уровне организации или уровне программы. Эти планы могут также использоваться в соединении с планами обеспечения безопасности, чтобы предоставить возможность организациям выбрать соответствующий набор мер безопасности и приватности в соответствии с требованиями предназначения/деятельности организации и средами, в которых работают организации. Включение фундаментальных концепций, связанных с управлением рисками информационной безопасности помогает гарантировать, что использование мер приватности осуществляется в рентабельном и основанном на риске способе, одновременно удовлетворяя согласующиеся требования. Стандартизированные меры приватности и процедуры оценки (разработанные, чтобы оценить эффективность мер безопасности) обеспечат более дисциплинированный и структурированный подход для того, чтобы он удовлетворял федеральные требования приватности и демонстрировал согласие с этими требованиями.

В целом, Приложение приватности выполняет нескольких важных задач. Приложение:

- Обеспечивает структурированный набор мер приватности, основанных на лучших практиках, который помогает организациям выполнить применимые федеральные законы, Правительственные распоряжения, директивы, инструкции, нормитивные акты, политики, стандарты, руководства и специфичные для организации документы;
- Устанавливает взаимосвязь и отношение между мерами обеспечения приватности и безопасности с целью определения соответствующих требований приватности и безопасности, которые могут наложиться в концепции и в реализации в федеральных информационных систем, программ и организаций;
- Демонстрирует применимость Основы управления рисками NIST при выборе, реализации, оценке и постоянном мониторинге мер приватности, развернутых в федеральных информационных системах, программах и организациях; и
- Способствует более тесному сотрудничеству между должностными лицами приватности и безопасности в федеральном правительстве, чтобы помочь достигнуть целей высших руководителей/ответственных в определении требований в федеральном законодательстве по приватности, политиках, нормитивных актах, директивах, стандартах и руководствах.

КАК ИСПОЛЬЗОВАТЬ ЭТО ПРИЛОЖЕНИЕ

Меры приватности, выделены в этой публикации главным образом для использования Высшим должностным лицом агентства по приватности (SAOP) / Директором по приватности (CPO) при работе с диспетчерами программ, владельцами предназначения/деятельности, владельцами/управляющими информацией, Директорами по информации, Директорами по безопасности, разработчиками/интеграторами информационных систем и ответственными за риски, чтобы определять, как лучше всего внедрить эффективную защиту приватности и практики (то есть, меры приватности) в рамках программ организации и информационных систем и сред, в которых они работают. Меры приватности облегчают усилия организации в выполнении требований приватности, влияющих на те программы и/или системы организаций, которые собирают, используют, поддерживают, предоставляют в общий доступ или ликвидируют персональную идентификационную информацию (PII) или других действий, которые повышают риски приватности. В то время как меры безопасности в Приложении F назначены низкому, умеренному и высокому уровням базовых мер безопасности в Приложении D, меры приватности выбраны и реализованы, основываясь на требованиях приватности организаций и потребности защитить PII людей, собираемых и поддерживаемых информационными системами и программами организаций, в соответствии с федеральным законодательством по приватности, политиками, директивами, нормативными актами, руководствами и лучшими практиками.

Организации анализируют и применяют каждую меру приватности относительно своих конкретных потребностей предназначения/деятельности и эксплуатации, основанных на их юридических полномочиях и обязанностях. Реализация мер приватности может измениться, основываясь на этом анализе (например, организации, которые определены, как *застрахованные сущности* в соответствии с Законом о переносимости и подконтрольности медицинского страхования [HIPAA], могут иметь дополнительные требования, которые конкретно не перечислены в этой публикации). Это облегчает организациям определить информационные практики, которые совместимы с законом и политикой и те, которые, возможно, необходимо рассмотреть. Это также облегчает организации адаптировать меры приватности, чтобы удовлетворить их определенные и конкретные потребности на уровне организации, уровне процесса предназначения/деятельности и уровне информационной системы. Организации с национальной безопасностью или правоохранительные органы принимают во внимание эти полномочия так же как и интересы приватности в определении того, как применять меры приватности в их эксплуатационных средах. Точно так же организации, подчиненные Закону о защите конфиденциальной информации и статистической эффективности (CIPSEA), реализуют меры приватности, непротиворечивые с этим законом. Все организации реализуют меры приватности, непротиворечивые с Законом о неприкосновенности частной жизни 1974, 5 U.S.C. § 552a согласно любым исключениям и/или льготам.

Улучшения мер приватности, описанные в Приложении J, отражают лучшие практики, которые организации должны стремиться достигнуть, но не являются обязательными. Организации должны решить, когда применить улучшения мер приватности, чтобы поддержать их установленные функции предназначения/деятельности. Конкретные *оверлеи* для приватности, разработанные в соответствии с руководством в Разделе 3.2 и Приложении I, могут также рассматриваться для облегчения адаптации базовых наборов мер безопасности в Приложении D с необходимыми мерами приватности, чтобы гарантировать, что требования и безопасности и приватности могут быть удовлетворены организациями. Многие из мер безопасности в Приложении F обеспечивают фундаментальную защиту информации для конфиденциальности, целостности и доступности в информационных системах организаций и средах, в которых эти системы применяются - защита, которая важна для сильной и эффективной приватности.

Организации документируют согласованные меры приватности, которые будут реализованы в программах и информационных системах организаций и средах, в которых они работают. Меры приватности, на усмотрение реализующих организаций, могут быть задокументированы в отдельный план обеспечения приватности или включены в другие документы управления рисками (например, планы обеспеченич безопасности системы). Организации также устанавливают соответствующие методологии оценки, чтобы определить степень, до которой меры приватности реализованы правильно, работают как предназначено и производя желаемый результат относительно удовлетворения установленных требований приватности. Оценки организациями мер приватности могут быть проведены SAOP/CPO самостоятельно или совместно с другими службами организации по управлению рисками, включая службу информационной безопасности.

Совет по реализации

- Выберите и реализуйте меры приватности, основанные на требованиях приватности организаций и потребности защитить персональную идентификационную информацию (PII) людей, собраемую и поддерживаемую системами и программами.
- Координируйте выбор и реализацию мер приватности с Функцией Ответственного за риски организации, владельцами предназначения/деятельности, архитекторами предприятия, Директором по информации, SAOP/CPO и Директором по информационной безопасности.
- Рассмотрите меры приватности в Приложении J с той же самой точки зрения как меры управления программой в Приложении G - то есть, меры обеспечения должны быть реализованы для каждой информационной системы организации независимо от категорирования по FIPS 199 для этой системы.
- Выберите и реализуйте дополнительные улучшения мер приватности, когда есть показанная потребность в дополнительной защите приватности для людей и PII.
- Примените меры приватности, непротиворечивые с любыми конкретными исключениями и льготами, включенными в законодательство, Правительственные распоряжения, директивы, политики и нормитивные акты (например, обеспечение правопорядка или рассмотрения национальной безопасности).

Каталог мер приватности представлен на страницах J-6…J-25 NIST Special Publication 800-53 Revision 4.