Специальная публикация NIST 800-53A
Пересмотр 4

Оценка мер обеспечения безопасности и приватности для Федеральных информационных систем и организаций

Построение эффективных планов оценки

ОБЪЕДИНЕННАЯ ЭКСПЕРТНАЯ ГРУППА
ПО ИНИЦИАТИВЕ ПРЕОБРАЗОВАНИЯ

Эта публикация доступна бесплатно на:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

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

Специальная публикация NIST 800-53A
Пересмотр 4

Меры обеспечения безопасности и приватности для Федеральных информационных систем и организаций

Построение эффективных планов оценки

ОБЪЕДИНЕННАЯ ЭКСПЕРТНАЯ ГРУППА
ПО ИНИЦИАТИВЕ ПРЕОБРАЗОВАНИЯ

Эта публикация доступна бесплатно на:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

Декабрь 2014
Включая дополнения от 18-12-2014

Министерство торговли США
Penny Pritzker, Министр

Национальный институт стандартов и технологий
Willie May, ИО заместитель министра торговли по стандартам и технологиям и ИО Директора

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 800-53A, Пересмотр 4
487 страниц (Декабрь 2014)
CODEN: NSPUE2

Эта публикация доступна бесплатно на: http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

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 объявленных периодов для публичных комментариев и предоставлять обратную связь в NIST. Все публикации Отдела компьютерной безопасности NIST 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 ряд процедур для проведения оценки мер безопасности и мер приватности, используемых в федеральных информационных системах и организациях. Процедуры оценки, выполняемые на различных фазах жизненного цикла разработки систем, непротиворечивы с мерами обеспечения безопасности и приватности в Специальной публикации NIST 800-53, Версия 4. Процедуры настраиваемы и могут быть легко адаптированы, чтобы предоставить организациям необходимую гибкость, для проведения оценки мер безопасности и оценки мер приватности, которые поддерживают процессы управления рисками организации и которые соответствуют заявленному допуску риска для организации. Также, наряду с руководством по анализу результатов оценки, предоставлена информация относительно создания эффективных планов оценки безопасности и планов оценки приватности.

Ключевые слова

Оценка; доверие; закон об электронном правительстве; FISMA; Закон о неприкосновенности частной жизни; меры приватности; требования приватности; Основы управления рисками; меры безопасности; требования безопасности.

Благодарность

Эта публикация была разработана Рабочей группой *объединённой экспертной группы по инициативе преобразования* совместно с представителями Гражданского, Оборонного и Разведывательного сообществ в продолжение усилий по созданию *единой основы информационной безопасности* для федерального правительства. Мы хотим 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 объединённые усилия значительно способствовали публикации. Высшие руководители, члены межведомственной рабочей группы и их организационная принадлежность включают:

Министерство обороны США

Terry Halvorsen
Директор по информации МО (ВРИО)

David De Vries
Первый заместитель Директора по информации МО (ВРИО)

Richard Hale
Заместитель Директора по информации по кибербезопасности

Dominic Cussatt
Директор, стратегия и политика кибербезопасности

Офис Директора Национальной разведки

Adolpho Tarasiuk Jr.
Директор по информации Разведывательного сообщества

Alan Royal
Заместитель Директора по информации Разведывательного сообщества

Susan Dorr
Директор, информационное доверие и Директор по информационной безопасности Разведывательного сообщества

Robert Drake
ВРИО Руководителя, Управление рисками и соответствие сервисов

Национальный институт стандартов и технологий

Charles H. Romine
Директор, Лаборатория информационных технологий

Donna Dodson
Советник по вопросам кибербезопасности, Лаборатория информационных технологий

Matthew Scholl
Руководитель, Отдел компьютерной безопасности

Ron Ross
Руководитель проекта реализации FISMA и объединенной экспертной группы

Комитет по Системам национальной безопасности

Terry Halvorsen
Председатель, CNSS

Sherrill Nicely
Сопредседатель, CNSS

Dominic Cussatt, Jeffrey Wilk, Daniel Dister
Сопредседатели подкомитетов CNSS

Межведомственная рабочая группа Объединенной экспертной группы по инициативе преобразования

Ron Ross *NIST*	Karen Quigg *MITRE Corporation*	Kelley Dempsey *NIST*	Patricia Toth *NIST*
Esten Porter *MITRE Corporation*	Christian Enloe *NIST*	Bennett Hodge *Booz Allen Hamilton*	Kevin Stine *NIST*

Мы хотим выразить нашу искреннюю признательность Elizabeth Lennon и Peggy Himes за их превосходное техническое редактирование и административную поддержку, а также Harold Booth за разработку XML-схемы и за его помощь в исправлении многих трудно находимых ошибок форматирования. Авторы также хотят выделить следующих людей за их существенное содействие в помощи по разработке начального контента этой публикации и совершенствование её контента во время последующих версий: Claire Barrett; Lindy Burkhart; Jonathan Cantor; Mitali Chatterjee; Jonathan Chiu; Sharon Ehlers; Jennifer Fabius; Peter Gouldmann; James Govekar; Terrance Hazelwood; Austin Hershey; Laurie Hestor; Arnold Johnson; Mary Kitson; Martha Landesberg; Naomi Lefkovitz; Jason Mackanick; Timothy Potter; Jennifer Puma; Roanne Shaddox; Terry Sherald; Gary Stoneburner; Julie Trei; Gail Tryon; Ricki Vanetesse; Cynthia Whitmer; и Peter Williams. Наконец, авторы с благодарностью подтверждают и ценят существенные содействия от людей и организаций в общественных и частных секторах, вдумчивые и конструктивные комментарии которых улучшили общее качество и полноценность этой публикации.

ПРОЦЕДУРЫ ОЦЕНКИ МЕР ПРИВАТНОСТИ

Приложение J, Процедуры оценки приватности, является новым дополнением к Специальной публикации NIST 800-53A. Приложение, когда будет завершено, обеспечит полный набор процедур оценки по мерам приватности в Приложении J Специальной публикации NIST 800-53. Новые процедуры оценки приватности разрабатываются и будут добавлены к приложению после процесса полного публичного рассмотрения и проверки. Во всей этой публикации была обновлена терминология с тем, чтобы включить ссылки на приватность во всех аспектах процесса оценки для учёта зеркального отражения факторов, которые являются существенными входами к текущему процессу санкциониро-вания безопасности. У каждой организации, использующей это руководство, есть гибкость, чтобы учесть процесс оценки приватности и интеграцию связанных с приватностью объектов в процессах управления рисками организации таким образом, чтобы лучшие средства поддержки целей предназначения и деятельности организации соответствовали политикам Министерства управления и бюджета.

Стандартизированные процедуры оценки мер приватности обеспечивают более упорядоченный и структурированный подход для того, чтобы определить соответствие федеральным требованиям приватности, а также способствуют более рентабельным методам определения такого соответствия. В структуре процедур оценки мер приватности в Приложении J и процедур оценки мер безопасности в Приложении F будет сильное сходство. Это подобие будет способствовать более тесному сотрудничеству между должностными лицами приватности и безопасности в федеральном правительстве, чтобы помочь достижению целей высших лидеров/руководителей в определении требований в федеральном законодательстве, директивах, политиках, нормативных актах, стандартах и руководствах по приватности.

Наконец, нужно отметить, что, так как процедуры оценки по мерам приватности добавлены в Приложение J, некоторая терминология, традиционно связанная с мерами безопасности и оценками мер безопасности, содержавшаяся в более ранних версиях этой публикации, изменяется, где необходимо, чтобы включать упоминание о приватности. Однако, есть некоторые связанные с безопасностью термины (например, категорирование безопасности, базовый набор мер безопасности, адаптированный базовый набор мер безопасности), которые уникальны в отношении мер безопасности и не имеют прямых аналогов в области приватности. В таких случаях, связанная с приватностью эквивалентная терминология не была добавлена в публикацию. Должностные лица приватности, по их усмотрению, могут принимать любые из связанных с безопасностью терминов в этой публикации в поддержку оценок мер приватности.

ФОРМАТ ПРОЦЕДУР ОЦЕНКИ

В этой версии Специальной публикации 800-53A представлен новый формат для процедур оценки. Формат отражает разложение целей оценки в более *чётко* определённые описания везде, где возможно - таким образом, обеспечивается возможность идентифицировать и оценить конкретные части мер безопасности и приватности. Изменения были инициированы для: (i) помощи в улучшении удобочитаемости процедур оценки; (ii) обеспечения лучшего формата и структуры для автоматизированных инструментов, когда информация оценки импортируется в такие инструменты; (iii) обеспечения большей гибкости в проведении оценок, путём предоставления организациям возможности нацелиться на определённые аспекты мер безопасности и мер приватности (выделяя определённые слабые места и/или недостатки в мерах обеспечения); (iv) повышения эффективности оценок безопасности и приватности; и (v) поддержания непрерывного мониторинга и продолжения санкционирования программы, путём предоставления большего числа составных частей мер обеспечения безопасности и приватности, которые могут быть оценены с определёнными организацией частотой и степенью строгости. Наличие возможности применить оценку и контроль ресурсов в предназначенном и точном способе и одновременно максимизировать использование технологий автоматизации, может иметь результат в более своевременных и рентабельных процессах оценки для организаций.

Примечание: Специальная публикация 800-53 будет соответственно обновлена, чтобы гарантировать, что система нумерации всех мер обеспечения безопасности и приватности непротиворечива с новым форматом, представленным в этой публикации.

ВЫРАВНИВАНИЕ НОМЕРОВ ПЕРЕСМОТРОВ

ЧТО ПРОИЗОШЛО С ПЕРЕСМОТРАМИ СПЕЦИАЛЬНОЙ ПУБЛИКАЦИИ 800-53A 2 И 3?

Номера пересмотров между NIST Специальными публикациями 800-53 и 800-53A были не выровнены изначально, потому что начальная публикация SP 800-53A не выпускалась до завершения публикации SP 800-53, Пересмотр 2. Когда SP 800-53, Пересмотр 3 была опубликована, SP 800-53A была обновлена в Пересмотре 1 для согласованности с обновлениями SP 800-53. Это несоответствие номеров пересмотров создало длительную неопределённость и путаницу, относительно того, какой пересмотр SP 800-53 непротиворечив с каким пересмотром SP 800-53A. Чтобы уменьшить эту неопределённость в будущем, номера пересмотров 2 и 3 были пропущены для SP 800-53A, и этой версии SP 800-53A дали номер пересмотра 4, так как эта версия непротиворечива с обновлениями SP 800 - 53, Пересмотр 4. Будущие пересмотры SP 800-53 и 800-53A будут поддерживать согласованность номеров пересмотров.

РАЗРАБОТКА ОБЩИХ ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОТРУДНИЧЕСТВО СРЕДИ ЧЛЕНОВ ОБЩЕСТВЕННОГО И ЧАСТНОГО СЕКТОРА

При разработке стандартов и руководств, требуемых FISMA, NIST консультируется с другими федеральными агентствами и министерствами, а так же с членами частного сектора, чтобы улучшить информационную безопасность, избежать ненужного и дорогостоящего дублирования усилий и гарантировать, что публикации NIST дополняют стандарты и руководства, используемые для защиты систем национальной безопасности. В дополнение к этому процессу всестороннего публичного рассмотрения и исследования, NIST сотрудничает с Офисом Директора национальной разведки (ODNI), Министерством обороны (DoD) и Комитетом по системам национальной безопасности (CNSS), чтобы установить единые рамки и общую основу для информационной безопасности в федеральном правительстве. Общая основа и рамки для информационной безопасности обеспечат Разведку, Оборону и Гражданские секторы федерального правительства и их подрядчиков более универсальными и непротиворечивыми способами управления риском к деятельности и активам организаций, людям, другим организациям и Нации, которые следуют из эксплуатации и применения информационных систем. Общая основа и рамки также обеспечат прочное основание для взаимного принятия решений о санкционировании безопасности и облегчат совместное использование информации. NIST также работает с членами общественного и частного секторов, чтобы установить конкретные отображения и отношения между стандартами и руководствами по обеспечению безопасности, разрабатываемыми NIST и Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC).

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

Оценки мер безопасности и оценки мер приватности это не контрольные перечни, простые да-нет результаты или генерирование документов чтобы передать результаты обследований или аудитов - скорее такие оценки это принципиальный механизм, используемый чтобы проверить, что реализованные меры безопасности и меры приватности удовлетворяют заявленным задачам и целям. Специальная Публикация 800-53A, *Оценка мер обеспечения безопасности и приватности в федеральных информационных системах и организациях*, написана, чтобы облегчить оценки мер безопасности и оценки мер приватности, осуществляемые в рамках эффективной основы управления рисками. Результаты оценки мер предоставляют должностным лицам организации:

- Свидетельство об эффективности реализованных мер;
- Показания в отношении качества процессов управления рисками, используемых в организации; и
- Информацию о достоинствах и недостатках информационных систем, которые поддерживают функции предназначение и деятельности организации в глобальной среде сложных и изменяющихся угроз.

Результаты, получаемые оценщиками, используются, чтобы определить полную эффективность мер обеспечения безопасности и приватности, связанных с информационными системами (включая специфичные для системы, общие и гибридные меры) и средами их эксплуатации и получить заслуживающие доверия и значимые результаты для процесса управления рисками организации. Хорошо выполненная оценка помогает: (i) определить обоснованность мер, содержащихся в планах обеспечения безопасности и планах обеспечения приватности организации, и, впоследствии, использовать в информационных системах организации и средах их эксплуатации; и (ii) способствовать рентабельному подходу к исправлению слабых мест или недостатков в системах организованным и упорядоченным способом, непротиворечивым с потребностями предназначения/деятельности организации.

Специальная публикация 800-53A является сопутствующим руководством к Специальной публикации 800-53, *Меры обеспечения безопасности и приватности для федеральных информационных систем и организаций*. Каждая публикация представляет руководство по реализации конкретных шагов в Основах управления рисками (RMF)[1]. Специальная публикация 800-53 закрывает Шаг 2 в RMF, выбор мер обеспечения безопасности и приватности (то есть, определяет, какие меры необходимы, чтобы управлять рисками к деятельности и активам организации, людям, другим организациям и Нации). Специальная Публикация 800-53A закрывает Шаг 4 RMF, Оценка, и Шаг 6 RMF, Мониторинг, и дает представление о процессах оценки безопасности и оценки приватности. Это руководство определяет, как создавать эффективные планы оценки и как анализировать и управлять результатами оценки.

Специальная публикация 800-53A позволяет организациям адаптировать представленные базовые процедуры оценки. Концепции адаптации, используемые в этом документе, подобны концепциям, описанным в Специальной публикации 800-53. Адаптация включает настройку процедур оценки для более близкого соответствия характеристикам информационной системы и среде ее эксплуатации. Процесс адаптации даёт организации гибкость для того, чтобы избегать подходов к оценке, которые являются излишне сложными или дорогостоящими, одновременно удовлетворяя требования оценки, установленным на основании применения фундаментальных концепций RMF. Адаптация может также включать дополнительные процедуры оценки или детали оценки, чтобы соответственно удовлетворить потребности управления рисками организации (например, добавляя системно/платформенно - специфическую информацию для выбранных мер). Решения по адаптации остаются на усмотрение

[1] Специальная публикация 800-37 даёт представление о применении RMF к федеральным информационным системам.

организации, чтобы максимизировать гибкость в разработке планов оценки - применение результатов оценок степени риска, чтобы определить степень, строгость и уровень интенсивности оценок. В то время как гибкость продолжает быть важным фактором в разрабатываемых планах оценки безопасности и планах оценки приватности, согласованность оценок - также важное рассмотрение. Главная проектная цель для Специальной публикации 800-53A состоит в том, чтобы служить основой оценки и исходной начальной точкой для процедур оценки, которые важны для достижения такой согласованности.

NIST инициировал проект Протокола автоматизации контента безопасности (SCAP)[2], который поддерживает подход по достижению непротиворечивых, рентабельных оценок мер безопасности. Основное назначение SCAP состоит в том, чтобы стандартизировать формат и спецификацию, используемые для того, чтобы передавать информацию о недостатках в безопасности и конфигурациях. Эта стандартизация облегчает автоматизированную оценку конфигурации систем, оценку уязвимостей, проверку обновлений, а так же агрегацию отчётов и функциональную совместимость между поддерживающими SCAP продуктами безопасности. В результате SCAP облегчает организации определение и сокращение уязвимостей, связанных с продуктами, которые не обновлены или небезопасно сконфигурированы. SCAP также включает спецификацию Открытого интерактивного языка контрольных списков (OCIL)[3], который обеспечивает возможность выразить описаний решений в процедурах оценки в Приложении F на основе, которая устанавливает совместимость с инструментами, поддерживающими SCAP. Оценки мер приватности обсуждены отдельно в Приложении J к этой публикации.

[2] Специальная Публикация 800-126 дает представление о технической спецификации SCAP. Дополнительные детали об инициативе SCAP, а так же свободно доступные справочные данные о SCAP, могут быть найдены в http://nvd.nist.gov.

[3] OCIL - основа для описания проверок безопасности, которые не могут быть оценены без некоторого человеческого взаимодействия или обратной связь. Он используется, чтобы определить состояние системы, путём предоставления одного или более анкетных опросов её намеченным пользователям. Язык включает конструкции для вопросов, инструкции по выбору пользователями ответов, реакции на вопросы, объекты и результаты оценки.

Опечатки

Следующие изменения были внесены в Специальную публикацию 800-53A, Версия 4. Обновления включают исправления, разъяснения или другие незначительные изменения в публикации, которые являются или *редакционными* или *существенными* по сути.

ДАТА	ТИП	ИЗМЕНЕНИЕ	СТРАНИЦА
12-18-2014	Редакция	Изменение “AT-4(b)[2][a]” на “AT-4(a)[2][a].”	F-60
12-18-2014	Редакция	Изменение “AT-4(b)[2][b]” на “AT-4(a)[2][b].”	F-60
12-18-2014	Редакция	Изменение “PL-8(c)[2]” на “PL-8(c)[3].”	F-241
12-18-2014	Редакция	Изменение “SA-1(a)(2)[1]” на “SA-1(b)(2)[1].”	F-269
12-18-2014	Редакция	Изменение “SI-1(b)(2)[1]” на “SI-1(b)(2)[2].”	F-369

ГЛАВА ОДИН

ВВЕДЕНИЕ

ПОТРЕБНОСТЬ ОЦЕНИВАТЬ ЭФФЕКТИВНОСТЬ МЕР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

В настоящее время информационные системы[4] представляют собой сложное объединение технологий (то есть, аппаратных средств, программного обеспечения и встроенного микропрограммного обеспечения), процессов и людей, работающих совместно, чтобы предоставить организациям возможность обрабатывать, хранить и своевременно передавать информацию для поддержки различных функций предназначения и деятельности. Степень, до которой организации пришли в зависимость от информационных систем, чтобы выполнять обычные, важные и критические функции предназначения и деятельности, означает, что защита базовых систем и среды их эксплуатации является первостепенной для успеха организации. Выбор соответствующих мер обеспечения безопасности и приватности для информационной системы - важная задача, у которой могут быть существенные последствия для деятельности и активов организации, а так же для благосостояния людей.[5] Меры обеспечения безопасности и приватности это меры защиты или контрмеры, предписанные информационной системе или организации, разработанные, чтобы защитить конфиденциальность, целостность и доступность ее информации.

После внедрения в информационную систему, меры обеспечения безопасности и приватности оцениваются, чтобы предоставить информацию, необходимую для определения их общей эффективности, то есть степени, до которой меры обеспечения реализованы правильно, работают как предназначено и производят желаемый результат относительно удовлетворения требований безопасности и приватности для системы и организации. Понимание полной эффективности реализованных мер обеспечения безопасности и приватности важно в определении риска, следующего из использования системы, для деятельности и активов организации, людей, для других организаций и Нации.

1.1 НАЗНАЧЕНИЕ И ПРИМЕНИМОСТЬ

Назначение этой публикации состоит в том, чтобы предоставить: (i) руководства для создания эффективных планов оценки безопасности и планов оценки приватности; и (ii) исчерпывающий набор процедур для того, чтобы оценить эффективность мер безопасности и мер приватности, используемых в информационных системах и организациях, поддерживающих исполнительные агентства федерального правительства. Руководства применяются к мерам обеспечения безопасности и приватности, определённым в Специальной публикации 800-53 (с уточнениями), *Меры обеспечения безопасности и приватности для федеральных информационных систем и организаций*. Руководства были разработаны, чтобы помочь достигнуть большей безопасности информационных систем федерального правительства посредством:

- Предоставления более непротиворечивых, сопоставимых и повторяемых оценок мер обеспечения безопасности и приватности с воспроизводимыми результатами;
- Продвижение лучшего понимания рисков к деятельности организаций, активам организаций, людям, другим организациям и Нации, следующих из эксплуатации и использования федеральных информационных систем;

[4] Информационная система - дискретный набор информационных ресурсов, специально организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или ликвидации информации.

[5] Выбирая меры безопасности и меры приватности для информационной системы, организация рассматривает также потенциальные воздействия на другие организации и, в соответствии с ПАТРИОТИЧЕСКИМ АКТОМ США от 2001 г. и Президентскими директивами по безопасности отечества, потенциальные воздействия национального уровня.

- Облегчения получения более рентабельных оценок мер безопасности и мер приватности, содействующих определению полной эффективности мер обеспечения; и
- Получения более полной, надёжной и доверенной информации для должностных лиц организации для поддержки решений по управлению рисками, взаимного обмена результатами оценки, совместного использования информации и согласия с федеральными законами, Правительственными распоряжениями, директивами, нормативными актами и политиками.

Эта публикация удовлетворяет требования закона об управлении безопасностью Федеральной информации (FISMA) и соответствует или превышает требования информационной безопасности и приватности, установленные для исполнительного агентства[6] Министерством управления и бюджета (OMB) в Циркуляре A-130, Приложение I, *Обязанности федерального агентства по поддержанию записей о людях*, и Приложение III, *Безопасность федеральных автоматизированных информационных ресурсов.* Руководства по безопасности в этой публикации применимы к федеральным информационным системам, кроме систем, которые определяются, как системы национальной безопасности как установлено в 44 U.S.C., Раздел 3542. Руководства были в общих чертах разработаны с учётом технической перспективы дополнить подобные руководств для систем национальной безопасности и могут быть использованы для таких систем с одобрения соответствующих федеральных чиновников, осуществляющих политику санкционирования по таким системам. У руководств в Приложении J может быть более широкая применимость, в зависимости от полномочий и предназначений организации. Правительства штатов, местные и племенные правительства, а так же организации частного сектора поощрены рассмотреть использование этих руководств, если это соответствующе.[7]

Организации используют эту публикацию совместно с одобренными планами обеспечения безопасности и планами обеспечения приватности в разработке жизнеспособных планов оценки для порождения и компиляции информации, необходимой, чтобы определить эффективность мер обеспечения безопасности и приватности, используемых в информационной системе и организации. Эта публикация была разработана с намерением дать возможность организациям адаптировать предоставленные базовые процедуры оценки. Процедуры оценки используются в качестве начальной точки для и как вход в план оценки. В разработке эффективных планов оценки безопасности и планов оценки приватности, организации учитывают существующую информацию о мерах обеспечения, которые должны быть оценены (например, результаты оценок риска организации, зависимости аппаратных средств, программного обеспечения или встроенного микропрограммного обеспечения от специфичных платформ, и любые процедуры оценки, требуемые в результате специфичных для организации мер обеспечения, не включённых в Специальную публикацию 800-53).[8]

Выбор соответствующих процедур оценки и строгости, интенсивности и области оценки зависит от трех факторов:

---

[6] Исполнительное агентство: (i) исполнительный департамент определённый в 5 U.S.C., Раздел 101; (ii) военный департамент определённый в 5 U.S.C., Раздел 102; (iii) независимое учреждение как определено в 5 U.S.C., Раздел 104 (1); и (iv) полностью находящаяся в собственности правительственная корпорация, полностью попадающая под действие 31 U.S.C., Глава 91. В этой публикации термин исполнительное агентство синонимичен с термином федеральное агентство.

[7] В соответствии с положениями FISMA и политикой OMB, всякий раз, когда взаимодействие федеральной информационной системы с информационными системами, которыми управляют правительства штатов/местные/племенные, подрядчики или получатели, включает обработку, хранение или передачу федеральной информации, применяются стандарты и руководства по информационной безопасности, описанные в этой публикации. Конкретные требования информационной безопасности и положения и условия взаимосвязи систем, выражаются в Меморандумах о понимании и соглашениях о безопасности взаимодействия, устанавливаемых участвующими организациями.

[8] Например, подробные сценарии тестирования, возможно, должны быть разработаны для конкретной операционной системы, сетевого компонента, промежуточного программного обеспечения или приложения, используемых в информационной системе, чтобы соответственно оценить некоторые характеристики определенной меры безопасности или приватности. Такие сценарии тестирования находятся на более низком уровне детализации, чем представленный процедурами оценки, содержавшимися в Приложениях F и J, и поэтому выходят за рамки этой публикации. Дополнительные детали для оценок представлены в поддерживающих примерах оценки, описанных в Приложении H.

- Категорирования безопасности информационной системы;[9]
- Требований доверия, которые организация намеревается учесть в определении общей эффективность мер обеспечения безопасности и приватности; и
- Мер обеспечения безопасности и приватности из Специальной публикации 800-53, определённых в одобренных планах обеспечения безопасности и приватности.[10]

Процесс оценки - это деятельность по накоплению информации, а не деятельность по порождению безопасности или приватности. Организации определяют самую рентабельную реализацию этого основного элемента в программах организации по информационной безопасности и приватности, применяя результаты оценок риска, рассматривая зрелость и уровень качества процессов управления рисками организации и используя в своих интересах гибкость концепций, описанных в этой публикации. Использование Специальной публикации 800-53A как начальной точки в процессе определения процедур для оценки мер обеспечения безопасности и приватности в информационных системах и организациях способствует непротиворечивому уровню безопасности и приватности и предоставляет необходимую гибкость, чтобы модифицировать оценку, основываясь на политиках и требованиях организации, известной информации об угрозах и уязвимостях, рассмотрениях по эксплуатации, в зависимости от информационной системы и платформы, и допуске для риска.[11] Информация, получаемая во время оценок мер обеспечения, может использоваться организацией для:

- Определения потенциальных проблем или недостатков в реализации организацией Основ управления риском;
- Определения слабых мест и недостатков, связанных безопасностью и приватностью в информационной системе и в среде, в которой работает система;
- Распределения по приоритетам решений по уменьшению риска и связанных действий по уменьшению риска;
- Подтверждению, что определённые слабые места и недостатки, связанные с безопасность и приватностью в информационной системе и в среде деятельности, учтены;
- Поддержки работ по мониторингу и ситуативному освоению информационной безопасности и приватности;
- Облегчения решений по санкционированию безопасности, решений по санкционированию приватности и продлению решений по санкционированию; и
- Информированию по бюджетным решениям и процессу капиталовложения.

Не ожидается, что организации используют *все* методы оценки и объекты оценки, содержащиеся в процедурах оценки, определённых в этой публикации для связанных мер обеспечения безопасности и приватности, развёрнутых в пределах или наследованных информационными системами организации. Скорее у организаций есть соответствующая гибкость, чтобы определить уровень необходимых усилий и доверие, требуемые для определённой оценки (например, какие методы оценки и объекты оценки, как считается, являются самыми полезными в получении требуемых результатов). Это определение делается на основе того, чтобы достигнуть целей оценки самым рентабельным способом и с достаточной уверен-

[9] Для систем национальной безопасности категорирование безопасности выполняется в соответствии с Инструкцией 1253 CNSS. Для других систем, кроме систем национальной безопасности, категорирование безопасности выполняется в соответствии с Федеральным стандартом обработки информации (FIPS) 199 и NIST Специальной публикацией 800-60.

[10] Меры обеспечения безопасности и приватности для информационной системы и организации документируются в планах обеспечения безопасности и планы обеспечения приватности после начального выбора и адаптации мер обеспечения, как описано в NIST Специальной публикации 800-53 и Инструкции CNSS 1253.

[11] В этой публикации термин риск используется, чтобы обозначить риск для деятельности организации (то есть, предназначения, функций, имиджа и репутации), активов организации, людей, других организаций и нации.

ностью, чтобы поддержать последующее определение результирующего риска для предназначения или деятельности. Организации должны сбалансировать ресурсы, расходуемые на развертывание мер обеспечения безопасности и приватности (то есть, мер защиты и контрмер, реализуемых для защиты безопасности и приватности), против ресурсов, расходуемых, чтобы определить полную эффективность мер обеспечения, и первоначально и на постоянной основе, через программы непрерывного мониторинга.

1.2 ЦЕЛЕВАЯ АУДИТОРИЯ

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

- Людей с обязанностями по разработке информационных систем (например, менеджеры программ, проектировщики и разработчики систем, системные интеграторы, инженеры по информационной безопасности);
- Людей с обязанностями по оценке и мониторингу информационной безопасности (например, Генеральные инспектора, оценщики систем, оценщики, независимые верификаторы/валидаторы, аудиторы, аналитики, владельцы информационных систем, поставщики общих мер безопасности);
- Люди с обязанности по информационным системам, безопасности, приватности и управлению и надзору за рисками (например, санкционирующие должностные лица, директора по информации, высшие сотрудники по информационной безопасности,[12] высшие должностные лица агентства по приватности/директора по приватности, менеджеры по информационной системе, менеджеры по информационной безопасности); и
- Люди с обязанностями по реализации и применению информационной безопасности (например, владельцы информационных систем, поставщики общих мер безопасности, владельцы/управляющие информацией, владельцы предназначения/деятельности, системные администраторы, сотрудники безопасности информационной системы).

1.3 СВЯЗАННЫЕ ПУБЛИКАЦИИ И ПРОЦЕССЫ ОЦЕНКИ

Специальная публикация 800-53A разработана, чтобы поддержать Специальную публикацию 800-37, *Руководство по применению основ управления рисками к федеральным информационным системам: Подход жизненного цикла безопасности*. В частности, процедуры оценки, содержащиеся в этой публикации и руководствах, предусмотренные для разработки планов оценки безопасности и приватности информационных систем организаций, непосредственно поддерживают действия по оценке и мониторингу, которые являются неотъемлемой частью процесса управления рисками. Это включает обеспечение близко к реальному времени должностных лиц организаций информацией, связанной с безопасностью и приватностью, относительно текущего состояния безопасности и приватности их систем и организаций.

Организации поощрены, когда это возможно, использовать в своих интересах результаты оценки и связанную документацию и свидетельства оценки, доступные для компонентов информационной системы от предыдущих оценок, включая независимое стороннее тестирование, оценку и подтверждение соответствия.[13] Тестирование продукта, оценка и подтверждение соответствия могут быть проведены для криптографических модулей и продуктов информационных технологий общего назначения,

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

[13] Результаты оценки могут быть получены из многих работ, которые обычно происходят во время жизненного цикла разработки систем. Например, результаты оценки получают во время тестирования и оценки новых компонентов информационной системы во время модернизации систем или работ по интеграции систем. Организации могут использовать в своих интересах предыдущие результаты оценки, когда это возможно, чтобы уменьшить полную стоимость оценок и сделать процесс оценки более эффективным.

таких как операционные системы, системы базы данных, межсетевые экраны, устройства обнаружения вторжений, Веб-браузеры, Веб-приложения, смарт-карты, биометрические устройства, персональные устройства проверки идентификационных данных, сетевые устройства и аппаратные платформы, с использованием национальных и международных стандартов. Если продукт компонента информационной системы определён как предназначенный для поддержки реализации определённой меры обеспечения безопасности или приватности в Специальной Публикации 800-53, то свидетельство, полученное во время процессов тестирования, оценки и подтверждения соответствия продукта (например, спецификации безопасности, исследования и результаты испытаний, отчёты подтверждения соответствия и сертификаты подтверждения соответствия)[14], используется в такой степени, насколько оно применимо. Это свидетельство может быть объединено со связанным с оценкой свидетельством, полученным из приложения процедур оценки в этой публикации, чтобы рентабельно получить информацию, необходимую для определения, эффективны ли меры обеспечения безопасности и приватности в своём приложении.

1.4 ОРГАНИЗАЦИЯ ЭТОЙ СПЕЦИАЛЬНОЙ ПУБЛИКАЦИИ

Последующая часть этой специальной публикации организована следующим образом:

- **Глава Два** описывает фундаментальные концепции, связанные с оценкой мер обеспечения безопасности и приватности включая: (i) интеграцию оценок в жизненный цикл разработки систем; (ii) важность общей для всей организации стратегии проведения оценки мер обеспечения безопасности и приватности; (iii) разработку эффективных образцов доверия, чтобы помочь повысить основания для уверенности в эффективности оцениваемых мер обеспечения безопасности и приватности; и (iv) формат и контент процедур оценки.
- **Глава Три** описывает процесс оценки мер обеспечения безопасности и приватности в информационных системах организации и средах их применения, включая: (i) работы, выполняемые организациями и оценщиками, чтобы подготовиться к оценке мер обеспечения безопасности и приватности; (ii) разработку планов оценки безопасности; (iii) проведение оценки мер обеспечения безопасности и приватности и анализ, документирование и представление отчётности по результатам оценки; и (iv) анализ после-оценочного отчёта и последующие работы, выполняемые организациями.
- **Поддерживающие приложения** предоставляют детализированную, связанную с оценкой информацию, включая: (i) основные ссылки; (ii) термины и определения; (iii) акронимы; (iv) описание методов оценки; (v) руководства по тестированию на возможность проникновения; (vi) каталог процедур оценки, которые могут использоваться, чтобы разработать планы оценки мер безопасности; (vii) контент отчётов об оценке безопасности; (viii) определение, формат и использование образцов оценки; (ix) автоматизацию поддержки для текущих оценок; и (x) каталог процедур оценки, которые могут использоваться, чтобы разработать планы оценки мер приватности.

[14] Организации рассматривают доступную информацию по продуктам компонентов информационной технологии, чтобы определить: (i) какие меры обеспечения безопасности и приватности реализуются продуктом; (ii) удовлетворяют ли эти меры обеспечения безопасности и приватности установленным требованиям к мерам обеспечения оцениваемой информационной системы; (iii) соответствует ли конфигурация продукта и средой, в которой работает продукт, со средой и конфигурацией продукта, заявленными поставщиком и/или разработчиком; и (iv) удовлетворяют ли требования доверия, заявленные в спецификации разработчика/поставщика, требования доверия к оценке этих мер обеспечения. Соответствие вышеупомянутым критериям обеспечивает осмысленное обоснование, что продукт является подходящим и удовлетворяет установленным требованиям к мерам обеспечения безопасности и приватности оцениваемой информационной системы.

ГЛАВА ДВА

ОСНОВЫ

ФУНДАМЕНТАЛЬНЫЕ ПОНЯТИЯ, СВЯЗАННЫЕ С ОЦЕНКАМИ МЕР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

Эта глава описывает фундаментальные понятия, связанные с оценкой мер обеспечения безопасности и приватности в информационных системах организаций и средах, в которых эти системы применяются, включая: (i) интеграцию оценок в жизненный цикл разработки систем; (ii) важность общей для всей организации стратегии проведения оценки мер обеспечения безопасности и приватности; (iii) разработку эффективных образцов доверия, чтобы помочь повысить основания для уверенности в эффективности оцениваемых мер обеспечения безопасности и приватности; и (iv) формат и контент процедур оценки. Хотя гибкость остаётся важным фактором при разработке планов оценки, согласованность оценок также является важным рассмотрением. Фундаментальная проектная цель для Специальной публикации 800-53A состоит в том, чтобы служить основой оценки и начальной точкой для процедур оценки, которые важны для достижения такой согласованности.

2.1 ОЦЕНКИ В ЖИЗНЕННОМ ЦИКЛЕ РАЗРАБОТКИ СИСТЕМ

Оценки безопасности и приватности могут быть эффективно выполнены на различных стадиях жизненного цикла[15] разработки систем, чтобы увеличить основу для уверенности в том, что меры обеспечения безопасности и приватности, используемые в составе или наследуемые информационной системой, эффективны в их применении. Эта публикация обеспечивает исчерпывающий набор процедур оценки, чтобы поддержать работы оценки безопасности и приватности всюду в жизненном цикле разработки систем. Например, оценки безопасности обычно проводятся разработчиками систем и системными интеграторами в фазах разработки/приобретения и реализации жизненного цикла. Оценки приватности также проводятся высшими должностными лицами агентств по приватности/сотрудниками по приватности и персоналом приватности на этих ранних фазах жизненного цикла. Это помогает гарантировать, что требуемые меры обеспечения безопасности и приватности для систем должным образом спроектированы и разработаны, правильно реализованы и непротиворечивы с установленной архитектурой информационной безопасности организации *прежде, чем* система будет введена в фазу эксплуатации и поддержки. Оценки безопасности в начальных фазах жизненного цикла разработки систем включают, например, анализ проекта и кода, сканирование приложений и регрессионное тестирование. Оценки приватности включают анализ, гарантирующий, что соблюдаются применимые законы и политики по приватности и что защита приватности встроена в проектирование систем. Связанные с безопасностью и приватностью слабые места и недостатки, определённые в начале жизненного цикла разработки систем, могут быть разрешены более быстро и в значительно более рентабельном способе до перехода к последующим фазам жизненного цикла. Цель состоит в том, чтобы определить меры обеспечения безопасности и приватности раньше в жизненном цикле, чтобы гарантировать, что проектирование систем и испытания подтверждают реализацию этих мер. Процедуры оценки, описанные в Приложениях F и J, поддерживают оценки, выполняемые во время начальных стадий жизненного цикла разработки систем.

Оценки безопасности и приватности проводятся также во время фазы эксплуатации и поддержки жизненного цикла, чтобы гарантировать, что меры обеспечения безопасности и приватности продолжают быть эффективными в среде эксплуатации и могут защитить от постоянно развивающихся угроз. Оценки безопасности, как правило, проводятся владельцами информационной системы, поставщиками общих мер безопасности, сотрудниками безопасности информационной системы, независимыми оценщиками, аудиторами и Генеральными инспекторами. Оценки приватности, как правило, проводятся высшими должностными лицами агентства по приватности/сотрудниками по приватности и персоналом

[15] В универсальном жизненном цикле разработки систем, как правило, есть пять фаз: (i) инициирование; (ii) разработка/приобретение; (iii) реализация; (iv) эксплуатация и поддержка; и (v) ликвидирование (ликвидация). Специальная публикация 800-64 даёт представление о рассмотрениях безопасности в жизненном цикле разработки систем.

приватности. Например, организации оценивают все меры безопасности и меры приватности, используемые в и наследуемые информационной системой во время начального санкционирования безопасности. В дальнейшем, после начального санкционирования, организации оценивают все реализованные меры безопасности на непрерывной основе в соответствии с её стратегией Непрерывного мониторинга информационной безопасности[16]. Меры приватности также оцениваются на непрерывной основе, чтобы гарантировать согласие с применимыми законами и политиками по приватности. Текущая оценка и мониторинг мер безопасности и мер приватности используют процедуры оценки, определённые в этой публикации. Частота таких оценок и мониторинга определяется организацией и/или владельцем информационной системы или поставщиком общих мер безопасности и одобряется санкционирующим должностным лицом. Наконец, в конце жизненного цикла оценки безопасности проводятся, чтобы гарантировать, что важная информация организации очищена до ликвидации информационной системы. Также проводятся оценки приватности, чтобы гарантировать приверженность графикам ретенции организации.

2.2 СТРАТЕГИЯ ПРОВЕДЕНИЯ ОЦЕНОК МЕРЫ ОБЕСПЕЧЕНИЯ

Организации поощрены разработать всеобъемлющую, общую для организации стратегию проведения оценок безопасности и приватности, облегчающую более рентабельные и непротиворечивые оценки через реестр информационных систем. Общая для организации стратегия начинается с применения начальных шагов Основ управления рисками ко всем информационным системам в организации, с представления организацией процесса категорирования безопасности и процесса выбора мер обеспечения безопасности и приватности (включая определение общих мер безопасности). Категорирование информационных систем, как общая для организации работа, учитывающее не только критичность и чувствительность информации, но также и архитектуру предприятия и архитектуру информационной безопасности, помогает гарантировать, что отдельные системы категорируются основываясь на предназначении и целях деятельности организации.[17] Максимизация числа используемых в организации общих мер безопасности: (i) значительно уменьшает стоимость разработки, реализации и оценки мер обеспечения безопасности и приватности; (ii) позволяет организациям централизовать и автоматизировать оценки мер обеспечения и амортизировать стоимость этих оценок для всех информационных систем организации; и (iii) повысить согласованность мер обеспечения безопасности и приватности. Подход к определению общих мер безопасности для всей организации в начале применения RMF облегчает более глобальную стратегию оценки этих мер обеспечения и совместное использование существенных результатов оценки с владельцами информационных систем и санкционирующими должностными лицами. Совместное использование результатов оценки среди ключевых должностных лиц организации в границах информационной системы обладает многими важными преимуществами, включая:

- Обеспечение возможности рассмотреть результаты оценки для всех информационных систем и сделать решения для работ по уменьшению риска, связанные с предназначения/деятельностью, согласно приоритетам организации, категорированию безопасности информационных систем и оценкам степени риска;
- Обеспечение более глобального представления слабых мест и недостатков, имеющих место в информационных системах, через организацию и возможность разработать решения для всей организации по проблемам информационной безопасности и приватности; и
- Увеличение базы знаний организации относительно угроз, уязвимостей и стратегий для более рентабельных решений по общим проблемам информационной безопасности и приватности.

Организации могут также способствовать более целенаправленному и рентабельному процессу оценки путём: (i) разработки более конкретных процедур оценки, которые адаптированы для их конкретных

[16] Специальных Публикаций 800-37 и 800-137 дают представление о непрерывном мониторинге мер безопасности.

[17] Меры приватности выбираются и реализуются независимо от категорирования безопасности информационной системы.

сред деятельности и требований (вместо того, чтобы передавать решение этих задач каждому оценщику по мерам обеспечения или команде оценки); и (ii) предоставления общих для всей организации инструментов, шаблонов и технологий для поддержки более непротиворечивых оценок в организации.[18]

Проведение оценок мер безопасности - основная ответственность владельцев информационных систем и поставщиков общих мер безопасности с надзором за ними соответствующими санкционирующими должностными лицами. Проведение оценок меры обеспечения приватности - основная ответственность высших должностных лиц агентств по приватности/директоров по приватности и персонала приватности. Есть также существенное участие в процесс оценки других сторон в организации, у которых есть непосредственная заинтересованность в результатах оценок. Другие заинтересованные стороны включают, например, владельцев предназначения/деятельности, владельцев/управляющих информацией (когда эти роли выполняются кем-то другим, кроме владельца информационной системы), персонал по информационной безопасности и назначенный штат по приватности. Обязательно, чтобы владельцы информационной системы и поставщики общих мер безопасности координировали с другими сторонами в организации, имеющими интерес в оценках мер обеспечения, чтобы помочь гарантировать, что базовые функции предназначения и деятельности организации соответственно учтены при выборе мер обеспечения безопасности и приватности, которые будут оцениваться.

ПРЕДОСТЕРЕЖЕНИЕ

Организации должны тщательно рассмотреть потенциальные воздействия использования процедур оценки, определённых в этой Специальной публикации, оценивая меры обеспечения безопасности и приватности в *эксплуатируемых* системах. Некоторые процедуры оценки, особенно те процедуры, которые непосредственно воздействуют на эксплуатацию или функции аппаратных средств, программного обеспечения или компонентов встроенного микропрограммного обеспечения информационной системы, могут непреднамеренно влиять на стандартную обработку, передачу или хранение информации, поддерживающей функции предназначения или деятельности организации. Например, критический компонент информационной системы может быть взят офлайн для целей оценки или компонент может внести отказ или отказать во время процесса оценки. Организации должны также обеспечить необходимые предосторожности, чтобы гарантировать, что функции предназначения и деятельности организаций продолжают поддерживаться информационными системами и что любые потенциальные воздействия на эффективность эксплуатации, следующие из работ оценки, рассмотрены заранее.

2.3 СОЗДАНИЕ ЭФФЕКТИВНЫХ ОБРАЗЦОВ ДОВЕРИЯ

Создание эффективных образцов доверия[19] для эффективных мер обеспечения безопасности и приватности является процессом, который включает: (i) компиляцию свидетельств для множества работ, проводимых во время жизненного цикла разработки систем, где меры обеспечения, использованные в информационной системе, реализованы правильно, работают как предназначено и производят желаемый результат относительно удовлетворения требований безопасности и приватности для системы и организации; и (ii) представление этих свидетельств таким образом, что принимающие решения лица в состоянии использовать их эффективно в принятии основанных на риске решений относительно эксплуатации или использования системы. Свидетельство, описанное выше, вытекает из

[18] Организации могут также обеспечить планы оценки безопасности, включая специализированные процедуры оценки для внешних поставщиков услуг, которые управляют информационными системами от имени этих организаций. Кроме того, эти планы могут рекомендовать поддерживать шаблоны, инструменты и технологии, а также быть далее адаптированы конкретно к контракту с поставщиком услуг, помогая сделать оценки более непротиворечивыми и максимизировать повторное использование связанных с оценкой объектов. Это повторное использование может улучшить безопасность через единообразие и уменьшить/устранить неопределённость контракта, приводя к уменьшению стоимости и риска для организации.

[19] Образец доверия это состав свидетельств, организованный в доказательство, демонстрирующее что некоторое утверждение об информационной системе поддерживается (то есть, обеспечено). Образец доверия необходим, когда важно показать, что система демонстрирует некоторое сложное качество, такое как защищённость, безопасность или надёжность.

реализации мер обеспечения безопасности и приватности в информационной системе и наследуемых системой (то есть, общих мер безопасности) и от оценок этой реализации. В идеале, оценщик основывается на ранее разработанных материалах, которые начинались со спецификации потребностей информационной безопасности и приватности организации и были далее разработаны во время проектирования, разработки и реализации информационной системы. Эти материалы, разработанные при реализации безопасности и приватности всюду по жизненному циклу информационной системы, представляют начальные свидетельства для образцов доверия.

Оценщики получают требуемое свидетельство во время процесса оценки, чтобы позволить соответствующим должностным лицам организации делать объективные суждения об эффективности мер обеспечения безопасности и приватности и полном состоянии безопасности и приватности информационной системы. Свидетельство оценки, необходимое чтобы сделать такие определения, может быть получено из многих источников включая, например, оценки продуктов и систем информационных технологий и, в случае оценок приватности, документации соответствия приватности, такой как Оценки воздействия на приватность и Уведомлений системы отчётов по Закону о неприкосновенности частной жизни. Оценки продуктов (также известные как испытания, оценка и подтверждение соответствия продуктов) проводятся, как правило, независимыми, сторонними испытательными организациями. Эти оценки исследуют функции безопасности и приватности продуктов и установленных параметров конфигурации. Оценки могут быть проведены, чтобы демонстрировать согласие отраслевым, национальным или международным стандартам по информационной безопасности, стандартам по приватности, воплощённым в действующих законах и политиках и заявлениях разработчика/поставщика. Так как многие продукты информационных технологий оцениваются коммерческими испытательными организациями и затем, впоследствии, развёртываются в миллионах информационных систем, эти типы оценок могут быть выполнены на большем уровне глубины и обеспечить более глубокую способность проникновения в суть возможностей безопасности и приватности определённых продуктов.

Оценки систем, как правило, проводятся разработчиками информационных систем, системными интеграторами, владельцами информационных систем, поставщиками общих мер безопасности, оценщиками, аудиторами, Генеральными инспекторами и персоналом по информационной безопасности и приватности организаций. Оценщики или команды оценки объединяют доступную информацию об информационной системе, такую как результаты оценок продуктов отдельных компонентов, при наличии, и проводят дополнительные оценки на уровне системы, используя множество методов и технологий. Оценки систем используются, чтобы скомпилировать и оценить свидетельство, необходимое должностным лицам организации, чтобы определить, насколько меры обеспечения безопасности и приватности, использованные в информационной системе, будут эффективно пригодны для смягчения рисков к деятельности и активам организации, людям, к другим организациям и Нации. Результаты оценок, проведенных с использованием специфичных для информационной системы и специфичных для организации процедур оценки, полученных из руководств в этой публикации, способствуют компиляции необходимого свидетельства, чтобы определить эффективность мер обеспечения безопасности и приватности в соответствии с требованиями доверия, задокументированными в планы обеспечения безопасности и приватности.

2.4 ПРОЦЕДУРЫ ОЦЕНКИ

Процедура оценки состоит из ряда *целей* оценки, каждая со связанным набором потенциальных *методов* оценки и *объектов* оценки. Цель оценки включает ряд *описаний решений*, связанных с определённой мерой обеспечения безопасности или приватности, подвергающейся оценке. Описания решений связаны с контентом меры обеспечения безопасности или приватности (то есть, функциональностью меры обеспечения безопасности/приватности), чтобы гарантировать прослеживаемость результатов оценки назад к фундаментальным требованиям меры обеспечения. Приложение процедуры оценки к мере обеспечения безопасности или приватности производит

результаты оценки. Эти результаты отражаются, или впоследствии используются, чтобы помочь определить полную эффективность меры обеспечения безопасности или приватности.

Объекты оценки определяют конкретные оцениваемые элементы и включают *спецификации*, *механизмы*, *работы* и *людей*. Спецификации - основанные на документе объекты (например, политики, процедуры, планы, требования безопасности и приватности системы, функциональные спецификации, эскизные проекты), связанные с информационной системой. Механизмы - конкретные аппаратные средства, программное обеспечение или встроенное микропрограммное обеспечение мер защиты и контрмер, используемые в информационной системе.[20] Работы – конкретные, связанные с защитой действия, поддерживающие информационную систему, которые включают людей (например, проведение операций по резервированию системы, контроль сетевого трафика, использование плана действий при непредвиденных обстоятельствах). Люди, или группы людей, являются людьми, применяющими спецификации, механизмы или работы, описанные выше.

Методы оценки определяют сущность действий оценщика и включают *исследования*, *опросы* и *испытания*. Метод *исследования* - процесс рассмотрения, обследования, наблюдения, изучения или анализа одного или более объектов оценки (то есть, спецификаций, механизмов или работ). Назначение метода исследования состоит в том, чтобы облегчить понимание оценщика, добиться разъяснения или получить свидетельство. Метод *опроса* - процесс обсуждений с людьми или группами людей в организации чтобы также облегчить понимание оценщика, добиться разъяснения или получить свидетельство. *Метод испытаний* - процесс проверки одного или более объектов оценки (то есть, работ или механизмов) при указанных условиях, чтобы сравнить фактическое и ожидаемое поведение. Во всех трёх методах оценки результаты используются в создании конкретных решений, требуемых в описаниях решений и, таким образом, достижении целей для процедур оценки. Полное описание методов оценки и объектов оценки приведено в Приложении D.

У методов оценки есть набор связанных атрибутов *глубины* и *покрытия*, которые помогают определить уровень усилий для оценки. Эти атрибуты являются иерархическими в сущности, обеспечивая возможности по определению строгости и области оценки для увеличивающегося доверия, которое может быть необходимо для некоторых информационных систем. Атрибут глубины определяет строгость и уровень детализации в исследованиях, опросах и процессах тестирования. Значения для атрибута глубины включают *основная*, *ограниченная* и *полная*. Атрибут покрытия определяет область или ширину исследований, опросов и процессов тестирования, включая количество и тип спецификаций, механизмов и работ, которые будут исследованы или протестированы, и количество и типы людей, которые будут опрошены. Подобно атрибуту глубины, значения для атрибута покрытия включают *основное*, *ограниченное* и *полное*. Соответствующие значения атрибутов глубины и покрытия для определённого метода оценки основаны на требованиях доверия, определённых организацией.[21] По мере усиления требований доверия по отношению к разработке, реализации и применению мер обеспечения безопасности и приватности в информационной системе или их наследованию, также имеют тенденцию усиливаться строгость и область работ оценки (что отражено в выборе методов и объектов оценки и назначении величины атрибутов глубины и покрытия). Приложение D обеспечивает подробное описание атрибутов методов оценки и значений атрибутов.

[20] Механизмы также включают устройства физической защиты, связанные с информационной системой (например, блокировки, кнопки, камеры видеонаблюдения, устройства противопожарной защиты, огнестойкие сейфы и т.д.).

[21] Для систем, не относящихся к системам национальной безопасности, организации удовлетворяют минимальные требования доверия, определённые в Специальной публикации 800-53, Приложение E.

Рисунок 1 иллюстрирует пример процедуры оценки, разработанной, чтобы оценить эффективность меры безопасности CP-9. Цель оценки для CP-9 взята из описания базовой меры безопасности, приведенной в Специальной публикации NIST 800-53, Приложение F. Потенциальные методы оценки и объекты добавлены к процедуре оценки.

CP-9	**РЕЗЕРВНОЕ КОПИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ**		
	ЦЕЛЬ ОЦЕНКИ: *Вынесите решение если организация:*		
	CP-9(a)	**CP-9(a)[1]**	*определяет частоту, соотносящуюся с целями времени восстановления и целями точки восстановления, как определено в плане действий в непредвиденных ситуациях информационной системы, чтобы провести резервное копирование пользовательской информации, содержащейся в информационной системе;*
		CP-9(a)[2]	*проводит резервное копирование пользовательской информации, содержащейся в информационной системе с определённой организацией частотой;*
	CP-9(b)	**CP-9(b)[1]**	*определяет частоту, соотносящуюся с целями времени восстановления и целями точки восстановления, как определено в плане действий в непредвиденных ситуациях информационной системы, чтобы провести резервное копирование системной информации, содержащейся в информационной системе;*
		CP-9(b)[2]	*проводит резервное копирование системной информации, содержащейся в информационной системе с определённой организацией частотой;*
	CP-9(c)	**CP-9(c)[1]**	*определяет частоту, соотносящуюся с целями времени восстановления и целями точки восстановления, как определено в плане действий в непредвиденных ситуациях информационной системы, чтобы провести резервное копирование документации информационной системы, включая документацию, связанную с безопасностью;*
		CP-9(c)[2]	*проводит резервное копирование документации информационной системы, включая документацию, связанную с безопасностью, с определённой организацией частотой; и*
	CP-9(d)	*защищает конфиденциальность, целостность и доступность информации резервного копирования в месте хранения.*	
	ПОТЕНЦИАЛЬНЫЕ МЕТОДЫ И ОБЪЕКТЫ ОЦЕНКИ: **Исследования**: [*ВЫБЕРИТЕ ИЗ:* Политика планирования на случай непредвиденных ситуаций; процедуры учёта резервного копирования информационной системы; план действий в непредвиденных ситуациях; место (а) хранения резервной копии данных; регистрационные файлы или записи резервных копий информационной системы; другие соответствующие документы или записи]. **Опросы**: [*ВЫБЕРИТЕ ИЗ:* Персонал организации с обязанностями по изготовлению резервных копий информационной системой; персонал организации с обязанностями по информационной безопасности]. **Испытания**: [*ВЫБЕРИТЕ ИЗ:* Процессы организации по проведению резервного копирования информационной системы; автоматизированные механизмы, поддерживающие и/или реализующие резервное копирование информационной системы].		

РИСУНОК 1: ПРОЦЕДУРА ОЦЕНКИ ПО МЕРЕ БЕЗОПАСНОСТИ

Цели оценки пронумерованы последовательно, сначала в соответствии с системой нумерации в Специальной публикации 800-53, а затем, где необходимо, чтобы дальше разделить требования мер обеспечения безопасности или приватности для облегчения оценки, используются последовательные числа или буквы, которые, чтобы сделать различие, **заключены в квадратные скобки** в противоположность круглым скобкам (например, CP-9(a), CP-9(a)[1], CP-9(a)[2], CP-9(b)**[**1**]**, CP-9(b)**[**2**]**, CP-9(c)**[**1**]**, CP-9(c)**[**2**]**, CP-9(d), и т.д.). Начальный, заключённый в квадратные скобки символ, всегда число. Для некоторых мер столбец с начальным обозначением меры обеспечения (например, CP-9, CP-9(a), CP-9(b), и CP-9(c) на рисунке 1) является просто заполнителем, чтобы помочь облегчить распределение мер обеспечения, поддерживая систему форматирования. Если явно не указано, для каждого идентифицированного метода оценки в процедуре оценки, значения атрибутов глубины и

покрытия, описанных в Приложении D, назначаются организацией и применяются оценщиком/командой оценки при выполнении метода оценки в отношении объекта оценки.

Если у меры обеспечения есть какие-либо улучшения (что определяется последовательными числами в круглых скобках, например, CP-9(3) для третьего улучшения для CP-9), цели оценки разрабатываются для каждого улучшения, используя тот же самый процесс, который относится к основной мере обеспечения. Результирующие цели оценки нумеруются последовательно таким же образом, как процедура оценки по основной мере обеспечения, сначала в соответствии с системой нумерации в Специальной публикации 800-53, и затем, чтобы облегчить оценки, используя заключённые в квадратные скобки последовательные числа или буквы, чтобы далее распределить требования улучшения мер обеспечения (например, CP-9(3)**[**1**]**, CP-9(3)**[**2**]**). Рисунок 2 иллюстрирует пример процедуры оценки, разработанной, чтобы оценить эффективность третьего улучшения к мере обеспечения безопасности CP-9.

<table>
<tr><td>CP-9(3)</td><td colspan="3">РЕЗЕРВНОЕ КОПИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ | РАЗДЕЛЬНОЕ ХРАНЕНИЕ ДЛЯ КРИТИЧЕСКОЙ ИНФОРМАЦИИ</td></tr>
<tr><td rowspan="4"></td><td colspan="3">ЦЕЛЬ ОЦЕНКИ:
Вынесите решение если организация:</td></tr>
<tr><td>CP-9(3)[1]</td><td>CP-9(3)[1][a]</td><td>определяет критическое программное обеспечение информационной системы и другую связанную с безопасностью информацию, требующую, чтобы резервные копии хранились в особых условиях; или</td></tr>
<tr><td></td><td>CP-9(3)[1][b]</td><td>определяет критическое программное обеспечение информационной системы и другую связанную с безопасностью информацию, требующую, чтобы резервные копии хранились в пожароустойчивом контейнере, который расположен вне автоматизированной системы; и</td></tr>
<tr><td>CP-9(3)[2]</td><td colspan="2">хранит резервные копии определённого организацией программного обеспечения информационной системы и другой связанной с безопасностью информации в особых условиях или в пожароустойчивом контейнере, который расположен вне автоматизированной системы.</td></tr>
<tr><td colspan="3">ПОТЕНЦИАЛЬНЫЕ МЕТОДЫ И ОБЪЕКТЫ ОЦЕНКИ:
Исследования: [ВЫБЕРИТЕ ИЗ: Политика планирования на случай непредвиденных ситуаций; процедуры учёта резервного копирования информационной системы; план действий в непредвиденных ситуациях; место (а) хранения резервной копии данных; документация по конфигурированию резервных копий информационной системы и связанная документация; регистрационные файлы или записи резервных копий информационной системы; другие соответствующие документы или записи].
Опросы: [ВЫБЕРИТЕ ИЗ: Персонал организации с обязанностями по планированию в непредвиденных ситуациях и реализации плана; персонал организации с обязанностями по изготовлению резервных копий информационной системой; персонал организации с обязанностями по информационной безопасности].</td></tr>
</table>

РИСУНОК 2: ПРОЦЕДУРА ОЦЕНКИ ПО УЛУЧШЕНИЮ МЕРЫ БЕЗОПАСНОСТИ

Напоминаем, что *числа* в круглых скобках сразу после обозначения основной меры обеспечения (как на рисунке 2) указывают на номер улучшения меры, в то время как *буквы* в круглых скобках сразу после обозначения основной меры обеспечения (как на рисунке 1) указывают на подраздел основной меры в структуре требований мер обеспечения. Когда следующий подраздел меры обеспечения необходим, чтобы поддержать оценку, заключенные в квадратные скобки символы, которые чередуются между числами и буквами (например, CP-9(3)[1], CP-9(3)[1][b]), используются с начальным заключенным в квадратные скобки символом, всегда являющимся числом, следует ли это за заключённой в круглые скобки буквой (основная мера обеспечения) или числом (улучшение меры обеспечения).

Протокол автоматизации контента безопасности (SCAP) поддерживает процесс оценки для мер безопасности и облегчает более эффективные и рентабельные оценки. SCAP - набор связанных спецификаций для автоматизации сбора и представления свидетельств в базируемый на стандарты формат, которые облегчают функциональную совместимость между SCAP-ориентированными инструментами. Спецификации SCAP определяют форматы, посредством которых критериями оценки, также называемыми *контентом SCAP*, можно обмениваться и обеспечивать инструменты оценки. Этот контент может использоваться, чтобы автоматизировать сбор и оценку свидетельств, полученных от

машинно-ориентированных и от человеко-ориентированных источников. SCAP также определяет форматы, которые фиксируют и допускают обмен результатами накопления и оценки объектов. Как правило, машинно-ориентированные объекты, которые могут быть накоплены и оценены с использованием SCAP, принадлежат к механизмам (например, установки конфигурации, установленные аппаратные средства/программное обеспечение, рабочее состояние контрмер). Дополнительно, ориентируемые на пользователя объекты, такие как те, которые принадлежат спецификациям и работам, могут быть собраны, используя Открытый интерактивный язык контрольных списков (OCIL). OCIL - спецификация компонента SCAP, который облегчает набор и представление данных интервью в основанном на стандартах формате. Управляемая контентом сущность SCAP-ориентированных автоматизированных решений может поддержать гибкую и непротиворечивую оценку мер обеспечения безопасности и приватности.

ГЛАВА ТРИ

ПРОЦЕСС

ПРОВЕДЕНИЕ ЭФФЕКТИВНЫХ ОЦЕНОК МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

Эта глава описывает процесс оценки мер обеспечения безопасности и приватности в информационных системах и средах деятельности организации, включая: (i) работы, выполняемые организациями и оценщиками, чтобы подготовиться к оценки мер обеспечения безопасности и приватности; (ii) разработку планов оценки безопасности и приватности; (iii) проведение оценок мер обеспечения и анализ, документирование и представление отчётов по результатам оценки; и (iv) анализ после-оценочного отчёта и последующие работы.

3.1 ПОДГОТОВКА К ОЦЕНКАМ МЕР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

Проведение оценок мер обеспечения безопасности и оценок мер обеспечения приватности в современных комплексных средах информационных технологий сложных инфраструктур и высоко доступных, важных для предназначения приложений может быть трудным, напряжённым и ресурсо-ёмким. Оценки мер обеспечения безопасности и приватности могут быть проведены различными сущностями организации с различными обязанностями по надзору. Тем не менее, успех требует кооперации и сотрудничества между всеми сторонами, имеющими непосредственный интерес в состоянии информационной безопасности или приватности организации, включая владельцев информационной системы, поставщиков общих мер безопасности, санкционирующих должностных лиц, директоров по информации, высших сотрудников по информационной безопасности, высших должностных лиц агентства по приватности /директоров по приватности, исполнительных директоров/руководителей агентств, персонал по безопасности и приватности, Генеральных инспекторов и OMB. Установление соответствующего набора ожиданий до, во время и после оценки является определяющим для достижения приемлемого результата - то есть, получения информации, необходимой, чтобы помочь санкционирующему должностному лицу принять обоснованное, базирующееся на риске решение о том, принять ли информационную систему в эксплуатацию или продолжать её эксплуатацию.

Всесторонняя подготовка организаций и инспекторов - важный аспект проведения эффективных оценок мер обеспечения безопасности и оценок меры обеспечения приватности. Предварительные работы определяют масштаб проблем, касающихся стоимости, календарного планирования и проведения оценки. С организационной точки зрения, подготовка к оценке мер обеспечения безопасности или приватности включает следующие ключевые работы:

- Обеспечение того, что соответствующие политики, охватывающие оценки мер обеспечения безопасности и приватности, соответственно, в наличии и понимаемы всеми элементами организации, на которые влияют;
- Обеспечение того, что все шаги RMF[22] до шага оценки мер обеспечения безопасности или приватности, были успешно завершены и получили соответствующий управленческий надзор;[23]
- Установление цели и области оценок (то есть, назначения оценок и того, что будет оцениваться);

[22] Несмотря на то, что RMF могут быть использованы для мер приватности (см. Специальную Публикацию 800-53, Приложение J), *выбор* мер приватности производится независимо от категорий безопасности информационных систем организации.

[23] Проведение оценки мер безопасности параллельно с фазами разработки/приобретения и реализации жизненного цикла позволяет раньше определить слабые места и недостатки и обеспечить самый рентабельный метод для начала корректирующих действий. Проблемы, найденные во время этих оценок, могут быть переданы санкционирующим должностным лицам для более раннего решения, если требуется. Результаты оценок мер безопасности, выполненных во время разработки и реализации систем, могут также использоваться (в соответствии с критериями повторного использования) во время процесса санкционирования безопасности, чтобы избежать задержек принятия систем или дорогостоящего повторения оценок.

- Обеспечение того, что меры обеспечения безопасности и приватности, определённые как общие меры безопасности (и общая часть гибридных мер обеспечения), были распределены соответствующим сущностям организации (то есть, поставщикам общих мер безопасности) для разработки и реализации;[24]
- Уведомление ключевых должностных лиц организации о предстоящих оценках и необходимости выделения ресурсов для выполнения оценок;
- Установление соответствующих каналов связи среди должностных лиц организации, заинтересованных в оценках;[25]
- Установление временных рамок для завершения оценок и ключевых вех моментов принятия решений, требуемых организации для эффективного управления оценками;
- Определение и выбор компетентных оценщиков/ команд оценщиков, которые будут ответственны за проведение оценок, рассмотрение проблемы независимости оценщиков;
- Сбор объектов для обеспечения оценщиков/команд оценщиков (таких, как политики, процедуры, планы, спецификации, проекты, записи, руководства администратора/оператора, документация по информационной системе, соглашения о взаимодействии, результаты предыдущих оценок, требования законов); и
- Установление механизма обмена между организацией и оценщиками и/или командой оценки, для минимизации неоднозначностей или недоразумений по реализации мер обеспечения безопасности или приватности и слабым местам/недостаткам мер обеспечения безопасности/ приватности, установленным во время оценок.

Оценщики/команды оценки мер обеспечения безопасности и приватности начинают готовиться к соответствующим оценкам посредством:

- Получения общего понимания деятельности организации (включая предназначение, функции и процессы деятельности) и того, как информационная система, которая является субъектом конкретной оценки, поддерживает эту деятельность организации;
- Получения понимания структуры информационной системы (то есть, архитектуры системы) и оцениваемых мер обеспечения безопасности или приватности (включая специфичные для системы, гибридные и общие меры безопасности);
- Определения сущностей организации, ответственных за разработку и реализацию общих мер обеспечения безопасности (или общей части гибридных мер), поддерживающих информационную систему;
- Встречи с соответствующими должностными лицами организации, чтобы гарантировать взаимопонимание целей оценки и предложенной строгости и области оценки;
- Получения объектов, необходимых для оценки (таких, как политики, процедуры, планы, спецификации, проекты, записи, руководства администратора и оператора, документация по информационной системе, соглашения о взаимодействии, результаты предыдущих оценок);

[24] Оценки мер безопасности и оценки мер приватности включают общие меры безопасности, которые являются ответственностью сущностей организации других, чем владелец информационной системы, наследующей меры обеспечения или гибридные меры обеспечения, где есть общая ответственность владельца системы (или программы) и назначенных сущностей организации.

[25] В зависимости от того оцениваются ли меры безопасности или меры приватности, эти люди, как правило, включают санкционирующих должностных лиц, владельцев информационной системы (или программы), поставщиков общих мер безопасности, владельцев предназначения/деятельности, владельцев/управляющих информацией, директоров по информации, высших сотрудников по информационной безопасности, высших должностных лиц агентства по приватности/директоров по приватности, персонал по приватности, Генеральных инспекторов, сотрудников безопасности информационной системы, пользователей организаций, которые поддерживает информационная система и оценщиков.

- Установления подходящих точек контакта в организации, требуемых, чтобы выполнить оценки;
- Получения результатов предыдущих оценок, которые могут быть соответственно снова использованы для текущей оценки (например, отчёты Генерального инспектора, аудиты, результаты сканирования уязвимостей, проверки физической безопасности, предшествующие оценки безопасности или приватности, проверки и оценки разработки, действия поставщика по устранению недостатков, оценки по ISO/IEC 15408 [Общие Критерии]); и
- Разработки планов оценки безопасности и приватности, которые могут быть интегрированы в единый план или разработаны отдельно.

При подготовке к оценке мер обеспечения безопасности или приватности собирается и делается доступной для оценщиков или команды оценки необходимая вводная информация.[26] До степени, необходимой чтобы поддержать конкретную оценку, и в зависимости от оцениваемых мер обеспечения безопасности или мер обеспечения приватности, организация определяет и предоставляет доступ к: (i) элементам организации, ответственным за разработку, документирование, распространение, рассмотрение и обновление всех политик обеспечения безопасности или приватности и связанных процедур по реализации совместимых с политикой мер; (ii) политикам обеспечения безопасности или приватности для информационной системы и любых связанных процедур по их реализации; (iii) людям или группам, ответственным за разработку, реализацию, эксплуатацию и поддержку мер обеспечения безопасности или приватности; (iv) любым материалам (таким, как планы обеспечения безопасности или приватности, записи, календарные планы, доклады об оценке, отчёты по результатам выполнения работ, соглашения, пакеты санкционирования), связанным с реализацией и применением мер обеспечения безопасности или приватности, которые будут оцениваться; и (v) конкретным объектам, которые будут оцениваться.[27] Доступность необходимой документации, а так же доступ к ключевому персоналу организации и оцениваемой информационной системе является определяющим для успешной оценки.

При выборе оценщиков по мерам обеспечения безопасности или приватности организации учитывают требуемые *техническую компетентность* и уровень *независимости*. Организации гарантируют, что оценщики обладают требуемыми навыками и технической компетентностью для успешного выполнения оценки специфичных для системы, гибридных и общих мер.[28] Это включает знание и опыт по конкретным аппаратным средствам, программному обеспечению и компонентам встроенного микропрограммного обеспечения, используемым организацией. Независимый оценщик - любой человек, способный к проведению беспристрастной оценки мер обеспечения безопасности и приватности, используемых в или наследуемых информационной системой. Беспристрастность подразумевает, что оценщики по мерам безопасности и оценщики по мерам приватности лишены любых возможных или фактических конфликтов интересов относительно разработки, эксплуатации и/или управления информационной системой или определения эффективности мер обеспечения безопасности или приватности.[29] Санкционирующее должностное лицо или уполномоченный представитель определяет требуемый уровень независимости для оценщиков, основываясь на результатах процесса категорирования безопасности информационной системы (в случае оценки мер безопасности) и риска для деятельности и активов организации, людей, других организаций и Нации. Санкционирующее должностное лицо определяет, достаточен ли уровень независимости оценщика, чтобы обеспечить уверенность, что приведенные

[26] Владельцы информационных систем (или программ) и сущности организации разрабатывающие, реализующие и/или администрирующие общие меры безопасности (то есть, поставщики общих мер безопасности) ответственны за предоставление оценщикам необходимой информации.

[27] В ситуациях, когда в организации имеется несколько ведущихся или планируемых оценок безопасности или приватности, организация централизованно управляет доступом к элементам, людям и объектам организации, поддерживающим оценки, чтобы гарантировать, рентабельное использование времени и ресурсов.

[28] Структура национальных сил кибербезопасности предоставляет информацию о наборах навыков и технической компетентности, необходимой оценщикам по мерам обеспечения безопасности или приватности. См. www.niccs.us-cert.gov/training/tc/framework.

[29] Контрактная услуга оценки считается независимой, если владелец информационной системы (или программы) не включён непосредственно в процесс заключения контракта или не может незаконно влиять на независимость оценщика (ов), проводящего оценку мер обеспечения приватности или безопасности.

результаты оценки правильны и могут использоваться, чтобы принять основанное на риске решение о том, принять ли информационную систему в эксплуатацию или продолжить её эксплуатацию.

Независимые услуги по оценке мер обеспечения безопасности и приватности могут быть получены от других элементов в организации или могут быть законтрактованы от сущностей государственного или частного сектора вне организации. В специальных ситуациях, например, когда организация, которой принадлежит информационная система, является небольшой или структура организации требует, чтобы оценки мер обеспечения безопасности или приватности были выполнены людьми, связанными с владельцем системы, которые участвуют в разработке, эксплуатации и/или управлении, независимость в процессе оценки может быть достигнута, при гарантии, что результаты оценки тщательно рассмотрены и проанализированы независимой командой оценщиков, чтобы проверить законченность, согласованность и достоверность результатов.[30]

3.2 РАЗРАБОТКА ПЛАНОВ ОЦЕНКИ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

План оценки безопасности и *план оценки приватности* определяют цели для оценки мер обеспечения безопасности и приватности, соответственно, и подробный путеводитель того, как провести такие оценки. Эти планы могут разрабатываться как один интегрированный план или как различные планы, в зависимости от потребностей организации. Следующие шаги рассматриваются оценщиками при разработке планов оценки мер обеспечения безопасность или приватности в информационных системах организации или наследуемых этими системами:

- Определите, какие меры обеспечения безопасности и приватности/улучшения мер обеспечения должны быть включены в оценки, основываясь на содержании плана обеспечения безопасности и плана обеспечения приватности и назначения и области оценок;
- Выберите соответствующие процедуры оценки, которые будут использоваться во время оценок, основываясь на мерах обеспечения безопасности или приватности и улучшениях мер, которые будут включены в оценки;
- Адаптируйте выбранные процедуры оценки (например, выберите соответствующие методы и объекты оценки, назначьте значения атрибутов глубины и покрытия);
- Разработайте дополнительные процедуры оценки, чтобы учесть любые требования безопасности или требования приватность или меры обеспечения, которые не достаточно закрыты Специальной публикацией 800-53;
- Оптимизируйте процедуры оценки, чтобы уменьшить дублирование усилий (например, упорядочивая и консолидируя процедуры оценки) и обеспечить рентабельные решения по оценке; и
- Оформите планы оценки и получите необходимое санкционирование для выполнения планов.

3.2.1 Определение, какие меры обеспечения безопасности или приватности должны быть оценены.

План обеспечения безопасности и план обеспечения приватности представляют краткий обзор требований безопасности и приватности, соответственно, для информационной системы и организации и описывают существующие или планируемые меры безопасности и меры приватности для удовлетворения этим требованиям. Оценщик начинает с мер обеспечения безопасности или приватности, описанных в планах обеспечения безопасности или приватности, и рассматривает назначение оценки. Оценка мер обеспечения безопасности или приватности может быть *полной* оценкой всех мер информационной системы или наследуемых системой (например, во время процесса первичного санкционирования безопасности или приватности) или *частичной* оценкой мер информационной системы или

[30] Санкционирующее должностное лицо консультируется с Министерством Генерального инспектора, высшим сотрудником по информационной безопасности, высшим должностным лицом агентства по приватности/директором по приватности и директором по информации, соответственно, чтобы обсудить последствия любых решений о независимости оценщика в описанных выше типах особых обстоятельств.

наследуемых системой (например, во время разработки системы, как часть целевой оценки вытекающей из изменений, влияющих на конкретные меры обеспечения, или когда меры обеспечения были ранее оценены и результаты приняты в процессе взаимности).

При конкретных оценках владельцы информационной системы и поставщики общих мер безопасности сотрудничают с должностными лицами организации, имеющими интерес в оценке (например, высшими сотрудниками по информационной безопасности, высшими должностными лицами агентства по приватности/ директорами по приватности, владельцами предназначения/информации, Генеральными инспекторами и санкционирующими должностным лицами) чтобы определить, какие меры обеспечения безопасности или приватности должны быть оценены. Определение мер, которые будут оценены, зависит от назначения оценки. Например, во время начальных фаз жизненного цикла разработки систем, конкретные меры, могут быть выбраны для оценки, чтобы способствовать раннему обнаружению недостатков и дефектов и более рентабельному подходу по уменьшению риска. После того, как первичное санкционирование для эксплуатации предоставлено, возможно, должны быть проведены целевые оценки, когда произведены изменения в системе, конкретных мерах обеспечения безопасности или приватности или в среде эксплуатации. В таких случаях фокус для оценки находится на мерах обеспечения безопасности или приватности, на которые, возможно, влияло изменение.

3.2.2 Выбор процедур оценки мер обеспечения безопасности или приватности.

Специальная публикация 800-53A предоставляет процедуры оценки по каждой мере обеспечения безопасности и приватности и улучшению меры обеспечения в Специальной публикации 800-53. По каждой мере обеспечения безопасности или приватности в плане обеспечения безопасности и приватности, спланированной для включения в оценку, оценщики выбирают соответствующую процедуру оценки из Приложения F (процедуры оценки безопасности) или Приложения J (процедуры оценки приватности). Выбранные процедуры оценки могут изменяться от оценки к оценке, основываясь на текущем контенте планов обеспечения безопасности и планов обеспечения приватности и назначения оценки (например, полная оценка, частичная оценка).

3.2.3 Адаптация процедур оценки.

Подобно тому, как меры безопасности и приватности из Специальной Публикации 800-53 адаптируются для предназначения организации, функций деятельности, характеристик информационной системы и среды эксплуатации, организации адаптируют процедуры оценки, перечисленные в Приложениях F и J, чтобы удовлетворить конкретные потребности организации. У организаций есть гибкость, чтобы выполнить процесс адаптации для всех информационных систем на уровне организации, на уровне отдельной информационной системы или используя комбинацию подходов на уровне организации и системы. Оценщики мер безопасности и оценщики мер приватности определяют, должна ли организация обеспечить дополнительное руководство по адаптации до начала процесса адаптации. Процедуры оценки адаптируются посредством:

- Выбора соответствующих методов и объектов оценки, необходимых для удовлетворения заявленной цели оценки;
- Выбора соответствующих значений атрибутов глубины и покрытия, чтобы определить строгость и область оценки;
- Определения общих мер безопасности, которые были оценены в соответствии с отдельно задокументированными планом оценки безопасности или планом оценки приватности, и не требуют повторного выполнения процедур оценки;
- Разработки процедур оценки, специфичных для информационной системы/платформы и для организации (которые могут быть адаптированы к процедурам в Приложениях F и J);
- Включения результатов из предыдущих оценок, результаты которых считаются применимыми; и

- Внесения соответствующих корректировок в процедуры оценки, чтобы быть в состоянии получить необходимые свидетельства оценки от внешних поставщиков.

Рассмотрения, связанные с методом и объектом оценки -

Очевидно, что организации могут специфицировать, документировать и конфигурировать свои информационные системы различными путями, и что контент и применимость существующих свидетельств оценки меняются. Это приводит к потребности применять различные методы оценки к различным объектам оценки, чтобы создать свидетельства оценки необходимые, чтобы определить, эффективны ли меры обеспечения безопасности или приватности в их приложении. Поэтому, методы и объекты оценки, представленные с каждой процедурой оценки, называют *потенциальными*, чтобы отразить необходимость выбирать методы и объекты, самые подходящие для конкретной оценки. Методы и объекты оценки, выбранные в качестве тех, которые считаются необходимыми для получения свидетельства, должны иметь определения, представленные в описаниях решений. Потенциальные методы и объекты в процедуре оценки предоставляются как ресурс, который помогает в выборе соответствующих методов и объектов, а не с намерением ограничить выбор. Организации используют своё суждение в выборе из потенциальных методов оценки и списка объектов оценки, связанных с каждым выбранным методом. Организации выбирают те методы и объекты, которые наиболее рентабельно способствуют созданию решений, связанных с целью оценки.[31] Мера качества результатов оценки основана на разумности обоснования, предоставляемого если нет конкретного набора применимых методов и объектов. В большинстве случаев нет необходимости применять каждый метод оценки к каждому объекту оценки, чтобы получить требуемые результаты оценки. А для некоторых оценок, может быть соответствующим, чтобы использовать метод не указанный в данный момент в наборе потенциальных методов.

Рассмотрения, связанные с глубиной и покрытием -

В дополнение к выбору соответствующих методов и объектов оценки, каждый метод оценки (то есть, исследование, опрос и испытание) связан с атрибутами глубины и покрытия, которые описаны в Приложении D. Значения атрибутов определяют строгость и область процедур оценки, выполняемых инспектором. Значения, выбираемые организацией, основываются на характеристиках оцениваемой информационной системы (включая требования доверия) и конкретных решениях, которые принимаются. Значения атрибутов глубины и покрытия связаны с требованиями доверия, определёнными организацией (то есть, строгость и область оценки увеличиваются в непосредственной связи с требованиями доверия). Для мер безопасности, контрольные списки SCAP обеспечивают основанный на профиле механизм, который облегчает адаптацию значений атрибутов и выбор конкретных требований к мерам обеспечения, основанных на необходимом уровне доверия, требуемым для информационной системы. Эти контрольные списки дают возможность настраиваемой, автоматизированной оценки, используя проверенные по SCAP продукты.

Рассмотрения, связанные с общими мерами обеспечения -

Оценщики отмечают, какие меры обеспечения безопасности или приватности (или части таких мер) в планах обеспечения безопасности или планах обеспечения приватности определяются как *общие меры.*[32] Так как оценка общих мер является ответственностью сущности организации, которая разрабатывает и реализует меры (то есть, поставщиков общих мер безопасности), процедуры оценки в Приложениях F и J, используемые для оценки этих мер, включают результаты оценки от этой сущности

[31] Выбор методов и объектов оценки (включая количество и тип объектов оценки) может быть значимым фактором в рентабельном достижении целей оценки.

[32] Общие меры поддерживают несколько информационных систем в организации, и меры защиты, предоставляемые этими мерами, наследуются отдельными системами. Поэтому, организация определяет соответствующий набор общих мер, чтобы гарантировать, что и строгость мер обеспечения (то есть, возможности безопасности) и уровень тщательности и интенсивности оценок мер обеспечения соразмерны с критичностью и/или чувствительностью отдельных информационных систем, унаследовавших эти меры обеспечения. Слабые места или недостатки в общих мерах имеют потенциал, чтобы оказать негативное влияние на значительные части организации и, таким образом, требуют существенного внимания.

организации. Общие меры, могут быть оценены ранее, как часть программы обеспечения информационной безопасности организации или программы обеспечения приватности или как часть информационной системы, обеспечивающей общие меры, наследуемые другими системами организации. Также могут быть отдельные планы оценки общих мер. В любой ситуации, владельцы информационной системы координируют оценку общих мер с соответствующими должностными лицами организации (такими, как Директор по информации, высший сотрудник по информационной безопасности, высшее должностное лицо агентства по приватности/директор по приватности, владельцы предназначения/ информации, санкционирующие должностные лица), получающими результаты оценок общих мер или, если общие меры не были оценены или требуют переоценки, делая необходимые приготовления, чтобы включить или сослаться на результаты оценки общих мер в текущей оценке.[33]

Другое рассмотрение в оценке общих мер обеспечения состоит в том, что иногда есть специфичные для системы аспекты общих мер, которые не закрываются сущностями организации, ответственными за общие аспекты мер обеспечения. Эти типы мер обеспечения упоминаются как *гибридные меры обеспечения*. Например, CP-2, мера безопасности планирования на случай непредвиденных ситуаций, может рассматриваться как гибридная мера для организации, если есть план действий в непредвиденных ситуациях, разработанный организацией для всех информационных систем организации. Развивая начальный план действий в непредвиденных ситуациях, владельцы информационной системы, как ожидается, скорректируют или адаптируют план действий в непредвиденных ситуациях по мере необходимости, когда появятся конкретные аспекты плана, которые должны быть определены для конкретной системы, где мера обеспечения используется. Для каждой гибридной меры обеспечения оценщики включают в планы оценки безопасности или планы оценки приватности части процедур оценки из Приложений F или J, связанные с частями мер обеспечения, которые специфичны для системы, чтобы гарантировать, что, наряду с результатами оценок общих мер, оценены все аспекты мер обеспечения.

Рассмотрения, связанные с системой/платформой и с организацией -

Процедуры оценки в Специальной публикации 800-53A могут быть адаптированы, чтобы учесть зависимости, специфичные для системы и платформы или специфичные для организации. Например, оценка реализации в UNIX меры обеспечения IA-2 по идентификации и аутентификации пользователей может включать явное исследование файла *.rhosts* для систем UNIX, так как неуместные записи в этом файле могут иметь результат в обходе пользовательской аутентификации. Результаты предыдущих испытаний могут быть также применены к текущей оценке, если методы этих испытаний обеспечивают высокую степень прозрачности (например, что было протестировано, когда было протестировано, как было протестированное). Протоколы тестирования, основанные на стандартах, таких как SCAP, являются примером того, как организации могут помочь достичь этого уровня прозрачности. SCAP обеспечивает прозрачность через использование стандартизированного контента, который определяет методы тестирования, и через стандартизированные результаты, которые указывают на то, какой контент использовался, какое состояние системы было протестировано, какое состояние было создано, какой инструмент использовался, чтобы выполнить тестирование и когда тестирование было выполнено.

Рассмотрения, связанные с повторным использованием свидетельств оценки -

Повторное использование результатов оценки ранее принятых или одобренных оценок состоит в рассмотрении массива свидетельств для того, чтобы определить общую эффективность мер безопасности или приватности. Ранее принятые или одобренные оценки включают: (i) оценки тех общих мер, которыми управляет организация и которые поддерживают многие информационные системы; (ii) оценки мер обеспечения безопасности или приватности, которые рассматриваются как часть реализации мер

[33] Если результаты оценки общих мер безопасности в настоящий момент не доступны, планы оценки оцениваемых информационных систем, которые зависят от этих мер, должны быть соответственно помечены. Оценки нельзя считать полными, пока результаты оценки общих мер безопасности не сделаны доступными для владельцев информационных систем.

обеспечения (например, CP-2 требует рассмотрения плана действий в непредвиденных ситуациях); или (iii) информацию, связанную с безопасностью, генерируемую по программе Непрерывного мониторинга информационной безопасности организации. Приемлемость использования предыдущих результатов оценки в оценке мер безопасности или оценке мер приватности координируется с и одобряется пользователями результатов оценки. Важно, чтобы владельцы информационной системы и поставщики общих мер безопасности сотрудничали с санкционирующими должностными лицами и другими соответствующими должностными лицами организации в определении приемлемости использования результатов предыдущих оценок. Рассматривая повторное использование результатов предыдущих оценок и значение этих результатов для текущей оценки, оценщики определяют: (i) достоверность свидетельств оценки; (ii) уместность предыдущего анализа; и (iii) применимость свидетельств оценки к текущим режимам эксплуатации информационной системы. Если результаты предыдущих оценок будут использованы, то дата исходной оценки и тип оценки документируются в плане оценки безопасности или плане оценки приватности и в отчёте об оценке безопасности или отчёте об оценке приватности. Когда применимо, стандартизированные результаты оценки безопасности, обеспечиваемые инструментами SCAP, могут быть снова использованы многими сторонами.

В определённых ситуациях может быть необходимо пополнить результаты предыдущих оценок при рассмотрении для повторного использования дополнительными работами по оценке, чтобы полностью учесть цели оценки. Например, если при независимой оценке продукта информационной технологии не тестировалась определённая конфигурация, настройки которой используются организацией в информационной системе, тогда оценщик, возможно, должен добавить результаты исходных испытаний дополнительным тестированием, чтобы закрыть эти настройки конфигурации для текущей среды информационной системы. Решение по повторному использованию результатов оценки документируется в плане оценки безопасности или плане оценки приватности и в заключительном отчёте об оценке безопасности или отчёте об оценке приватности, и в соответствии с федеральным законодательством, политиками, директивами, стандартами и руководствами.

Следующие элементы рассматриваются при проверке допустимости результатов предыдущих оценок для повторного использования:

- **Изменение с течением времени условий, связанных с мерами безопасности и мерами приватности.**

Меры обеспечения безопасности и приватности, которые считались эффективными во время предыдущих оценок, возможно, могут стать не эффективными в связи с изменением условий в информационной системе или среде её эксплуатации, включая информацию о появлении угроз. Результаты оценок, которые считались ранее приемлемыми, больше, возможно, не являются достоверными свидетельствами для определения эффективности мер обеспечения безопасности или приватности и, поэтому, будет требоваться переоценка. Применение предыдущих результатов оценок к текущей оценке требует выявления любых изменений, которые произошли, начиная с предыдущей оценки, и воздействия этих изменений на предыдущие результаты. Например, многократное использование результатов предыдущих оценок исследования политик и процедур организации по безопасности или приватности, может быть приемлемо, если определено, что не было любых существенных изменений в указанных политиках и процедурах. Многократное использование результатов оценок, приведенных во время предыдущего санкционирования информационной системы, является рентабельным методом для поддержания работ непрерывного мониторинга и требований к ежегодной отчётности по FISMA, когда связанные меры не изменились и есть адекватные причины для уверенности в их продолжительном применении.

- **Количество времени, которое прошло с предыдущих оценок.**

Вообще, по мере увеличения периода времени между текущими и предыдущими оценками, достоверность и полезность результатов предыдущих оценок уменьшается. Прежде всего, это следствие того, что информационная система или среда, в которой работает информационная система, с большей

вероятностью изменятся с течением времени, возможно снижая состоятельность исходных условий или предположений, на которых базировалась предыдущая оценка.

- **Степень независимости предыдущих оценок.**

Независимость оценщика может быть критическим фактором в определённых типах оценок. Степень независимости, требуемая от оценки к оценке, должна быть непротиворечивой. Например, являются не соответствующими повторному использованию результаты предыдущей самооценки, где не требовалась независимость оценщика, в текущей оценке, требующей большей степени независимости.

Рассмотрения, связанные с внешними информационными системами -

Процедуры оценки в Приложениях F и J должны быть скорректированы соответствующим образом, чтобы учесть оценку внешних информационных систем.[34] Поскольку организации не всегда имеют прямое управление мерами обеспечения безопасности или приватности, используемыми во внешних информационных системах, или достаточную обозримость разработки, реализации и оценки этих мер, возможно должны быть применены альтернативные подходы оценки, приводящие к необходимости адаптировать процедуры оценки, описанные в Приложениях F и J. Где требуется доверие к согласованности мер обеспечения безопасности или приватности в информационной системе или наследуемых системой, задокументированных в контрактах или соглашениях об уровне обслуживания, оценщики рассматривают эти контракты или соглашения и, где необходимо, адаптируют процедуры оценки, чтобы оценить меры обеспечения безопасности или приватности или результаты оценки мер безопасности или оценки мер приватности, представленные в этих соглашениях. Кроме того, оценщики принимают во внимание любые другие оценки, которые были проведены или находятся в процессе проведения для внешних информационных систем, на которые полагаются в части защиты оцениваемой информационной системы. Применимая информация от этих оценок, если считается достоверной, включается в отчёт об оценке безопасности или отчёт об оценке приватности соответственно.

3.2.4 Разработка процедур оценки по специфичным для организации мерам обеспечения.

Основываясь на политиках организации, предназначении или функциональных требованиях к деятельности и на оценке риска, организации могут хотеть разработать и реализовать дополнительные (специфичные для организации) меры обеспечения безопасности или приватности или улучшения мер обеспечения для их информационных систем, которые выходят за рамки Специальной публикации 800-53. Такие меры обеспечения документируются в план обеспечения безопасности или план обеспечения приватности как меры обеспечения, не найденные в Специальной публикации 800-53. Чтобы оценить меры обеспечения безопасности или приватности в этой ситуации, оценщики используют руководства в Главе Два, чтобы разработать процедуры оценки по этим мерам обеспечения и улучшениям мер обеспечения. Разработанные процедуры оценки впоследствии интегрируются в план оценки безопасности или план оценки приватности соответственно.

3.2.5 Оптимизация выбранных процедур оценки, чтобы гарантировать максимальную производительность.

У оценщиков есть большая гибкость в организации планов оценки, которые удовлетворяют потребностям организация и которые обеспечивают лучшую возможность для получения ей необходимых свидетельств, чтобы определить эффективность мер обеспечения безопасности или приватности, уменьшая полную стоимость оценки. Объединение и консолидация процедур оценки являются одной из областей, где эта гибкость может быть применена. Во время оценки информационной системы методы оценки

[34] *Внешняя информационная система* - информационная система или компонент информационной системы, которая находится за пределами границы санкционирования, установленной организацией, и для которой у организации, как правило, нет прямого управления приложением требуемых мер обеспечения безопасности и приватности или оценкой эффективности мер обеспечения безопасности и приватности. Специальные публикации 800-37 и 800-53 обеспечивают дополнительное разъяснение по внешним информационным системам и эффекту использования мер безопасности в этих типах сред.

применяются много раз к различным объектам оценки в пределах определённого семейства мер обеспечения безопасности или приватности. Чтобы сэкономить время, уменьшить стоимость оценки и максимизировать полноценность результатов оценки, оценщики рассматривают выбранные процедуры оценки для семейств мер обеспечения безопасности или приватности и комбинируют или консолидируют процедуры (или части процедур) когда это возможно или практично. Например, оценщики могут консолидировать опросы ключевых должностных лиц организации, имеющими дело с различными темами, связанными с безопасности или приватностью. Оценщики имеют другие возможности для существенной консолидации и снижения издержек путём исследования всех политик и процедур из семейств мер безопасности и мер приватности одновременно или организовывая группы связанных политик и процедур, которые могли бы быть исследованы как объединённая сущность. Получение и исследование установок конфигурации для подобных аппаратных и программных компонентов в информационной системе является другим примером, который может обеспечить существенную действенность оценки.

Дополнительной областью для рассмотрения при оптимизации процесса оценки является последовательность, в которой оцениваются меры обеспечения безопасности или приватности. Оценка некоторых мер безопасности и мер приватности перед другими может обеспечить полезную информацию, которая облегчает понимание и более эффективные оценки других мер. Например, меры безопасности, такие как CM-2 (Базовая конфигурация), CM-8 (Реестр компонентов информационной системы), PL-2 (План обеспечения безопасности системы), RA-2 (Категорирование безопасности) и RA-3 (Оценка степени риска) дают общее описание информационной системы. Оценка этих мер безопасности в начале процесса оценки может обеспечить базовое понимание информационной системы, которое может помочь в оценке других мер безопасности. Дополнительное руководство для многих мер безопасности и мер приватности также определяет связанные меры, которые могут обеспечить полезную информацию в организации процедур оценки. Например, AC-19 (Контроль доступа для портативных и мобильных устройств) перечисляет меры безопасности MP-4 (Хранение носителей информации) и MP55 (Транспортировка носителей информации) как связанные с AC-19. Так как AC-19 связана с MP-4 и MP-5, то последовательность, в которой проводятся оценки для AC-19, MP-4 и MP-55 может облегчить повторное использование информации оценки одной меры при оценке других связанных мер.

3.2.6 Завершение плана оценки и получение санкционирования выполнить план.

После выбора процедур оценки (включая разработку необходимых процедур, не содержащихся в каталоге процедур Специальной публикации 800-53A), адаптации процедур для условий, специфичных для информационной системы/платформы и специфичных для организации, оптимизации процедур для эффективности, и учёта потенциала неожиданных событий, воздействующих на оценку, план оценки считается завершённым и календарный план установленным, включая ключевые вехи для процесса оценки. Когда план оценки безопасности или план оценки приватности завершён, план рассматривается и одобряется соответствующим должностным лицом организации,[35] чтобы гарантировать, что план: (i) полный; (ii) непротиворечивый с целями безопасности или приватности организации соответственно и оценкой риска для организации; и (iii) рентабельный относительно ресурсов, выделенных для оценки.

3.3 ПРОВЕДЕНИЕ ОЦЕНОК МЕР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

После одобрения организацией плана оценки безопасности или плана оценки приватности, оценщик (и) или команда оценки выполняют план в соответствии с принятым календарным планом. Определение размера и организационной структуры команды оценки (то есть, набора навыков, технической компетентности и опыта оценки людей, составляющих команду) является частью решений управления

[35] Организации устанавливают процесс одобрения плана оценки безопасности и приватности с конкретными должностными лицами организации (например, владельцы информационных систем, поставщики общих мер безопасности, сотрудники безопасности информационной системы, высшие сотрудники по информационной безопасности, высшие должностные лица агентства по приватности/директора по приватности, санкционирующие должностные лица), обозначаемыми как одобряющие органы.

рисками принимаемых организацией, требующей и инициирующей оценку. Результаты оценок мер безопасности и оценок мер приватности документируются в *отчёты по оценке безопасности* и *отчёты по оценке приватности* соответственно, которые являются ключевыми источниками к пакету санкционирования, разрабатываемому владельцами информационной системы и поставщиками общих мер безопасности для санкционирующих должностных лиц.[36] Отчёты по оценке безопасности и отчёты по оценке приватности включают информацию от оценщиков (в форме результатов об оценке) необходимую, чтобы определить эффективность мер обеспечения безопасности или приватности, используемых в или наследуемых информационной системой. Эти отчёты об оценке - важный фактор в определении риска санкционирующим должностным лицом. Организации могут разработать *сводку* оценки из детальных результатов, которые получены оценщиками во время оценок мер безопасности и оценок мер приватности. Сводка оценки может предоставить санкционирующему должностному лицу сокращённую версию доклада об оценке, сосредоточенную на основных моментах оценки, резюме ключевых результатов и рекомендациях по учёту слабых мест и недостатков в оценённых мерах обеспечения безопасности или приватности. Приложение G предоставляет информацию о рекомендуемом контенте отчётов об оценке.

Цели оценки достигаются путём применения определяемых методов оценки к выбранным объектам оценки и компиляцией/получением свидетельств необходимых для принятия решения, связанного с каждой целью оценки. Каждое описание решения, содержащееся в процедуре оценки, выполняемой оценщиком, даёт один из следующих результатов: (i) *удовлетворяет (S)*; или (ii) *другое, чем удовлетворяет (O)*. Результат «удовлетворяет» указывает, что для части меры обеспечения безопасности или приватности, учитываемой описанием решения, полученная информация оценки (то есть, собранные доказательства) указывает, что цель оценки для меры была достигнута, приводя к полностью приемлемому результату. Результат «другое, чем удовлетворяет» указывает, что для части меры обеспечения безопасности или приватности, учитываемой описанием решения, полученная информация оценки указывает на потенциальные аномалии в применении или реализации мер, которые должны быть учтены организацией. Результат «другое, чем удовлетворяет» может также указывать, что по причинам, определённым в отчёте об оценке, оценщик был не в состоянии получить достаточную информацию, чтобы принять конкретное решение, требующееся в описании решения. Для результатов оценки, которые являются *другое, чем удовлетворяет*, организации могут определять *подкатегории* результатов, указывающих на серьёзность и/или критичность слабых мест или обнаруженных недостатков и потенциальные отрицательные воздействия на деятельность организации (то есть, предназначение, функции, имидж или репутацию), активы организации, людей, другие организации и Нацию. Определение таких подкатегорий может помочь установить приоритеты для необходимых действий по уменьшению риска.

Результатом работы оценщика является объективная, основанная на фактах фиксация того, что было найдено относительно оценённых мер обеспечения безопасности или приватности. Для каждого результата другого, чем удовлетворяет оценщики указывают, на какие части мер обеспечения безопасности или приватности влияет результат (то есть, аспекты мер, которые считаются не удовлетворительными или не смогли быть оценены) и описывают, как мера отличается от планируемого или ожидаемого состояния. Потенциал для компрометации конфиденциальности, целостности и доступности, вследствие результатов *других, чем удовлетворяет*, также отмечается оценщиком в докладе по оценке безопасности или приватности. Эти замечания отражают недостатки указанной защиты и последствия, которые могли произойти в результате (то есть, рабочая станция, набор данных, доступ корневого уровня). Работы по определению и принятию риска проводятся при постоценке организации, как часть стратегии управления рисками, установленной организацией. В эти работы по управлению рисками вовлекается высшее руководство организации, включая, например, руководителей агентств, владельцев предназначения/деятельности, владельцев/управляющих информацией, ответственных за риски (функция) и санкциони-

[36] В соответствии со Специальной публикацией 800-37, пакет санкционирования безопасности состоит из плана обеспечения безопасности, отчёта по оценке безопасности и плана действий и вех (POAM).

рующих должностных лиц, после консультаций с соответствующим техническим персоналом организации (например, высшими сотрудниками по информационной безопасности, высшими должностными лицами агентства по приватности/директорами по приватности, директорами по информации, владельцами информационной системы, поставщиками общих мер безопасности и оценщиками). Результаты оценки мер обеспечения безопасности и приватности документируются с уровнем детализации, подходящим для оценки в соответствии с форматом создания отчётов, предписанным политикой организации, руководствами NIST и политикой OMB. Формат создания отчётов соответствует типу проведенной оценки (например, самооценка владельцами информационной системы и поставщиками общих мер безопасности, независимая проверка и подтверждение соответствия, независимые оценки, поддерживающие процесс санкционирования, автоматизированные оценки или независимые аудиты или проверки).

Владельцы информационной системы и поставщики общих мер безопасности полагаются на квалификацию и техническое мнение оценщиков по: (i) оценке мер обеспечения безопасности и приватности в информационной системе и наследуемых системой; и (ii) предоставлению рекомендаций по тому, как исправить слабые места или недостатки в мерах и уменьшить или устранить выявленные уязвимости. Результаты оценки, представляемые оценщиком (то есть, результаты *удовлетворяет* или *другое, чем удовлетворяет*, определение частей мер обеспечения безопасности или приватности, которые приводят к не удовлетворительному результату и описание результирующего потенциала для компрометации информационной системы или среды её эксплуатации), предоставляются владельцам информационной системы и поставщикам общих мер безопасности в начальных отчётах об оценке безопасности и отчётах об оценке приватности. Владельцы систем и поставщики общих мер безопасности могут реагировать на представленные рекомендации оценщика прежде, чем отчёты об оценке будут завершены, если есть конкретные возможности исправить слабые места или недостатки в мерах обеспечения безопасности или приватности или исправить и/или разъяснить недоразумения или интерпретации результатов оценки.[37] Меры обеспечения безопасности или приватности, которые изменяются, улучшаются или добавляются во время этого процесса, переоцениваются оценщиком до выдачи заключительных отчётов об оценке.

3.4 АНАЛИЗ РЕЗУЛЬТАТОВ ОТЧЁТА ОБ ОЦЕНКЕ

Результаты оценок мер безопасности и оценок мер приватности в конечном счёте влияют на реализацию мер обеспечения, контент планов обеспечения безопасности и планов обеспечения приватности и соответствующего плана действий и вех. Соответственно, владельцы информационной системы и поставщики общих мер безопасности, рассматривая отчёты об оценке безопасности и отчёты об оценке приватности и обновлённую оценку степени риска параллельно с назначенными должностными лицами организации (такими, как, санкционирующие должностные лица, директора по информации, высшие сотрудники по информационной безопасности, высшие должностные лица агентства по приватности/директора по приватности, владельцы предназначения/информации) решают, какие соответствующие шаги требуются в ответ на слабые места и недостатки, выявленные во время оценки. Путём использования меток *удовлетворяет* и *другое, чем удовлетворяет*, формат создания отчётов по результатам оценки предоставляет должностным лицам организации обзор по конкретным слабым местам и недостаткам в мерах обеспечения безопасности или приватности в информационной системе или наследуемых системой и облегчает упорядоченный и структурированный подход к реагированию на риски в соответствии с приоритетами организации. Например, владельцы

[37] Исправление слабых мест или недостатков в мерах обеспечения безопасности или приватности или выполнение рекомендаций во время анализа начальных отчётов об оценке безопасности или отчётов об оценке приватности владельцами информационной системы или поставщиками общих мер безопасности не предназначен, чтобы заменить формальный процесс организации по реагированию на риски, который осуществляется после предоставления итоговых отчётов. Скорее это предоставляет владельцу информационной системы или поставщику общих мер безопасности с возможностью учесть слабые места или недостатки, которые могут быть быстро исправлены. Однако, в ситуациях где существуют ограниченные ресурсы для исправления слабых мест и недостатков, обнаруженных во время оценок мер безопасности или оценок мер приватности, организации могут без ущерба решить, что ожидание оценки степени риска для расположения по приоритетам усилий по устранению является лучшим планом действий.

информационной системы или поставщики общих мер безопасности после консультаций с назначенными должностными лицами организации, могут решить, что некоторые результаты оценки, отмеченные как другое, чем удовлетворяет, имеют незначимую сущность и представляют незначимый риск для организации. Наоборот, владельцы систем или поставщики общих мер безопасности могут решить, что некоторые результаты, отмеченные как другое, чем удовлетворяет, являются существенными, требуя немедленных восстановительных мероприятий. Во всех случаях организация рассматривает каждый результат оценщика другое, чем удовлетворяет и применяет его суждение относительно тяжести или значимости результата и является ли результат достаточно существенным, чтобы быть достойным дальнейшего исследования или корректирующего действия.[38]

Участие высшего руководства в процессе смягчения может быть необходимым, чтобы гарантировать, что ресурсы организации эффективно выделены в соответствии с приоритетами организации, обеспечивая ресурсы сначала для информационных систем, которые поддерживают самые критические и чувствительные предназначения для организации или исправления недостатков, которые имеют самый высокий уровень риска. В конечном счёте, результаты оценки и любые последующие действия по уменьшению (обусловленные обновлённой оценкой степени риска), инициируемые владельцами информационной системы или поставщиками общих мер безопасности в сотрудничестве с назначенными должностными лицами организации, инициируют обновления ключевых документов, используемых санкционирующими должностными лицами для определения статуса безопасности или приватности информационной системы и её пригодности для санкционирования эксплуатации. Эти документы включают планы обеспечения безопасности и планы обеспечения приватности, отчёты об оценке безопасности и отчёты об оценке приватности и соответствующий план действий и вех.

3.5 ОЦЕНКА ВОЗМОЖНОСТЕЙ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

В соответствии со Специальной публикацией NIST 800-53, организации могут определить набор возможностей по безопасности или возможностей по приватности, предваряющих процесс выбора мер безопасности или мер приватности. Концепция *возможности*[39] признаёт, что защита информации, обрабатываемой, хранимой или передаваемой информационными системами, редко ограничивается одной мерой защиты или контрмерой. В большинстве случаев, такая защита следует из выбора и реализации ряда взаимно усиливающих мер безопасности и мер приватности. Каждая мера способствует общей определённой для организации возможности - некоторые меры, потенциально способствуют в большей степени, а другие меры способствуют в меньшей степени. Например, организации хотят определить возможность к *безопасной удалённой аутентификации*. Эта возможность может быть достигнута реализацией ряда мер безопасности из Специальной публикации 800-53, Приложения F (то есть, IA-2 [1], IA-2 [2], IA-2 [8], IA-2 [9], и SC-8 [1]).

Возможности безопасности и приватности могут учитывать много областей, которые могут включать технические средства, физические средства, процедурные средства или любую их комбинацию. Используя концепцию возможности, организации могут получить большую видимость и лучшее понимание: (i) отношений (то есть, зависимостей) среди мер обеспечения; (ii) результатов конкретных отказов мер обеспечения на определённых организацией возможностях; и (iii) потенциальную серьёзность слабых мест или недостатков мер обеспечения. Однако, этот подход может добавить сложность оценкам и требовать анализа отказа первопричины, когда на конкретные возможности влияет отказ определённых мер обеспечения безопасности или приватности, чтобы определить, какая мера или меры способствуют отказу. Чем большее число мер обеспечения, включено в определённую

[38] Действия по реагированию на потенциальный риск включают принятие риска, уменьшение риска, отклонение риска и перенос/совместное использование риска. Специальная публикация NIST 800-39 даёт представление о действиях по реагированию на риск с точки зрения управления рисками.

[39] *Возможность безопасности* или *возможность приватности* - комбинация взаимно усиливающих мер обеспечения безопасности или приватности (т.е., мер защиты и контрмер), реализуемых техническими средствами (т.е., функциональностью аппаратных средств, программного обеспечения и встроенного микропрограммного обеспечения), физическими средствами (т.е., физическими устройствами и защитными мерами) и процедурными средствами (т.е., процедурами, выполняемыми людьми).

организацией возможность, тем более трудным может быть установить первопричину отказов. Могут быть также взаимодействия среди определённых возможностей, которые могут способствовать сложности оценок. Если определено, что мера обеспечения не способствует ни определённой возможности, ни полной безопасности системы, организация пересматривает Шаг 2 RMF, адаптируя набор мер обеспечения и документируя обоснование в плане обеспечения безопасности.

Традиционно, оценки проводятся на мера-по-мере базисе получения результатов, которые характеризуются как прохождение (то есть, мера удовлетворяется) или отказ (то есть, мера не удовлетворяется). Однако, отказ по отдельной мере или в некоторых случаях, отказ по многим мерам, может *не* влиять на полные возможности по безопасности или возможности по приватности, требуемые организацией. Нельзя сказать, что такие меры не *способствуют* безопасности или приватности системы и/или организации (как определено требованиями по безопасности и требованиями по приватности во время фазы инициирования жизненного цикла разработки систем), а скорее, что такие меры могут не поддерживать определённые возможности по безопасности или возможности по приватности. Кроме того, каждая реализованная мера безопасности или мера приватности могут не обязательно поддерживать или требоваться для поддержания возможности, определённой организацией.

Когда организации используют концепцию возможностей, и автоматизированные и ручные оценки принимают во внимание все меры безопасности и меры приватности, которые включают возможности по безопасности или по приватности. Оценщики знают, как меры обеспечения взаимодействуют, чтобы обеспечить такие возможности. Таким образом, когда оценки определяют отказ в возможности, может быть проведен анализ первопричины, чтобы определить конкретную меру или меры, которые ответственны за отказ, основываясь на установленных отношениях среди мер. Кроме того, использование более широкой конструкции возможности позволяет организациям оценивать *серьёзность* уязвимостей, обнаруженных в их системах и организациях и определять, влияет ли отказ определённой меры безопасности или меры приватности (связанный с уязвимостью) или решать не разворачивать некоторую меру обеспечения во время начального процесса адаптации (шаг Выбора RMF) на полную возможность, необходимую для защиты предназначения/деятельности. Например, отказу меры безопасности, считающейся критической для определённой возможности безопасности, может быть назначен более высокий рейтинг серьёзности, чем неудавшейся мере меньшей важности для возможности.

В конечном счёте, решения о санкционировании (то есть, решения по принятию риска) делаются основываясь на степени, до которой требуемые возможности по безопасности и возможности по приватности были эффективно достигнуты и выполняют требования по безопасности и требования по приватности, определённые организацией. Эти основанные на риске решения непосредственно связаны с допуском риска для организации, который определён как часть стратегии управления рисками организации.

ОЦЕНКИ, ОСНОВАННЫЕ НА ВОЗМОЖНОСТИ

Группирование мер обеспечения в возможности по безопасности и возможности по приватности требует проведение анализа первопричин, чтобы определить, может ли отказ определённой возможности по безопасности или приватности быть прослежен до отказа одной или более мер обеспечения безопасности или приватности, основываясь на установленных отношениях среди мер обеспечения. Структура процедур оценки в этой публикации с разложением на уровне признаков и маркировкой целей оценки, связанных с конкретным контентом мер обеспечения безопасности и приватности, поддерживает такой анализ первопричин. Таким образом, оценки мер обеспечения безопасности и приватности (определённых как часть возможностей) могут быть адаптированы основываясь на руководстве в Разделе 3.2.3 и Специальной публикации 800-137, чтобы определить расход ресурса (например, частоту и уровень усилий), связанного с такими оценками. Эта дополнительная точность в оценках важна в поддержании стратегий непрерывного мониторинга, разрабатываемых организациями и решениями высших руководителей по продлению санкционирования.

Рисунок 3 суммирует процесс оценки мер безопасности и мер приватности включая работы, выполняемые во время пред-оценки, оценки и пост-оценки.

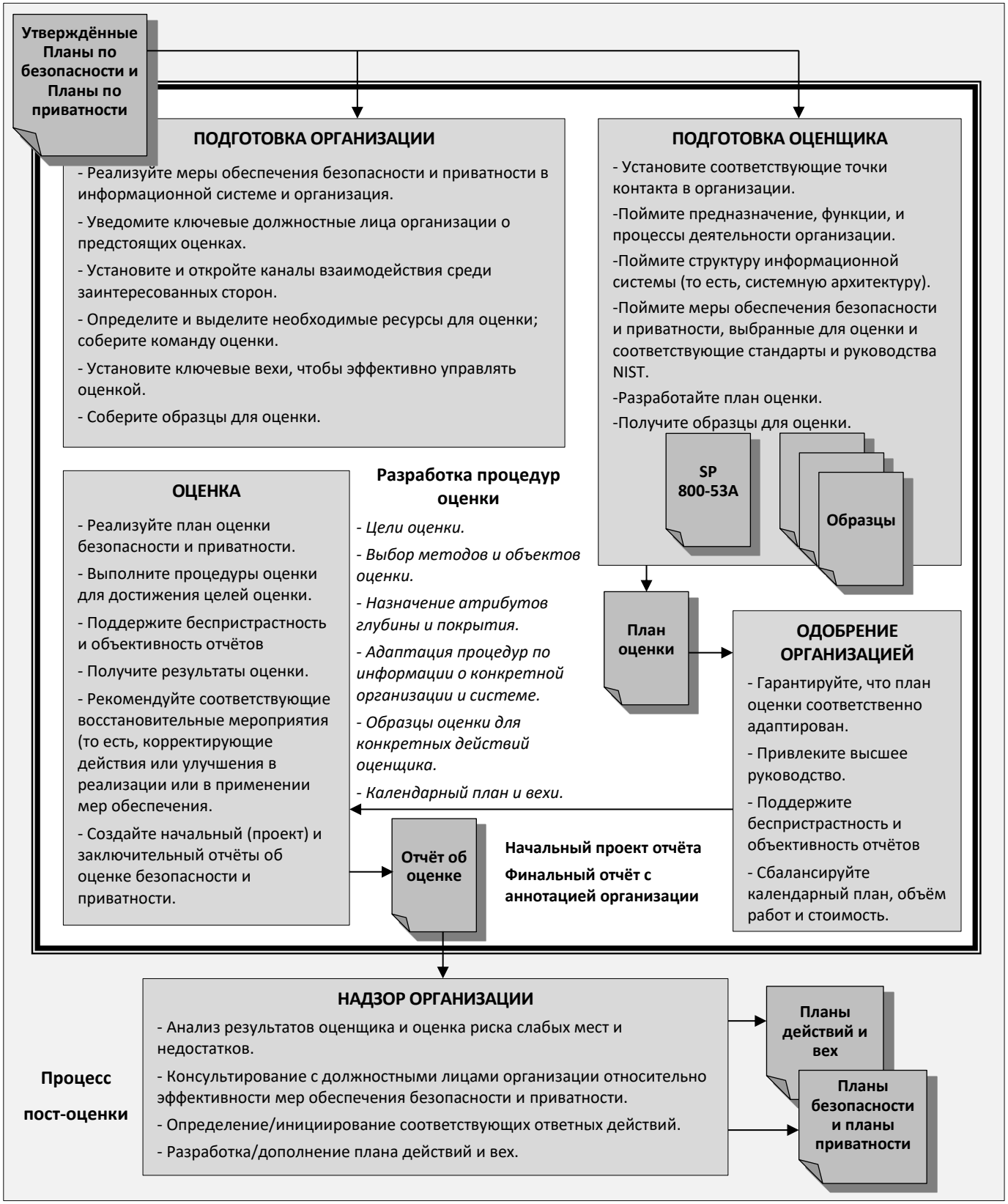

РИСУНОК 3. ОБЗОР ПРОЦЕССА ОЦЕНКИ МЕР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

ПРИЛОЖЕНИЕ A

ССЫЛКИ

ЗАКОНЫ, ПОЛИТИКИ, ДИРЕКТИВЫ, ИНСТРУКЦИИ, СТАНДАРТЫ И РУКОВОДСТВА

ЗАКОНОДАТЕЛЬСТВО

1. Закон об электронном правительстве [включает FISMA] (P.L. 107-347), декабрь 2002. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf (по состоянию на 04.12.14).
2. Федеральный закон об управлении безопасностью информации (P.L. 107-347, Title III), декабрь 2002. http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf (по состоянию на 04.12.14).
3. Закон о неприкосновенности частной жизни 1974 (P.L. 93-579), декабрь 1974. <http://www.justice.gov/opcl/privacy-act-1974> (по состоянию на 04.12.14).

ПОЛИТИКИ, ДИРЕКТИВЫ, ИНСТРУКЦИИ

1. Комитет по системам национальной безопасности (CNSS) Инструкция 4009, *Национальный глоссарий информационного доверия*, апрель 2010. <https://www.cnss.gov/CNSS/issuances/Instructions.cfm> (по состоянию на 04.12.14).
2. Комитет по системам национальной безопасности (CNSS) Инструкция 1253, Версия 2, *Категорирование безопасности и выбор мер безопасности для систем национальной безопасности*, март 2014. <https://www.cnss.gov/CNSS/issuances/Instructions.cfm> (по состоянию на 04.12.14).
3. Министерство управления и бюджета, Циркуляр A-130, Приложение I, Переходящий Меморандум #4, *Обязанности федерального агентства по поддержанию записей о физических лицах*, ноябрь 2000. <http://www.whitehouse.gov/omb/circulars_a130_a130appendix_i> (по состоянию на 04.12.14).
4. Министерство управления и бюджета, Циркуляр A-130, Приложение III, Переходящий Меморандум #4, *Управление федеральными информационными ресурсами*, ноябрь 2000. <http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii> (по состоянию на 04.12.14).
5. Министерство управления и бюджета Меморандум 02-01, *Руководство по подготовке и представлению планов действий и вех по обеспечению безопасности*, октябрь 2001. <http://www.whitehouse.gov/omb/memoranda_m02-01> (по состоянию на 04.12.14).

СТАНДАРТЫ

1. Публикация 199 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Стандарты по категорированию безопасности федеральной информации и информационных систем*, февраль 2004. <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf> (по состоянию на 04.12.14).
2. Публикация 200 Федеральных стандартов обработки информации Национального института стандартов и технологий, *Минимальные требования безопасности для Федеральной информации и информационных систем,* март 2006. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf> (по состоянию на 04.12.14).
3. ИСО/МЭК 15408, *Критерии оценки безопасности информационных технологий*, (текущий).

РУКОВОДСТВА

1. Национальный институт стандартов и технологий Специальная публикация 800-18, Пересмотр 1, *Руководство по разработке планов обеспечения безопасности для Федеральных информационных систем*, февраль 2006. <http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf> (по состоянию на 04.12.14).

2. Национальный институт стандартов и технологий Специальная публикация 800-30, Пересмотр 1, *Руководство по проведению оценок степени риска,* сентябрь 2012. <http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf> (по состоянию на 04.12.14).

3. 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. http://dx.doi.org/10.6028/NIST.SP.800-37r1.

4. Национальный институт стандартов и технологий Специальная публикация 800-39, *Управление риском информационной безопасности: Обзор организаций, предназначения и информационных систем, март 2011.* <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf> (по состоянию на 04.12.14).

5. Национальный институт стандартов и технологий Специальная Публикация 800-40, Пересмотр 3, *Руководство по технологиям корпоративного управления обновлениями*, июль 2013. http://dx.doi.org/10.6028/NIST.SP.800-40r3.

6. Национальный институт стандартов и технологий Специальная Публикация 800-53, Пересмотр 4, *Меры обеспечения безопасности и приватности для Федеральных информационных систем и организаций*, апрель 2013. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

7. Национальный институт стандартов и технологий Специальная публикация 800-59, *Руководство по идентификации информационных систем как систем национальной безопасности,* август 2003. <http://csrc.nist.gov/publications/nistpubs/800-59/SP800-59.pdf> (по состоянию на 04.12.14).

8. Национальный институт стандартов и технологий Специальная публикация 800-60, Пересмотр 1, *Руководство по отображению типов информации и информационных систем к категориям безопасности,* август 2008. http://csrc.nist.gov/publications/PubsSPs.html#800-60 (по состоянию на 04.12.14).

9. Национальный институт стандартов и технологий Специальная публикация 800-64, Пересмотр 2, *Рассмотрения безопасности в жизненном цикле разработки систем*, октябрь 2008. <http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf> (по состоянию на 04.12.14).

10. Национальный институт стандартов и технологий Специальная публикация 800-115, *Техническое руководство по проверке и оценке информационной безопасности*, сентябрь 2008. <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf> (по состоянию на 04.12.14).

11. 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. <http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf>

12. Национальный институт стандартов и технологий Специальная публикация 800-137, *Непрерывный мониторинг информационной безопасности для федеральных информационных систем и организаций,* сентябрь 2011. <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf> (по состоянию на 04.12.1404.12.14).

ПРИЛОЖЕНИЕ B

ГЛОССАРИЙ

ОБЩИЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Это приложение обеспечивает определения для терминологии по безопасности, используемой в Специальной публикации 800-53A. Термины в глоссарии непротиворечивы с терминами, используемыми в комплекте стандартов и руководств по обеспечению безопасности связанных с FISMA, разрабатываемых NIST. Если иначе не заявлено, все термины, использованные в этой публикации, также непротиворечивы с определениями, содержавшимися в Инструкции 4009 CNSS, *Национальном глоссарии информационного доверия*.

Activities Действия (работы)	Объект оценки, который включает конкретные, связанные с защитой занятия или мероприятия, поддерживающие информационную систему, с привлечением людей (например, проведение действий по резервному копированию систем, контроль сетевого трафика).
Adequate Security Адекватная Безопасность [Циркуляр OMB A-130, Приложение III]	Безопасность, соразмерная с риском и величиной вреда, следующего из потери, неправильного употребления или несанкционированного доступа к или модификации информации.
Agency Агентство	См. *Executive Agency.*
Assessment Оценка	См. *Security Control Assessment* или *Privacy Control Assessment.*
Assessment Findings Результаты оценки	Результаты оценки, полученные приложением процедуры оценки к мере безопасности, мере приватности или улучшению меры, чтобы достигнуть цели оценки; выполнение описания решения в процедуре оценки оценщиком, результаты которого либо *удовлетворяет* либо *другое, чем удовлетворяет*.
Assessment Method Метод оценки	Один из трёх типов действий (то есть, исследование, опрос, испытание) выбираемый оценщиками при получении свидетельства во время оценки.
Assessment Object Объект оценки	Элемент (то есть, спецификации, механизмы, действия, люди), в отношении которого применяется метод оценки во время оценки.
Assessment Objective Цель оценки	Набор описаний решений, который определяет желаемый результат оценки мер безопасности, мер приватности или улучшений мер обеспечения.
Assessment Procedure Процедура оценки	Набор *целей* оценки и связанный набор *методов* оценки и *объектов* оценки.
Assessor Оценщик	См. *Security Control Assessor* или *Privacy Control Assessor приватности*.
Assurance Доверие	Основание для уверенности, что набор намеченных мер безопасности или мер приватности в информационной системе или организации эффективен в его приложении.

Assurance Case Образец доверия *[Институт программной инженерии, университет Карнеги-Меллона]*	Структурированный набор аргументов и состав свидетельств, показывающих, что информационная система удовлетворяет определённым утверждениям относительно заданного качественного показателя.
Authentication Аутентификация [FIPS 200]	Проверка идентификационных данных пользователя, процесса или устройства, обычно как предпосылка к предоставлению доступа к ресурсам в информационной системе.
Authenticity Аутентичность	Свойство, определяющее подлинность и возможность проверять и доверять; уверенность в законности передачи, сообщения или автора сообщения. См. *Аутентификация*.
Authorization (to operate) Санкционирование (эксплуатировать) [NIST SP 800-37, Уточнённый]	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 и мер приватности.
Authorization Boundary Граница санкционирования [NIST SP 800-37]	Все компоненты информационной системы, которая санкционирована для эксплуатации санкционирующим должностным лицом, исключая отдельно санкционированные системы, с которыми соединена информационная система.
Authorizing Official Санкционирующее должностное лицо [NIST SP 800-37]	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.
Authorizing Official Designated Representative Уполномоченный представитель санкционирующего должностного лица [NIST SP 800-37, Adapted]	Должностное лицо организации, действующее от имени санкционирующего должностного лица в выполнении и координации требуемых действий, связанных с санкционированием безопасности или санкционированием приватности.
Availability Доступность [44 U.S.C., Sec. 3542]	Обеспечение своевременного и надёжного доступа к и использования информации.
Basic Testing Базовое тестирование	Методология тестирования, которая предполагает не знание внутренней структур и деталей реализации объекта оценки. Также известна, как тестирование методом "чёрного ящика".
Black Box Testing Тестирование методом "чёрного ящика"	См. *Basic Testing*

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.
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*.
Common Control Общая мера [NIST SP 800-37, Уточнённый]	Мера безопасности или мера приватности, которая является наследуемой одной или более информационными системами организации. См. *Security Control Inheritance* или *Privacy Control Inheritance*.
Common Control Provider Поставщик общих мер [NIST SP 800-37, Уточнённый]	Должностное лицо организации, ответственное за разработку, реализацию, оценку и мониторинг общих мер (то есть, мер безопасности и мер приватности, наследуемых информационными системами).
Compensating Security Controls Компенсирующие меры безопасности [NIST SP 800-53]	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.
Comprehensive Testing Всеобъемлющее тестирование	Методология тестирования, которая предполагает явное и существенное знание внутренней структуры и деталей реализации объекта оценки. Также известна как тестирование методом "белого ящика".
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 собственической информации.

Controlled Unclassified Information Контролируемая неклассифицированная информация	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 Соединённых 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. Впредь, обозначение CUI заменяет *Чувствительная, но Несекретная* (SBU).
Coverage Покрытие	Атрибут, связанный с методом оценки, который определяет область или объём объектов оценки, включённых в оценку (например, типы объектов, которые будут оценены и число объектов, которые будут оценены в типе). Значениями для атрибута покрытия, иерархическими от меньшего покрытия до большего покрытия, являются базовое, ограниченное и полное.
Depth Глубина	Атрибут, связанный с методом оценки, который определяет строгость и уровень детализации, связанный с применением метода. Значениями для атрибута глубины, иерархическими от меньшей глубины до большей глубины, являются базовая, ограниченная и полная.
Environment of Operation Среда эксплуатации [NIST SP 800-37]	Физическое окружение, в котором информационная система обрабатывает, хранит и передаёт информацию.
Examine Исследование	Тип метода оценки, который характеризуется процессом проверки, осмотра, рассмотрения, наблюдения, изучения или анализа одного или более объекта оценки, чтобы облегчить понимание, достигнуть разъяснения или получить свидетельство, результаты которого используются, чтобы поддержать определение мер безопасности или эффективности мер приватности в течение долгого времени.
Executive Agency Исполнительное агентство [41 U.S.C., Sec. 403]	Исполнительный департамент, определённый в 5 U.S.C., Раздел 101; военный департамент, определённый в 5 U.S.C., Раздел 102; независимое учреждение, как определено в 5 U.S.C., Раздел 104 (1); и полностью находящаяся в собственности Правительства корпорация, полностью попадающая под действие 31 U.S.C., Глава 91.
Federal Agency Федеральное агентство	См. *Executive Agency.*
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.
Focused Testing Ограниченное тестирование	Методология тестирования, которая предполагает некоторое знание внутренней структуры и деталей реализации объекта оценки. Также известна, как тестирование методом «серого ящика».
Gray Box Testing Тестирование «серого ящика»	См. *Focused Testing*
Hybrid Control	Мера безопасности или мера приватности, которая реализована в

Гибридная мера [CNSSI 4009, Уточненный]	информационной системе частично как общая мера безопасности и частично как специфичная для системы мера безопасности. См. *Common Control* и *System-Specific Control*.
Individuals Физические лица	Объект оценки, который включает людей, применяющих спецификации, механизмы или действия.
Industrial Control System Индустриальная система управления	Информационная система, используемая для контроля производственных процессов, таких как производство, обработка продукта, изготовление и распространение. Индустриальные системы управления включают системы диспетчерского управления и сбора данных (SCADA), используемые для контроля географически распределённых активов, а так же распределённые системы управления (DCSs) и малые системы управления, использующие контроллеры с программируемой логикой, чтобы контролировать ограниченные процессы.
Information Информация [FIPS 199]	Частный случай типа информации.
Information Owner Владелец информации [CNSSI 4009]	Должностное лицо с установленными законом или исполнительными полномочиями для указанной информации и ответственностью за установление мер безопасности при её генерации, сборе, обработке, распространении 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 Program Plan План Программы информационной безопасности [NIST SP 800-53]	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 System Информационная система [44 U.S.C., Sec. 3502]	Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, совместного использования, распространения или ликвидации информации.
Information System Boundary Границы информационной системы	См. *Authorization Boundary*.
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 Security Officer Сотрудник безопасности информационной системы	Человек с ответственностью, возложенной высшим сотрудником по информационной безопасности агентства, санкционирующим должностным лицом, должностным лицом руководства или владельцем информационной системы за поддержание соответствующего эксплуатационного состояния безопасности для информационной системы или программы.

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. *Risk*.
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 приёме данных или информации исполнительным агентством. Для целей предыдущего предложения, оборудование используется исполнительным агентством, если оборудование используется исполнительным агентством непосредственно или используется подрядчиком в соответствии с контрактом с исполнительным агентством который: (i) требует использования такого оборудования; или (ii) требует использования, до существенной степени, такого оборудования в исполнении сервиса или оснащении продукта. Термин информационная технология включает компьютеры, вспомогательное оборудование, программное обеспечение, встроенное микропрограммное обеспечение, и подобные процедуры, сервисы (включая службу поддержки) и связанные ресурсы.
Information Type Тип информации [FIPS 199]	Конкретная категория информации (например, приватная, медицинская, имущественная, финансовая, следственная, чувствительная для подрядчика, управления безопасностью) определённая организацией или, в некоторых случаях, согласно конкретному закону, Правительственному распоряжению, директиве, политике или нормативному документу.
Integrity Целостность [44 U.S.C., Sec. 3542]	Защита против неправомерной модификации или уничтожения информации, включающая обеспечение неотказуемости и аутентичности информации.
Interview Опрос	Тип метода оценки, который характеризуется процессом проведения обсуждений с людьми или группами в организации, чтобы облегчить понимание, добиться разъяснения или получить свидетельства, результаты которого используются, чтобы поддержать определение эффективности мер безопасности и мер приватности в течение долгого времени.
Mechanisms Механизм	Объект оценки, который включает специфические, связанные с защитой элементы (например, аппаратные средства, программное обеспечение или встроенное микропрограммное обеспечение), используемые в пределах или на границе информационной системы.
Ongoing Assessment Текущая оценка	Непрерывная оценка эффективности реализации мер безопасности или мер приватность; в отношении мер безопасности, субъект действий по Непрерывному мониторингу информационной безопасности (ISCM).

National Security Information Информация национальной безопасности	Информация, которая была определена в соответствии с Правительственным распоряжением 12958, уточнённым Правительственным распоряжением 13292, или любым предшествующим порядком, или законом об Атомной энергии 1954, с уточнениями, как требующая защиты против несанкционированного раскрытия и маркирована, чтобы указать на её классифицированный статус.
National Security System Система национальной безопасности [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 вооружёнными 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.
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).
Penetration Testing Тестирование проникновения	Тестовая методология в который оценщики, используя всю доступную документацию (например, проект системы, исходный код, руководства) и работающие с конкретными ограничениями, пытаются обойти или преодолеть средства защиты информационной системы.
Plan of Action and Milestones План действий и вех [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.
Privacy Capability Возможность приватности	Комбинация взаимно усиливающих мер приватности (то есть, мер защиты и контрмер), реализуемых техническими средствами (то есть, функциональностью аппаратных средств, программного обеспечения и встроенного микропрограммного обеспечения), физическими средствами (то есть, физическими устройствами и защитными мерами) и процедурными средствами (то есть, процедурами, выполняемыми людьми).
Privacy Control Assessment Оценка мер приватности	Проверка или оценка мер приватности для определения степени, до которой меры реализованы правильно, применяются как предназначено и производят желаемый результат относительно удовлетворения требований приватности для информационной системы или организации.

Privacy Control Assessor *Оценщик мер приватности*	Человек, группа или организация, ответственные за проведение оценки мер приватности.
Privacy Control Enhancement Улучшение мер приватности	Усиление возможностей приватности с целью: (i) создания дополнительной, но связанной, функциональности базовых мер; и/или (ii) увеличения стойкости базовых мер.
Privacy Control Inheritance Наследование мер приватности	Ситуация, в которой информационная система или приложение получают защиту от мер приватности (или части мер приватности), 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*.
Privacy Plan План обеспечения приватности	Формальный документ, который представляет описание требований приватности для информационной системы или программы и описывает реализованные или планируемые меры приватности для удовлетворения этим требованиям. План обеспечения приватности может быть интегрирован в план обеспечения безопасности организации или разработан как отдельный план.
Privacy Requirements Требования приватности	Требования, предъявленные к организации, программе информатизации или информационной системе, которые получены из применимых законов, Правительственных распоряжений, директив, политик, стандартов, инструкций, нормативных актов, процедур или потребностей предназначения/деятельности организации, чтобы гарантировать, что защита приватности реализована при сборе, использовании, совместном использовании, хранении, передаче и ликвидации информации.
Reciprocity Соглашение о взаимности	Совместное соглашение среди участвующих организаций, чтобы принять оценки безопасности другого участника с целью повторного использования ресурсов информационной системы и/или принять оценённое другим участником состояние с безопасностью, в качестве общей информации
Records Записи	Записи (автоматизированные и/или ручные) свидетельства выполняемых действий или достигнутых результатов (например, формы, отчёты, 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 определённых элементов).

Risk Риск [CNSSI 4009]	Мера степени, до которой сущности угрожают потенциальные обстоятельство или событие, и, как правило, функция от: (i) неблаго-приятных воздействий, которые возникли бы, если бы обстоятельство или событие произошли; и (ii) вероятности случая. [Примечание: риски безопасности, связанные с информационной системой, это те риски, которые являются результатом потери конфиденциальности, целостности или доступности информации или информационных систем и отражают потенциальные неблагоприятные воздействия на деятельность организации (включая предназначение, функции, имидж или репутацию), активы организации, людей, другие организации и Нацию. Неблагоприятные воздействия на Нацию включают, например, компрометацию информационных систем, которые поддерживают критические инфраструктурные приложения или являются определяющими для непрерывности правительственной деятельности, как определено Департаментом безопасности отечества.]
Risk Assessment Оценка риска	Процесс определения 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) [NIST SP 800-37, уточнённый]	Человек или группа в организации, который помогает обеспечивать, что: (i) связанные с риском рассмотрения безопасности и приватности 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 рисками безопасности и приватности, связанными с информационными системами, непротиворечиво с организацией, отражает допуск для риска организации и рассмотрение наряду с другими рисками организации, влияющими на успех в предназначении/деятельности.
Risk Management Управление рисками [CNSSI 4009, уточнённый]	Процессы управлении рисками для деятельности организации (включая предназначение, функции, имидж и репутацию), активов организации, людей, других организаций и Нации, являющимися результатом применения информационных систем, и включающие: (i) проведение оценки риска; (ii) реализацию стратегии уменьшения рисков; (iii) применение методов и процедур по непрерывному мониторингу состояния с безопасностью и приватностью в информационных системах.
Security Authorization Санкционирование безопасности	См. *Authorization.*

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.
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 предназначено 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]	Один из наборов минимальных мер безопасности, определённых для федеральных информационных систем в специальной публикации NIST 800-53 и Инструкции CNSS 1253.
Security Control Enhancement Улучшение мер безопасности	Усиление возможностей по безопасности с целью: (i) создания дополнительной, но связанной, функциональности базовых мер; и/или (ii) увеличения стойкости базовs[мер.
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 сущностями другими, чем ответственные за систему или приложение; сущностями, или внутренними или внешними к организации, где система или приложение находятся. См. *Общие меры безопасности*.
Security Controls Меры безопасности [NIST SP 800-53]	Меры защиты или контрмеры, предписанные для информационных систем или организаций, которые разработаны для защиты конфиденциальности, целостности и доступности их информации и удовлетворения набору установленных требований безопасности.
Security Impact Analysis Анализ воздействия на безопасность [NIST SP 800-37]	Анализ, проводимый должностным лицом организации, чтобы определить степень, до которой изменения в информационной системе влияют на состояние безопасности системы.
Security Objective Цель безопасности, [FIPS 199]	Конфиденциальность, целостность или доступность.

Security Plan План безопасности [NIST SP 800-18]	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 or Information Security Program Plan.*
Security Requirements Требования безопасности [FIPS 200]	Требования, предъявленные к информационной системе, которые получены из действующих законов, Правительственных распоряжений, директив, политик, стандартов, инструкций, нормативных актов, процедур или потребностей предназначения/деятельности, чтобы гарантировать конфиденциальность, целостность и доступность информации, которая обрабатывается, хранится или передаётся.
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, подчинённые 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.*
Specification Спецификация	Объект оценки, который включает объекты, основанные на документах (например, политики, процедуры, планы, требования безопасности системы, функциональные спецификации, эскизные проекты), связанных с информационной системой.
Subsystem Подсистема	Основное подразделение или компонент информационной системы, состоящее из информации, информационных технологий и персонала, которое выполняет одну или более конкретные функции.
System Система	См. *Information System*.
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 Control Мера обеспечения, специфичная для системы [NIST SP 800-37, уточнённый]	Мера безопасности или мера приватности для информационной системы, которая не определялась как общая мера или часть гибридной меры, которая должна быть реализована в информационной системе.

Tailoring Адаптация [NIST SP 800-53]	Процесс, посредством которого базовые наборы мер безопасности изменяются путём: (i) определения и назначения общих мер безопасности; (ii) приложения объектовых особенностей при применении и реализации базовых мер; (iii) выбора компенсирующих мер безопасности; (iv) назначения конкретных значений определённым организацией параметрам мер безопасности; (v) дополнения базовых наборов дополнительными мерами безопасности или улучшениями мер; и (vi) предоставления дополнительной уточняющей информации для реализации мер. [Примечание: Определённые действия по адаптации могу также применяться к мерам приватности.]
Tailoring (Assessment Procedures) Адаптация (Процедуры оценки)	Процесс, посредством которого для процедур оценки, определённых в Специальной публикации 800-53A, осуществляется корректировка или уточнение контекста, чтобы соответствовать характеристикам оцениваемой информационной системы, предоставляя организациям гибкость, чтобы удовлетворить конкретные требования организации и избежать чрезмерного ограничения подходов оценки.
Tailored Security Control Baseline Адаптированный базовый набор мер безопасности	Набор мер безопасности, являющийся результатом применения руководства по адаптации к базовому набору мер безопасности. См. *Tailoring*.
Test Испытание	Тип метода оценки, который характеризуется процессом проверки одного или более объектов оценки при указанных условиях для сравнения фактического и ожидаемого поведения, результаты которого используются, чтобы поддержать определение эффективности мер безопасности или мер приватности в течение длительного времени.
Threat Угроза [CNSSI 4009]	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]	Процесс формальной оценки уровня угрозы информационной системе или интерпретация и описание существа угрозы.
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.
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 Assessment Оценка уязвимостей [CNSSI 4009, Уточнённый]	Систематизированное исследование информационной системы или продукта, позволяющее определить соответствие мер безопасности и приватности, идентифицировать недостатки безопасности и приватности, обеспечить данные, по которым можно предсказать эффективность предложенных мер безопасности и приватности, и подтвердить соответствие таких мер после реализации.
White Box Testing Тестирование белого ящика	См. *Comprehensive Testing*.

ПРИЛОЖЕНИЕ C

АКРОНИМЫ

ОБЩИЕ СОКРАЩЕНИЯ

CIO	Chief Information Officer, Директор по информации
CPO	Chief Privacy Officer, Директор по приватности
CNSS	Committee on National Security Systems, Комитет по системам национальной безопасности
CUI	Controlled Unclassified Information, Контролируемая неклассифицированная информация
COTS	Commercial Off-The-Shelf, Коммерческий серийный продукт
DoD	Department of Defense, Министерство обороны
FIPS	Federal Information Processing Standards, Федеральные стандарты обработки информации
FISMA	Federal Information Security Management Act, Закон об управлении безопасностью федеральной информации
ICS	Industrial Control System, Система управления производственным процессом
IEC	International Electrotechnical Commission, Международная электротехническая комиссия
ISO	International Organization for Standardization, Международная организация по стандартизации
NCP	National Checklist Program, Национальная программа контрольного списка
NIST	National Institute of Standards and Technology, Национальный институт стандартов и технологий
NSA	National Security Agency, Агентство национальной безопасности
OCIL	Open Checklist Interactive Language, Открытый интерактивный язык контрольных списков
ODNI	Office of the Director of National Intelligence, Офис директора национальной разведки
OMB	Office of Management and Budget, Министерство управления и бюджета
PKI	Public Key Infrastructure, Инфраструктура публичных ключей
POAM	Plan of Action and Milestones, План действий и вех
RMF	Risk Management Framework, Основы управления рисками
SAOP	Senior Agency Official for Privacy, Высшее должностное лицо агентства по приватности
SCAP	Security Content Automation Protocol, Протокол автоматизации контента безопасности
SP	Special Publication, Специальная публикация
U.S.C.	United States Code, Свод законов Соединённых штатов

ПРИЛОЖЕНИЕ D

ОПИСАНИЯ МЕТОДОВ ОЦЕНКИ

ОПРЕДЕЛЕНИЯ МЕТОДОВ ОЦЕНКИ, ПРИМЕНИМЫЕ ОБЪЕКТЫ И АТРИБУТЫ

Это приложение определяет три метода оценки, которые могут использоваться оценщиками во время оценок мер обеспечения безопасности и приватности: (i) *исследование*; (ii) *опрос*; и (iii) *испытание*. В определение каждого метода оценки включены типы объектов, к которым метод может быть применён. Применение каждого метода описано с точки зрения атрибутов *глубины* и *покрытия*, развивающихся от *базового* до *ограниченного* к *полному*. Значения атрибута коррелируют с требованиями доверия, определёнными организацией.[40]

Атрибут глубины определяет строгость и уровень детализации оценки. Для атрибута глубины значение атрибута *ограниченная* включает и наращивает строгость оценки и уровень детализации, определённые для значения атрибута *основная*; значение атрибута *полная* включает и наращивает строгость оценки и уровень детализации, определённые для значения атрибута *ограниченная*.

Атрибут покрытия адресует область или объём оценки. Для атрибута покрытие значение атрибута *ограниченное* включает и наращивает количество и типы объектов оценки, определённые для значения атрибута *основное*; значение атрибута *полное* включает и наращивает количество и типы объектов оценки, определённые для значения атрибута *ограниченное*.

Использование **полужирного текста** в описании метода оценки указывает на контент, который был добавлен и появляется впервые, в описании, указывающем на большую строгость и уровень детализации для значения атрибута.

[40] Для всех систем, кроме систем национальной безопасности, организации обеспечивают удовлетворение минимальным требованиям доверия, определённым в Специальной публикации 800-53, Приложение E.

МЕТОД ОЦЕНКИ: Исследование

ОБЪЕКТЫ ОЦЕНКИ: Спецификации (например, политики, планы, процедуры, системные требования, проекты)
Механизмы (например, функциональность, реализованная в аппаратных средствах, программном обеспечении, встроенном микропрограммном обеспечении)
Работы (например, эксплуатация системы, администрирование, управление; использование)

ОПРЕДЕЛЕНИЕ: Процесс проверки, обследования, рассмотрения, наблюдения, изучения или анализа одного или более объектов оценки для облегчения понимания, достижения разъяснения или получения свидетельств, результаты которого используются, чтобы поддержать определение существования, функциональности, корректности, законченности и потенциала для улучшения с течением времени мер обеспечения безопасности и приватности.

ДОПОЛНИТЕЛЬНОЕ РУКОВОДСТВО: Типичные действия оценщика могут включать, например: рассмотрение политик, планов и процедур обеспечения безопасности информации; анализ документации проекта системы и спецификаций интерфейсов; наблюдение применения резервного копирования системы; рассмотрение результатов использования плана действий в непредвиденных ситуациях; наблюдение за действиями по реакции на инциденты; изучение технических описаний и руководств пользователя/администратора; проверка, изучение или наблюдение за использованием механизмов информационных технологий в аппаратных средствах/программном обеспечении информационной системы; или проверка, изучение или наблюдение за мерами по физической безопасности, имеющими отношение к эксплуатации информационной системы.

SCAP-проверенные инструменты, которые поддерживают спецификацию компонент OCIL, могут быть использованы для автоматизации сбора объектов оценки от конкретных, ответственных людей в организации. Результирующая информация может затем быть исследована оценщиками во время оценок мер обеспечения безопасности и приватности.

АТРИБУТЫ: Глубина, Покрытие

- Атрибут *глубина* определяет строгость и уровень детализации в процессе исследования. Есть три возможных значения для атрибута глубины: (i) *основная*; (ii) ограниченная; и (iii) полная.
  - Основное исследование: Исследование, которое состоит из высокоуровневых рассмотрений, проверок, наблюдений или обследований объектов оценки. Этот тип исследования проводится с использованием ограниченного объёма данных или документации (например, описания функционального уровня для механизмов; высокоуровневые описания процессов для работ; существующих документов для спецификаций). Основные исследования обеспечивают уровень понимания мер обеспечения безопасности и приватности, необходимых для того, чтобы определить, реализованы ли меры обеспечения и свободны ли от очевидных ошибок.
  - Ограниченное исследование: Исследование, которое состоит из высокоуровневых рассмотрений, проверок, наблюдений или обследований **и более всестороннего изучения/анализа** объекта оценки. Этот тип исследования проводится, используя **значительный** объём данных или документации (например, описания функционального уровня **и, где соответствующе и доступно, информация проекта высокого уровня** для механизмов; высокоуровневые описания процессов **и процедур реализации** для работ; существующие документы **и связанные документы** для спецификаций). **Ограниченные** исследования обеспечивают уровень понимания мер обеспечения безопасности и приватности, необходимый для того, чтобы определить, реализованы ли меры обеспечения и свободны ли от очевидных ошибок **и увеличена ли основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено**.
  - Полное исследование: Исследование, которое состоит из высокоуровневых рассмотрений, проверок, наблюдений или обследований и более всестороннего, **детализированного и досконального** изучения/анализа объекта оценки. Этот тип исследования проводится, используя **обширный** объём данных или документации (например, описания функционального уровня и где соответствующе и доступно, информация проекта высокого уровня, **информация проекта низкого уровня и информация по реализации** для механизмов; высокоуровневые описания процесса и **детализированные** процедуры реализации для работ; существующие документы и связанные документы для спецификаций[41]). **Полные исследования** обеспечивают уровень понимания мер обеспечения безопасности и приватности, необходимый для того, чтобы определить, реализованы ли меры обеспечения и свободны ли от очевидных ошибок и увеличена ли **ещё более** основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено **на непрерывной и непротиворечивой основе, и что есть поддержка для постоянного совершенствования эффективности мер обеспечения**.

[41] В то время как для механизмов, при продвижении от основного до ограниченного к полному исследованию, возможна дополнительная документация, документация, связанная со спецификациями и работами, для ограниченных и полных исследований, может оставаться той же самой или подобной, но со строгостью исследований этих документов, увеличенной на полном уровне.

- Атрибут *покрытие* определяет область или объём процесса исследования и включает типы объектов оценки для исследования, число объектов, которые будут исследованы (в типе), и конкретные объекты, которые будут исследованы.[42] Есть три возможных значения для атрибута покрытия: (i) *основное*; (ii) ограниченное; и (iii) полное.
  - Основное исследование: Исследование, которое использует репрезентативную выборку объектов оценки (по типам и числу в типе), чтобы обеспечить уровень покрытия, необходимый для того, чтобы определить, реализованы ли меры обеспечения безопасности и приватности и свободны ли от очевидных ошибок.
  - Ограниченное исследование: Исследование, которое использует репрезентативную выборку объектов оценки (по типам и числу в типе) **и другие специфические объекты оценки, которые считаются особенно важными для достижения цели оценки,** чтобы обеспечить уровень покрытия, необходимый для того, чтобы определить, реализованы ли меры обеспечения безопасности и приватности и свободны ли от очевидных ошибок **и увеличена ли основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено**.
  - Полное исследование: Исследование, которое использует **достаточно обширную выборку** объектов оценки (по типам и числу в типе) и другие специфические объекты оценки, которые считаются особенно важными для достижения цели оценки, чтобы обеспечить уровень покрытия, необходимый для того, чтобы определить, реализованы ли меры обеспечения безопасности и приватности и свободны ли от очевидных ошибок и увеличена ли **ещё более** основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено **на непрерывной и непротиворечивой основе, и что есть поддержка для постоянного совершенствования эффективности мер обеспечения**.

[42] Организация, рассматривая различные факторы (например, доступные ресурсы, важность оценки, полные цели и объекты оценки для организации), обсуждает с оценщиками и определяет направление по типам, числу и конкретным объектам, которые будут исследованы для конкретного значения характеризуемого атрибута.

МЕТОД ОЦЕНКИ: Опрос

ОБЪЕКТЫ ОЦЕНКИ: Люди или группы людей.

ОПРЕДЕЛЕНИЕ: Процесс проведения обсуждений с людьми или группами в организации для облегчения понимания, достижения разъяснения или получения свидетельств, результаты которого используются, чтобы поддержать определение существования, функциональности, корректности, законченности и потенциала для улучшения с течением времени мер обеспечения безопасности и приватности.

ДОПОЛНИТЕЛЬНОЕ РУКОВОДСТВО: Типичные действия оценщика могут включать, например, опрос руководителей агентства, директоров по информации, высших сотрудников агентства по информационной безопасности, санкционирующих должностных лиц, владельцев информации, владельцев предназначения и информационных систем, сотрудников безопасности информационных систем, руководителей служб безопасности информационных систем, работников отдела кадров, менеджеров людских ресурсов, менеджеров по средствам, инструкторов, операторов информационных систем, сетевых и системных администраторов, начальников объектов информатизации, сотрудников по физической безопасности и пользователей.

SCAP-проверенные инструменты, которые поддерживают спецификацию компонент OCIL, могут быть использованы для автоматизации процесса проведения опроса конкретных людей или групп людей. Результирующая информация может затем быть исследована оценщиками во время оценок мер обеспечения безопасности и приватности.

АТРИБУТЫ: Глубина, Покрытие

- Атрибут *глубина* определяет строгость и уровень детализации в процессе опроса. Есть три возможных значения для атрибута глубины: (i) *основная*; (ii) *ограниченная*; и (iii) *полная*.
  - Основной опрос: Опрос, который состоит из всеобъемлющих, высокоуровневых обсуждений с людьми или группами люди. Этот тип опроса проводится с использованием набора обобщённых, высокоуровневых вопросов. Основные опросы обеспечивают уровень понимания мер обеспечения безопасности и приватности, необходимый для того, чтобы определить, реализованы ли меры обеспечения и свободны ли от очевидных ошибок.
  - Ограниченный опрос: Опрос, который состоит из всеобъемлющих, высокоуровневых обсуждений **и более углубленных обсуждений в определённых областях** с людьми или группами людей. Этот тип опроса проводится с использованием набора обобщённых, высокоуровневых вопросов **и более углубленных вопросов в определённых областях, где реакции указывают на потребность в более углубленном изучении**. **Ограниченные** опросы обеспечивают уровень понимания мер обеспечения безопасности и приватности, необходимый для того, чтобы определить, реализованы ли меры обеспечения и свободны ли от очевидных ошибок **и увеличена ли основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено**.
  - Полный опрос: Опрос, который состоит из всеобъемлющих, высокоуровневых обсуждений и более углубленных, **направленных** обсуждений в определённых областях с людьми или группами людей. Этот тип опроса проводится с использованием набора обобщённых, высокоуровневых вопросов и более углубленных, **направленных** вопросов в определённых областях, где реакции указывают на потребность в более углубленном изучении. **Полные** опросы обеспечивают уровень понимания мер обеспечения безопасности и приватности, необходимый для того, чтобы определить, реализованы ли меры обеспечения и свободны ли от очевидных ошибок и увеличена ли **ещё более** основа для уверенности, что меры обеспечения реализованы правильно и работающий как предназначено **на непрерывной и непротиворечивой основе, и что есть поддержка для постоянного совершенствования эффективности мер обеспечения**.
- Атрибут *покрытие* определяет область или объём процедуры опроса и включает типы людей, которые будут опрошены (по роли в организации и связанным обязанностям), числу людей, которые будут опрошены (в типе) и конкретных людей, которые будут опрошены.[43] Есть три возможных значения для атрибута покрытия: (i) *основное*; (ii) ограниченное; и (iii) полное.
  - Основной опрос: Опрос, который использует репрезентативную выборку людей из ключевых ролей для организации, чтобы обеспечить уровень покрытия, необходимый для того, чтобы определить, реализованы ли меры обеспечения безопасности и приватности и свободны ли от очевидных ошибок.
  - Ограниченный опрос: Опрос, который использует репрезентативную выборку людей из ключевых ролей для организации **и других конкретных людей, считающихся особенно важными для достижения целей оценки,**

[43] Организация, рассматривая различные факторы (например, доступные ресурсы, важность оценки, полные цели и объекты оценки для организации), обсуждает с оценщиками и определяет направление по типам, числу и конкретным людям, которые будут опрошены для конкретного значения характеризуемого атрибута.

чтобы обеспечить уровень покрытия, необходимый для того, чтобы определить, являются ли меры обеспечения безопасности и приватности реализованными и свободны ли от очевидных ошибок **и увеличена ли основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено**.

- Всесторонний опрос: Опрос, который использует **достаточно большую выборку** людей из ключевых ролей для организации и других конкретных людей, считающихся особенно важными для достижения целей оценки, чтобы обеспечить уровень покрытия, необходимый для того, чтобы определить, являются ли меры обеспечения безопасности и приватности реализованными и свободны ли от очевидных ошибок и увеличена ли **ещё более** основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено **на непрерывной и непротиворечивой основе, и что есть поддержка для постоянного совершенствования эффективности мер обеспечения**.

МЕТОД ОЦЕНКИ: Испытание

ОБЪЕКТЫ ОЦЕНКИ: Механизмы (например, аппаратные средства, программное обеспечение, встроенное микропрограммное обеспечение)
Работы (например, эксплуатация системы, администрирование, управление; использование)

ОПРЕДЕЛЕНИЕ: Процесс проверки одного или более объектов оценки при указанных условиях для сравнения фактического и ожидаемого поведения, результаты которого используются, чтобы поддержать определение существования, функциональности, корректности, законченности мер обеспечения безопасности и приватности, и потенциала для улучшения в течение длительного времени.[44]

ДОПОЛНИТЕЛЬНОЕ РУКОВОДСТВО: Типичные действия оценщика могут включать, например: тестирование контроля доступа, идентификации и аутентификации и аудит механизмов; проверка настроек безопасной конфигурации; проверка устройств контроля физического доступа; проведение тестирования на возможность проникновения для ключевых компонентов информационной системы; проверка проведения резервного копирования информационной системы; проверка возможностей по реагированию на инциденты; и проверка возможностей планирования на случай непредвиденных ситуаций.

SCAP-проверенные инструменты могут использоваться для автоматизации сбора объектов оценки и оценки ожидаемого поведения этих объектов. Использование SCAP является соответствующим по отношению к тестированию механизмов, которое включает оценку фактического машинного состояния. Каталоги Национальной программы контрольных списков содержат много SCAP-поддерживаемых контрольных списков, которые являются подходящими для того, чтобы оценить состояние конфигурации конкретных операционных систем и приложений. SCAP-проверенные инструменты могут использовать эти контрольные списки, чтобы определить совокупное соответствие системы по отношению ко всем установкам конфигурации в контрольном списке (например, CM-6) или конкретным конфигурациям, которые соответствуют мерам обеспечения безопасности или приватности, которые имеют отношение к одной или более установкам конфигурации. SCAP-проверенные инструменты могут также определить отсутствие патча или наличие уязвимого состояния. Результаты, полученные инструментами SCAP, могут быть исследованы оценщиками как часть оценок мер обеспечения безопасности и приватности.

АТРИБУТЫ: Глубина, Покрытие

- Атрибут *глубин*а определяет типы испытаний, которые будут проведены. Есть три возможных значения для атрибута глубины: (i) *основные* испытания; (ii) *ограниченные* испытания; и (iii) *полные* испытания.
  - Основные испытания: Методология испытаний (также известная как *испытание методом "черного ящика"*), которая предполагает не знание внутренней структуры и деталей реализации объекта оценки. Этот тип испытаний проводится с использованием функциональной спецификации для механизмов и высокоуровневых описаний процедур для работ. Основные испытания обеспечивают уровень понимания мер обеспечения безопасности и приватности, необходимый для того, чтобы определить, реализованы ли меры обеспечения и свободны ли от очевидных ошибок.
  - Ограниченные испытания: Методология испытаний (также известная как *испытание методом "серого ящика"*), которая предполагает **некоторое** знание внутренней структуры и деталей реализации объекта оценки. Этот тип испытаний проводится с использованием функциональной спецификации **и ограниченной информации по архитектуре системы (например, проект высокого уровня)** для механизмов и высокоуровневых описаний процедур **и описаний высокого уровня по интеграции в эксплуатационную среду** для работ. Ограниченные испытания обеспечивают уровень понимания мер обеспечения безопасности и приватности, необходимый для того, чтобы определить, реализованы ли меры обеспечения и свободны ли от очевидных ошибок **и увеличена ли основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено**.
  - Полные испытания: Методология испытаний (также известная как *испытание методом "белого ящика"*), которая предполагает **подробные и значительные** знания внутренней структуры и деталей реализации объекта оценки. Этот тип испытаний проводится с использованием функциональной спецификации, **обширной** информации по архитектуре системы (например, проект высокого уровня, **проект низкого уровня) и представления реализации (например, исходный код, схемотехника)** для механизмов и высокоуровневых описаний процедур и **подробного**

[44] Испытания, как правило, используются, чтобы определить, выполняют ли механизмы или работы ряд предопределенных спецификаций. Испытания могут быть также выполнены, чтобы определить характеристики мер обеспечения безопасности или приватности, которые обычно не связаны с предопределенными спецификациями, примером такого тестирования, является тестирование на возможность проникновения. Руководства для проведения тестирования на возможность проникновения представлены в Приложении E.

описания интеграции в эксплуатационную среду для работ. Полные испытания обеспечивают уровень понимания мер обеспечения безопасности и приватности, необходимый для того, чтобы определить, реализованы ли меры обеспечения и свободны ли от очевидных ошибок и увеличена ли **ещё более** основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено **на непрерывной и непротиворечивой основе, и что есть поддержка для постоянного совершенствования эффективности мер обеспечения**.

- Атрибут *покрытие* определяет область или объём процесса испытаний и включает типы объектов оценки, которые должны быть испытаны, число объектов, которые будут испытаны (в типе) и конкретные объекты, которые будут испытаны.[45] Есть три возможных значения для атрибута покрытия: (i) *основное*; (ii) *ограниченное*; и (iii) *полное*.

  - Основные испытания: Испытания, которые используют репрезентативную выборку объектов оценки (по типам и числу в типе), чтобы обеспечить уровень покрытия, необходимый для того, чтобы определить, реализованы ли меры обеспечения безопасности и приватности и свободны ли от очевидных ошибок.
  - Ограниченные испытания: Испытания, которые используют репрезентативную выборку объектов оценки (по типам и числу в типе) **и другие специфические объекты оценки, которые считаются особенно важными для достижения цели оценки**, чтобы обеспечить уровень покрытия, необходимый для того, чтобы определить, реализованы ли меры обеспечения безопасности и приватности и свободны ли от очевидных ошибок **и увеличена ли основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено**.
  - Полные испытания: Испытания, которые используют **достаточно большую выборку** объектов оценки (по типам и числу в типе) и другие специфические объекты оценки, которые считаются особенно важными для достижения цели оценки, чтобы обеспечить уровень покрытия, необходимый для того, чтобы определить, реализованы ли меры обеспечения безопасности и приватности и свободны ли от очевидных ошибок и увеличена ли **ещё более** основа для уверенности, что меры обеспечения реализованы правильно и работают как предназначено **на непрерывной и непротиворечивой основе, и что есть поддержка для постоянного совершенствования эффективности мер обеспечения**.

[45] Организация, рассматривая различные факторы (например, доступные ресурсы, важность оценки, полные цели и объекты оценки для организации), обсуждает с оценщиками и определяет направление по типам, числу и конкретным объектам, которые будут испытаны для конкретного значения характеризуемого атрибута. Для испытаний, связанных с механизмами, атрибут покрытия также определяет степень проводимых испытаний (например, для программного обеспечения, число тестов и тестируемых модулей; для аппаратных средств, диапазон входных значений, число испытываемых компонентов и диапазон факторов окружающей среды, при которых проводятся испытания).

ПРИЛОЖЕНИЕ E

ТЕСТИРОВАНИЕ ПРОНИКНОВЕНИЯ

ИНСТРУМЕНТЫ И ТЕХНОЛОГИИ ОЦЕНКИ ПО ОПРЕДЕЛЕНИЮ СЛАБЫХ МЕСТ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Организации могут рассмотреть дополнительное контролируемое тестирование на возможность проникновения (тестирование проникновения) в арсенале их инструментов и технологий, используемых для оценки мер обеспечения безопасности и приватности в информационных системах организаций. Тестирование проникновения - определённый тип оценки, в котором оценщики моделируют действия нарушителя некоторого класса при использовании определённого набора документации (то есть, образца той документации, которой нарушитель этот класса будет, возможно, обладать), и работе с другими конкретными ограничениями, чтобы попытаться обойти возможности информационной системы по безопасности или приватности. Тестирование проникновения проводится как контролируемая попытка нарушить меры обеспечения безопасности и приватности, используемые в информационной системе, используя технологии нарушителя и соответствующие аппаратные и программные инструменты. Результаты тестирование проникновения представляются конкретному оценщику или группе оценщиков в конкретный момент времени, используя согласованные *правила воздействия*. Учитывая сложность информационных технологий обычно используемых сегодня организациями, тестирование проникновения может быть рассмотрено не как средство проверки возможностей информационной системы по безопасности или приватности, а скорее как средство для: (i) улучшения понимание системы организацией; (ii) выявления слабых мест или недостатков в системе; и (iii) определения уровня усилий, требуемых со стороны противников, для нарушения мер защиты системы.

Использование тестирования проникновения, может быть регулярным и/или случайным в соответствии с политикой организации и оценками риска организации. Внимание по выполнению тестов проникновения может быть уделено: (i) к любой недавно разработанной информационной системе (или к унаследованной системе, подвергающейся значительному обновлению) прежде, чем система будет санкционирована для применения; (ii) после произведения важных изменений в среде, в которой работает информационная система; и (iii) когда обнаружен новый тип атаки, которая может воздействовать на систему. Организации активно контролируют среду информационных систем и среду угроз (например, новые уязвимости, технологии атак, новые технологии развёртывания, обучения и освоения безопасности и приватности пользователями) чтобы определять изменения, которые требуют внеочередного тестирования проникновения.

Организации определяют, какие компоненты в информационной системе являются предметом тестирования проникновения и профиль нарушителя, который будет принят для использования при тестировании проникновения. Организации обучают выбранный персонал по использованию и поддержке инструментов и технологий тестирования проникновения. Эффективные инструменты тестирования проникновения имеют возможность легко обновлять список технологий атак и годных для использования уязвимостей, используемых при применении. Организации обновляют список технологий атак и годных для использования уязвимостей, применяемых при тестировании проникновения, основываясь на оценке риска организации или когда определены и сообщены существенно новые уязвимости или угрозы. Когда это возможно, организации используют инструменты и технологии атак, которые включают возможности проведения тестирования проникновения, имеющиеся в информационных системах, и меры обеспечения безопасности и приватности в автоматизированном способе.[46]

Информацией, полученной из процесса тестирования проникновения, можно поделиться с соответствующим персоналом организации, чтобы помочь расположить по приоритетам уязвимости в

[46] Хотя автоматизированные инструменты тестирования проникновения обеспечивают повторяемые результаты и уменьшают используемые ресурсы, организации тщательно рассматривают потенциальный вредный эффект автоматизированных воздействий на доступность систем, когда применяются автоматизированные инструменты тестирования проникновения. Кроме того, тестирование проникновения, основанное исключительно на автоматизированных инструментах, может не обеспечить уровень предпринятой компрометации систем, которую организации могли бы испытать от фактического нарушителя.

информационной системе, которые очевидно являются предметом компрометации нарушителем принятого профиля, эквивалентного тому, который используется в применяемом тестировании проникновения. Назначение приоритетов помогает определить эффективные стратегии по устранению установленных уязвимостей и смягчению связанных рисков к деятельности и активам организации, людям, к другим организациям и Нации, следующим из эксплуатации и использования информационной системы. Тестирование проникновения может быть интегрировано в процесс тестирования сетевой безопасности и процесс управления обновлениями и уязвимостями. Специальная публикация 800-40 даёт представление об управлении обновлениями и уязвимостями. Специальная публикация 800-115 даёт представление об испытаниях сетевой и информационной безопасности.

Рассмотрения тестирования проникновения

Организации рассматривают следующие критерии в разработке и реализации программы контролируемого тестирования проникновения. Эффективный тест на проникновение:

- Идёт дальше сканирования уязвимостей, чтобы предоставить явное и часто яркое подтверждение рисков для предназначения и является индикатором уровня усилий, которые должен был бы приложить противник, чтобы нанести ущерб деятельности и активам организации, людям, другим организациям или Нации;
- Подходит к информационной системе при тестировании как противник, рассматривая уязвимости, неправильные системные конфигурации, доверенные отношения между организациями и структурные слабые места в среде;
- Имеет ясно определённую область и содержит, как минимум:

  - определение среды предмета тестирования (например, средства, пользователи, группы организации);

  - определение атакуемой области, которая должна быть протестирована (например, серверы, настольные системы, беспроводные сети, Веб-приложения, системы обнаружения и предотвращения вторжений, межсетевые экраны, почтовые ящики, состояние освоения и обучение безопасности пользователями, состояние реакции на инциденты);

  - определение источников угроз для моделирования (например, перечисление используемых профилей нарушителя: внутренний нарушитель, случайный нарушитель, один или группа внешних целенаправленных нарушителей, преступная организация);

  - определение целей для моделируемого нарушителя (например, получение доступа доменного администратора к структуре LDAP организации (упрощённый протокол доступа к каталогам), доступ и изменение информации в финансовой системе организации);

  - определение уровня расходуемых усилий (время и ресурсы); и

  - определение правил воздействия.

- Полностью документирует все действия, производимые во время тестирования, включая все использованные уязвимости и как уязвимости были объединены в атаки;
- Получает результаты, указывающие на вероятность инцидента для данного нарушителя при использовании уровня усилий команды, которые необходимо израсходовать для проникновения в информационную систему, как индикатор сопротивления проникновению в систему;
- Проверяет существующие меры обеспечения безопасности и приватности (включая механизмы уменьшения риска, такие как межсетевые экраны, системы обнаружение и предотвращения вторжений);
- Обеспечивает проверяемый и восстанавливаемый журнал регистрации всех действий, выполненных во время тестирования; и
- Предоставляет доказательные результаты с информацией о возможных мерах по устранению для проведенных успешных атак.

ПРИЛОЖЕНИЕ F

ПРОЦЕДУРЫ ОЦЕНКИ БЕЗОПАСНОСТИ

ЦЕЛИ, МЕТОДЫ И ОБЪЕКТЫ ДЛЯ ОЦЕНКИ МЕР БЕЗОПАСНОСТИ

Это приложение представляет, каталог процедур по оценке мер безопасности и улучшений мер из Специальной публикации 800-53.[47] Оценщики выбирают процедуры оценки из каталога в соответствии с руководством, представленным в Разделе 3.2. Так как содержание плана обеспечения безопасности влияет на разработку плана оценки безопасности и оценки, то, вероятно, будут процедуры оценки в каталоге, которые оценщики не будут использовать потому, что: (i) связанные меры безопасности или улучшения мер не содержатся в плане обеспечения безопасности для информационной системы;[48] или (ii) меры безопасности или улучшения мер не оцениваются в определённое время.

Цели оценки пронумерованы последовательно, сначала в соответствии с системой нумерации в Специальной публикации 800-53, а затем, где необходимо, чтобы дальше разделить требования мер обеспечения безопасности или приватности для облегчения оценки, используются последовательные числа или буквы, которые, чтобы сделать различие, **заключены в квадратные скобки** в противоположность круглым скобкам (например, CP-9(a), CP-9(a)[1], CP-9(a)[2] и т.д.). Начальный заключённый в квадратные скобки символ всегда число. Для некоторых мер безопасности столбец с начальным обозначением меры обеспечения (например, CP-9, CP-9(a)) является просто заполнителем, чтобы помочь облегчить распределение мер безопасности, поддерживая систему форматирования. Если явно не указано, для каждого идентифицированного метода оценки в процедуре оценки, значения атрибутов *глубины* и *покрытия*, описанных в Приложении D, назначаются организацией и применяются оценщиком или командой оценки при выполнении метода оценки в отношении объекта оценки.

Если у меры безопасности есть какие-либо улучшения (что определяется последовательными числами в круглых скобках, например, CP-9(3) для третьего улучшения для CP-9), цели оценки нумеруются последовательно таким же образом, как процедура оценки по основной мере безопасности, сначала в соответствии с системой нумерации в Специальной публикации 800-53, и затем, используя заключённые в квадратные скобки последовательные числа или буквы, чтобы далее распределить требования улучшения мер обеспечения (например, CP 9-(3)[1], CP-9(3)[2]).

Один и тот же объект оценки может появиться во многих списках объектов в различных процедурах оценки. Один и тот же объект, может использоваться во многих контекстах, чтобы получить необходимую информацию или свидетельство для определённого аспекта оценки. Оценщики используют, когда это соответствующе, основные ссылки для получения необходимой информации, чтобы сделать конкретные определения, требуемые целью оценки. Например, ссылка на политику контроля доступа появляется в процедурах оценки по AC-2 и AC-7. Для процедуры оценки AC-2, оценщики используют политику контроля доступа, чтобы найти информацию о той части политики, которая определяет управление учётной информацией для информационной системы. Для процедуры

[47] В случае любых различий между целями оценки, определёнными для того, чтобы оценить меры безопасности, и базовыми значениями, выраженными описаниями мер безопасности, определёнными в новой версии Специальной Публикации 800-53, Специальная Публикация 800-53 остаётся определяющим выражением мер обеспечения или улучшений.

[48] Выполнение RMF включает выбор начального набора мер безопасности, используемого в или наследуемого информационной системой организации, следующего из процесса *адаптации* мер безопасности. Процесс адаптации, вероятно, будет изменять набор мер безопасности, которые будут включаться в заключительный план обеспечения безопасности. Поэтому, выбор процедур оценки из каталога доступных процедур базируется исключительно на контенте плана обеспечения безопасности после того, как работы адаптации завершены.

оценки AC-7, оценщики используют политику контроля доступа, чтобы найти информацию о той части политики, которая определяет неудачные попытки входа в систему для информационной системы.

Оценщики ответственны за объединение и консолидацию процедур оценки, когда это является возможным или практичным. Оптимизация процедур оценки может сэкономить время, уменьшить стоимость оценки и максимизировать полноценность результатов оценки. Оценщики оптимизируют процедуры оценки, определяя лучшее упорядочивание процедур. Оценка некоторых мер безопасности перед другими может предоставить информацию, которая облегчает понимание и оценку других мер безопасности.

СОВЕТЫ ПО РЕАЛИЗАЦИИ

СОВЕТ #1: Выбирайте только те процедуры оценки из Приложения F, которые соответствуют мерам безопасности и улучшениям мер в *одобренном плане обеспечения безопасности* и которые должны быть включены в оценку.

СОВЕТ #2: процедуры оценки, выбранные из Приложения F, являются только *примерами* процедур, которые служат начальной точкой для организаций, готовящихся к оценкам. Эти процедуры оценки адаптируются по мере необходимости, в соответствии с руководством в Разделе 3.2, чтобы адаптировать процедуры к конкретным требованиям и операционным средам организации.

СОВЕТ #3: Относительно *процедур оценки* в Приложении F оценщики должны применить только те процедуры, методы и объекты, которые необходимы для того, чтобы сделать заключительное определение, что конкретная цель мер безопасности удовлетворена или не удовлетворена (см. Раздел 3.3).

СОВЕТ #4: Оценщики применяют к каждому методу оценки, значения для глубины и покрытия (описанные в Приложении D), которые соразмерны с характеристиками информационной системы (включая требования доверия) и конкретные действия по оценке, которые поддерживают получение определения эффективности рассматриваемых мер безопасности. Значения, выбранные для атрибутов глубины и покрытия, указывают на относительное усилие, требуемое в применении метода оценки к объекту оценки (то есть, строгость и область работ, связанных с оценкой). Атрибуты глубины и покрытия, пока это как не повторено в каждой процедуре оценки в этом приложении, могут быть представлены следующим образом:

Опрос: [*НАЗНАЧЬТЕ ЗНАЧЕНИЯ АТРИБУТА:* <глубина>, <покрытие>].

[*ВЫБЕРИТЕ ИЗ:* Персонал организации с обязанностями по планированию на случай непредвиденных ситуаций и реализации плана].

СОВЕТ #5: Оценщики могут счесть полезной связанную с оценкой информацию в Дополнительном разделе Руководства каждой меры безопасности, описанной в Специальной Публикации 800-53. Эта информация может использоваться, чтобы выполнить более эффективные оценки с приложением процедур оценки.

Примечание: когда оценивается соответствие агентства руководству NIST, аудиторы, Генеральные Инспектора, эксперты и/или оценщики рассматривают замысел концепций безопасности и принципов связанным с определённым руководящим документом и тем, как агентство применяет руководство в контексте его конкретных обязанностей по предназначению, эксплуатационных сред и конкретных условий организации.

ПРЕДОСТЕРЕЖЕНИЕ

Несмотря на то, что набор ***потенциальных методов оценки*** включён в следующий каталог процедур оценки, это не подразумевает их обязательность или исключительность. В зависимости от определённых условий оцениваемой информационной системы или организации, могут требоваться не все методы или могут быть также использованы другие методы оценки. Кроме того, набор ***потенциальных объектов оценки***, перечисленных в каталоге, не предназначен, чтобы быть обязательным, а скорее это набор, из которого необходимый и достаточный набор объектов для данной оценки может быть выбран, чтобы сделать соответствующие определения.

Каталог процедур оценки мер безопасности представлен на страницах F-4…F-411 NIST Special Publication 800-53A Revision 4.

ПРИЛОЖЕНИЕ G

ОТЧЁТЫ ОБ ОЦЕНКЕ

ДОКУМЕНТИРОВАНИЕ РЕЗУЛЬТАТОВ ОЦЕНКИ МЕР ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И ПРИВАТНОСТИ

Главное назначение *отчётов об оценке безопасности и приватности* состоит в предоставлении результатов оценки мер обеспечения безопасности и приватности соответствующим должностным лицам организации. Отчёт об оценке безопасности включён в пакет санкционирования безопасности наряду с планом обеспечения безопасности (включая обновлённую оценку степени риска) и планом действий и вех для предоставления санкционирующим должностным лицам информации, необходимой, чтобы принять основанные на риске решения о том, принять ли информационную систему в эксплуатацию или продолжить её эксплуатацию. Организации могут также включать подобные материалы, связанные с приватностью, в пакет санкционирования, чтобы передать важную информацию санкционирующим должностным лицам. Все проблемы связанные с соответствием со связанным с приватностью законодательством, директивами, нормативными актами или политиками координируются с Высшим должностным лицом агентства по приватности (SAOP)/Директором по приватности.[49] По мере того, как оценка и процесс санкционирования становятся в реальности более динамичными, основанными в большой степени на аспектах непрерывного мониторинга процесса как интегрированная и сильно связанная часть жизненного цикла разработки систем, возможность обновить доклады об оценке безопасности и приватности часто становится критическим аспектом программ информационной безопасности и приватности.

Важно подчеркнуть взаимосвязь, описанную в Специальной публикации 800-37, среди трёх ключевых документов в пакете санкционирования (то есть, плана обеспечения безопасности, отчёта об оценке безопасности и плана действий и вех). Именно эти документы обеспечивают самое надёжное показание относительно полного состояния безопасности информационной системы и возможностей системы защитить до необходимой степени деятельность и активы организации, людей, другие организации и Нацию. Обновления к этим ключевым документам должны обеспечиваться на непрерывной основе в соответствии с программой непрерывного мониторинга, установленной организацией. Обновления к подобным документам, связанным с приватностью, происходят с частотой и форматом, определёнными SAOP в координации с санкционирующими должностными лицами.

Доклады об оценке безопасности и приватности обеспечивают упорядоченный и структурированный подход для документирования результатов оценщика и рекомендаций по исправлению любых слабых мест или недостатков в мерах обеспечения безопасности и приватности.[50] Это приложение предоставляет шаблон для сообщения о результатах оценок мер обеспечения безопасности и приватности. Организации не ограничены конкретным форматом шаблона; однако, ожидается, что полный отчёт об оценке будет включать в себя информацию, подобную представленной в шаблоне для каждой оценённой меры обеспечения безопасности и приватности, которая предшествует сводке, представляющей перечень всех оценённых мер обеспечения безопасности и приватности и полный статус каждой меры.

[49] В соответствии с политикой Министерства управления и бюджета (OMB), оценка соответствия с применимыми мерами обеспечения приватности приложения J, должна быть проведена Высшим должностным лицом агентства по приватности (SAOP) или уполномоченным представителем SAOP. Санкционирование SAOP требуется как *предварительное условие* для выпуска санкционирования на эксплуатацию. У организаций есть гибкость, чтобы определить соответствующий процесс для санкционирования SAOP.

[50] В то время как обоснование для каждого определения, сделанного как часть формальных *Отчётов об оценке безопасности* и *приватности*, полный набор записей, полученных как часть оценки, вероятно, не включается в отчёт. Однако, организации сохраняют часть этих записей, необходимых для того, чтобы сопроводить журнал аудита свидетельства оценки, облегчая повторное использование свидетельства и способствуя воспроизводимости действий оценщика.

Основные элементы для создания отчёта об оценке

Следующие элементы включаются в отчёты об оценке безопасности и приватности:[51]

- Название информационной системы;
- Категорирование безопасности;
- Оценённый объект (ы) информатизации и дата (ы) оценки;
- Имя/идентификация оценщика;
- Результаты предыдущих оценок (если снова использовались);
- Указатель мер обеспечения безопасности/приватности или улучшений мер обеспечения;
- Выбранные методы и объекты оценки;
- Значения атрибутов глубины и покрытия;
- Сводка выводов оценки (указание на удовлетворительные или другие, чем удовлетворительные);
- Комментарии оценщика (слабые места или отмеченные недостатки); и
- Рекомендации оценщика (приоритеты, устранение, корректирующие действия или улучшения).

Результаты Оценки

Каждое описание определения, выполненное оценщиком, имеет результатом один из следующих выводов: (i) удовлетворительно (S); или (ii) другое, чем удовлетворительно (O). Рассмотрите следующий пример для меры безопасности CP-2(3). Инспектор выполняет процедуру оценки по CP-2(3) и получает следующие результаты:

<table>
<tr><th>CP-3</th><th colspan="3">ОБУЧЕНИЕ ДЕЙСТВИЯМ В НЕПРЕДВИДЕННЫХ СИТУАЦИЯХ</th></tr>
<tr><td rowspan="7"></td><td colspan="3">ЦЕЛЬ ОЦЕНКИ:
Определите, предоставляет ли организация обучение действиям в непредвиденных ситуациях пользователям информационной системы в соответствии с установленными ролями и обязанностями:</td></tr>
<tr><td rowspan="2">CP-3(a)</td><td>CP-3(a)[1]</td><td>в пределах определённого организацией периода времени для установленных ролей или ответственности по действиям в непредвиденных ситуациях; (S)</td></tr>
<tr><td>CP-3(a)[2]</td><td>определяет период времени, в пределах которого должно быть проведено обучение действиям в непредвиденных ситуациях пользователей информационной системы с установленными ролями или ответственностью по действиям непредвиденных ситуациях; (S)</td></tr>
<tr><td>CP-3(b)</td><td colspan="2">когда требуется при изменении информационной системы; (O)</td></tr>
<tr><td rowspan="2">CP-3(c)</td><td>CP-3(c)[1]</td><td>впоследствии, в соответствии с определённой организацией частотой; (S)</td></tr>
<tr><td>CP-3(c)[2]</td><td>определяет частоту для обучения действиям в непредвиденных ситуациях. (S)</td></tr>
<tr><td colspan="3">КОММЕНТАРИИ И РЕКОМЕНДАЦИИ:
CP 3 (b) отмечен как другое, чем удовлетворено, потому что оценщики не смогли найти свидетельство того, что организация предоставляла пользователям информационной системы обучение действиям в непредвиденных ситуациях , в соответствии с их установленными ролями и обязанностями, когда произошли существенные изменения в системе.</td></tr>
</table>

Во время фактической оценки мер обеспечения безопасности и приватности выводы по оценке, комментарии и рекомендации документируются в соответствующих, определённых организацией,

[51] Информация доступная в других ключевых документах организации (например, планы обеспечения безопасности или приватности, оценки степени риска, планы действий и вех, или планы оценки безопасности или приватности), не должна дублироваться в отчётах об оценке безопасности и приватности.

формах создания отчётов. Организации поощрены разработать стандартные шаблоны для отчётов, которые содержат основные элементы для создания отчётов об оценке, описанные выше. Когда это возможно, используется автоматизация, чтобы сделать сбор данных оценки и создание отчётов рентабельными, своевременными и эффективными.

ПРИЛОЖЕНИЕ H

ПРИМЕРЫ ОЦЕНКИ

ОБРАБОТАННЫЕ ПРИМЕРЫ ДЕЙСТВИЙ ОЦЕНЩИКА, ПРОЛУЧЕННЫЕ ИЗ ПРОЦЕДУР ОЦЕНКИ

ПРЕКРАЩЕНИЕ ПРОЕКТА ПРИМЕРОВ ОЦЕНКИ

NIST инициировал *Проект разработки примеров оценки* в октябре 2007 в совместном партнёрстве с Министерствами юстиции, Энергетики, Перевозок и Разведывательным ведомством. Межведомственная экспертная группа разрабатывала полный комплект примеров оценки, основанных на процедурах оценки в Специальной публикации 800-53A, Версия 1. Дальнейшего развития примеров оценки, в связи с публикацией Специальной публикации 800-53A, Версия 4, не требуется. Все ранее разработанные примеры оценки будут продолжать быть доступными и могут быть загружены с вебсайта NIST из http://csrc.nist.gov/sec-cert. Материал, содержавшийся в Приложении H, включая шаблоны образцов для разработки примеров оценки, также будет доступным в архивных версиях Специальной публикации 800-53A, Версия 1.

ПРИЛОЖЕНИЕ I

ТЕКУЩАЯ ОЦЕНКА И АВТОМАТИЗАЦИЯ

ИСПОЛЬЗОВАНИЕ АВТОМАТИЗИРОВАННЫХ ТЕХНОЛОГИЙ ДЛЯ ДОСТИЖЕНИЯ БОЛЕЕ ЭФФЕКТИВНЫХ ОЦЕНОК

Текущая оценка безопасности это непрерывная оценка эффективности реализации мер безопасности.[52] Она является существенным подмножеством действий по *Непрерывному мониторингу информационной безопасности* (ISCM).[53] Текущая оценка охватывает Шаги 3 и 4 ISCM и начинается как часть Шага 3 ISCM, *Реализация*, когда сбор информации, связанной с безопасностью, начинается в соответствии с определённой организацией частотой. Текущая оценка, продолжающаяся по мере порождения связанной с безопасностью информации, как части Шага 3 ISCM, коррелируется, анализируется и докладывается высшим руководителям, как часть Шага 4 ISCM. Как отмечено в Специальной публикации 800-137, связанная с безопасностью информация порождается, коррелируется, анализируется и докладывается с использованием автоматизированных инструментов до такой степени, как это возможно и практично, чтобы делать так. Когда не возможно и не практично использовать автоматизированные инструменты, связанная с безопасностью информация порождается, коррелируется, анализируется и докладывается с использованием ручных или процедурных методов. Таким образом, высшим руководителям предоставляют связанную с безопасностью информацию, необходимую, чтобы принять верные, основанные на риске решения относительно рисков информационной безопасности для назначения/деятельности.[54]

Автоматизация оценок является фундаментальным элементом в помощи организациям по управлению рисками информационной безопасности. Развивающиеся угрозы создают проблему для организаций, которые проектируют, реализуют и управляют сложными информационными системами, которые содержат много компонентов аппаратных средств, встроенного микропрограммного обеспечения и программного обеспечения. Возможность оценивать все реализованные меры безопасности так часто как необходимо с использованием ручных или процедурных методов стала непрактичной для большинства организаций вследствие размера, сложности и области инфраструктур их информационных технологий.

Одна из стратегий по увеличению числа мер безопасности, для которых оценка/мониторинг могут быть автоматизированы, зависит от определения *спецификации требуемого состояния* и выражения требуемого состояния в той форме, которая может быть автоматически сравнена с реальным положением. Требуемое состояние – это определённая величина или *спецификация*, с которой может быть сравнено значение реального положения. Несоответствие двух величин указывает на то, что имеются недостатки в эффективности одной или более мер безопасности. Например, политика организации может заявлять, что учётные записи пользователя будут заблокированы после трёх неудачных попыток входа в систему. Спецификация требуемого состояния должна быть в конфигурации применимых устройств таким образом, чтобы заблокировать учётные записи после трёх неудачных попыток входа в систему. Если во время автоматизированной оценки собранная относящаяся к безопасности информация указывает, что конкретное устройство сконфигурировано так, что учётные записи блокируются только после *пяти* неудачных попыток входа в систему, то выявлено несоответствие между требуемым состоянием (три попытки, позволенные перед блокировкой) и реальным положением (пять попыток, позволенных перед блокировкой). Это несоответствие может отражать проблему с эффективностью мер безопасности Специальной публикации 800-53 AC-7, Неудачные попытки входа в систему, AC-2, Управление доступом и УК-2, Базовая конфигурация. Когда такая стратегия используется, связанная с безопасностью информация, сгенерированная по работам ISCM, эквивалентна результатам оценки мер безопасности.

[52] Концепции и технологии, используемые организациями для текущей оценки мер безопасности, могут также быть эффективно использованы для текущей оценки мер обеспечения приватности.

[53] Специальная Публикация 800-137 дает представление о Непрерывном мониторинге информационной безопасности.

[54] Непрерывный мониторинг может быть эффективно применен к мерам обеспечения приватности, в соответствии с концепциями, технологиями и принципами, описанными в Специальной публикации 800-137. Высшие должностные лица агентства по приватности (SAOPs) / Директора по приватности (CPOs) обеспечиваю руководство по текущему мониторингу мер приватности.

Чтобы эффективно автоматизировать оценки меры безопасности, используя стратегию спецификации требуемого состояния, важно выполнить следующие предпосылки:

- Определить автоматизированные спецификации реального состояния/поведения;
- Определить основанные на данных спецификации требуемого состояния (сопоставляемого с реальным состоянием); и
- Определить метод вычисления/определения недостатков (различий между требуемым и реальным состоянием /поведением).

Когда предпосылки выполнены, система оценки может автоматически вычислить, где имеются различия между требуемым состоянием и реальным состоянием (недостатки) и использовать эту информацию для создания отчётов об оценке безопасности и представления этих отчётов назначенному персоналу через консоль управления безопасностью (инструментальная панель).

Когда используются автоматизированные инструменты для проведения оценки, используется *тестовый* метод оценки.[55] Организация определяет и документирует: (i) конкретные возможности[56] или меры безопасности, которые оцениваются автоматизированным инструментом; (ii) частоту, с которой инструмент будет оценивать возможности или меры; и (iii) требования к анализу и отчётности для возможностей или мер обеспечения.

Чтобы помочь автоматизировать текущую оценку, NIST и Департамент безопасности отечества (DHS) взаимодействовали для разработки процесса, который совершенствует *тестовый* метод оценки и гарантирует, что процесс непротиворечив с Основами управления рисками, которые описаны в Специальной публикации 800-37 и руководстве по ISCM в Специальной публикации 800-137. Автоматизация метода испытаний для оценки безопасности продвигается в форме нового сервиса от DHS, известного как программа Непрерывной диагностики и смягчения (CDM).

Переход от ручных к автоматизированным оценкам требует времени для реализации системы сбора данных, чтобы поддержать автоматизированные оценки, и консоли управления безопасностью, чтобы представить результаты оценки. Он также требует времени и усилий по изменению и обновлению процесса оценки. Больше информации относительно автоматизации поддержки для текущих оценок и тому, как DHS программа CDM облегчает текущую оценку, представлено в проекте Межведомственного отчёта NIST 8011, *Автоматизация поддержки для текущей оценки* (планируется к публикации в FY2015).

[55] Если необходимы большие глубина и покрытие, чтобы обеспечить дополнительное доверие, автоматизированный метод испытаний может быть усилен при помощи ручных/процедурных методов оценки (то есть, опросов, исследований или ручных испытаний).

[56] Если определены возможности безопасности, документируется отображение всех отдельных мер, которые поддерживают возможности. Если организации определяют множественные возможности, следует ожидать отношений "многие многим" между мерами безопасности и возможностями. См. Раздел 3.5 для дополнительной информации относительно оценок возможностей безопасности.

ПРИЛОЖЕНИЕ J

ПРОЦЕДУРЫ ОЦЕНКИ ПРИВАТНОСТИ

ЦЕЛИ, МЕТОДЫ И ОБЪЕКТЫ ДЛЯ ОЦЕНКИ МЕР ОБЕСПЕЧЕНИЯ ПРИВАТНОСТИ

БУДУЩЕЕ МЕСТО ПРОЦЕДУР ОЦЕНКИ МЕР ОБЕСПЕЧЕНИЯ ПРИВАТНОСТИ

NIST, в кооперации и сотрудничестве с Подкомиссией лучших практик Директора по информации (CIO) Совета Комитета по приватности, инициировал межведомственное усилие по разработке процедур оценки по мерам обеспечения приватности, содержащихся в Специальной публикации 800-53, Приложение J. Формат для процедур оценки приватности будет подобен формату процедур оценки безопасности в Приложении F. Процедуры оценки и дополнительный материал, который будет включён в это приложение, подвергнутся обширному общему анализу тем же самым способом, которым исследовались меры обеспечения приватности в Специальной Публикации 800-53 до включения в заключительную публикацию. Организации должны консультироваться со своими высшими должностными лицами агентства по приватности/директорами по приватности для руководства по оценке мер обеспечения приватности в Специальной публикации 800-53, Приложении J, до того времени, когда процедуры оценки по Приложению J будут завершены.