Обзор NIST SP 800-53, Пересмотр 4
Меры обеспечения безопасности и приватности для федеральных информационных систем и организаций

Kelley Dempsey
Отдела компьютерной безопасности
Лаборатория информационных технологий

Greg Witte
Doug Rike
G2, Inc.
Annapolis Junction, MD

19 февраля 2014

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

Краткий обзор

Этот отчет представляет краткий обзор NIST Специальной публикации (SP) 800-53, Пересмотр 4, *Меры обеспечения безопасности и приватности для федеральных информационных систем и организаций*, который был опубликован 30 апреля 2013.

Ключевые слова

доверие; компьютерная безопасность; FIPS Публикация 199; FIPS Публикация 200, FISMA; Закон о неприкосновенности частной жизни; Основа управления рисками; меры безопасности; требования безопасности

Правовая оговорка

Любое упоминание о коммерческих продуктах или ссылках на коммерческие организации предназначено только для информации; это не подразумевает рекомендацию или одобрение NIST, и при этом это не подразумевает, что упомянутые продукты являются обязательно наилучшими из имеющихся по предназначению.

Дополнительная информация

Для дополнительной информации о программах Отдела компьютерной безопасности NIST, проектах и публикациях, посетите Ресурсный центр компьютерной безопасности, csrc.nist.gov. Информация относительно других усилий NIST и Лаборатории информационных технологий (ITL) доступна в www.nist.gov и www.nist.gov/itl.

Оглавление

Список иллюстраций

1 Введение

В апреле 2013, NIST опубликовал обновление, Пересмотр 4, Специальной публикации NIST 800-53, Меры обеспечения безопасности и приватности для федеральных информационных систем и организации. Руководство было разработано и сопровождено Объединенной экспертной группой по инициативе преобразования Межведомственной рабочей группы, частью продолжающегося партнерства по информационной безопасности между Министерства обороны США, Разведывательного ведомства, Комитета по системам национальной безопасности, Департамента безопасности отечества, и федеральных гражданских агентств США.

SP 800-53, Пересмотр 4, http://dx.doi.org/10.6028/NIST.SP.800-53r4, была обновлена, чтобы отразить развивающиеся технологии и пространство угрозы. Примеры специфических проблемных областей включают облачные и мобильные вычисления; угрозы посвященного лица; безопасность приложений; риски системы поставок; постоянные развивающиеся угрозы; и доверенность, доверие, и устойчивость информационных систем. Версия также содержит новое приложение мер безопасности приватности и связанное руководство по реализации (Приложение J), базирующееся на Принципах честной информационной практики (FIPPs), http://www.nist.gov/nstic/NSTIC-FIPPs.pdf, широко распространённой основе определенных принципов, предназначенных для использования при оценке и рассмотрении систем, процессов или программ, которые влияют на приватность личностей.

SP 800-53, Пересмотр 4, являются частью Специальных публикаций NIST 800-й серии http://csrc.nist.gov/publications/PubsSPs.html, которые информируют относительно исследований, руководств и других работ Лаборатории информационных технологий NIST (ITL), связанных с компьютерной безопасностью. Публикация предоставляет исчерпывающий набор мер безопасности, три базовых набора мер безопасности (низкого, умеренного и высокого воздействия), и руководство по адаптации соответствующих базовых наборов к конкретным потребностям согласно предназначению организации, средам деятельности и используемым технологиям.

В соответствии с увеличением риска в отношении к конфиденциальности, целостности и/или доступности информационных систем, может также соответственно увеличиваться потребность в дополнительных мерах обеспечения безопасности, чтобы защитить систему. SP 800-53, Пересмотр 4, определяет базовые наборы мер безопасности как начальную точку для процесса выбора мер безопасности. Базовые наборы выбираются, основываясь на категории безопасности и связанном уровне воздействия информационных систем, как описано в Публикации 199 Стандартов обработки федеральной информации (FIPS) http://csrc.nist.gov/publications/PubsFIPS.html#199, *Стандарты для категорирования безопасности федеральной информации и информационных систем*, и Публикации 200 FIPS, http://csrc.nist.gov/publications/PubsFIPS.html#200, Минимальные требования безопасности для федеральной информации и информационных систем.

Отдельное руководство, 800-53A SP, http://csrc.nist.gov/publications/PubsSPs.html#SP-800-53-A%20-Rev.%201, *Руководство по оценке мер безопасности в федеральных информационных системах и организациях*, обеспечивает конкретные руководства, которые облегчают периодическую оценку мер безопасности, чтобы гарантировать, что меры безопасности были реализованы правильно, работают как предназначено и выполняют требования безопасности организации.

2 NIST SP 800-53, Пересмотр 4, и Основы управления рисками (RMF)

NIST SP 800-39, Управление рисками информационной безопасности, определяет управление рисками как "программу и поддерживающие процессы, чтобы управлять риском информационной безопасности для деятельности организации (включая предназначение, функции и репутацию), активов организации, людей, других организаций и Нации". Чтобы интегрировать процесс управления рисками во всей организации и учесть ее предназначение и коммерческие интересы, использован трехуровневый подход. Процесс выполняются на трёх уровнях с целью непрерывного совершенствования в связанных с риском работах организации, с эффективным взаимодействием между уровнями и заинтересованными сторонами. Рисунок 1 иллюстрирует трехуровневый подход к управлению рисками.

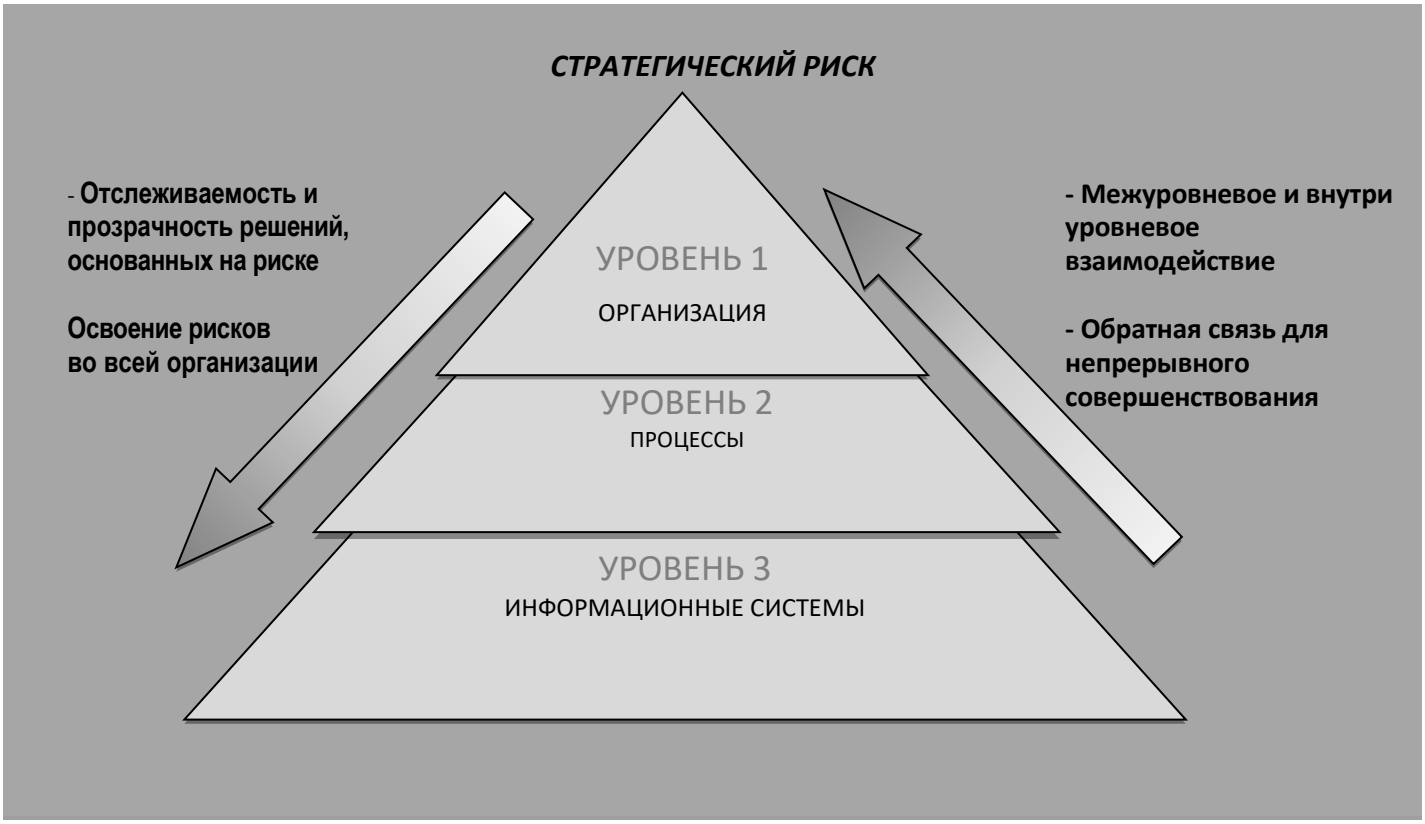

РИСУНОК 1: 3-УРОВНЕВЫЙ ПОДХОД К УПРАВЛЕНИЮ РИСКАМИ

Основы управления рисками (RMF) NIST, описанные в NIST Специальная Публикация 800-37, Пересмотр 1, http://csrc.nist.gov/publications/PubsSPs.html#SP-800-37-Rev.%201, *Руководство по применения основ управления рисками к федеральным информационным системам: Подход жизненного цикла безопасности*, являются методологией для реализации управления рисками на уровне информационных систем. RMF (изображенные на рисунке 2) идентифицируют шесть различных шагов, которые обеспечивают упорядоченный и структурированный процесс по интеграции работ управления рисками информационной безопасности в жизненный цикл разработки систем. RMF учитывает проблемы безопасности организаций, относящиеся к проектированию, разработке, реализации, применению и ликвидации информационных систем и сред, в которых работают эти системы.

Меры безопасности в SP 800-53, Пересмотр 4, поддерживают Шаг Два из RMF, и подробный каталог этих мер безопасности приведен в Приложении F. Для простоты использования при выборе мер безопасности и в процессе спецификации, меры безопасности организованы в восемнадцать семейств,

каждое из которых содержит меры безопасности, связанные с общей темой безопасности семейства. Меры безопасности включают аспекты политики, надзора, контроля, ручных процессов, отдельных действий или автоматизированных механизмов, реализованных информационными системами/ устройствами. Структура меры безопасности содержит следующие компоненты: (I) раздел меры безопасности; (II) раздел дополнительного руководства; (III) раздел улучшений меры безопасности; (IV) раздел ссылок; и (V) раздел приоритета и принадлежности к базовому набору мер безопасности.

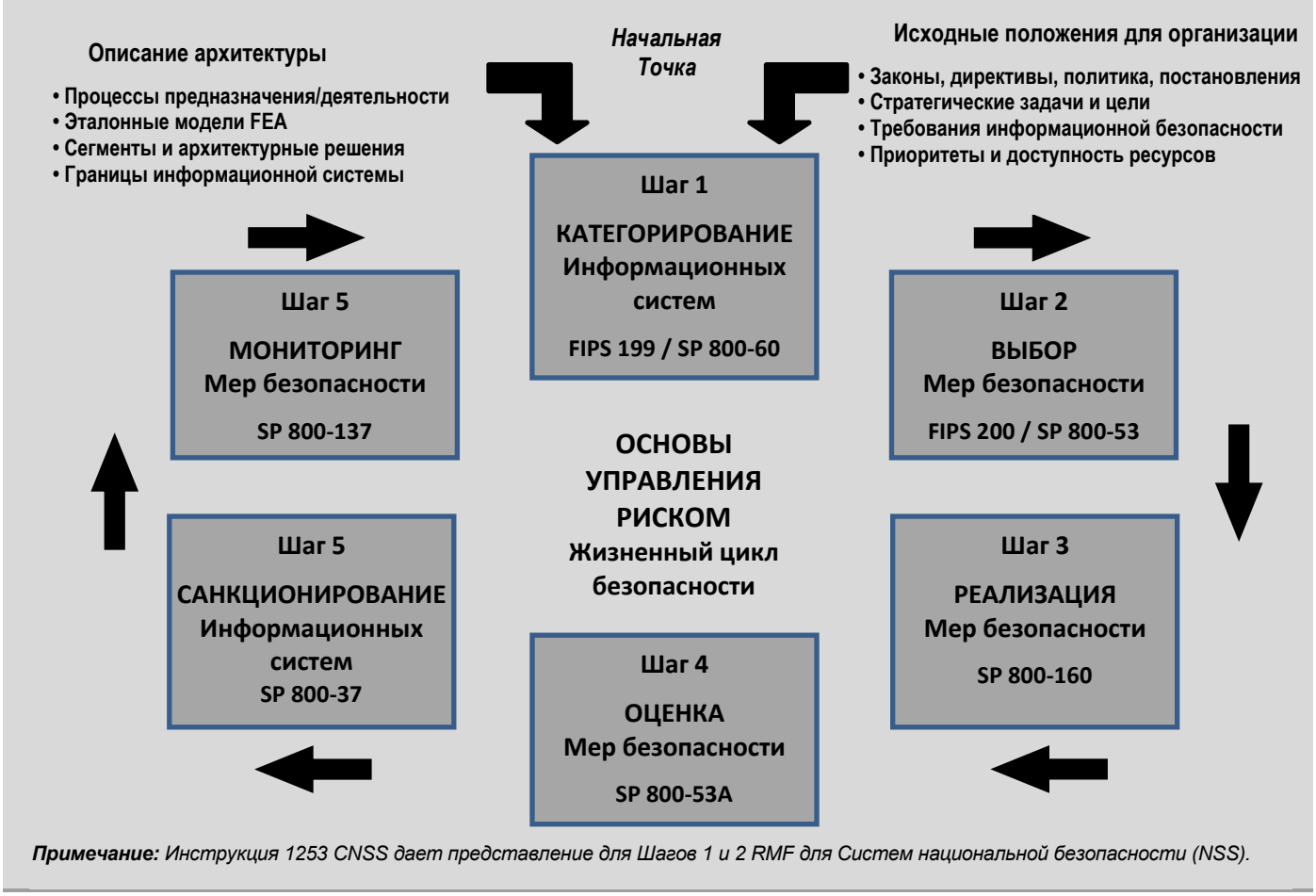

РИСУНОК 2: ОСНОВЫ УПРАВЛЕНИЯ РИСКОМ

3 Базовые наборы мер безопасности и адаптация

Чтобы помочь организациям в соответствующем выборе мер безопасности для информационных систем, представлена концепция базовых наборов мер безопасности. Базовые наборы мер безопасности - начальная точка для процесса выбора мер безопасности и их выбор основан на категории безопасности и связанном уровне воздействия информационных систем, определенных в соответствии с Публикацией 199 FIPS и Публикацией 200FIPS, соответственно (Шаг Один из RMF). SP 800-53, Пересмотр 4, определяет, что "меры безопасности и улучшения мер безопасности, перечисленные в начальных базовых наборах мер безопасности, являются не минимумом, скорее предложенной начальной точкой от которой меры безопасности и улучшения мер безопасности, могут быть удаленными или добавленными." Приложение D содержит перечисление мер безопасности базовых наборов мер безопасности, соответствующих информационным системам низкого воздействия, умеренного воздействия и высокого воздействия, используя наивысшее значение, определенное в Публикации 200 FIPS.

Базовые наборы мер безопасности учитывают потребности безопасности широкого и разнообразного круга потребителей, и их разработка основана на многих общих предположениях, включая общие экологические, эксплуатационные и функциональные рассмотрения. Базовые наборы мер безопасности предполагают также типичные угрозы, обращенные к общим информационным системам. Точное формулирование базовых предположений является основным элементом в начальном шаге структурирования риска процесса управления рисками, описанного в NIST SP 800-39 http://csrc.nist.gov/publications/PubsSPs.html#SP-800-39. Чтобы гарантировать, что определён соответствующий набор мер безопасности, чтобы обеспечить безопасность соразмерную риску, организации адаптируют меры безопасности, чтобы выровнять с конкретными потребностями безопасности. Организации могут выполнить адаптацию на уровне организации для всех информационных систем, в поддержку определенного направления деятельности или процесса предназначения/ деятельности, на уровне отдельной информационной системы или при использовании комбинации вышеупомянутого. Процесс адаптации состоит из нескольких шагов, как описано в SP 800-53, Пересмотр 4, Раздел 3.2. Эти действия включают:

- Определение и обозначение общих мер безопасности - мер безопасности, которые могут быть наследованными одной или более информационными системами. Если информационная система наследует общие меры безопасности, такие как меры безопасности среды в информационном центре, то эта система не должна явно реализовывать эти меру безопасности.
- Применение объектовых особенностей - они, когда применяются в соединении с руководством по управлению риском, могут устранить ненужные меры безопасности из начальных базовых наборов мер безопасности, и помочь гарантировать, что организации выберут *только* те меры безопасности, которые должны обеспечить соответствующий уровень защиты для информационных систем. Когда объектовые особенности применены, возможно потребуется выбрать компенсирующие меры безопасности, чтобы обеспечить альтернативные средства выполнения требований безопасности.
- Дополнение базовых наборов мер безопасности - если нужно учесть конкретные угрозы и уязвимости выбираются дополнительные меры безопасности и улучшения мер безопасности.

4 Документирование процесса выбора мер безопасности

Чтобы помочь в работах по анализу, планировании обеспечения безопасности и оценках степени риска, организации документируют соответствующие решения, принятые во время процесса выбора мер безопасности, обеспечивая обоснование для этих решений. Эта документация важна, когда изучаются рассмотрения безопасности для информационных систем организации относительно потенциального воздействия на предназначение и деятельность организации.

Результирующий адаптированный базовый набор мер безопасности и поддерживающее обоснование для решений по выбору (включая использование любых ограничений для информационных систем, требуемых организацией) документируется в планы безопасности системы. Документирование существенных решений управления рисками в процессе выбора мер безопасности является обязательным с тем, чтобы у авторизующих должностных лиц был доступ к необходимой информации, чтобы сделать информированные решения об авторизации для информационных систем организации, как демонстрируется на рисунке 3.

РИСУНОК 3: ПРОЦЕСС ВЫБОРА МЕР БЕЗОПАСНОСТИ

5 Доверие

Приложение E в SP 800-53, Версии 4, представляет собой обновление для руководства относительно доверия к безопасности. Этот раздел структурирует методы для агентств по установлению мер уверенности, что реализованные меры безопасности обеспечивают возможности безопасности, требуемые для защиты критических операций предназначения и деятельности.

Критерии того, является ли мера безопасности, связанной с доверием или связанной с функциональностью, основаны на полных характеристиках меры безопасности. В общем, связанные с доверием меры безопасности это меры безопасности которые: (I) определяют процессы, процедуры, технологии или методологии для проектирования и разработки компонентов систем и информационных систем; (II) обеспечивают поддерживающие эксплуатационные процессы, включая улучшение качества систем, компонентов или процессов; (III) предоставляют свидетельство безопасности для действий по разработке или эксплуатации; (IV) определяют эффективность мер безопасности или риск; или (V) улучшают навыки, квалификацию и понимание персонала.

Приложение E обеспечивает три таблицы, которые определяют конкретные, связанные с доверием меры безопасности, которые включены в базовые наборы мер безопасности низкого, умеренного и высокого воздействия, описанные в Приложении D. Описание мер безопасности помогает организации в определении мер безопасности, необходимых для удовлетворения минимальным требованиям доверия. Там, где требуется дополнительное доверие, чтобы достигнуть целей управления рисками, Таблица E-4 представляет дополнительные меры безопасности и улучшения мер безопасности, чтобы достигнуть улучшенного доверия. Реализующие должны знать, что обозначение связанных с доверием мер безопасности не предназначено, чтобы подразумевать больший важный уровень для таких мер безопасности. Достижение адекватной безопасности для информационных систем организации требует корректной комбинации мер безопасности, связанных с функциональностью и с доверием.

6 Меры безопасности

Приложение F, Каталог мер безопасности, предоставляет широкий диапазон контрмер для организаций и информационных систем. Меры безопасности разработаны так, чтобы быть нейтральными в отношении технологий с тем, чтобы фокус находился на *фундаментальных* контрмерах, необходимых для защиты информации организации во время обработки, хранения или передачи. Поэтому SP 800-53, Пересмотр 4, не дает представление о приложении мер безопасности к конкретным технологиям, средам деятельности или функциям предназначения/деятельности. Эти специфические области могут быть учтены с использованием оверлеев (см. ниже).

Со многими мерами безопасности включены улучшения мер безопасности, которые выбираются, чтобы увеличить стойкость основной меры безопасности. Улучшения мер обеспечения предназначены, чтобы быть реализованными только одновременно с реализацией основной меры безопасности.

Некоторые меры безопасности и улучшения мер безопасности включают одно или более описаний *выбора* и *присвоения*. Это переменные параметры, которые организации определяют, обеспечивая возможность адаптировать меры безопасности, основываясь на конкретных требованиях безопасности, средах деятельности и допустимом риске для организации. Параметры, назначенные и/или выбранные организациями для данной основной меры безопасности, применяются также ко всем улучшениям меры безопасности, связанным с этой мерой безопасности.

Первая мера безопасности в каждом семействе (называемая тире-1 мера безопасности) определяет политики и процедуры, необходимые для эффективной реализации всех других мер безопасности в каждом семействе. Поэтому, требования по разработке политик и процедур не повторяются в отдельных мерах безопасности.

Многие меры безопасности и улучшения включают дополнительное руководство. Дополнительное руководство обеспечивает дополнительную информацию о мере безопасности или улучшении, чтобы помочь организациям определить, разработать и/или реализовать меры безопасности, но не включает любые дополнительные требования.

SP 800-53, Пересмотр 4, включает много изменений по отношению к SP 800-53, Пересмотр 3, - 295 мер безопасности и улучшений мер безопасности были добавлены, в то же время как приблизительно 100 мер безопасности и улучшений мер безопасности были изъяты или включены в другие. Из восемнадцати семейств мер безопасности в SP 800-53, Пересмотр 4, семнадцать семейств описаны в каталоге меры безопасности в Приложении F, и соответствуют семнадцати минимальным требованиям безопасности для федеральной информации и информационных систем в Публикации 200 FIPS, *Минимальные требования безопасности для федеральной информации и информационных систем.*

Одно дополнительное семейство, семейство Управление программой (PM), представляет меры безопасности непосредственно для программ информационной безопасности. Это семейство описано в Приложении G SP 800-53, Пересмотр 4. Хотя это не упомянуто конкретно в FIPS 200, раздел PM представляет меры безопасности на уровне организации, а не на уровне информационной системы. Меры безопасности PM, как правило, реализуются на уровне организации и предписываются на отдельные информационные системы организации. Они дополняют меры безопасности в Приложении F и сосредотачиваются на программных, 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 программой способом, подобном тому, как руководство применяется к мерам безопасности в Приложении F.

7 Международные стандарты по информационной безопасности

Многие организации используют известные международные стандарты информационной безопасности в качестве основания или в качестве дополнительного источника мер безопасности для управления рисками. Для помощи в выборе и сравнении, SP 800-53, Пересмотр 4, содержит таблицы отображения, чтобы предоставить организациям общую индикацию покрытия мер безопасности относительно ISO/IEC 27001, http://www.iso.org/iso/catalogue_detail?csnumber=42103, *Информационная технология – Методы и средства обеспечения безопасности-Системы управления информационной безопасностью-Требования* и ISO/IEC 15408, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341, *Информационная технология - Методы и средства обеспечения безопасности - Критерии оценки безопасности информационных технологий*. ISO/IEC 27001 применяется ко всем типам организаций и определяет требования для того, чтобы создать, реализовать, управлять, контролировать, анализировать, сопровождать и улучшать задокументированную систему управления информационной безопасностью (ISMS) в контексте коммерческих рисков. ISO/IEC 15408 (также известный как Общие Критерии) обеспечивает функциональные требования и требования доверия для разработчиков информационных систем и компонентов информационных системы (то есть, продуктов информационных технологий). Так как многие из технических мер безопасности, определенных в Приложении F, реализуются 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 предоставить свидетельства, что некоторые меры безопасности реализованы правильно, работают как предназначено и дают требуемый эффект в удовлетворении заявленным требованиям безопасности.

8 Оверлеи

Чтобы помочь гарантировать, что выбранные и реализованные меры безопасности достаточны, чтобы соответственно смягчить риски к деятельности и активам организации, SP 800-53, Пересмотр 4, представляет концепцию оверлеев. Оверлей представляет набор мер безопасности, улучшений мер безопасности и дополнительное руководство для использования всем сообществом или учёта специализированных требований, технологий или уникального предназначения и среды деятельности. Например, федеральное правительство может решить установить общеправительственный набор мер безопасности и руководство по реализации для инфраструктуры публичных ключей (PKI) систем, который может быть единообразно применён к информационным системам.

Много оверлеев может быть применено к одному базовому набору мер безопасности. Адаптированные наборы базовых мер безопасности, которые являются результатом процесса разработки оверлея, могут быть более или менее строгими, чем исходные базовые наборы мер безопасности. Оценки степени риска предоставляют необходимую информацию, чтобы определить, находится ли риск от реализации специализированных базовых наборов мер безопасности в пределах допуска риска организаций или сообществ по интересам, разрабатывающих оверлеи.

Общее руководство по оверлейным программам представлено в разделе 3.3, а шаблон оверлея представлен в Приложении I. Шаблон включен только как пример - организации могут хотеть использовать другие форматы или изменить формат в этом приложении, основываясь на потребностях организации и типе разрабатываемого оверлея. Уровень детализации, включаемой в оверлей, относится на усмотрение организации, инициирующей оверлей, но должен быть достаточной ширины и глубины, чтобы обеспечить соответствующее обоснование и мотивировку для разработанного результирующего адаптированного базового набора мер безопасности, включая любые основанные на риске решения, принятые во время процесса разработки оверлея.

Типовой оверлейный шаблон состоит из восьми разделов:

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

9 Приватность

Федеральные агентства обязаны гарантировать, что защита приватности включена в планирование информационной безопасности. С этой целью, SP 800-53, Пересмотр 4, содержит в себе восемь новых семейств мер обеспечения приватности, которые основаны на принятых международном уровне Принципах честной информационной практики (FIPPs), http://www.nist.gov/nstic/NSTIC-FIPPs.pdf. Быстрое распространение средств социального общения, Умной Сетки, мобильных и облачных вычислений, а также переход от структурированных к неструктурированным данным и метаданным среды, добавило существенные сложности и проблемы для федеральных организаций в сохранении приватности. Эти проблемы значительно выходит за рамки традиционного представления защиты приватности как безопасности информационных технологий, которая фокусируется, прежде всего, на обеспечении конфиденциальности.

Семейства мер безопасности описаны подобным образом как в Приложении F (Меры безопасности) и Приложении G (Меры управления программами информационной безопасности программ информационной безопасности всей организации). SP 800-53, Пересмотр 4, напоминает читателям на необходимость рассматривать меры обеспечения приватности в Приложении J с той же самой точки зрения как меры управления программой в Приложении G - то есть, меры безопасности реализуются для каждой информационной системы организации независимо от категорирования этой системы по FIPS 199. Приложение J определяет меры безопасности, улучшения мер безопасности, руководство и ссылки для следующих новых семейств:

- Полномочия и Назначение (AP);
- Подконтрольность, аудит, и управление рисками (AR);
- Качество и целостность данных (DI);
- Минимизация и хранение данных (DM);
- Персональное участие и восстановление (IP);
- Безопасность (SE);
- Открытость (TR);
- Ограничения на использование (UL).

Использование этих стандартизированных мер обеспечения приватности обеспечит более дисциплинированный и структурированный подход для удовлетворения федеральным требованиям приватности и демонстрации соответствия этим требованиям. Организации должны решить, когда применять улучшения мер безопасности, чтобы поддержать их конкретные предназначения и функции деятельности. Конкретные оверлейные программы для приватности могут также облегчать адаптацию базовых наборов мер безопасности в Приложении D с необходимыми мерами безопасности приватности, чтобы гарантировать, что требования и безопасности и приватности могут быть удовлетворены организациями.