| Специальная публикация NIST 800-39 | Управление рисками информационной безопасности |
|---|---|

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

*Представление об организации, предназначении и информационных системах*

**ОБЪЕДИНЁННАЯ ЦЕЛЕВАЯ ГРУППА ПО ИНИЦИАТИВЕ ПРЕОБРАЗОВАНИЯ**

# ИНФОРМАЦИЯ БЕЗОПАСНОСТЬ

Отдела компьютерной безопасности
Лаборатория информационных технологий
Национальный институт стандартов и технологий
Гейтерсбург, MD 20899-8930

***Март 2011***

**Американское Министерство торговли**
*Gary Locke, министр*

**Национальный институт стандартов и технологий**
*Patrick D. Gallagher, директор*

## Отчёты по технологиям компьютерных систем

Лаборатория информационных технологий (ITL) Национального института стандартов и технологий (NIST) содействует развитию экономики и общественного благосостояния США, обеспечивая техническое руководство национальной инфраструктурой измерений и стандартов. ITL разрабатывает тесты, методы испытаний, справочные данные, осуществляет подтверждение реализации концепций и технический анализ для содействия развитию и продуктивному использованию информационных технологий. Обязанности ITL включают разработку управленческих, административных, технических и физических стандартов и руководств для обеспечения экономически эффективной безопасности и приватности информации, не связанной с национальной безопасностью, в федеральных информационных системах. Специальные публикации 800-серии содержат информацию относительно исследований, рекомендаций и усилий ITL в области безопасности информационных систем, и ее совместной деятельности с промышленными, правительственными и научными организациями.

## Полномочия

Эта публикация была разработана NIST в соответствии с его обязанностями, установленными согласно Федеральному закону об управлении информационной безопасностью (FISMA), Общественный закон (P.L). 107-347. NIST отвечает 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 как противоречащее стандартам и руководствам, определёнными 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 не является объектом авторского права в Соединённых Штатах. Однако упоминание приветствовалось бы NIST.

NIST Специальная Публикация 800-39, 88 страниц

**(Март 2011)**

Некоторые коммерческие организации, оборудование или материалы могут быть указаны в этом документе для адекватного описания экспериментальной процедуры или концепции. Такое указание не подразумевает рекомендацию или одобрение со стороны NIST, а также не подразумевает, что эти сущности, материалы или оборудование обязательно являются лучшими из доступных для данной цели.

В этой публикации могут быть ссылки на другие разрабатываемые в настоящий момент публикации 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, если они существуют, остаются в силе. Для целей планирования и перехода федеральные агентства имеют возможность постоянно отслеживать разработку этих новых публикаций NIST.

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

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

## Соответствие стандартам и руководствам NIST

В соответствии с положениями FISMA,[1] министр торговли, на основе стандартов и руководств, разработанных NIST, должен установить стандарты и руководства, относящиеся к федеральным информационным системам. Министр должен сделать стандарты обязательными и предписанными к исполнению в той степени, в которой это будет необходимо для повышения эффективности работы или безопасности федеральных информационных систем. Установленные стандарты должны включать стандарты информационной безопасности, которые обеспечивают минимальные требования информационной безопасности и иначе необходимы для повышения безопасности федеральной информации и информационных систем.

- Федеральные стандарты обработки информации (FIPS) утверждаются Министром торговли и выпускаются NIST в соответствии с FISMA. FIPS обязательны и предписаны для федеральных агентств.[2] FISMA требует, чтобы федеральные агентства выполняли эти стандарты, и, поэтому, агентства не могут отказаться от их использования.
- Специальные Публикации (SPs) разрабатываются и выпускаются NIST в качестве рекомендаций и руководящих документов. Федеральные агентства должны следовать тем Специальным публикациям NIST, которые определены в Федеральных стандартах обработки информации, за исключением программ и систем, относящихся к национальной безопасности. FIPS 200 предписывает использование Специальной публикации 800-53 с вносимыми изменениями. Кроме того, политика OMB (включая Инструкции OMB об отчётности по FISMA и управлению приватностью для Агентств) гласит, что за исключением программ и систем национальной безопасности, федеральные агентства должны следовать определённым Специальным публикациям NIST.[3]
- Другие, связанные с безопасностью публикации, включая межведомственные отчёты (NISTIRs) и Бюллетени ITL, предоставляют техническую и другую информацию о работах NIST. Эти публикации обязательны только тогда, когда это определено OMB.
- Соответствующие календарные планы для стандартов и руководств обеспечения безопасности NIST устанавливаются OMB в политиках, директивах или меморандумах (например, Руководстве по ежегодной отчётности по FISMA).[4]

---

[1] Закон об электронном Правительстве (P.L. 107-347) признаёт важность информационной безопасности для экономики и интересов национальной безопасности Соединённых Штатов. Раздел III закона об электронном Правительстве, названный как Федеральный закон об управлении информационной безопасностью (FISMA), подчёркивает необходимость разработки, документировании и реализации организациями общей для организации программы по обеспечению безопасности информационных систем, поддерживающих её деятельность и активы.

[2] Термин *агентство* используется в этой публикации вместо более общего термина *организация* только в тех случаях, где его использование непосредственно связано с другими исходными документами, такими как федеральное законодательство или политика.

[3] Несмотря на то, что федеральные агентства обязаны в соответствии с политикой OMB следовать некоторым конкретным Специальным публикациям NIST, имеется гибкость в том, как агентства применяют руководство. Федеральные агентства применяют концепции и принципы безопасности, определённые в Специальных публикациях NIST, в соответствии с и в контексте предназначения, функций и условий деятельности агентства. Следовательно, применение руководства NIST федеральными агентствами может привести к различным решениям по обеспечению безопасности, которые одинаково приемлемы, совместимы с руководством и отвечают определению OMB адекватной безопасности для федеральных информационных систем. Учитывая высокий приоритет обмена информацией и прозрачности в рамках федерального правительства, агентства также учитывают совместимость в разработке их решений по информационной безопасности. Оценивая соответствие федерального агентства Специальным публикациям NIST, генеральные инспекторы, эксперты, аудиторы и оценщики систем рассматривают насколько концепции и принципы безопасности ясно сформулированы в соответствии с конкретным руководящим документом и как агентство применяет руководство в контексте его обязанностей по предназначению/деятельности, среды деятельности и конкретных условий организации.

[4] Если не указано иное, все ссылки на публикации NIST в этом документе (т.е., Федеральные стандарты обработки информации и Специальные публикации) относятся к последней версии публикации.

## Благодарность

Эта публикация была разработана *объединённой целевой группой по инициативе преобразования* межведомственной рабочей группы совместно с представителями гражданского, оборонного и разведывательного сообществ в рамках постоянной работы 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***

Teresa M. Takai
*Заместитель Министра обороны по сетям и информационной интеграции / Директор по информации DoD (ВРИО)*

Gus Guissanie
*Второй помощник министра обороны (ВРИО)*

Dominic Cussatt
*Старший советник по политике*

Barbara Fleming
*Старший советник по политике*

***Офис Директора Национальной разведки***

Adolpho Tarasiuk Jr.
*Советник Директора Национальной разведки и разведывательного сообщества, Директор по информации*

Charlene P. Leubecker
*Представитель Разведывательного сообщества, Директор по информации*

Mark J. Morrison
*Директор, Разведывательное сообщество, информационное доверие*

Roger Caslow
*Руководитель, Отдел программ управления рисками и информационной безопасности*

***Национальный институт стандартов и технологий***

Cita M. Furlani
*Директор, Лаборатория информационных технологий*

William C. Barker
*Советник по вопросам кибербезопасности, Лаборатория информационных технологий*

Donna Dodson
*Руководитель, Отдел компьютерной безопасности*

Ron Ross
*Руководитель проекта реализации FISMA*

***Комитет по Системам национальной безопасности***

Teresa M. Takai
*ВРИО Председателя, CNSS*

Eustace D. King
*CNSS Подкомитет, Сопредседатель*

Peter Gouldmann
*CNSS Подкомитет, Сопредседатель*

Lance Dubsky
*CNSS Подкомитет, Сопредседатель*

***Межведомственная рабочая группа Объединенной экспертной группы по инициативе преобразования***

Ron Ross
*NIST, Руководитель JTF*

Deborah Bodeau
*MITRE Корпорация*

Peter Williams
*Booz Allen Hamilton*

Gary Stoneburner
*Johns Hopkins APL*

Cheri Caddy
*Разведывательное сообщество*

Karen Quigg
*MITRE Корпорация*

Jennifer Fabius-Greene
*MITRE Корпорация*

Peter Gouldmann
*Госдепартамент*

Richard Graubart
*MITRE Корпорация*

Kelley Dempsey
*NIST*

Arnold Johnson
*NIST*

Christian Enloe
*NIST*

В дополнение к вышеупомянутым благодарностям, особое спасибо Peggy Himes и Elizabeth Lennon за их превосходное техническое редактирование и административную поддержку и Bennett Hodge, Cassandra Kelly, Marshall Abrams, Marianne Swanson, Patricia Toth, Kevin Stine и Matt Scholl за их ценные соображения и содействие. Авторы также с благодарностью подтверждают и ценят значительное содействие от людей и организаций в государственных и частных секторах, на национальном и международном уровне, чьи вдумчивые и конструктивные комментарии улучшили общее качество, завершённость и полноценность этой публикации.

***РАЗРАБОТКА ОБЩИХ ОСНОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ***

СОТРУДНИЧЕСТВО МЕЖДУ ОРГАНИЗАЦИЯМИ ГОСУДАРСТВЕННОГО И ЧАСТНОГО СЕКТОРА

При разработке стандартов и руководств, требуемых FISMA, NIST консультируется с другими федеральными агентствами и ведомствами, а также с частным сектором, чтобы повысить уровень информационной безопасности, избежать ненужного и дорогостоящего дублирования усилий и обеспечить соответствие публикаций NIST стандартам и руководствам, используемым для защиты систем национальной безопасности. В дополнение к процессу всеобъемлющей общественной экспертизы и проверки, NIST сотрудничает с Офисом Директора национальной разведки (ODNI), Министерством обороны (DoD) и Комитетом по системам национальной безопасности (CNSS) для создания общей основы информационной безопасности в федеральном правительстве. Общая основа информационной безопасности обеспечит разведывательному, оборонному и гражданскому секторам федерального правительства и их подрядчикам более единообразные и непротиворечивыми способы управления рисками для деятельности и активов организации, людей, других организаций и нации, которые возникают в результате эксплуатации и использования информационных систем. Общая основа для информационной безопасности также обеспечит прочную основу для взаимного принятия результатов оценки безопасности и облегчит обмен информацией. NIST также работает с организациями общественного и частного сектора для установления сопоставления и взаимосвязей между стандартами и руководствами по безопасности, разработанными NIST и Международной организацией по стандартизации (ISO) и Международной электротехнической комиссией (IEC).

***ПРЕДОСТЕРЕЖЕНИЕ***

ПРЕДНАЗНАЧЕННАЯ ОБЛАСТЬ ПРИМЕНЕНИЯ И ИСПОЛЬЗОВАНИЯ ЭТОЙ ПУБЛИКАЦИИ

Руководство, представленное в этой публикации, предназначено, ***только*** для управления рисками, связанными с безопасностью информации, возникающими или связанными с эксплуатацией и использованием информационных систем или средой, в которой работают эти системы. Руководство ***не*** предназначено для замены или подмены других связанных с риском мероприятий, программ, процессов или подходов, которые организации реализовали или намереваются реализовать в области управления рисками, охватываемых другим законодательством, директивами, политиками, программными инициативами или требованиями, определяемыми назначением/деятельностью. Скорее, описанное здесь руководство управления рисками информационной безопасности, дополняет и должно использоваться как часть более комплексной программы Управления рисками предприятия (ERM).

## Оглавление

## Пролог

*"... Посредством процесса управления рисками руководители должны учитывать риск для интересов США от противников, использующих киберпространство в своих интересах, и от наших собственных усилий по использованию глобальной природы киберпространства для достижения целей в военных, разведывательных и деловых операциях..."*

*"... Для разработки планов деятельности необходимо оценить сочетание угроз, уязвимостей и воздействий, чтобы выявить важные тенденции и решить, где следует приложить усилие, чтобы устранить или уменьшить возможности угрозы; устранить или уменьшить уязвимости; и оценить, скоординировать и устранить конфликты во всех операциях в киберпространстве..."*

*"... Руководители всех уровней несут ответственность за обеспечение готовности и безопасности в той же степени, как в любой другой сфере..."*

- НАЦИОНАЛЬНАЯ СТРАТЕГИЯ ОПЕРАЦИЙ В КИБЕРПРОСТРАНСТВЕ

ОФИС ПРЕДСЕДАТЕЛЯ, ОБЪЕДИНЕННЫЙ КОМИТЕТ НАЧАЛЬНИКОВ ШТАБОВ, АМЕРИКАНСКОЕ МИНИСТЕРСТВО ОБОРОНЫ

## ГЛАВА ОДИН

# ВВЕДЕНИЕ

НЕОБХОДИМОСТЬ ИНТЕГРИРОВАННОГО УПРАВЛЕНИЯ РИСКАМИ В МАСШТАБАХ ВСЕЙ ОРГАНИЗАЦИИ

**И**нформационные технологии общепризнаны как механизм, который двигает американскую экономику, давая промышленности конкурентное преимущество на мировых рынках, давая возможность федеральному правительству предоставлять лучшие услуги его гражданам и способствуя большим экономическим возможностям страны. Организации[5] в государственных и частных секторах зависят от высокотехнологичных *информационных систем*[6], чтобы успешно выполнять их функции предназначения и деятельности. Информационные системы могут включать разнообразные объекты начиная от высокопроизводительных суперкомпьютеров, рабочих станций, персональных компьютеров, сотовых телефонов и персональных цифровых секретарей до очень специализированных систем (например, систем оружия, телекоммуникационных систем, систем управления производством/процессами и систем экологического контроля). Информационные системы подвергаются серьёзным *угрозам*, которые могут оказывать негативный эффект на деятельность организации (т.е., предназначение, функции, имидж или репутацию), активы организации, людей, другие организации и нацию, используя известные и неизвестные уязвимости, чтобы ставить под угрозу конфиденциальность, целостность или доступность информации, обрабатываемой, хранимой или передаваемой этими системами. Угрозы информации и информационным системам могут включать целенаправленные атаки, экологические разрушения и человеческие/машинные ошибки и приводить к большому вреду национальным и экономическим интересам безопасности Соединённых Штатов. Поэтому необходимо, чтобы руководители и менеджеры на всех уровнях понимали свои обязанности и были определены ответственными за управление рисками информационной безопасности - то есть рисками, связанными с эксплуатацией и использованием информационных систем, которые поддерживают функции предназначение и деятельности их организаций.

Риски организациям могут включать много видов риска (например, риск управления программами, инвестиционный риск, бюджетный риск, риск юридической ответственности, риск защищённости, инвентарный риск, риск цепочки поставок и риск безопасности). Риск безопасности, связанный с деятельностью и использованием информационных систем, является только одним из многих компонентов рисков организации, который высшие руководители/руководители учитывают, как часть их постоянных обязанностей по управлению рисками. Эффективное управление рисками требует, чтобы организации действовали в очень сложной, взаимосвязанной окружающей среде, используя новейшие и устаревшие информационные системы - системы, на которые организации полагаются для достижения их предназначения и выполнения важных функций их деятельности. Руководители должны знать, что необходимо принимать четкие, хорошо обоснованные решения, основанные на рисках, чтобы сбалансировать выгоды, получаемые от эксплуатации и использования этих информационных систем, с риском того, что эти же системы станут средством, с помощью которого целенаправленные атаки, экологические сбои или человеческие ошибки приведут к провалу предназначения или деятельности. Управление рисками информационной безопасности, как и управление рисками в целом, является не точной наукой. Оно объединяет лучшие коллективные суждения людей и групп в организациях, ответственных за стратегическое планирование, надзор, управление и повседневную деятельность, предоставляя необходимые и достаточные меры противодействия рискам для соответствующей защиты функций предназначения и деятельности этих организаций.

---

[5] Термин *организация* описывает сущность любого размера, сложности или положения в организационной структуре (например, федеральное агентство или, если применимо, любой из его операционных элементов), которая определена для выполнения установленных процессов предназначения/деятельности и которая использует информационные системы для поддержки этих процессов.

[6] Информационная система - дискретный набор информационных ресурсов, специально организованных для сбора, обработки, обслуживания, использования, обмена, распространения или ликвидации информации. В контексте этой публикации определение включает среду, в которой функционирует информационная система (т.е., люди, процессы, технологии, средства и киберпространство).

Сложные взаимосвязи между предназначением, процессами предназначения/деятельности и информационными системами, поддерживающими эти предназначения/процессы, требуют интегрированного, общего для всей организации представления по управлению рисками.7 Если не указано иное, указания на риск в этой публикации относятся к риску информационной безопасности от деятельности и использования информационных систем организации, включая процессы, процедуры и структуры в организациях, которые влияют или затрагивают проектирование, разработку, реализацию и последующую эксплуатацию этих систем. Роль информационной безопасности в управлении рисками для деятельности и использования информационных систем также важна по отношению к успеху организаций в достижении их стратегических задач и целей. Исторически, высшие руководители/ руководители имели очень узкое представление об информационной безопасности или как о техническом вопросе или как об ограничении, которые независимы от рисков для организации и традиционных процессов управления и жизненного цикла. Эта чрезвычайно ограниченная точка зрения часто приводила к несоответствующему рассмотрению того, как риски информационной безопасности, также, как и другие риски организации, затрагивает возможность организаций успешно выполнять их функции предназначения и деятельности. Данная публикация рассматривает информационную безопасность в более широком контексте для организаций по достижению успеха в предназначении/ деятельности. Целью является:

- обеспечить, чтобы высшие руководители/руководители поняли важность управления рисками информационной безопасности и создали соответствующие руководящие структуры для управления такими рисками;
- обеспечить, чтобы процесс управления рисками организации эффективно осуществлялся на трех уровнях: организации, процессах предназначения/деятельности и информационных системах;
- способствовать климату в организации, при котором риск информационной безопасности рассматривался бы в контексте проектирования процессов предназначения/деятельности, определения всеобъемлющей архитектуры предприятия и процессов жизненного цикла разработки систем; и
- помочь людям с обязанностями по внедрению или эксплуатации информационных систем лучше понять, как риск информационной безопасности, связанный с их системами, трансформируется в риск для всей организации, который может, в результате, повлиять на успех в предназначении/деятельности.

Для успешного выполнения функций предназначения и деятельности организации, связанными с процессами, зависящими от информационных систем, высшие руководители/руководители должны стремиться сделать управление рисками фундаментальным требованием предназначения/деятельности. Такая приверженность высшего руководства обеспечивает наличие достаточных ресурсов для разработки и внедрения эффективных программ всей организации по управлению рисками. Понимание и устранение рисков является *стратегической* способностью и фактором, *способствующим* выполнению функций предназначения и деятельности в организациях. Эффективное управление рисками информационной безопасности в масштабах всей организации требует наличия следующих ключевых элементов:

- возложение обязанностей по управлению рисками на высших руководителей/руководителей;
- постоянное признание и понимание высшими руководителям/руководителями рисков информационной безопасности для деятельности и активов организации, людей, других организаций и Нации, возникающих при эксплуатации и использования информационных систем;
- установление допустимого риска для организации и доведение допустимого риска по всей организации, включая руководство по тому, как допустимый риск влияет на текущую деятельность по принятию решений;[8] и
- Ответственность высших руководителей/руководителей за их решения по управлению рисками и за реализацию эффективных, общих для организации программ управления рисками.

[7] Агрегирование различных типов риска по всей организации выходит за рамки этой публикации.

[8] Оценка *остаточного риска* (который изменяется со временем) для определения приемлемого риска зависит от порога, установленного организацией для *допустимого риска*.

## 1.1 НАЗНАЧЕНИЕ И ПРИМЕНИМОСТЬ

Специальная Публикация NIST 800-39 является ведущим документом в серии стандартов и руководств по информационной безопасности, разработанных NIST в соответствии с FISMA. Назначение Специальной публикации 800-39 состоит в том, чтобы предоставить руководство по интегрированной, общей для организации программе управления рисками информационной безопасности для деятельности организации (т.е., предназначения, функций, имиджа и репутации), активов организации, людей, других организаций и Нации, следующим из эксплуатации и использования федеральных информационных систем. Специальная публикация 800-39 обеспечивает структурированный, и в тоже время гибкий подход по управлению рисками, который намеренно носит широкий характер, а конкретные детали по оценке, реагированию и мониторингу рисками на непрерывной основе, предоставляются другими, поддерживающими стандартами и руководствами по безопасности NIST. Руководство, представленное в этой публикации, не предназначено, чтобы заменить или подменить связанные с риском мероприятия, программы, процессы или подходы, которые организации внедрили или намереваются внедрить в области управления рисками, охватываемые другим законодательством, директивами, политиками, программными инициативами или требованиями предназначения/ деятельности. Скорее руководство по управлению рисками, представленное здесь, дополняет и должно использоваться в качестве части более комплексной программы Управления рисками предприятия (ERM).

Эта публикация удовлетворяет требованиям FISMA и соответствует или превосходит требования по информационной безопасности, установленные для исполнительных агентств[9] Министерством управления и бюджета (OMB) в Циркуляре A-130, Приложение III, *Безопасность федеральных автоматизированных информационных ресурсов*. Руководящие принципы в этой публикации применимы ко всем федеральным информационным системам кроме тех, которые относятся к системам национальной безопасности, как определено в 44 U.S.C., Раздел 3542. Руководство специально разрабатывались с технической точки зрения, чтобы дополнить аналогичное руководство для систем национальной безопасности и может быть использованы для таких систем с одобрения соответствующих федеральных должностных лиц, осуществляющих политику санкционирования для таких систем. Государственным, местным и племенным органам власти, а также организации частного сектора рекомендуется рассмотреть использование этого руководства в соответствующих случаях.

## 1.2 ЦЕЛЕВАЯ АУДИТОРИЯ

Данная публикация предназначена для различных групп специалистов по управлению рисками, включая:

- Лиц, несущих ответственность за управление рисками (например, руководители агентств, генеральные директора, исполнительные директора);
- Лиц, несущих ответственность за исполнение функций предназначения/деятельности организации (например, владельцы предназначения/деятельности, владельцы/управляющие информацией, санкционирующие должностные лица);
- Лиц, несущих ответственность за приобретение продуктов информационных технологий, услуг или информационных систем (например, должностные лица, ответственные за приобретение, должностные лица по закупкам, сотрудники по заключению контрактов);
- Лиц, несущих ответственность за надзор, управление и эксплуатацию информационной безопасности (например, ИТ-директора, главные директора по информационной безопасности,[10] менеджеры по информационной безопасности, владельцы информационных систем, поставщики общих мер безопасности);

[9] *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 определённое в 5 U.S.C., Раздел 104 (1); и (iv) и полностью находящаяся в собственности Правительства корпорация, полностью попадающая под действие 31 U.S.C., Глава 91. В этой публикации термин *исполнительное агентство* синонимичен с термином *федеральное агентство*.

[10] На уровне *агентства*, эта должность известна как Главный директор по информационной безопасности Агентства. Организации могут также именовать эту позицию как Директор по информационной безопасности.

- Лиц, несущих ответственность за проектирование, разработку и внедрение информационных систем/ безопасности (например, руководители программ, архитекторы предприятия, архитекторы информационной безопасности, инженеры по информационным системам/безопасности; интеграторы информационных систем); и
- Лиц, несущих ответственность за оценку и мониторинг информационной безопасности (например, оценщики систем, испытатели проникновения, оценщики мер безопасности, независимые верификаторы/валидаторы, генеральные инспекторы, аудиторы).

## 1.3 СВЯЗАННЫЕ ПУБЛИКАЦИИ

Подход к управлению рисками, описанный в этой публикации, поддержан серией стандартов и руководств по безопасности, необходимых для управления рисками информационной безопасности. В частности, Специальные публикации, разработанные Объединённой экспертной группой по инициативе преобразования[11], поддерживающие унифицированную основу информационной безопасности для федерального правительства, включают:

- Специальная публикация 800-37, *Руководство для применения основ управления рисками к федеральным информационным системам: Подход на основе жизненного цикла безопасности*;
- Специальная публикация 800-53, *Рекомендуемые меры безопасности для федеральных информационных систем и организаций*;
- Специальная публикация 800-53A, *Руководство по оценке мер безопасности в федеральных информационных системах и организациях*; и
- Проект специальной публикации 800-30, *Руководство по проведению оценок риска*.[12]

В дополнение к упомянутым выше публикациям Объединённой экспертной группы Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC) публикуют стандарты по управлению рисками и информационной безопасности, включая:

- ISO/IEC 31000, *Управление рисками - Принципы и руководства*;
- ISO/IEC 31010, *Управление рисками - Технологии оценки риска*;
- ISO/IEC 27001, *Информационные технологии - Методы безопасности - Системы управления информационной безопасностью - Требования*; и
- ISO/IEC 27005, *Информационные технологии - Методы безопасности - Системы управления рисками информационной безопасности*.

Предназначение NIST включает гармонизацию международных и национальных стандартов в соответствующих случаях. Концепции и принципы, содержавшиеся в этой публикации, предназначены для внедрения в федеральных информационных системах и организациях системы управления информационной безопасностью и процесса управления рисками, подобных описанным в стандартах ISO/IEC. Это уменьшает нагрузку на организации, которые должны соответствовать как стандартам ISO/IEC, так и стандартам и руководствам NIST.

[11] Обзор каждой публикации Объединённой экспертной группы по инициативе преобразования, подобный резюме, может быть получен в соответствующих ITL Бюллетенях безопасности NIST в http://csrc.nist.gov.

[12] Специальная публикация 800-39 заменяют исходную Специальную Публикацию 800-30 в качестве источника для руководства по управлению рисками. Специальная публикация 800-30 пересматривается, с целью представление руководства по оценке рисков в качестве вспомогательного документа к Специальной публикации 800-39.

## 1.4 ОРГАНИЗАЦИЯ ЭТОЙ СПЕЦИАЛЬНОЙ ПУБЛИКАЦИИ

Остаток от этой специальной публикации организован следующим образом:

- **Глава Два** описывает: (i) компоненты управления рисками; (ii) многоуровневый подход к управлению рисками; (iii) управление рисками на уровне организации (Уровень 1); (iv) управление рисками на уровне процесса предназначения/деятельности (Уровень 2); (v) управление рисками на уровне информационной системы (Уровень 3); (vi) риски, имеющие отношение к доверию и доверенности; (vii) влияние культуры организации на риски; и (viii) взаимосвязи между ключевыми концепциями управления рисками.
- **Глава Три** описывает процесс управления рисками информационной безопасности основанный на жизненном цикле, включая: (i) общий обзор процесса управления рисками; (ii) как организации устанавливают контекст для решений, основанных на риске; (iii) как организации оценивают риск; (iv) как организации реагируют на риск; и (v) как организации контролируют риск в течении времени.
- **Поддерживающие приложения** предоставляют дополнительную информацию по управлению рисками, включая: (i) общие ссылки; (ii) термины и определения; (iii) акронимы; (iv) роли и обязанности; (v) задачи процесса управления рисками; (vi) модели управления; (vii) модели доверия; и (viii) стратегии реагирования на риски.

ГЛАВА ДВА

# ОСНОВНЫЕ ПРИНЦИПЫ

ФУНДАМЕНТАЛЬНЫЕ ПОНЯТИЯ, СВЯЗАННЫЕ С УПРАВЛЕНИЕМ РИСКАМИ

Эта глава описывает фундаментальные концепции, связанные с управлением рисками информационной безопасности в организации, включая: (i) компоненты управления рисками; (ii) многоуровневый подход к управлению рисками; (iii) управление рисками на уровне 1 (уровень организации); (iv) управление рисками на уровне 2 (уровень процесса предназначения/деятельности); (v) управление рисками на уровне 3 (уровень информационной системы); (vi) риски, относящиеся к доверию и доверенности; (vii) влияние культуры организации на риски; и (viii) взаимосвязи между ключевыми концепциями управления рисками.

## 2.1 КОМПОНЕНТЫ УПРАВЛЕНИЯ РИСКАМИ

Управление рисками - это сложная, многогранная деятельность, которая требует участия всей организация - от высших руководителей/руководителей, обеспечивающих стратегическое видение и цели и задачи организации на высшем уровне до руководителей среднего уровня, планирующих, выполняющих и управляющим проектами и до сотрудников на переднем крае, эксплуатирующих информационные системы, поддерживающие функции предназначения/деятельности организации. Управление рисками – это комплексный процесс, который требует от организаций: (i) *описание* рисков (т.е., создание контекста для основанных на риске решений); (ii) *оценки* рисков; (iii) *реагирования* на риски, которые определены; и (iv) *мониторинга* рисков на постоянной основе, используя эффективное взаимодействие организаций и обратную связь для непрерывного совершенствования деятельности организаций, связанной с рисками. Управление рисками выполняется как целостная, общая для организации деятельность, которая учитывает риски от стратегического до тактического уровня, обеспечивая интеграцию принятия решений с учетом риска во все аспекты деятельности организации.[13] Следующие разделы кратко описывают каждый из четырёх компонентов управления рисками.

Первый компонент управления рисками определяет, как организации *описывает* риски или устанавливают контекст риска - то есть, описывают среду, в которой принимаются основанные на риске решения. Назначение компонента описания риска состоит в том, чтобы сформировать *стратегию управления* рисками, которая касается того, как организации намерены оценивать риски, реагировать на риски и мониторить риски, делая явными и прозрачными представление о рисках, которое организации обычно используют в выработке инвестиционных и эксплуатационных решений. Описание рисков закладывает основу для управления рисками и устанавливает границы для основанных на риске решений в организациях. Формирование реалистичных и правдоподобных описаний рисков требует, чтобы организации определили: (i) предположения относительно рисков (например, предположений об угрозах, уязвимостях, последствиях/воздействиях и вероятности возникновения, которые касаются того, как риски оценивают, на них реагируют и контролируют в течение времени); (ii) ограничения на риски (например, ограничения на рассмотрение альтернатив по оценке, реагированию и мониторингу риска); (iii) допустимость рисков (например, уровни рисков, типы рисков и степень неопределённости рисков, которая приемлема); и (iv) приоритеты и компромиссы (например, относительная важность функций предназначения/деятельности, компромиссы между различными типами рисков, с которыми организации сталкиваются, периоды времени, в которые организации должны учитывать риски и любые факторы неопределённости, которые организации рассматривают при реагировании на риски). Компонент описания рисков и связанная стратегия управления рисками также включают любые решения стратегического уровня о том, как риски к деятельности и активам организации, людям, другим организациям и нации, должны управляться высшими руководителями/ руководителями.

[13] Комплексное управление рисками всей организации включает, например, рассмотрение: (i) стратегических задач/целей организаций; (ii) необходимой приоритизации функций предназначения/деятельности организаций; (iii) процессы предназначения/деятельности; (iv) архитектур предприятия и информационной безопасности; и (v) процессов жизненного цикла разработки систем.

Второй компонент управления рисками определяет, как организации *оценивают* риски в контексте описанных рисков организаций. Назначение компонента оценки риска состоит в том, чтобы определить: (i) угрозы организациям (т.е., деятельности, активам или людям) или угрозы, направленные через организации против других организаций или нации; (ii) уязвимости, внутренние и внешние к организациям;[14] (iii) ущерб (т.е., последствия/воздействия) организациям, который может иметь место, с учетом возможности использования уязвимостей угрозами; и (iv) вероятность того, что ущерб будет иметь место. Конечный результат - определение риска (т.е., степени ущерба и вероятности появления ущерба). В поддержку компонента оценки степени риска, организации определяют: (i) инструменты, технологии и методологии, которые используются для оценки риска; (ii) предположения, связанные с оценкой риска; (iii) ограничения, которые могут повлиять на оценку риска; (iv) роли и обязанности; (v) то, как информация об оценке риска собирается, обрабатывается и передаётся в организациях; (vi) как оценка риска проводятся в организациях; (vii) частота оценок риска; и (viii) как получается информация об угрозах (т.е., источники и методы).

Третий компонент управления рисками определяет, как организации *реагируют* на риски после того, как риски определены, основываясь на результатах оценки рисков. Назначение компонента реагирования на риски состоит в том, чтобы обеспечить непротиворечивую для всей организации реакцию на риски в соответствии с описанными рисками организации: (i) разработку альтернативных планов действий по реагированию на риски; (ii) оценку альтернативных планов действий; (iii) определение соответствующих планов действий, соответствующих допустимым рискам организации; и (iv) реализацию мер реагирования на риски, основанных на выбранных планах действий. Для поддержки компонента реагирования на риски, организации описывают типы реакций на риски, которые могут быть реализованы (т.е., принятие, предотвращение, снижение, распределение или передачу рисков). Организации также определяют инструменты, технологии и методологии, используемые для разработки планов действий по реагированию на риски, способы оценки планов действий, и способы передачи информации о реагировании на риски в организациях и, при необходимости, внешним организациям (например, внешним поставщикам услуг, партнерам по цепочке поставок).[15]

Четвёртый компонент управления рисками определяет, как организации *мониторят* риски в течение времени. Назначением компонента мониторинга риска является: (i) проверка того, что спланированные меры реагирования на риски реализуются и требования информационной безопасности, вытекающие из/относящиеся к функциям предназначения/деятельности организаций, федеральному законодательству, директивам, нормативным документам, политикам и стандартам, и руководствам выполнены; (ii) определение текущей эффективности мер реагирования на риски после реализации; и (iii) выявление влияющих на риски изменений в информационных системах организаций и среде, в которой системы эксплуатируются.[16] Для поддержки компонента мониторинга риска, организации описывают, как проверяется соответствие требованиям и как определяется текущая эффективность мер реагирования на риски (например, типы инструментов, технологий и методологий, используемых для определения достаточности/корректности мер реагирования на риски и того, правильно ли реализованы меры по снижению рисков, действуют ли они по назначению и дают ли желаемый эффект в отношении снижения рисков). Кроме того, организации описывают, как отслеживаются изменения, которые могут повлиять на текущую эффективность мер реагирования на риски.

[14] Уязвимости организаций не ограничены информационными системами, но могут включать, например, уязвимости в структуре управления, процессах предназначения/деятельности, архитектуре предприятия, архитектуре информационной безопасности, средствах, оборудовании, процессах жизненного цикла разработки систем, работе системы поставок и внешних поставщиков услуг.

[15] Руководство по управлению рисками системы поставок представлены в Межведомственном отчёте NIST 7622.

[16] Среда деятельности включает, но не ограничивается: пространство угроз; уязвимости; функции предназначения/деятельности; процессы предназначения/деятельности; архитектуры предприятия и информационной безопасности; информационные технологии; персонал; средства; взаимосвязи системы поставок; методы управления/специфику организаций; процессы закупок/поставки; политики/процедуры организаций; предположения, ограничения, допустимые риски и приоритеты/компромиссы организаций).

Как указано в четырёх компонентах управления рисками, описанных выше, организации, в зависимости от обстоятельств, также рассматривают внешние взаимосвязи по рискам. Организации определяют внешние организации, с которыми связаны фактические или потенциальные риски (т.е., организации, которые могут навязать риски, передать или сообщить риски в другие организации, а также те организации, которым организации могут навязать, передать или сообщить риски). Внешние взаимосвязи по рискам включают, например, поставщиков, клиентов или обслуживаемое население, партнёров по предназначению/деятельности и/или поставщиков услуг. Для организаций, имеющих дело с постоянно развивающимися угрозами (т.е., долгосрочной схемой целенаправленных, сложных атак), риск, создаваемый внешними партнёрами (особенно поставщикам в цепочке поставок), может стать более явным. Организации устанавливают практику обмена относящейся к рискам информацией (например, информацией об угрозах и уязвимостях) с внешними организациями, включая те, с которыми у организации есть отношения риска, а также те, которые могут предоставить или получить связанную с риском информацию (например, Центры обмена информацией и анализа [ISAC], Группы реагирования на компьютерные инциденты [CERT]).

Рисунок 1 иллюстрирует процесс управления рисками, а также информационные и коммуникационные потоки между компонентами. Черные стрелки представляют *основные* потоки в рамках процесса управления рисками, при этом *описани*е риска обеспечивает информацией все последующие пошаговые действия от *оценки* риска до *реагировани*я на риски и до *мониторинг*а рисков. Например, один из основных результатов компонента описания риска - описание источников и методов, которые организации используют для получения информации об угрозах (например, открытые источники, секретные отчеты разведывательного сообщества). Результаты, относящиеся к информации об угрозах, являются первичным входом к компоненту оценки риска и соответственно передаются в этот компонент. Другой пример иллюстрирует первичный результат компонента оценки риска, то есть, определение риска. Результат компонента оценки риска передаётся к компоненту реагирования на риски и является первичным входом для этого компонента. Другой первичный вход к компоненту реагирования на риски - результат компонента описания риска, стратегия управления рисками, которая определяет, как организация должна реагировать на риски. Вместе эти входы, наряду с любыми дополнительными входами, используют лица, принимающие решения при выборе между потенциальными планами действий по реагированию на риски.

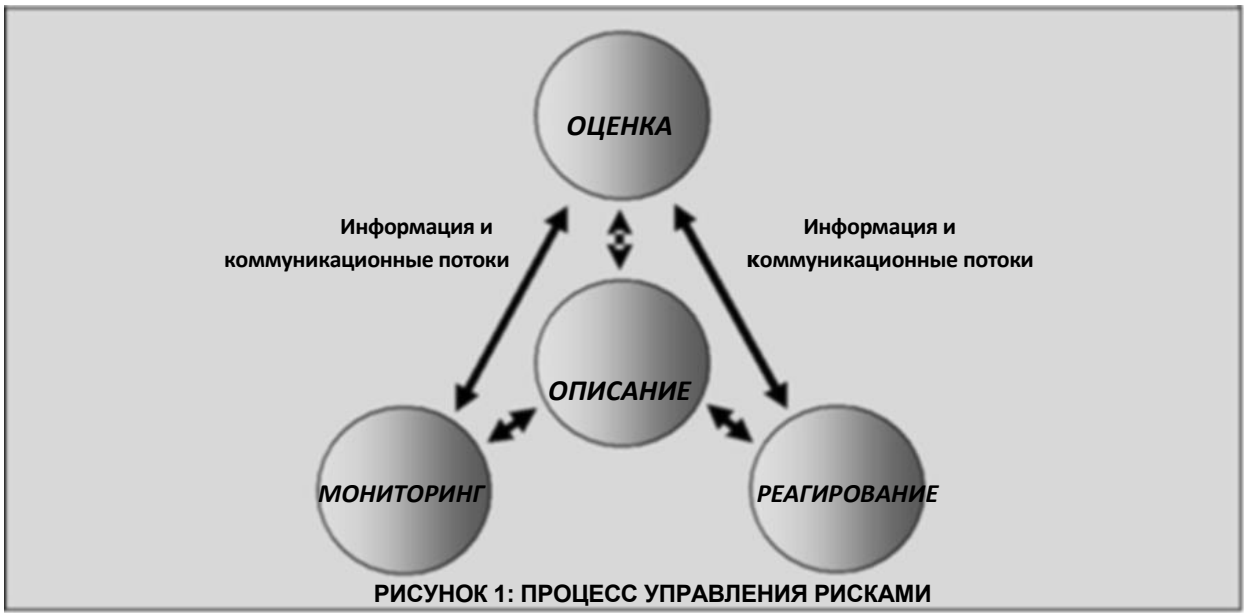


**РИСУНОК 1: ПРОЦЕСС УПРАВЛЕНИЯ РИСКАМИ**

Двунаправленный характер стрелок указывает на то, что информационные и коммуникационные потоки между компонентами управления рисками, а также порядок выполнения компонентов, могут быть гибкими и соответствующими динамическому характеру процесса управления рисками. Например, новое

законодательство, директивы или политики могут требовать от организаций немедленного внедрения дополнительных мер реагирования на риски. Эта информация передаётся непосредственно от компонента описания рисков к компоненту реагирования на риски, где выполняются конкретные действия по достижению соответствия новому законодательству, директивам или политикам, иллюстрируя очень динамичную и гибкую сущность информации, по мере её продвижения в процессе управления рисками. Глава Три предоставляет полное описание процесса управления рисками в масштабах организации, включая спецификации для входов/начальных условий, действий и выходов/последствий.

## 2.2 МНОГОУРОВНЕВОЕ УПРАВЛЕНИЕ РИСКАМИ

Для интеграции процесса управления рисками в рамках всей организации, применяется трехуровневый подход, который рассматривает риски на: (i) уровне *организации*; (ii) уровне *процессов предназначения/деятельности*; и (iii) уровне *информационной системы*. Процесс управления рисками осуществляется последовательно на всех трёх уровнях с общей целью непрерывного совершенствования деятельности организации, связанной с рисками и эффективного междууровневого и внутриуровневого взаимодействия всех заинтересованных сторон, имеющих общий интерес в успехе предназначения/деятельности организации. Рисунок 2 иллюстрирует трёхуровневый подход к управлению рисками, а также некоторые из его ключевых характеристик.

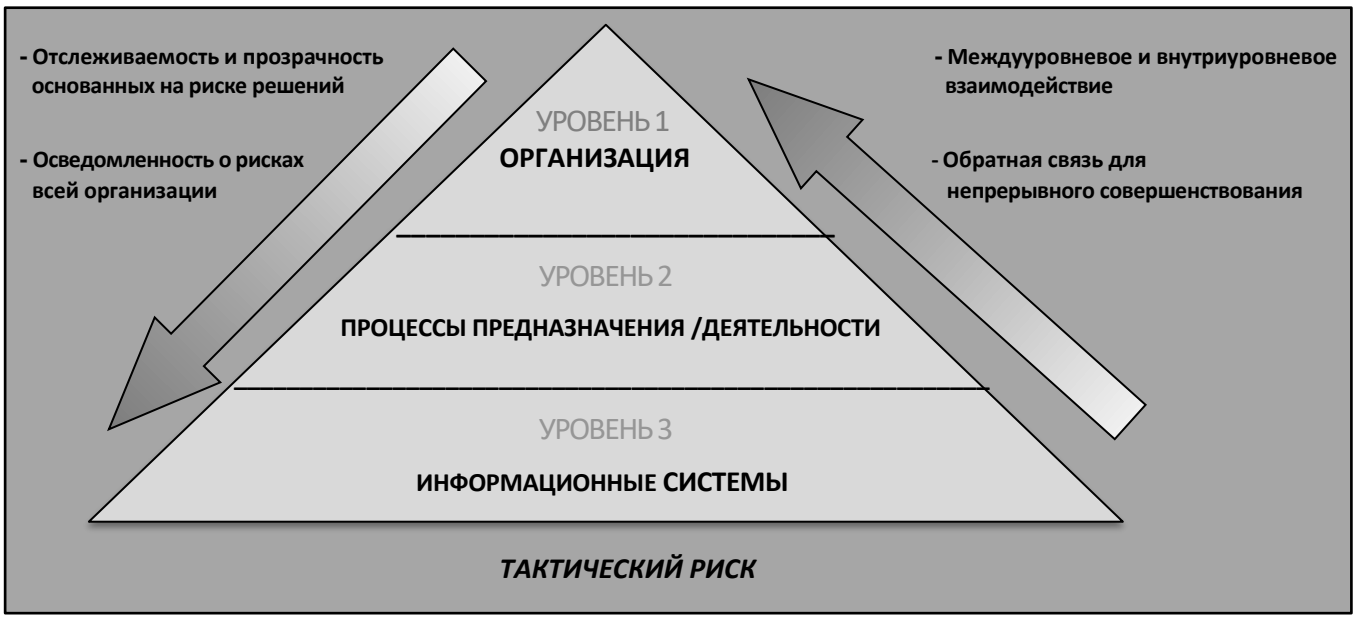


**РИСУНОК 2: МНОГОУРОВНЕВОЕ УПРАВЛЕНИЕ РИСКАМИ В МАСШТАБАХ ВСЕЙ ОРГАНИЗАЦИИ**

Уровень 1 рассматривает риски с точки зрения *организации*. Уровень 1 реализует первый компонент управления рисками (т.е. описание рисков), обеспечивая контекст для всей деятельности организаций по управлению рисками. Деятельность по управлению рисками на Уровне 1 непосредственно влияет на деятельность, осуществляемую на Уровнях 2 и 3. Например, функции предназначения и деятельности, определённые на Уровне 1, влияют на проектирование и разработку процессов предназначения/деятельности, создаваемых на Уровне 2, чтобы выполнить эти функции предназначения/деятельности. Уровень 1 определяет приоритетность функций предназначения/деятельности, которые, в свою очередь, управляют стратегиями инвестирования и решениями по финансированию, таким образом, влияя на разработку архитектуры предприятия (включая встроенную архитектуру информационной безопасности) на Уровне 2 и выделение и развертывание управленческих, эксплуатационных и технических мер безопасности на Уровне 3.

Другие примеры деятельности на Уровне 1, которая затрагивает деятельность на Уровне 2 и 3, включают выбор общих мер безопасности, предоставление руководящих указаний от ответственного за риски (функция)[17] санкционирующим должностным лицам и установление порядка восстановления информационных систем, поддерживающих критические операции предназначения и деятельности. В Разделе 2.3 представлено более подробное описание конкретных видов деятельности, связанных с Уровнем 1.

Уровень 2 рассматривает риск с точки зрения *процесса предназначения/деятельности* и опирается на контекст риска, решения по риску и деятельность по управлению риском на Уровне 1. Деятельность по управлению рисками на Уровне 2включает: (i) определение процессов предназначения/деятельности, необходимых для поддержания функций предназначения и деятельности организаций; (ii) определение приоритетов процессов предназначения/деятельности в отношении стратегических целей и задач организаций; (iii) определение типов информации, необходимой для успешного выполнения процессов предназначения/деятельности, критичности/чувствительности информации и информационных потоков, внутренних и внешних для организаций; (iv) включение требований[18] информационной безопасности в процессы предназначения/ деятельности; и (v) построение архитектуры предприятия[19] со встроенной архитектурой информационной безопасности[20], которая способствует рентабельным и эффективным решениям в области информационных технологий, соответствующих стратегическим целям и задачам организации и показателям эффективности. Деятельность на Уровне 2 непосредственно затрагивает деятельность, осуществляемую на Уровне 3. Например, архитектура информационной безопасности, являющаяся частью архитектуры предприятия, разрабатываемая на Уровне 2, влияет на и определяет установление потребностей в защите информации, которые, в свою очередь, влияют на и определяют распределение мер безопасности по конкретным компонентам информационных систем организации на Уровне 3. Решения по архитектуре предприятия на Уровне 2 влияют на проектирование информационных систем на Уровне 3, включая типы информационных технологий, приемлемых для использования при разработке этих систем. Деятельность, осуществляемая на Уровне 2, может также обеспечить полезную обратную связь с Уровнем 1, что может привести к пересмотру описания рисков организации или повлиять на деятельность по управлению рисками, осуществляемую на Уровне 1, например, на деятельность ответственного за риски (функция). В разделе 2.4 приводится более подробное описание конкретных видов деятельности, связанных с Уровнем 2.

Уровень 3 рассматривает риск с точки зрения *информационной системы* и руководствуется контекстом риска, решениями по риску и деятельностью по риску на Уровнях 1 и 2. Деятельность по управлению рисками на Уровне 3 включает: (i) категорирование информационных систем организации; (ii) распределение мер безопасности между информационными системами организации и средами, в которых эти системы эксплуатируются, в соответствии с установленной архитектурой предприятия и встроенной архитектурой информационной безопасности организации; и (iii) управление выбором, внедрением, оценкой, санкционированием и текущим мониторингом установленных мер безопасности как части упорядоченного и структурированного процесса жизненного цикла разработки систем, реализуемого во всей организации. На Уровне 3, владельцы информационных систем, поставщики общих мер безопасности, инженеры по системам и безопасности и сотрудники безопасности информационных систем принимают основанные на риске решения относительно внедрения, эксплуатации и мониторинга

[17] Ответственный за риски (функция) описан в Разделе 2.3.2.

[18] Требования информационной безопасности могут быть получены из множества источников (например, законодательство, политики, директивы, нормативные документы, стандарты и требования организации по предназначению/деятельности/ эксплуатации). Требования безопасности уровня организации документируются в план программы информационной безопасности или эквивалентный документ.

[19] Федеральные эталонные модели архитектуры предприятия и решения по сегментации и архитектуре определены в Программе OMB по архитектуре федерального предприятия (FEA), *Документе Объединенной эталонной модели FEA*, Версия 2.3, октябрь 2003 и *методологии архитектуры федеральных сегментов (FSAM*) OMB*,* январь 2009, соответственно.

[20] *Архитектура информационной безопасности* описывает связанные с безопасностью аспекты архитектуры предприятия, которые включаются в архитектуру предприятия, становясь неотъемлемой частью разработки архитектуры, - это подархитектура, полученная из архитектуры предприятия, а не отдельно определенный уровень или архитектура.

информационных систем организации. На основе этих ежедневных решений, основанных на эксплуатационном риске, санкционирующие должностные лица принимают последующие основанные на рисках решения о том, разрешено ли эксплуатировать первоначально санкционированные информационные системы в установленных средах эксплуатации или продолжать получать санкционирование на эксплуатацию на постоянной основе. Эти текущие, основанные на риске решения основываются на процессе управления рисками с указаниями от ответственного (функции) за риски и различных архитектурных соображений, поддерживающих процессы предназначения/ деятельности. Кроме того, деятельность на Уровне 3 предоставляет существенную обратную связь с Уровнями 1 и 2. Например, новые уязвимости, обнаруженные в информационной системе организации, могут иметь системные последствия, которые распространяются на всю организацию. Эти же уязвимости могут инициировать изменения в архитектуре предприятия и встроенной архитектуре информационной безопасности или могут потребовать корректировки допустимого риска организации. В разделе 2.5 приводится более подробное описание конкретных действий, связанных с Уровнем 3.

***Пока успех предназначения и деятельности организаций зависит от информационных систем, эти системы должны быть надежными. Чтобы быть надежными перед лицом сложных угроз, информационные системы должны использоваться разумно в соответствии с достигнутой степенью защиты и устойчивостью.***

## 2.3 УРОВЕНЬ ОДИН - ПРЕДСТАВЛЕНИЕ ОБ ОРГАНИЗАЦИИ

Уровень 1 рассматривает риск с точки зрения организации, создавая и внедряя структуры *управления*, которые соответствуют стратегическим целям и задачам организаций и требованиям, определенным федеральными законами, директивами, политиками, нормативными документами, стандартами и функциями предназначения/деятельности. Структуры управления обеспечивают надзор за деятельностью по управлению рисками, осуществляемой организациями, и включают: (i) установление и назначение *ответственного за риски (функция)*; (ii) разработку стратегии управления рисками организации, включая определение *допустимого риска*; и (iii) разработку и осуществление общих для организации *инвестиционных стратегий* по информационным ресурсам и информационной безопасности.

### *2.3.1. Управление*

В целом *управление* - набор обязанностей и практик, используемых ответственными за организацию лицами (например, советом директоров и высшим руководством в корпорации, руководителем федерального агентства) с явной целью: (i) обеспечение стратегического курса; (ii) обеспечение достижения целей предназначения и деятельности организации; (iii) подтверждения надлежащего управления рисками; и (iv) проверки ответственного использования ресурсов организации.[21] Риски и ресурсы, могут быть связаны с различными секторами организации (например, юридическим, финансовым, информационных технологий, соответствия нормативным требованиям, информационной безопасности). Различные сектора требуют специализированных знаний для управления рисками, связанными с этими секторами. Таким образом, управление в организациях часто организуется по секторам.[22] Пять результатов управления, связанных с управлением рисками в масштабах организации, следующие:

[21] Это определение адаптировано от Института управления ИТ. Королевский институт управленческих бухгалтеров и Международная федерация бухгалтеров также приняли это определение в 2004.

[22] Хотя управление часто организуется по секторам, организациям полезно установить единый согласованный подход к управлению. Единый подход к управлению позволяет координировать деятельность по управлению отдельными секторами и обеспечить последовательный подход к управлению в масштабах всей организации.

- Стратегическое согласование решений по управлению рисками с функциями предназначения и деятельности, соответствующими целям и задачам организации;
- Выполнение процессов управления рисками, для описания, оценки, реагирования на и мониторинга рисков для деятельности и активов организации, людей, других организаций и Нации;
- Эффективное и рациональное распределение ресурсов для управления рисками;
- Получение практических результатов деятельности, путём измерения, мониторинга и отчётности по показателям управления рисками, обеспечивающих достижение целей и задач организации; и
- Получение результата за счёт оптимизации инвестиций в управление рисками в поддержку целей организаций.[23]

В рамках управления организацией, высшие руководители/руководители в консультации и сотрудничестве с ответственным за риски (функция), определяют: (i) типы решений по управлению рисками, которые зарезервированы за конкретными ролями высшего руководства (например, руководителей агентств или генеральных директоров, финансовых директоров, директоров по информации, директоров по информационной безопасности);[24] (ii) типы решений по управлению рисками, которые считаются общими для всей организации и типы решений, которые могут быть делегированы подчинённым организациям или другим ролям в организации (например, системным инженерам и инженерам по безопасности, владельцам предназначения/деятельности, архитекторам предприятия, архитекторам информационной безопасности, поставщикам общей инфраструктуры или услуг, санкционирующим должностным лицам); и (iii) как решения по управлению рисками будут передаваться к и от ответственных за риски (функция). Три различных типа моделей управления (т.е. централизованная, децентрализованная и гибридная), описаны в Приложении F. Независимо от используемой модели (моделей) управления, для эффективного управления рисками необходимо четкое распределение и подотчетность за принятие риска.

***Твёрдое руководство - лучший индикатор приверженности высшего руководства эффективному, последовательному управлению рисками во всей организации для достижения постоянного успеха в предназначении/ деятельности.***

### *2.3.2. Ответственный за риски (функция)*

Ответственный за риски - функциональная роль, установленная в организациях для обеспечения более комплексного подхода во всей организации к управлению рисками. Ответственный за риски (функция) служит общим ресурсом управления рисками для высших руководителей/руководителей, владельцев предназначения/деятельности, директоров по информации, директоров по информационной безопасности, владельцев информационных систем, поставщиков общих мер безопасности,[25] архитекторов предприятия, архитекторов информационной безопасности, инженеров по информационным системам/ безопасности, менеджеров/специалистов по безопасности информационных систем и любых других заинтересованных сторон, имеющих конкретный интерес в успехе предназначения/деятельности организаций. Ответственный за риски (функция) взаимодействует с высшими руководителями/ руководителями по:

- Установлению ролей и обязанностей по управлению рисками;

[23] Результаты управления информационной безопасностью адаптированы из документа Института руководства ИТ, Руководство информационной безопасностью: *Руководство для советов директоров и высшего руководства*, 2-й выпуск, 2006.

[24] Перечисление различные должностей в организации не связано с какими-то конкретными отношениями (коллегиальными или иными) или уровнем полномочий.

[25] *Поставщик общих мер безопасности* – должностное лицо организации, ответственное за разработку, внедрение, оценку и мониторинг общих мер безопасности (т.е., мер безопасности, наследуемых информационными системами).

- Разработке и реализации *стратегии управления рисками* для всей организации, которая направляет и обеспечивает информацией решения по рискам организации (включая то, как риски описывают, оценивают, реагируют на них и мониторят в течение времени);[26]
- Управлению угрозами и уязвимостями информации в отношение информационных систем организации и сред, в которых эти системы эксплуатируются;
- Созданию общих для организации форумов по рассмотрению всех типов и источников рисков (включая агрегированные риски);
- Определению риска организации, основываясь на агрегированном риске от эксплуатации и использования информационных систем и соответствующих сред эксплуатации;
- Обеспечению надзора за деятельностью по управлению рисками, выполняемой организациями, для обеспечения последовательных и эффективных решений, основанные на оценке риска;
- Выработке более глубокого понимания рисков относительно стратегического видения организаций и их интегрированной деятельности;
- Созданию эффективных механизмов и представлению себя в качестве центра по передаче и обмену относящейся к рискам информации среди ключевых заинтересованных сторон внутри организаций за их пределами;
- Определению степени автономности для зависимых организаций, разрешенной головной организацией относительно описания, оценки, реагирования на и мониторинга риска;[27]
- Содействию взаимодействию и сотрудничеству среди санкционирующих должностных лиц, включая действия по санкционированию безопасности, требующие общей ответственности (например, совместное/усиленное санкционирование);[28]
- Обеспечению того, чтобы решения по санкционированию безопасности учитывали все факторы, необходимые для успеха в предназначении и деятельности; и
- Обеспечению того, чтобы общая ответственность за поддержку функций предназначения и деятельности организации с использованием внешних поставщиков, получала необходимое освещение и возлагалась на соответствующих должностных лиц, принимающих решения.

Ответственный за риски (функция) не предполагает ни конкретную организационную структуру, ни формальную ответственность, закреплённую за каким-либо человеком или группой в организации. Руководители агентств или организаций могут принять решение сохранить ответственного за риски (функция) или делегировать эту функцию. Ответственному за риски (функция) требуется сочетание навыков, опыта и взглядов, для понимания стратегических целей и задач организации, функций пред-назначения/деятельности организации, технических возможностей и ограничений, а также ключевых полномочий и указаний, определяющих деятельность организации. Чтобы обеспечить это необходимое сочетание, ответственный за риски (функция) может быть выполняться одним человеком или подразделением (при поддержке опытного персонала) или специально созданной группой (например,

[26] Решения по рискам организации включают инвестиционные решения (см. Раздел 2.3.4). *Допустимый риск* организации определяется как часть компонента описания риска (см. Раздел 2.3.3) и устанавливается в стратегии управления рисками.

[27] Поскольку зависимые организации, ответственные за выполнение производных или смежных задач, могут уже иметь инвестиции в их собственные методы описания, оценки, реагирования на и мониторинга риска, головные организации могут разрешить большую степень автономии в рамках отдельных частей организации или всей организации в целом, чтобы минимизировать затраты. Когда допускается разнообразие видов деятельности по управлению рисками, организации могут решить использовать, когда это возможно, некоторые средства передачи и/или синтеза связанной с риском информации, полученной в результате этих видов деятельности, чтобы результаты различных видов деятельности могли коррелироваться надлежащим образом.

[28] Специальная Публикация NIST 800-37 даёт руководство по совместному и усиленному санкционированию.

совет по рискам, исполнительный руководящий комитет, совет исполнительного руководства).[29] Ответственный за риски (функция) вписывается в организационную структуру управления таким образом, чтобы способствовать повышению эффективности и максимизации результативности. Хотя в масштабах организации ответственный за риски (функция) относится к уровню 1, его роль подразумевает постоянную связь и надзор за деятельностью по управлению рисками владельцев предназначения/ деятельности, санкционирующих должностных лиц, владельцев информационных систем, поставщиков общих мер безопасности, директоров по информации, директоров по безопасности информации, инженеров по информационным системам и по безопасности, руководителей/сотрудников по безопасности информационных систем и других заинтересованных сторон на Уровнях 2 и 3.

***Чтобы быть эффективными, общие для организации программы управления рисками требуют твёрдой приверженности, непосредственного участия и постоянной поддержки от высших руководителей/руководителей. Цель состоит в том, чтобы узаконить управление рисками в повседневной деятельности организаций как приоритет и неотъемлемую часть того, как организации осуществляют деятельность в киберпространстве, признавая, что это важно для успешного выполнения предназначения в средах деятельности с высоким уровнем угроз.***

### *2.3.3. Стратегия управления рисками*

*Стратегия управления рисками* организации, являющийся одним из ключевых результатов описания риска, рассматривает как организации намерены оценивать, реагировать на и мониторить риск - риск, связанный с эксплуатацией и использованием информационных систем организации. Стратегия управления рисками представляет явно конкретные предположения, ограничения, допустимые риски и приоритеты/компромиссы, используемые в организациях для принятия инвестиционных и эксплуатационных решений. Стратегия управления рисками также включает любые решения стратегического уровня и соображения о том, как высшие руководители/руководители должны управлять рисками информационной безопасности в отношении деятельности и активов организации, людей, других организаций и нации. Стратегия управления рисками всей организации включает, например, однозначное выражение допустимого риска для организации, приемлемые методики оценки риска, стратегии реагирования на риски, процесс последовательной оценки рисков в организации относительно допустимого риска организации, и способы мониторинга риска в течение времени. Использование ответственного за риски (функция) может способствовать последовательному применении стратегии управления рисками во всей организации. Стратегия управления рисками всей организации может получать информацию по связанным с риском данным из других источников, как внутренних, так и внешних по отношению к организации, чтобы обеспечить всеобъемлющую и всестороннюю стратегию.

Важным мероприятием по управлению рисками на Уровне 1, а также частью описания риска является определение *допустимого риска*. Допустимый риск - это уровень риска или степень неопределённости, которые приемлемы для организации, и является ключевым элементом описания риска организации. Допустимый риск влияет на все компоненты процесса управления рисками, оказывая непосредственное влияния на решения по управлению рисками, принимаемые высшими руководителями/руководителями в масштабах всей организации и создавая важные ограничения для этих решений. Например, допустимый риск влияет на характер и степень надзора за управлением рисками, реализуемого в организациях, степень и строгость проводимых оценок риска, а также содержание стратегий организаций по реагированию на риски. Что касается оценки рисков, то более терпимые к риску организации могут быть озабочены только теми угрозами, с которыми сталкивались подобные организации, в то время как менее терпимые к риску организации могут расширить список угроз, включив в него те угрозы, которые теоретически возможны, но которые не наблюдались в средах эксплуатации. Что касается реагирования

[29] Организации подчеркивают потребность привлечения к ответственным за риски (функция) высших руководителей/руководителей в сферах предназначения/деятельности, для обеспечения надлежащего планирования информационной безопасности, выделение ресурсов и управление рисками.

на риск, то менее терпимые к риску организации вероятно потребуют дополнительных оснований для уверенности в эффективности выбранных мер и контрмер безопасности или предпочтут меры и контрмеры безопасности, которые более проверены и имеют подтверждённый опыт применения. Такие организации могут также решить использовать несколько мер и контрмер защиты из разных источников (например, антивирусное программное обеспечение для клиентов и серверов, предоставляемые различными поставщиками). Другой пример, иллюстрирующий влияние допустимого риска на реагирование на риски, заключается в том, что допустимый риск может также влиять на требования организации к доверию, обеспечиваемому конкретными информационными технологиями. Две организации могут выбрать одни и те же информационные технологии, но их относительный уровень допустимого риска может повлиять на уровень оценки, требуемой для развертывания.

Не существует лучшего уровня допустимого риска организации. Скорее уровень допустимого риска: (i) в целом свидетельствует о культуре организации; (ii) потенциально различен для различных типов ущерба/компромиссов; и (iii) сильно зависит от индивидуальных субъективных оценок допустимого риска высших руководителей/руководителей. Тем не менее, последствия решений о рисках, основанных на допустимом риске, потенциально глубоки: менее терпимые к риску организации, могут не достичь необходимых возможностей предназначения/деятельности, чтобы избежать того, что кажется неприемлемым риском; в то время как более терпимые к риску организации могут сосредоточиться на краткосрочной эффективности предназначения/деятельности в ущерб подготовки себя к будущим неудачам. Важно, чтобы организации проявляли должную осмотрительность в определении допустимого риска, понимая, насколько фундаментально это решение для эффективности программы управления рисками.

### *2.3.4. Стратегии инвестирования*

Стратегии инвестирования[30] играют важную роль в деятельности организаций по управлению рисками. Эти стратегии обычно отражают долгосрочные стратегические цели и задачи организаций, а также соответствующие стратегии управления рисками, разработанные и реализуемые для обеспечения успех в предназначении и деятельности. В основе всех стратегий инвестирования лежит признание того, что существует ограниченное количество ресурсов, доступных для инвестирования в помощь организациям по эффективному управлению рисками - то есть в эффективное устранение рисков для достижения постоянного успеха в предназначении/деятельности.

#### Предназначения и приоритеты в области рисков

Организации обычно выполняют различное предназначение и занимаются различными типами функций деятельности. Это особенно верно для крупных и сложных организаций, у которых есть различные компоненты организации, каждый из которых обычно сосредоточен на одном или двух основных предназначениях. Хотя все эти компоненты организации и связанные функции предназначения/ деятельности, вероятно, важны и играть ключевую роль в общем успехе организаций, в действительности они не одинаково важны. Чем выше критичность функций предназначения и деятельности организации, тем более необходимо для организации обеспечить адекватное управление рисками. Такие функции предназначения и деятельности, вероятно, потребуют большего уровнем инвестиций в управление риском, чем функции предназначения/деятельности, которые считаются менее важным. Определение относительной важности функций предназначения/ деятельности и, следовательно, уровня инвестиций в управление рисками, это то, что решается на Уровне 1, выполняется на Уровне 2 и влияет на деятельность по управлению рисками на Уровне 3.

#### Ожидаемые потребности в реагировании на риски

Есть большое разнообразие в природе потенциальных угроз для организаций, начиная от хакеров, пытающихся просто нарушать веб-сайты организаций (например, кибер-вандализм), угроз посвященного

[30] Стратегии инвестирования могут включать подходы организации к: (i) замене устаревших информационных систем (например, постепенное введение элементов, полная замена); (ii) аутсорсингу и использованию внешних поставщиков информационных систем и услуг; и (iii) внутренней разработке по сравнению с приобретением коммерчески доступных продуктов информационных технологий.

лица, сложных террористических групп/организованных преступных группировок, стремящихся осуществить утечку чувствительной информации, до вооруженных сил национальных государств, стремящихся уничтожить или разрушить критически важные предназначения, атакуя информационные системы организаций.[31] Стратегические инвестиции, требуемые для устранения риска от более традиционных противников (например, хакеров, осуществляющих действия небольшими группами с ограниченными возможностями), значительно отличаются от инвестиций, требуемых для устранения риска, связанного с постоянными развивающимися угрозами, характерных для продвинутых противников (например, национальных государств или террористических групп с очень высокими уровнем знаний и ресурсов, которые стремятся создать постоянные плацдармы в организациях с целью препятствия выполнению отдельным аспектам предназначения организаций). Для борьбы с менее сложными угрозами, организации могут сосредоточить свои усилия в Уровне 3 – инвестируя в обеспечение того, чтобы необходимые меры защиты и контрмеры (например, меры безопасности, услуги безопасности и технологии) были получены, реализованы правильно, работали по назначено и приносили желаемый эффект в отношение выполнения политик информационной безопасности и устранения известных уязвимостей. В дополнение к этим основным инвестициям организации могут также инвестировать в процессы непрерывного мониторинга для обеспечения того, чтобы полученные меры безопасности, услуги и технологии эффективно работали на протяжении всего жизненного цикла разработки систем.

Когда организации должны учитывать долговременные развивающиеся угрозы, то очевидно, что адекватный учёт соответствующих рисков на Уровне 3 не выполним, потому что необходимые решения по обеспечению безопасности в настоящее время не доступны на коммерческом рынке. В этих случаях организации должны целеустремленно инвестировать за пределами Уровня 3 для значительных возможностей реагирования на Уровне 2, и в некоторой степени на уровне 1. Сущность инвестиций на Уровне 3, очевидно, изменяется от реализации существующих решений до добавления стратегического внимания на инвестирование в передовые технологии информационной безопасности (главным образом экспериментируя с инновационными решениями/технологиями для безопасности и осуществляя их раннее внедрение), или инвестируя в усилия по научным исследованиям по информационной безопасности и осуществляя усилия по учёту конкретных технологических пробелов.[32] Инвестиции в информационную безопасность по учёту долговременных развивающихся угроз могут потребовать расходов в течение нескольких лет, по мере трансформации новых решений и технологий по обеспечению безопасности от исследований до разработок и полноценного развертывания. Долгосрочное видение стратегического инвестирования в потребности реагирования на риски в организациях может помочь уменьшать постоянное внимание на краткосрочные уязвимости, обнаруживаемые в информационных системах - уязвимости, которые существуют вследствие сложности продуктов и систем информационных технологий и свойственных этим продуктам и системам слабых мест.

### Ограничения на стратегические инвестиции

Возможности организаций предоставить стратегические инвестиции в информационную безопасность ограничены. Когда необходимое стратегическое инвестиционное финансирование или стратегические ресурсы[33] недоступны, чтобы учитывать конкретные потребности, организации могут быть вынуждены пойти на компромиссы. Например, организации могли бы расширить период времени, требуемый для достижения стратегических целей информационной безопасности. Альтернативно, организации могли бы приоритезировать инвестиции в управлении рисками, решив обеспечить ресурсы (финансовые или другие), чтобы учесть некоторые критические стратегические потребности раньше, чем другие менее критические потребности. Все инвестиционные решения требуют от организаций приоритезировать риски и оценивать потенциальные воздействия, связанные с альтернативными планами действий.

---

[31] Угрозы, описанные выше, являются подмножеством всеобъемлющего пространства угрозы, которое также включает ошибки, связанные с недосмотром и бездействием, стихийными бедствиями и несчастными случаями.

[32] Эта стратегия инвестирования изменяется от управления уязвимостями и исправлениями к долгосрочной стратегии устранения пробелов информационной безопасности таких, как отсутствие продуктов информационных технологий с доверием, необходимым для достижения устойчивости информационной системы перед лицом долговременных развивающихся угроз.

[33] В некоторых случаях, ограничения могут быть не финансовыми по своей природе, но ограничениями в числе людей с соответствующей квалификацией/экспертными знаниями или ограничения относительно состояния технологии.

## 2.4 УРОВЕНЬ ДВА - ПРЕДСТАВЛЕНИЕ ПРОЦЕССОВ ПРЕДНАЗНАЧЕНИЯ/ДЕЯТЕЛЬНОСТИ

Уровень 2 учитывает риски с точки зрения *процессов предназначения/деятельности* путём проектирования, разработки и реализации процессов предназначения/деятельности, которые поддерживают функции предназначения/деятельности на Уровне 1. Процессы предназначения/деятельности организации определяют и обосновывают разработку архитектуры предприятия, которая обеспечивает упорядоченную и структурированную методологию управления сложностью инфраструктуры информационных технологий организации. Ключевой компонент архитектуры предприятия - встроенная архитектура информационной безопасности, которая обеспечивает путеводитель, обеспечивающий определение и распределение требований и потребностей в защите информационной безопасности, обусловленных процессами предназначения/деятельности, между соответствующими информационными системами организации и средами, в которых эти системы функционируют

### *2.4.1. Риск-ориентированные процессы предназначения/деятельности*

Действия по управлению рисками на Уровне 2 начинаются с идентификации и установления *риск-ориентированных процессов предназначения/деятельности* для поддержания функций предназначения и деятельности организации. Риск-ориентированный процесс предназначения/ деятельности – это процесс, который явно учитывает вероятный риск, который возник бы, если бы такой процесс был реализован. Риск-ориентированные процессы предназначения/деятельности разработаны, чтобы управлять риском в соответствии со стратегией управления рисками, определенной на Уровне 1 и явно учитывать риск, оценивая действия по предназначению/деятельности и решения на Уровне 2.[34] Реализация риск-ориентированных процессов предназначения/деятельности требует полного понимания функций предназначения/деятельности организаций и отношений между функциями предназначения/деятельности и процессами поддержки. Это понимание - предпосылка к созданию процессов предназначения/ деятельности, достаточно эластичных, чтобы противостоять большому разнообразию угроз, включая стандартные и сложные кибератаки, ошибки/случайности и стихийные бедствия. Важной частью внедрения риск-ориентированных процессов является пониманием высшими руководителями/руководителями: (i) типов источников угроз и событий угроз, которые могут оказывать негативное влияние на способность организаций успешно выполнять их функции предназначения/ деятельности);
(ii) потенциальных неблагоприятных воздействий/последствий для деятельности и активов организации, людей, других организаций или Нации, если конфиденциальность, целостность или доступность информации или информационных систем, используемых в процессе предназначения/деятельности, ставятся под угрозу; и (iii) возможной устойчивости к такой компрометации, которая может быть достигнута при данном определении процесса предназначения/деятельности с учётом реалистичных ожиданий в отношении устойчивости информационных технологий.

Ключевым результатом определения на Уровне 2 процессов предназначения/деятельности является выбранная стратегия реагирования на риски[35] для этих процессов в пределах ограничений, определенных в стратегии управления рисками. Стратегия реагирования на риски включает определение потребностей в защите информации и распределение этих потребностей по компонентам процесса (например, распределение защиты в информационных системах, защите в средах эксплуатации этих систем и выделение альтернативных путей выполнения предназначения/ деятельности, в зависимости от возможности компрометации).

### *2.4.2. Архитектура предприятия*

Существенным фактором риска, влияющим на способность организаций успешно выполнить функции предназначения и деятельности - сложность информационных технологий, используемых в информационных системах. Чтобы учесть эту сложность и связанный потенциальный риск, организациям нужен упорядоченный и структурированный подход для управления активами информационных

[34] Определение процессов предназначения/деятельности организации включает определение типов информации, которые необходимы организации для успешного выполнения этих процессов, критичности и/или чувствительности информации и информационных потоков, внутренних и внешних к организации.

[35] Стратегии реагирования на риски описаны в Приложении H.

технологий, поддерживающих их процессы предназначения/деятельности. Обеспечение большей ясности и понимание инфраструктуры информационных технологий организаций, включая проектирование и разработку связанных информационных систем, является предпосылкой для увеличения устойчивости и разумного использования этих систем перед лицом все более и более сложных угроз. Такой тип ясности и понимания может быть эффективно достигнут посредством разработки и реализации архитектуры предприятия.

Архитектура предприятия - практика управления, используемая организациями, чтобы максимизировать эффективность процессов предназначения/деятельности и информационных ресурсов, способствующих достижению успеха в предназначении/деятельности. Архитектура предприятия устанавливает ясную и однозначную связь инвестиций (включая инвестиции в информационную безопасность) с измеримым повышением производительности для всей организации или части организации. Архитектура предприятия также обеспечивает возможность стандартизировать, объединить и оптимизировать активы информационных технологий. Эти действия в конечном счете создают информационные системы, которые более прозрачны и поэтому, легче понимаемы и защищаемы. В дополнение к созданию путеводителя для более эффективного и рентабельного использования информационных технологий в организациях, архитектура предприятия обеспечивает общий язык для обсуждения вопросов управления рисками, связанных с предназначением, процессами деятельности и целями деятельности, что позволяет улучшить координацию и интеграцию усилий и инвестиций через границы организационной и деловой активности. Хорошо разработанная архитектура предприятия, реализованная во всей организации, способствует более эффективным, рентабельным, непротиворечивым и взаимосвязанным возможностям информационной безопасности, способствующих организациям лучше защищать функции предназначения и деятельности – и, в конечном счете, эффективнее управлять риском.

Архитектура Федерального предприятия (Federal Enterprise Architecture) (FEA) определяет набор взаимосвязанных *эталонных моделей*, включающих модели *производительности*, *деятельности*, *сервисного компонента*, *данных* и *технических характеристик*, а также более подробные архитектуры *сегментов* и *решений,* которые являются производными от архитектуры *предприятия*.[36] Активы организации (включая программы, процессы, информацию, приложения, технологию, инвестиции, персонал и средства) отображаются на эталонные модели уровня предприятия, чтобы создать сегментно-ориентированное представление организаций. Сегменты - элементы организаций, описывающие области предназначения, общие/совместные сервисы деятельности и сервисы, общие для организации. С инвестиционной точки зрения архитектура сегмента определяет решения для экономической модели или группы экономических моделей, поддерживающих конкретные области предназначения или общие/совместные сервисы. Основные заинтересованные стороны для архитектуры сегмента - владельцы предназначения/деятельности. Архитектура решений, тесно связанная с архитектурой сегмента, определяет активы информационных технологий в организациях, используемые для автоматизации и улучшения процессов предназначения/деятельности. Областью архитектуры решений обычно является разработка и реализация всех или части информационных систем или решений по деятельности, включая решения по информационной безопасности. Основные заинтересованные стороны для архитектуры решений - разработчики информационных систем и интеграторы, владельцы информационных систем, инженеры по информационным системам/безопасности и конечные пользователи.

***Концепции FEA, определяющие процессы деятельности, ориентированные на потребности и результаты, применяются организациями, признающими, что эффективное управление рисками, возникающими при работе в киберпространстве со сложными и высокотехнологичными угрозами, является ключевой потребностью и показателем эффективности.***

[36] Архитектура Федерального предприятия описана в серии документов, опубликованных Офисом управления программой FEA OMB. Дополнительная информация об эталонных моделях FEA и архитектурах сегментов и решений может быть найдена в Документе объединенной эталонной модели FEA и Практическом руководстве по FEA, соответственно.

Архитектура предприятия также продвигает концепции *сегментации*, *избыточности* и устранения *единых точек отказа* - все концепции, которые могут помочь организациям эффективнее управлять риском. Сегментация важна, потому что она позволяет организациям отделить функции предназначения и деятельности, а также информационные системы, компоненты систем или подсистемы, поддерживающие эти функции предназначения и деятельности от других функций предназначения, деятельности и поддерживающих систем. Сегментация помогает определять более управляемые компоненты и потенциально уменьшать степень вреда от успешного использования угрозами уязвимостей. Архитектура сегментов поддерживает концепцию сегментации на высоких уровнях организаций, и эта концепция реализуется через архитектуру решений (включая разложение информационных систем и сетей в подсистемы и подсети если необходимо).

В архитектуре предприятия также очень важна концепция резервирования. При высокой вероятности взлома или компрометации, когда угрозы используют уязвимости информационных систем организации, отказ или деградация одного или нескольких компонентов информационных систем неизбежны. Чтобы увеличить устойчивость информационных систем в рамках реагирования на риски, информационные системы организаций обеспечивают режим обработки отказов, который помогает гарантировать переключение от нарушенных компонентов на соответствующие резервные компоненты с подобными возможностями. Этот тип возможностей важен для противодействия долговременным развивающимся угрозам в ситуациях, когда организациям может потребоваться действовать в условиях кибератаки в пониженном режиме, но при этом обеспечивать достаточный уровень возможностей для достижения успеха в предназначении/деятельности. архитектуры сегментов и решений поддерживают концепцию резервирования, устанавливая упорядоченный и структурированный подход к разработке и реализации ключевых архитектурных решений, которые способствуют дублированию критических компонентов информационных систем где это необходимо.

Наконец, концепция общей точки отказа и устранение таких точек отказа легко поддерживается архитектурой предприятия. Существенная наглядность и прозрачность архитектурного проектирования на уровне организации позволяет выявить потенциальные единые точки отказа в начале процесса разработки. Поэтому, единые точки отказа эффективно учитываются архитектурами сегментов и решений. Неспособность устранения потенциальных единых точек отказа на ранних шагах проектирования архитектуры может привести к тяжелым или катастрофическим последствиям, когда эти точки отказа распространяются в информационных системах и фактический отказ вызывает потерю способности предназначения/деятельности.

### *2.4.3. Архитектура информационной безопасности*

*Архитектура информационной безопасности* - неотъемлемая часть архитектуры предприятия организации. Она представляет ту часть архитектуры предприятия, которая непосредственно посвящена устойчивости информационных систем и предоставляет архитектурную информацию для реализации возможностей по безопасности.[37] Основное назначение архитектуры информационной безопасности состоит в том, чтобы обеспечить последовательное и рентабельное выполнение *требований информационной безопасности*, определяемых процессами предназначения/деятельности, в информационных системах организаций и среде, в которой эти системы функционируют, в соответствии со стратегией управления рисками организации[38]. Архитектура информационной безопасности также, включает требования безопасности из законодательства, директив, политик, нормативных документов, стандартов и руководств по архитектуре сегментов. В конечном счете архитектура информационной безопасности представляет подробный путеводитель, позволяющий проследить путь от стратегических целей и целей организаций высшего уровня, через конкретные потребности защиты предназначения/деятельности к конкретным решениям по информационной безопасности, обеспечиваемым людьми, процессами и технологиями.

[37] Как правило, версия архитектуры информационной безопасности существует для каждой *эталонной модели* архитектуры предприятия, включая производительность, деятельность, сервисный компонент, данные и технические характеристики.

[38] Организации используют подобные инженерные принципы и технологии для систем и обеспечения безопасности чтобы гарантировать, что требования информационной безопасности эффективно реализованы в информационных системах организации.

Требования информационной безопасности, определенные в архитектуре сегментов, реализуются в архитектуре решений в форме организационных, эксплуатационных и технических мер безопасности. Меры безопасности используются в или наследуются отдельными информационными системами и средой, в которой функционируют системы. Распределение[39] мер безопасности соответствует архитектуре информационной безопасности, а также таким концепциям, как эшелонированная защита и широкая защита. Рисунок 3 иллюстрирует процесс объединяющихся требований информационной безопасности в архитектуру предприятия и связанные информационные системы, поддерживающие процессы предназначения/деятельности организаций.

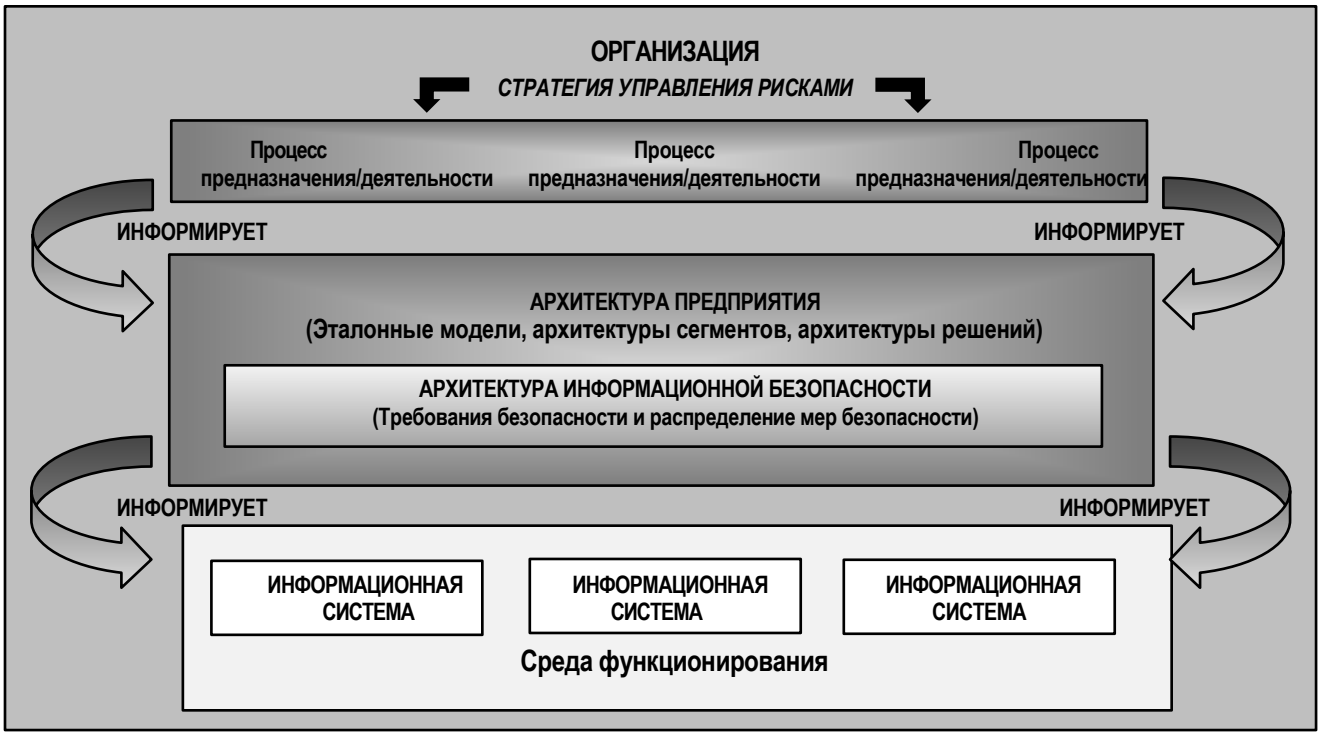


**РИСУНОК 3: ИНТЕГРАЦИЯ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Подводя итог, можно сказать, что вопросы управления рисками могут рассматриваться как неотъемлемая часть архитектуры предприятия путём:

- Разработки архитектур сегментов, связанных со стратегическими задачами и целями организации, определением функций предназначения/деятельности и связанных процессов предназначения/деятельности;
- Выявление случаев, когда эффективное реагирование на риски является критическим элементом в успехе функций предназначения и деятельности организаций;
- Определения соответствующих требований информационной безопасности архитектурного уровня в определенных организацией сегментах, на основе стратегии управления рисками организации;
- Включения архитектуры информационной безопасности, реализующей требования информационной безопасности архитектурного уровня;

[39] Выделение мер безопасности происходит вниз с уровня компонентов информационной системы, использующих меры безопасности, в выбранные компоненты систем, определённые для обеспечения конкретных возможностей безопасности. Конкретное руководство по тому, как включать требования информационной безопасности в архитектуру предприятия, представлено в Профиле безопасности и приватности FEA.

- Перевода требований информационной безопасности из архитектуры сегментов в конкретные меры безопасности для информационных систем/среды функционирования, как часть архитектуры решений;
- Распределение организационных, эксплуатационных и технических мер безопасности для информационных систем и сред функционирования, в соответствии с архитектурой информационной безопасности; и
- Документирования решений управления рисками на всех уровнях архитектуры предприятия.[40]

Архитектура предприятия предоставляет упорядоченный и структурированный подход к достижению консолидации, стандартизации и оптимизации активов информационных технологий, которые используются в организациях. Снижение рисков может быть достигнуто посредством полной интеграции процессов управления[41] во всей организации, обеспечивая, таким образом, большую степень безопасности, приватности, надежности и рентабельности функций предназначения и деятельности, выполняемых организациями. Такой комплексный подход включения стратегии управления рисками организации в архитектуру предприятия дает высшим руководителями/руководителям возможность принимать более обоснованные решения, основанные на оценке рисков, в динамичных средах деятельности - решения, основанные на компромиссах между выполнением и совершенствованием функций предназначения и деятельности организаций и управления многими видами и источниками рисков, которые должны рассматриваться в их обязанностях по управлению рисками.

***Использование архитектуры предприятия может значительно улучшить состояние риска организации, обеспечив большую прозрачность и ясность в деятельности по проектированию и разработке - позволяя более последовательно применять принцип «разумного использования» технологий во всей организации; оптимизировать компромиссы между величиной извлекаемой пользы от информационных систем, поддерживающих функции предназначения/деятельности организации, и риска от их применения.***

## 2.5 УРОВЕНЬ ТРИ - ПРЕДСТАВЛЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Все информационные системы, включая эксплуатируемые системы, разрабатываемые системы, и системы подвергаемые модернизации, находятся в некоторой фазе жизненного цикла разработки систем.[42] В дополнение к мероприятиям по управлению рисками, выполняемым на Уровне 1 и Уровне 2 (например, отражение стратегии управления рисками организации в архитектуру предприятия и встроенную архитектуру информационной безопасности), на Уровне 3 мероприятия по управлению рисками также интегрируются в жизненный цикл разработки информационных систем организации. Деятельность по управлению рисками на Уровне 3 отражает стратегию управления рисками организации и любые риски, связанные с требованиями по стоимости, календарному планированию и производительности для отдельных информационных систем, поддерживающих функции предназначения/деятельности организаций. Деятельность по управлению рисками осуществляется на каждой фазе жизненного цикла разработки систем, причём результаты каждой фазы оказывают влияние на последующие фазы.

[40] Деятельность, требуемую для эффективного включения информационной безопасности в архитектуру предприятия, ведут ключевые заинтересованные стороны в организациях, включая владельцев предназначения/деятельности, директоров по информации, директоров по безопасности ИТ, санкционирующее должностное лицо и ответственного за риски (функция).

[41] Процесс управления - процесс планирования и контроля результативности или осуществления деятельности организации (например, программ, проектов, задач, процессов). Процессы управления часто упоминаются как системы оценки результативности и управления.

[42] В жизненных циклах разработки систем, как правило, есть пять фаз: (i) инициирование; (ii) разработка/приобретение; (iii) реализация; (iv) эксплуатация/поддержка; и (v) ликвидация. Организации могут использовать различные процессы жизненного цикла разработки систем включая, например, водопад, спираль или гибкая разработка.

Например, определение требований[43] является критической частью любого процесса разработки систем и начинается очень рано в жизненном цикле, как правило, в фазе *инициирования*. Последняя информация об угрозах, которая доступна организациям, или текущие предположения организации относительно угроз, могут значительно влиять на требования к информационной системе и типы решений, которые, как считают организации, приемлемы (с технологической и эксплуатационной точки зрения) перед лицом таких угроз. Требования к информационной безопасности являются подмножеством функциональных требований, предъявляемых к информационным системам, и включаются в жизненный цикл разработки систем одновременно с другими требованиями. Требования к информационной безопасности определяют необходимую функциональность безопасности[44] для информационных систем и уровень доверия к этой функциональности (см. Раздел 2.6 по доверию к информационным системам).

Организации также решают проблемы управления рисками во время фазы *разработки/приобрет*ения жизненного цикла разработки систем (например, проектирование систем, разработка/интеграция систем и демонстрация). Как в ответ на конкретную и достоверную информацию об угрозах, так и в ответ на предположения об угрозах, потенциальные уязвимости информационных систем организации, связанные с проектированием, могут быть уменьшены во время этой фазы, путём выбора менее восприимчивых альтернатив. Риск системы поставок во время фазы приобретения информационной системы - также проблемная область для организаций. Чтобы учесть риск системы поставок во время фазы разработки/ приобретения, организации реализуют конкретные меры безопасности, считающиеся организацией необходимыми. Организации также рассматривают риски с точки зрения среды, в которой информационные системы предназначены функционировать, выбирая наиболее соответствующие меры безопасности. Чтобы быть эффективными, меры безопасности должны взаимодополняющими, использоваться с реалистическими ожиданиями по эффективности, и реализовываться как часть ясно определённой архитектуры безопасности на уровне информационной системы, которая согласуется с архитектурой безопасности, встроенной в архитектуру предприятия организации. Например, когда некоторые технические меры безопасности менее эффективны в достижении уровней доверия в информационных системах организации, организационные и эксплуатационные меры безопасности используются как компенсационные меры безопасности обеспечивая, таким образом, другую возможность управления риском.

Следующая за инициированием, разработкой и приобретением, фаза *реализации* жизненного цикла разработки систем предоставляет возможность организации определить эффективность выбранных мер безопасности, используемых в или наследуемых разрабатываемыми информационными системами до начала фактической эксплуатации. Ожидания, сформированные во время этой фазы, могут быть сравнимы с фактическим поведением в процессе внедрения информационных систем. С учётом текущей информации по угрозам, которая доступна организациям, и предположений организации об угрозах, информации, полученной во время оценок эффективности и потенциальных неблагоприятных воздействий на функции предназначения/деятельности организации, может возникнуть необходимость, модифицировать или поменять планируемую реализацию информационной системы. Для обоснования предлагаемых изменений возможно потребуется подготовка связанной с рисками информации.

После одобрения для эксплуатации, информационные системы переходят в фазу *эксплуатации/поддержки* жизненного цикла разработки систем. Мониторинг эффективности мер безопасности и любых изменений в организационных информационных системах и среде, в которой функционируют эти системы, гарантирует, что выбранные меры реагирования на риски действуют, как предназначено на непрерывной основе. Постоянный мониторинг имеет первостепенное значение для поддержания ситуативной осведомлённости о рисках для функций предназначения и деятельности организации – осведомлённости, которая необходима для определения необходимого направления корректировок, когда риск

[43] Требования безопасности информации могут быть получены из многих источников (например, законодательство, политики, директивы, нормативные документы, стандарты и требования предназначения/деятельности/эксплуатации организации).

[44] Функциональности безопасности - набор мер безопасности, используемых в или наследуемых информационной системой или среда, в которой работает система. Меры безопасности, описанные в Специальной публикации NIST 800-53, реализуются комбинацией людей, процессов и технологий.

превышает допустимый риск для организации. Во время фазы *ликвидации* жизненного цикла разработки систем стандартной процедурой для организаций является контролируемое удаление до ликвидации любой информации из информационных систем, которая может привести к негативным последствиям в случае её компрометации, а также оценка любых рисков, связанных с этими действиями.[45]

Ранняя интеграция требований информационной безопасности в жизненный цикл разработки систем - самый рентабельный метод для реализации стратегии управления рисками организации на Уровне 3.[46] Включение управления рисками в жизненный цикл разработки систем гарантирует, что процесс управления рисками не будет изолирован от других процессов управления, используемых организацией, чтобы разрабатывать, приобретать, реализовывать, применять и сопровождать информационные системы, поддерживающие функции предназначения и деятельности организации. Чтобы поддержать интеграцию в жизненный цикл разработки систем, управление рисками (включая вопросы информационной безопасности) также включается в программы, планирование и бюджетирование работ, чтобы помочь гарантировать, что соответствующие ресурсы будут доступны при необходимости - таким образом облегчая формирование программных и проектных вех, устанавливаемых организациями. Чтобы включить управление рисками в программы, планирование и бюджетирование работ, профессионалы по части рисков и информационной безопасности должны являться неотъемлемой часть команд и структур, используемых для учёта требований информационных систем и организаций.

Общая *устойчивость* информационных систем организации (т.е., как хорошо системы работают когда находятся под воздействием) является ключевым фактором и критерием качества работы в определении потенциальной жизнеспособности функций предназначения/деятельности. Использование определенной информационной технологии может внедрить присущие ей уязвимости в эти информационные системы, что приводит к риску, который, вероятно, придется снижать реинжинирингом текущих процессов предназначения/деятельности. *Разумное использование* информационных технологий при проектировании, разработке и реализации информационных систем организации имеет первостепенную важность в управлении риском.

***Выполнение требований и мероприятий по обеспечению информационной безопасности - неотъемлемая часть жизненного цикла разработки систем, гарантирующая, что высшие руководители/руководители учитывают риски для деятельности и активов организации, людей, других организаций и Нации, следующие из эксплуатации и использования информационных систем, и принимают соответствующие меры по проявлению должной осмотрительности организации.***

## 2.6 ДОВЕРИЕ И ДОВЕРЕННОСТЬ

*Доверие* - важная концепция, связанная с управлением рисками. То, как организации относятся к доверию, влияет на их поведения и их внутренние и внешние доверенные отношения. В этом разделе представлены некоторые концептуальные подходы к пониманию доверия, определяется понятие «*доверенност*ь» и показывается, как концепция доверенности может использоваться в развитии *доверенных отношений*. Приложение G описывает несколько *моделей доверия*, которые могут быть применены в контексте организации, и рассматривает, как доверие может быть измерено. Важность

[45] Хотя представление жизненного цикла разработки систем выражено как линейный поток, в действительности, знания, полученные во время более поздней фазы жизненного цикла, или изменения в требованиях к системе или средам эксплуатации может продиктовать пересмотр более ранней фазы. Например, изменения в угрозах среды во время фразы эксплуатации/поддержки могут продиктовать потребность инициировать новые или пересмотреть возможности системы.

[46] Основы управления риском (RMF), описанные в Специальной публикации NIST 800-37, обеспечивают структурированный процесс, который объединяет работы управления рисками в жизненный цикл разработки систем. RMF работает прежде всего на Уровне 3, но также и взаимодействует с Уровнем 1 и Уровнем 2 (например, обеспечивая обратную связь от решений по санкционированию к ответственному за риски [функция], распространяя обновленную информацию о рисках к санкционирующим должностным лицам, поставщикам общих мер безопасности и владельцам информационных систем).

управления организацией, культуры и транспарентности[47] также рассматривается относительно доверия и его влияния на управление рисками.

Доверие, это уверенность в том, что сущность будет вести себя предсказуемым образом при указанных обстоятельствах. Сущностью может быть человек, процесс, объект или любая комбинация таких компонентов. Сущность может иметь любой размер от отдельного аппаратного компонента или программного модуля, до элемента оборудования, идентифицируемого по марке и модели, объекта информатизации или местоположения, организации и государства. Доверие, хотя имеет субъективное определение, может быть основано на объективных данных и субъективных элементах. Объективные основания для доверия могут включать, например, результаты тестирования и оценки продукта информационной технологии. Субъективная уверенность, уровень комфорта и опыт могут дополнять (или даже заменять) объективные данные, или заменить их в случае их отсутствия. Доверие обычно относится к конкретным обстоятельствам или ситуации (например, сумма денег, включённая в сделку, чувствительность или критичность информации, или является ли безопасность проблемой, связанной с угрозой человеческим жизням). Доверие обычно не транзитивно (например, вы доверяете другу, но не обязательно другу друга). Наконец, доверие обычно достигается, базируясь на опыте или измерении. Однако в некоторых организациях, доверие, может быть предоставлено политикой (см. G Приложения, *модель предоставленного* доверия).

*Доверенность* - атрибут человека или организации, которая предоставляет другим уверенность в квалификации, возможностях и надежности этой сущности по реализации конкретных задач и выполнению возложенных обязанностей. Доверенность - также особенность продуктов и систем информационных технологий (см. Раздел 2.6.2 по *доверенности информационных систем*). Атрибут доверенности, относится ли он к людям, процессам или технологиям, может быть измерен если не количественно, то, по крайней мере, в относительных величинах.[48] Определение доверенности играет ключевую роль в установлении доверенных отношений среди людей и организаций. Доверенные отношения - ключевые факторы в решениях по рискам, принимаемых высшими руководителями/руководителями.

### *2.6.1. Установление доверия среди организаций*

Стороны устанавливают доверенные отношения основываясь на потребностях в предназначении и деятельности.[49] Доверие среди сторон, как правило, существует в виде континуума с различной степенью доверия, достигаемой в зависимости от ряда факторов. Организации могут делиться информацией и получать услуги информационных технологий, даже если их доверенные отношения далеки от полного доверия. Степень доверия, требуемая организациям для установления партнерских отношений, может сильно варьироваться в зависимости от многих факторов, включая вовлеченные организации и специфику ситуации (например, предназначение, задачи и цели потенциальных партнеров, критичность/ чувствительность деятельности, включенной в партнерство, допустимость риска организаций, участвующих в партнерстве и исторические отношения среди участников). Наконец, уровень доверия среди сущностей - не статическое качество, и может варьироваться со временем, при изменении обстоятельств.

---

[47] *Транспарентность* достигается путём обеспечения *наглядности* в деятельности по управлению рисками и информационной безопасности, выполняемыми организациями, участвующими в партнерствах (например, использование общих стандартов безопасности, языка спецификаций для мер безопасности, включая общие меры безопасности, процедуры оценки, методологию оценки риска; определение общих образцов и шаблонов свидетельств, используемых в принятии решений, связанных с риском).

[48] Текущее состояние практики для измерения *доверенности*, позволяет достоверно различать различные уровни доверенности и способно к созданию иерархической шкалы доверенности между аналогичными случаями измерительной деятельности (например, результаты оценки по ISO/IEC 15408 [Общие критерии]).

[49] Доверенные отношения могут быть: (i) формально установленными, например, путём документирования связанной с доверием информации в контрактах, соглашения об уровне обслуживания, предложениях по работам, меморандумах о соглашениях/понимании или соглашениях по безопасности взаимодействия; (ii) расширяемыми, межорганизационными или внутриорганизационными по своей природе; и/или (iii) представленными простыми (двусторонними) отношениями между двумя партнерами или более комплексными многие-ко многим отношениями среди многими различными партнерами.

Для достижения функций предназначения и деятельности организации всё больше полагаются на сервисы информационных систем[50] и информацию, предоставляемые внешними организациями, а также на партнёрские отношения. Эта уверенность требует *доверенных отношений* между организациями.[51] Во многих случаях, доверенные отношения с внешними организациями, хотя и приводят к большей производительности и экономической эффективности, но могут также привести к большему риску для организации. Этот риск учитывается стратегиями управления рисками, установленными организациями, которые принимают во внимание стратегические цели и задачи организаций.

Эффективное устранение рисков, связанных с растущей зависимостью от внешних поставщиков услуг и сотрудничества с внутренними и международными участниками государственного и частного секторов, требует, чтобы организации:

- Определили типы услуг/информации, которые будут предоставлены организациям или типы информации, которая будет совместно использоваться/обмениваться в рамках любых предполагаемых партнёрских соглашений;
- Установили уровень контроля или влияния организации на внешние организации, участвующие в таких партнёрских соглашениях;
- Описали, как услуги/информация должны быть защищены в соответствии с требованиями по безопасности информации организаций;
- Получили соответствующую информацию из внешних организаций, чтобы определить доверенность, поддерживать и сопровождать доверие (например, видимость деловой практики и решений по рискам/информационной безопасности для понимания допустимости риска);
- Сбалансировали соответствующим образом требования, базирующиеся на предназначении/ деятельности, для поддержки обмена информацией, учитывая при этом риск работы с конкурентными или враждебными сущностями и риск того, что другие организации, не являясь не конкурирующими, ни враждебными, могут быть путём, для нападения таких сущностей;
- Определили, находится ли имеющийся риск для деятельности и активов организации, людей, других организаций или нации, следующий из постоянного использования услуг/информации или участия в партнерстве, на допустимом уровне; и
- Определили, что решения установить доверенные отношения выражают приемлемый риск.

Степень доверия организации к внешним организациям может варьироваться в широких пределах: от тех, которые пользуются большим доверием (например, деловые партнеры по совместному предприятию, которые совместно используют общую бизнес-модель и общие цели) до тех, которые пользуются меньшим доверием и могут представлять собой более серьезные источники риска (например, деловые партнеры в одном проекте, которые одновременно являются конкурентами или противниками). Специфические особенности установления и поддержания доверия могут отличаться от организации к организации, исходя их требований предназначения/деятельности, участников, вовлечённых в доверенные отношения, критичности/чувствительности информации, которой обмениваются, или типов предоставляемых услуг, истории отношений между организациями и полного риска для организаций, участвующих в отношениях. Приложение G содержит несколько моделей доверия, которые организации могут использовать, имея дело с внешними организациями.

Во многих ситуациях доверие, установленное между организациями, может предоставлять не полный спектр совместного пользования информацией или полных условий услуг. Когда организация определяет, что доверенность другой организации не позволяет полный обмен информацией или использование внешних услуг, организация может: (i) снизить риск, перевести риск, или совместно использовать риск,

[50] Внешние сервисы информационной системы - сервисы, которые реализованы за пределами традиционной системы граница санкционирования (т.е., сервисы, которые используются информационной системой организации, но не являются её частью).

[51] Внешние поставщики или партнеры по предназначению/деятельности могут быть как государственными, так и частными сущностями, внутренними или международными.

используя одну или несколько компенсационных мер безопасности; (ii) принять больший уровень риска; или (iii) избежать риска, выполняя функции предназначения/деятельности со сниженными уровнями функциональности или возможно без функциональности вообще.

***Ясное понимание и принятие высшими руководителями/руководителями риска для деятельности и активов организации, людей, других организаций и нации (отражающее допустимость риска для организации) осуществляется в соответствии со стратегией управления рисками организации и является необходимым условием для установления доверенных отношений между организациями.***

### *2.6.2. Доверенность информационных систем*

Концепция доверенности может также быть применена к информационным системам, продуктам и услугам информационных технологий, которые составляют эти системы. Доверенность определяет степень, с которой можно ожидать, что информационные системы (включая продукты информационных технологий, из которых системы созданы) сохранять конфиденциальность, целостность и доступность обрабатываемой информации, хранимой или передаваемой системами при полном спектре угроз. Доверенные информационные системы – это системы, обладающие уровнем доверенности, необходимым для функционирования в пределах установленных уровней *риска* несмотря на нарушения в среде, человеческие ошибки и целенаправленные атаки, которые, как ожидается, произойдут в среде их эксплуатации. Два фактора, затрагивающие доверенность информационных систем:

- *Функциональность безопасности* (т.е., свойства/функции безопасности, используемые в системе); и
- *Доверие к безопасности* (т.е., основания для уверенности, что функциональность безопасности эффективна в её применении)[52]

Функциональность безопасности может быть достигнута при использовании в информационных системах организации и их среде эксплуатации комбинации организационных, эксплуатационных и технических мер безопасности из Специальной публикации NIST 800-53.[53] При выработке и реализации необходимых мер безопасности руководствуются и используют информацию архитектуры предприятия, установленной организациями.

Доверие к безопасности - критический аспект в определении доверенности информационных систем. Доверие - мера уверенности, что средства, методы, процедуры и архитектура безопасности информационной системы точно проводят и осуществляют политику безопасности.[54] Доверие достигается посредством: (i) мер, принимаемых разработчиками и внедренцами[55] в отношении проектирования, разработки, реализации и применения функциональности безопасности (т.е., мер безопасности); и (ii) мер, принимаемых оценщиками, для определения степени, с которой функциональность реализована правильно, работает, как предназначено, и производит желаемый результат относительно выполнения требований безопасности для информационных систем и среды их эксплуатации.[56] Разработчики и внедренцы могут увеличить доверие в функциональности безопасности, использовав четко определенную политику безопасности и модели политики, структурированные и

[52] Доверия также представляет основания для уверенности, что предусмотренная функциональность информационной системы является корректной, всегда применима (при необходимости) и является стойкой к обходу или вмешательству.

[53] Задействование соответствующих мер безопасности для информационных систем и среды эксплуатации осуществляется на первых трёх шагах Основ управления рисками (т.е., классификация, выбор и реализация).

[54] *Политика безопасности* - набор критериев для предоставления услуг безопасности.

[55] В этом контексте, разработчик/внедренец - человек или группа людей, ответственных за проектирование, разработку, внедрение или эксплуатацию мер безопасности для информационной системы или вспомогательной инфраструктуры.

[56] Для систем, отличных от систем национальной NIST безопасности, организации выполняют минимальные требования доверия, определенные в Специальной публикации NIST 800-53, приложение E.

строгие технологии разработки аппаратных средств и программного обеспечения и соответствующие принципы инженерии систем/безопасности.

Доверие для продуктов и систем информационных технологий обычно основано на проведенных оценках (и связанном получении свидетельств оценки) во время шагов инициирования, приобретения/разработки, реализации и эксплуатации/сопровождения жизненного цикла разработки систем. Например, свидетельство, связанное с разработкой, может включать технологии и методы, используемые при проектировании и разработке функциональности безопасности. Эксплуатационное свидетельство может включать отчеты о дефектах и устранении, отчетность о результатах инцидентов безопасности и результаты постоянного мониторинга мер безопасности. Независимые оценки квалифицированными экспертами могут включать исследования свидетельств, а также тестирование, проверки и аудиты реализации выбранной функциональности безопасности.[57]

Концепции доверия и доверенности тесно связаны. Доверие способствует определению доверенности относительно продукта информационных технологий или информационной системы. Разработчики/внедренцы продуктов или систем информационных технологий могут представлять свидетельства доверия путём создания соответствующих образцов (например, результаты независимого тестирования и оценки, проектная документация, спецификации низкого или высокого уровня, анализ исходного кода). Организации использующие продукты или системы информационных технологий могут проводить или полагаться на других, чтобы проводить, некоторую форму оценки продуктов или систем. Организации могут также иметь непосредственное взаимодействие с продуктом или системой, или могут получать информацию об исполнении продукта или системы от третьих лиц. Организации, как правило, оценивают все доступные свидетельства доверия, часто применяя различные дополнительные факторы чтобы определить доверенность продукта или системы в зависимости от обстоятельств.

Продукты и системы информационных технологий, показывающие более высокую степень доверенности (т.е., продукты/системы, имеющие соответствующую функциональность и доверие), как ожидается, покажут более низкий уровень скрытых дефектов разработки и реализации и более высокую степень сопротивления проникновению по отношению к масштабу угроз, включая сложные кибератаки, стихийные бедствия, случайности и намеренные/неумышленные ошибки. Восприимчивость функций предназначения/деятельности организаций к известным угрозам, среда эксплуатации, где информационные системы развернуты, и максимально допустимый уровень риска к деятельности и активам организации, людям, другим организациям или нации, определяют степень необходимой доверенности.

***Доверенность - ключевой фактор при выборе и разумном использовании продуктов информационных технологий, используемых в информационных системах организаций. Недостаточное внимание к доверенности продуктов и систем информационных технологий может оказать негативное влияние на способность организации успешно выполнить установленные ей функции предназначения/деятельности.***

[57] Специальная публикация NIST 800-53A дает представление об оценке мер безопасности в федеральных информационных системах.

## 2.7 КУЛЬТУРА ОРГАНИЗАЦИИ

*Культура* организации относится к величинам, убеждениям и нормам, которые влияют на поведение и действия высших руководителей/руководителей и отдельных членов организаций. Культура описывает способ, которым совершаются действия в организациях, и может объяснить, почему происходят некоторые действия. Есть прямая связь между культурой организации и тем, как организации отвечают на неопределённость и потенциал для краткосрочных выгод, являющихся источником долгосрочных потерь. Культура организации формирует и даже до, возможно, значительной степени, определяет стратегию управления рисками организации. Как минимум, когда представленная стратегия управления рисками не совместима с культурой организации, то, вероятно, что стратегию будет трудно, если не невозможно реализовать. Осознание и учёт значительного влияния культуры на связанные с риском решения высших руководителей/руководителей организаций, может быть ключевым к достижению эффективного управления риском.

Признание влияния культуры организации на внедрение общей для организации программы управления рисками очень важно, поскольку это может отражать серьёзные изменения в организации. Этими изменениями нужно эффективно управлять, и понимание культуры организации играет важную роль в достижении таких изменений во всей организации. Внедрение эффективной программы управления рисками может представлять собой значительные изменения в масштабах всей организации, направленные на приведение людей, процессов и культуры организации в соответствие с новыми или пересмотренными целями и задачами организации, стратегией управления рисками и механизмами обмена информацией, связанной с рисками, между сущностями. Чтобы эффективно управлять такими изменениями, организации включают культурные аспекты в качестве фундаментального компонента в свои взгляды и процессы принятия решений на стратегическом уровне (например, при разработке стратегии управления рисками). Если высшие руководители/руководители понимают важность культуры, то у них больше шансов достичь стратегических целей и задач организации путём успешного управления рисками.

Культура также влияет на уровень принимаемого риска. Культура отражена в готовности организации принять новые и передовые информационные технологии. Например, организации, которые заняты исследованиями и разработками, могут быть более склонны к расширению технологических границ. Такие организации в большей степени склонны к раннему внедрению новых технологий и, следовательно, чаще рассматривают их с точки зрения потенциальной выгоды от их использования и потенциального вреда. Напротив, организации, занимающиеся вопросами безопасности, более консервативны по своей природе и менее склонны к расширению технологических границ - они с большим подозрением относятся к новым технологиям, особенно если они предоставляются организацией, с которой они не знакомы и которой не доверяют. Кроме того, организации такого типа менее склонны к раннему внедрению новых технологий и более склонны рассматривать потенциальный ущерб, наносимый внедрением новых технологий. Другой пример - это организации, имеющие опыт разработки собственных приложений и сервисов или приобретения приложений и сервисов исключительно для своего использования. Эти организации, могут неохотно использовать приложения и сервисы, предоставляемые извне, и это нежелание может приводить к снижению риска. Другие организации напротив, могут стремиться максимизировать преимущества, достигаемые современными сетецентричными архитектурами (например, сервис-ориентированные архитектуры, облачные вычисления), в которых аппаратные средства, программное обеспечение и услуги, как правило, предоставляются внешними организациями. Так как организации, как правило, не имеют прямого контроля над работами по оценке, аудиту и надзору за внешними поставщиками, то могут быть подвергнуты большому риску.

В дополнение к воздействию культуры на перспективы управления рисками организации, между организациями могут также быть культурные проблемы. Когда две или больше организаций действуют совместно для достижения общей цели, есть возможность, что культурные различия в каждой из них могут привести к различным стратегиям управления рисками, склонности к риску и готовности принять

риск.[58] Например, предположим, что две организации сотрудничают, чтобы создать общую службу безопасности, предназначенную для борьбы с постоянно развивающимися угрозами. Культура одной из организаций может быть ориентирована на предотвращение несанкционированного разглашения информации, в то время как культура другой организации может иметь акцент на непрерывность предназначения. Различия в фокусе и акценте, следующие из культуры организаций, могут порождать различные приоритеты и ожидания относительно того, какие услуги безопасности следует приобретать, потому что организации по-разному понимают сущность угроз. Такие культурные несоответствия возникают не только между организациями, но и внутри них, когда различные компоненты организации (например, компоненты информационных технологий, операционные компоненты) имеют различные ценности и, возможно, допустимые риски. Пример внутреннего несоответствия может наблюдаться в больнице, где имеются различные культуры между защитой неприкосновенности частной жизни пациентов и доступностью медицинской информации медицинским работникам для назначений лечения.

Культура как формирует, так и формируется людьми в организациях. Влияние и воздействие культуры ощущается на всех трёх уровнях в многоуровневом подходе к управлению рисками. Высшие руководители/руководители и непосредственно, и косвенно на Уровне 1 структуры управления определяют реакцию организаций на различные подходы к управлению рисками. Высшие руководители/руководители устанавливают допустимый уровень риска для организаций как формально (например, через публикацию стратегии и руководящих документов), так и неформально (например, посредством действий, которые вознаграждают и штрафуют, степень согласованности в действиях и степень подконтрольности). Направление, задаваемое высшими руководителями/руководителями, и понимание существующих ценностей и приоритетов организаций, является основными факторами, определяющими, как управляют риском в организациях.

## 2.8 ОТНОШЕНИЯ МЕЖДУ КЛЮЧЕВЫМИ КОНЦЕПЦИЯМИ РИСКА

Как обозначено обсуждениями выше, есть множество связанных с риском концепций (например, допустимость риска, доверие и культура), все из которых оказывают влияние на управление рисками. Концепции не действуют в вакууме; напротив, между ними часто существует тесная взаимосвязь (например, культура организации, а также ее структуры и процессы управления часто влияют на темпы изменений и реализацию стратегии управления рисками). По этой причине ответственному за риски (функции) и другим сторонам, участвующим в принятии решений организации, основанных на рисках, необходимо знать и понимать все эти концепции. Ниже приводится несколько примеров взаимосвязей между концепциями, связанными с риском. Перечень взаимосвязей не является исчерпывающим и служит лишь для иллюстрации того, как объединение концепций, связанных с риском, может привести к непредвиденным последствиям, как положительным, так и отрицательным по своему масштабу.

### *2.8.1. Управление, допустимость риска и доверие*

Как часть реализации стратегии управления рисками организации на Уровне 1, ответственный за риски (функция) устанавливает методы обмена связанной с риском информацией с внешними сущностями. Что касается демонстрации должной осмотрительности при управлении рисками, то организации, менее терпимые к риску, скорее всего, потребуют больше подтверждающих свидетельств, чем организации, более терпимые к риску. Такие организации могут доверять (и, следовательно, сотрудничать) только тем организациям, с которыми у них были длительные и успешные отношения (см. модель прямого исторического доверия в Приложении G). Степень централизации[59] в организации, может быть отражением допустимого риска организации и/или её готовности доверять партнёрским организациям. Некоторые организации выбирают децентрализованную структуру управления по таким причинам, как сильно отличающиеся сферы предназначения/деятельности или потребность в повышенном разделении

[58] Аналогичная ситуация может существовать между зависимыми элементами организации, когда этим элементам предоставляют изрядное количество автономии и операционных полномочий.

[59] Дополнительной информации о моделях управления может быть найдена в Приложении F.

между направлениями предназначения/деятельности вследствие чувствительности работ. Причины децентрализации могут отражать и вероятно влиять на допустимость риска. Например, при отсутствии организаций-партнеров, отвечающих установленным критериям доверия, менее терпимым к риску организациям может потребоваться значительно больше подтверждающих свидетельств должной осмотрительности (например, доступ к оценкам степени риска, планам обеспечения безопасности, отчетам по оценке безопасности, решениям по принятию риску), чем обычно требуется в подобных ситуациях (см., подтверждённую модель доверия в Приложении G).

### *2.8.2. Доверие и культура*

Существует также потенциальная взаимосвязь между понятиями "риск", "доверие" и "культура". Изменения в требованиях предназначения/деятельности (например, новое требование предназначения или деятельности по связи информационных систем в целях обмена информацией) могут потребовать принятия большего риска, чем типично для этой организации. В краткосрочной перспективе могут потребоваться дополнительные меры по установлению и/или укреплению доверия (например, повышение прозрачности между взаимодействующими организациями). Такие меры способствуют укреплению доверия и развитию представлений и норм организации в долгосрочной перспективе. Взаимодействие между доверием и культурой может также наблюдаться при наличии разрывов и дублировании ответственности между компонентами организации, что может повлиять на возможность быстрого выполнения предлагаемых действий (особенно новых). Например, многие организации с децентрализованной структурой управления могут медленнее принимать изменения, если не было активных усилий по расширению координации и повышению доверия среди компонентов организации. Предположим, что некоторые организации получили указание от вышестоящих органов (см. модель мандатного доверия в Приложении G) более свободно обмениваться информацией с аналогичными организациями. Если организации имеют историю и культуру жесткого контроля информации, они могут не захотеть делиться информацией с внешними организациями, даже если им это предписано. В таких ситуациях организации могут потребовать от организаций-партнеров предоставить конкретные свидетельства того, какие меры были приняты для защиты информации, предназначенной для обмена, до ее представления.

### *2.8.3. Инвестиционная стратегия и допустимый риск*

Инвестиционные стратегии и допустимый риск организации также взаимосвязаны. Организации могут понимать, что есть потребность учесть постоянно развивающиеся угрозы, когда противники достигли определенной степени проникновения и точки опоры в информационных системах организации и окружающей среде, в которой используются эти системы. Стратегические инвестиции, которые требуются, чтобы учесть эти типы угроз, могут, частично зависеть от допустимого риска организаций. Менее терпимые к риску организации могут фокусировать инвестиции на информационных технологиях, которые препятствуют тому, чтобы противники получили дальнейший доступ в организации и/или ограничили ущерб, наносимый организациям, даже в ущерб достижению некоторых из многочисленных преимуществ для предназначения/деятельности, которые может обеспечить автоматизация. Более терпимые к риску организации могут фокусировать инвестиции на информационных технологиях, которые обеспечивают больше преимуществ предназначению/деятельности, даже если эти преимущества достигаются за счет получения противниками некоторых выгод или преимуществ от компрометации информационных систем и вспомогательной инфраструктуры.

### *2.8.4. Культура и допустимый риск*

Важной частью управления рисками в организациях является определение допустимого уровня риска для конкретного вида потерь. Допустимость риска может быть описана как комбинация культурной готовности организации принять определенные виды потерь и субъективных, связанных с риском, действий высших руководителей/руководителей. Основанные на риске решения организаций часто отражают совмещение допустимости риска высшими руководителями/руководителями и допустимости

риска, которая встроена в культуру организаций. При определении допустимости риска для организации изучаются ценности, убеждения и нормы организации, чтобы понять, почему принимаются компромиссные решения в отношении риска. Для некоторых организаций, в особенности для тех организаций, которые имеют дело с критической и/или чувствительной информацией, идентифицирующей персональной информацией или классифицированными данными, акцент часто делается на предотвращение несанкционированного раскрытия. Напротив, в организациях, движимых комбинацией культуры организации и сущностью функций их предназначения и деятельности, акцент делается на поддержание доступности информационных систем для достижения постоянной работоспособности. Как часть определения допустимых рисков организаций проводится оценка риска, которая выявляет виды и уровни рисков, которым могут быть подвергнуты организации. При этом учитывается как вероятность, так и последствия нежелательных событий (см. Главу Три, Процесс управления рисками).

ГЛАВА ТРИ

# ПРОЦЕСС

ПРИМЕНЕНИЕ КОНЦЕПЦИЙ УПРАВЛЕНИЯ РИСКАМИ в ОРГАНИЗАЦИИ

Эта глава описывает процесс управления риском информационной безопасности, включая: (i) общий обзор процесса управления риском; (ii) как организации устанавливают контекст для основанных на риске решений; (iii) как организации оценивают риск, рассматривая угрозы, уязвимости, вероятность и последствия/воздействие; (iv) как организации реагируют на однажды определенный риск; и (v) как организации контролируют риск в течение долгого времени при изменении потребностей предназначения/деятельности, сред эксплуатации и поддерживающих информационных систем. Процесс управления рисками, введенный в Главе Два, описан в этой главе в соответствии с его применением на трёх уровнях управления рисками. Каждый из шагов в процессе управления рисками (т.е., описание риска, оценка риска, реагирование на риск и мониторинг риска), описан структурированным образом, фокусирующемся на *входных данных* или *предварительных условиях*, необходимых чтобы инициировать шаг, конкретных *действиях*, которые составляют шаг и *результатах* или *дальнейших условиях*, следующих из шага[60]. Влияние концепций риска, описанных в Главе Два (например, допустимость риска, доверие и культура), также обсуждены в контексте процесса управления рисками и его многоуровневого применения. Рисунок 4 иллюстрирует процесс управления рисками в применении к уровням - организация, процесс предназначения/деятельности и информационные системы. Двунаправленные стрелки на рисунке указывают, что информация и коммуникационные потоки между компонентами управления рисками, а также порядок выполнения компонентов, могут быть гибкими и отвечать динамичному характеру процесса управления рисками по мере его применения на всех трёх уровнях.

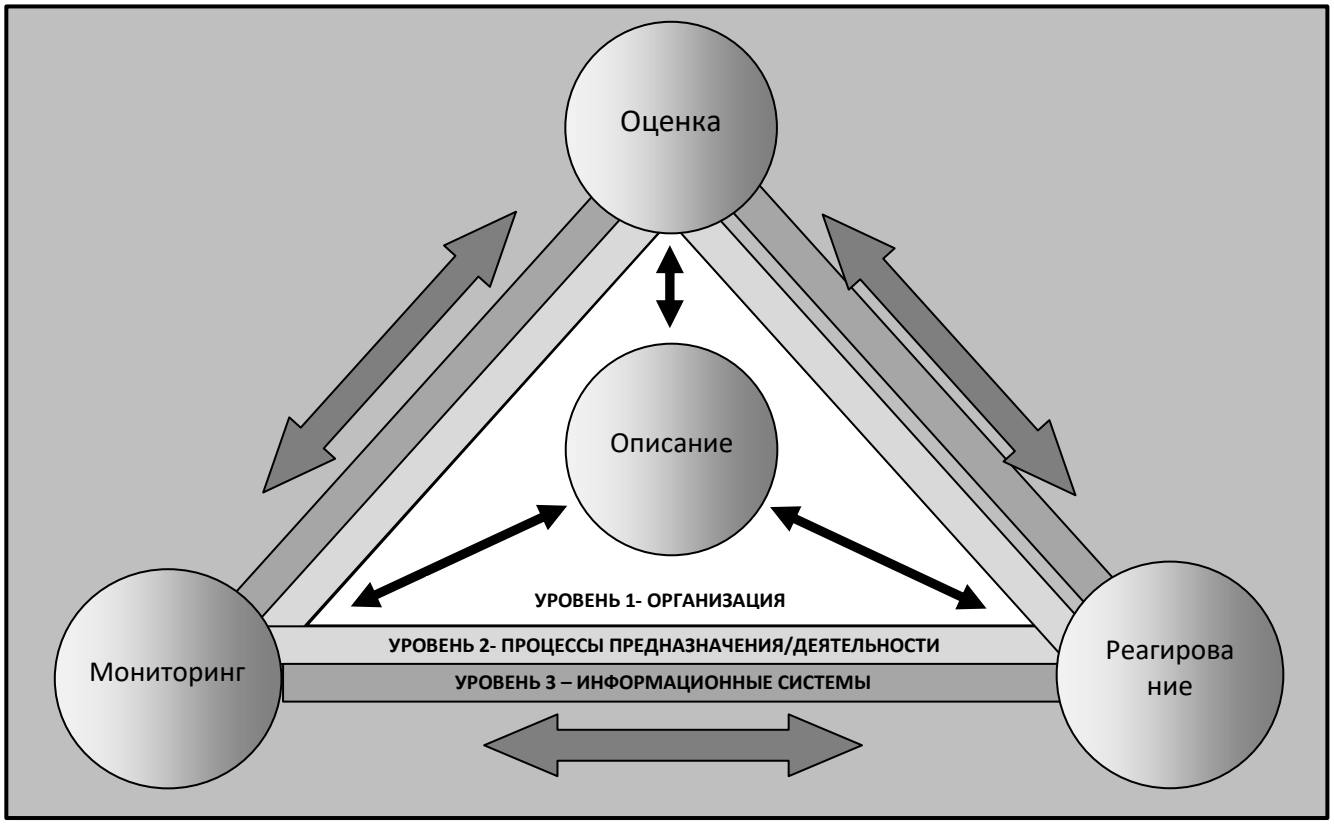


**РИСУНОК 4: ПРИМЕНЕНИЕ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ НА УРОВНЯХ**

[60] Дополнительное разъяснение по выбранным шагам в процессе управления рисками (например, оценка риска, мониторинг риска) могут быть найдены в других Специальных Публикациях NIST, перечисленных в Приложении А.

Шаги в процессе управления рисками не последовательны по своей сути. Шаги выполняются по-разному, в зависимости от конкретного уровня, где шаг применяется и от предшествующих действий, связанных с каждым из шагов. Неизменным является то, что результаты или постусловия конкретного шага управления рисками непосредственно влияют на один или несколько других шагов управления рисками в процессе управления рисками. Организации обладают значительной гибкостью в выборе шагов управления рисками (например, последовательности, степени строгости, формальности и тщательности применения) и способов фиксации и распространения результатов каждого шага - как внутри организации, так и за её пределами. В конечном счете, целью применения процесса управления рисками и связанных с ним концепций является достижение лучшего понимания риска информационной безопасности в контексте более широких действий и решений организаций, в частности, в отношении деятельности и активов организации, людей, других организаций и нации.

## 3.1 ОПИСАНИЕ РИСКОВ

Описание рисков устанавливает контекст и обеспечивает общий взгляд на то, как организации управляют риском. Основным результатом описания рисков является разработка *стратегии управления рисками*, в которой рассматривается, как организация собирается оценивать риски, реагировать на них и мониторить их. Стратегия управления рисками четко определяет конкретные предположения, ограничения, допустимые риски и приоритеты/компромиссы, используемые в организациях при принятии инвестиционных и операционных решений. Стратегия управления рисками также включает любые решения и рассмотрения стратегического уровня о том, как высшие руководители/руководители должны управлять рисками для деятельности и активов организации, людей, других организаций и нации.

На Уровне 1, высшие руководители/руководители, в консультации и сотрудничестве с ответственным за риски (функция), определяют описание структуры рисков организации, включая типы поддерживаемых решений по рискам (например, реагирование на риски), способы и условия оценки рисков для поддержки этих решений по рискам, а также способы мониторинга рисков (например, с какой степенью детализации, в какой форме и с какой периодичностью). На Уровне 2, владельцы предназначения/деятельности применяет их понимание описания структуры рисков организации, чтобы учесть соображения, специфические для функций предназначения/деятельности организации (например, дополнительные предположения, ограничения, приоритеты и компромиссы). На Уровне 3, руководители программ, владельцы информационных систем и поставщики общих мер безопасности применяют свое понимание описания структуры рисков организации, основываясь на том, как решения, принимаемые на Уровнях 1 и 2, применяются для управления рисками.

Основы управления рисками[61] являются основным средством для учёта рисков на Уровне 3. В RMF рассматриваются вопросы, связанные с проектированием, разработкой, внедрением, эксплуатацией и ликвидацией информационных систем организации и сред, в которых эти системы функционируют. Описание рисков может быть адаптировано на Уровне 3, основываясь на текущей фазе жизненного цикла разработки систем, который ещё больше ограничивает потенциальное реагирование на риски. Первоначально, описание рисков организации может быть не явным или может быть определено в терминах, которые не соответствуют уровням управления рисками. В отсутствие точных описаний рисков (описание предположений, ограничений, допустимости рисков и приоритетов/компромиссов), у владельцев предназначения/деятельности могут быть различные взгляды на риски или на то, как управлять ими. Это препятствует общему пониманию на Уровне 1 того, как риски информационной безопасности влияют на риски организации, а на Уровне 2, того, как риски, принятые для одной функции предназначения или деятельности потенциально влияют на риски в отношении других функций предназначения/деятельности. Различия в допустимости рисков и базовых предположениях, ограничениях и приоритетах/компромиссах обусловлены эксплуатационными и/или архитектурными соображениями и должны быть поняты и приняты высшими руководителями/руководителями соответствующих организаций.

[61] Основы управления рисками (Risk Management Framework (RMF)), которые действует прежде всего на Уровне 3, описаны в Специальной публикации NIST 800-37.

## ШАГ 1: ОПИСАНИЕ РИСКОВ

### *Входные данные и предварительные условия*

Описание рисков - набор допущений, ограничений, допустимых рисков и приоритетов/компромиссов, которые определяют подход организации к управлению рисками. Описание рисков определяется структурой управления, финансовым положением, законодательной/нормативной средой, инвестиционной стратегией, культурой и отношениями доверия, сложившимися внутри организации и между организациями. Входные данные к шагу описания рисков включают, например, законы, политики, директивы, нормативные документы, договорные отношения и финансовые ограничения, которые налагают ограничения на потенциальные решения организаций по рискам. Другие входные данные для описания рисков могут включать, например, конкретную информацию по организациям, позволяющую четко сформулировать: (i) определение отношений доверия и моделей доверия (см. Приложение G), вытекающих из существующих меморандумов о взаимопонимании или соглашений (MOUs или MOAs); и (ii) определение структур и процессов управления, которые указывают на объём или пределы полномочий по принятию решений по рискам, которые могут быть делегированы владельцам предназначения или деятельности. Ключевое предварительное условие для описания рисков - приверженность высшего руководства определению чёткой стратегии управления рисками и возложение на владельцев предназначения/деятельности ответственности и подотчётности за реализацию стратегии.

Рекомендации, подготовленные на шаге описания рисков, а также базовые предположения, ограничения, допустимые риски и приоритеты/компромиссы, использованные для разработки этих рекомендаций, могут быть несоответствующими одной или нескольким функциям предназначения или деятельности организаций. Кроме того, у среды рисков есть потенциал изменяться с течением времени. При этом, процесс управления рисками предусматривает обратную связь к шагу описания рисков от других шагов в процессе следующим образом:

- *Оценка рисков:* Информация, полученная в ходе оценки рисков, может повлиять на исходные предположения, изменить ограничения, касающиеся соответствующего реагирования на риски, определить дополнительные компромиссы или изменить приоритеты. Например, характеристика противников (включая представление тактики, технологий и процедур), или информация об источниках уязвимости могут не соответствовать тому, как некоторые организации реализуют свои функции предназначения/деятельности; информация об источниках угроз/уязвимостей, которая полезна для одной функции предназначения/деятельности, может, на самом деле, быть полезной для других; или руководство организации по оценке сомнительных рисков, может быть слишком обременительным или недостаточно определенным, чтобы быть полезным для одной или более функций предназначения/деятельности.
- *Реагирование на риски:* Информация, обнаруженная во время разработки альтернативных планов действий, может показать, что при описании рисков из рассмотрений были удалены или было недостаточно раскрыты некоторые потенциально высоко значимые альтернативы. Эта ситуация может заставить организации пересмотреть исходные предположения или рассмотреть способы изменить установленные ограничения.
- Мониторинг рисков: Мониторинг мер безопасности организациями, может показывать, что класс мер безопасности или конкретная реализация мер безопасности, относительно неэффективны, требуют инвестиций в людей, процессы или технологию. Эта ситуация может привести к изменениям в предположениях о том, какие типы реагирования на риски предпочтительны для организаций. Мониторинг среды деятельности может показывать изменения в характере угроз (например, изменения в тактике, технологиях и процедурах, наблюдаемых во всех информационных системах организации; увеличение частоты и/или интенсивности атак на конкретные функции предназначения/деятельности), которые будут являться причиной для организаций, чтобы пересмотреть исходные предположения об угрозах и/или искать другие источники информации об угрозах. Значительное продвижение в защитных или превентивных эксплуатационных и технических решениях могут породить потребность пересмотреть инвестиционную стратегию, определенную во время шага описания. Мониторинг законодательной/нормативной среды может также влиять на изменения в предположениях или ограничениях. Кроме того, мониторинг понесенных рисков может привести к потребности пересмотреть допустимый риск организации, если существующая формулировка допустимого риска окажется не соответствующей реалиям операционной деятельности.

### *Действия*

ПРЕДПОЛОЖЕНИЯ О РИСКАХ

**ЗАДАЧА 1-1:** Определение предположений, влияющих на оценку, реагирование и мониторинг рисков в организации.

**Дополнительное Руководство:** Организации, которые определяют, характеризуют и предоставляют представительные примеры источников угроз, уязвимостей, последствий/воздействий и определения вероятности способствуют созданию общей терминологии и системы отсчёта для сравнения и устранения рисков в различных сферах предназначения/деятельности. Организации могут также выбирать соответствующие методологии оценки рисков, в зависимости от формы управления, культуры организации и того, насколько различаются функции предназначения/деятельности в соответствующих организациях. Например, организации с высоко централизованными структурами управления могут выбрать для использования одну методологию оценки рисков. Организации с гибридными структурами управления могут выбирать различные методологии оценки рисков для Уровня 2 и дополнительную методологию оценки рисков для Уровня 1, которая ассимилирует и согласовывает данные, результаты и наблюдения оценок рисков на Уровне 2. Альтернативно, когда автономия и разнообразие центральны в культуре организации, организации могут определить требования для степени строгости и формы результатов, оставив выбор конкретных методологий оценки рисков владельцам предназначения/деятельности.

*Источники угроз*

Угрозы вызывают события, имеющие нежелательные последствия или неблагоприятные воздействия на деятельность и активы организаций, людей, другие организации и нацию. Источники угроз включают: (i) враждебные кибератаки/физические атаки; (ii) человеческие ошибки или нарушения инструкций; или (iii) природные и антропогенные катастрофы. Для угроз, вызванных враждебными кибератаками или физическими атаками, организации предоставляют краткую характеристику видов тактики, технологий и процедур, используемых противниками, которые должны быть рассмотрены по отношению к мерам защиты и контрмерам (т.е. мерам безопасности), развернутым на Уровне 1 (уровень организации), на Уровне 2 (уровень предназначения/ деятельности) и на Уровне 3 (уровень информационной системы) с явным указанием тех, которые должны быть устранены, а также явным указанием тех, которые не учитываются мерами защиты/контрмерами. Противников можно характеризовать в терминах уровней угроз (на основе возможностей, мотиваций и целей) или с дополнительной детализацией. Организации делают явные предположения относительно целей, мотиваций и возможностей источников угроз. Затем организации определяют набор репрезентативных событий угроз. Этот набор событий угроз определяет руководство на уровне детализации, с которым описываются события. Организации также определяют условия для учета событий угроз при оценках рисков. Например, организации могут ограничить оценки рисков теми событиями угроз, которые фактически наблюдались (как внутри, так и снаружи партнерами или подобными организациями), или, в качестве альтернативы, указать, что могут быть рассмотрены также события угроз, описанные заслуживающими доверия исследователями. Наконец, организации определяют источники информации об угрозах, которые, как установлено, являются авторитетными и полезными (например, секторальные центры обмена и анализа информации [ISAC]). С учётом доверенных отношений определяют, от каких партнеров, поставщиков и клиентов получена информация об угрозах, а также ожидания, возлагаемые на этих партнеров, поставщиков и клиентов на последующих шагах процесса управления рисками. Устанавливая общие отправные точки для выявления источников угроз на Уровне 1, организации обеспечивают основу для агрегирования и консолидации результатов оценок рисков на Уровне 2 (включая оценки рисков, проводимые для объединённых областей предназначения и деятельности или для поставщиков общих мер безопасности) в общую оценку рисков для организации в целом. На Уровне 2 владельцы предназначения/деятельности могут определять дополнительные источники информации об угрозах, относящиеся к функциям предназначения или деятельности организаций. Эти источники, как правило, основываются на i) конкретном секторе деятельности или критической инфраструктуры (например, сектор ISAC); ii) оперативных условиях, характерных для конкретных предназначений или направлений деятельности (например, морское пространство, воздушное пространство); и iii) внешние зависимости (например, GPS или спутниковая связь). Характеристики источников угроз уточняются для функций предназначения/деятельности, устанавливаемых организациями, причем результаты заключаются в том, что некоторые источники угроз могут не вызывать особую озабоченность, в то время как другие могут быть описаны более подробно. На Уровне 3 руководители программ, владельцы информационных систем и поставщики общих мер безопасности рассматривают фазу жизненного цикла разработки системы для определения уровня детализации, с которым могут рассматриваться угрозы. Большая спецификация угроз, как правило, доступна позже в течение жизненного цикла.

*Уязвимости*

Организации определяют подходы для характеристики уязвимостей, непротиворечивые с характеристиками источников угроз и событий. Уязвимости могут быть связаны с пригодными для использования слабыми местами или недостатками в: (i) аппаратных средствах, программном обеспечении или микропрограммных компонентах, которые составляют информационные системы организации (или мерах безопасности, используемых в этих системах или наследуемых ими); (ii) процессах предназначения/ деятельности и архитектурах предприятия (включая встроенные архитектуры информационной безопасности), реализованных организациями; или (iii) организационных структурах или процессах управления. Уязвимости могут также быть связаны с восприимчивостью организаций к неблагоприятным воздействиям, последствиям или вреду от внешних источников (например, физическое разрушение инфраструктуры, не находящейся в собственности, такой как сети электроснабжения). Организации предоставляют рекомендации по рассмотрению зависимостей от внешних организаций как уязвимостей в проводимых оценках риска. Рекомендации могут основываться на типах доверенных отношений, установленных организациями с внешними поставщиками. Организации определяют степень конкретности описания уязвимостей (например, общие термины, идентификаторы Common Vulnerability Enumeration [CVE], идентификация слабых мест/недостатков мер безопасности), давая некоторые представительные примеры, соответствующие представленным угрозам. Организационные структуры и процессы управления определяют порядок обмена информацией об уязвимостях между организациями. Организации могут также определить источники информации об уязвимостях, которые считаются авторитетными и полезными. На Уровне 2, владельцы предназначения/деятельности могут определить дополнительные источники информации об уязвимостях (например, сектор ISAC для получения информации об уязвимостях, специфичных для этого сектора). На уровне 3, руководители программ, владельцы информационной системы и поставщики общих мер безопасности рассматривают шаг в жизненном цикле разработки систем и, в частности, включенные в систему технологии, для определения уровня детализации, с которым можно рассматривать уязвимости. Организации делают явными любые предположения о степени уязвимости организации или информационной системы к конкретным источникам угроз (по имени или типу).

*Последствия и воздействия*

Организации представляют руководство по оценке воздействия на деятельность организации (т.е., предназначение, функции, имидж и репутацию), активы организации, людей, другие организации и нацию (например, используя FIPS 199, Инструкцию 1253 CNSS или более детальный подход). Организации могут испытывать последствия/воздействия неблагоприятных событий на уровне информационной системы (например, невыполнение требований), на уровне процесса предназначения/деятельности (например, неспособность полностью достигнуть целей предназначения/деятельности) и на уровне организации (например, неспособность выполнить законодательные или нормативные требования, подрыв репутации или отношений, или подрыв долгосрочной жизнеспособности). На Уровне 1 организации определяют какие последствия и типы воздействия нужно рассмотреть на Уровне 2, уровне процесса предназначения/деятельности. Неблагоприятное событие может иметь множество последствий и различных типов воздействия на разных уровнях и в различные сроки. Например, раскрытие чувствительной информации (такой, как персональная идентификационная информация) в конкретной сфере предназначения/ деятельности (например,

в отделе кадров) может иметь последствия и негативное влияние для всей организации с ущербом для репутации; последствие/воздействие на информационную систему для многих систем позволяет нападающему легче преодолеть меры безопасности идентификации и аутентификации; и последствие/воздействие на процесс предназначения/деятельности (для одной или более сфер предназначения/деятельности) позволяет нападающему фальсифицировать информацию, на которой базируются будущие решения. Чтобы гарантировать согласованность, организации определяют на Уровне 1, как должны оцениваться последствия/воздействия, испытываемые в различные периоды времени. На Уровне 2, владельцы предназначения/деятельности могут соответственно усилить рекомендации организации. Типы последствий и воздействий, учитываемые в писаниях риска, предназначены для того, чтобы обеспечить основу для определения, агрегирования и/или консолидации результатов оценки риска и облегчить взаимодействие по рискам. На Уровне 2 и Уровне 3 организации также представляют руководство относительно степени, в какой степени при оценке риска должен учитываться риск к другим организациям и нации. Организация делает любые явные предположения о степени воздействия/последствий, связанными с конкретными источниками угроз (по имени или типу) или через конкретные уязвимости (индивидуально или по типу).

*Вероятность*

Организации могут использовать различные подходы для определения вероятности событий угроз. Некоторые организации рассматривают вероятность того, что событие угрозы будет иметь место и вероятность того, что если оно произойдет, то оно приведет к отрицательным последствиям, как отдельные факторы, в то время как другие организации оценивают вероятность угрозы как комбинацию этих факторов. Кроме того, некоторые организации предпочитают количественные оценки риска, в то время как другие организации, особенно когда оценка связана с высокой степенью неопределенности, предпочитают качественные оценки риска. Определения вероятности могут быть основаны или на предположениях об угрозах или на фактических данных об угрозах (например, исторических данных по кибератакам, исторических данных по землетрясениям или конкретная информация о возможностях, намерениях и целях противника). При наличии конкретных и достоверных данных об угрозах (например, типы кибератак, тенденции кибератак, частота атак), организации могут использовать эмпирические данные и статистический анализ, чтобы определить более конкретные вероятности появления событий угроз. Организации выбирают метод, непротиворечивый с культурой организации и допустимым риском. Организации также могут сделать явные предположения относительно вероятности того, что событие угрозы приведет к негативным последствиям, следующим образом: (i) наихудший случай (т.е. атака будет успешной, если нет веских объективных причин считать иначе); (ii) наилучший случай (т.е. атака не будет успешной, если нет конкретной достоверной информации об обратном); или (iii) нечто среднее между наилучшим и наихудшим случаями (например, наиболее вероятный случай). Организации документируют все основные предположения. Организации могут использовать эмпирические данные и статистический анализ для обоснования любого из подходов, используемых для определения вероятности наступления угрожающих событий. Организации выбирают метод, соответствующий культуре организации, пониманию среды деятельности и допустимому риску.

ОГРАНИЧЕНИЯ ПО РИСКАМ

**ЗАДАЧА 1-2:** Определение ограничений на проведение оценки рисков, реагирования на риски и мониторинга рисков в организации.

**Дополнительное Руководство:** Выполнение процесса управления рисками может быть ограничено различными способами, часть из которые являются прямыми и очевидными, а другие косвенными. Финансовые ограничения могут ограничить набор работ по управлению рисками непосредственно (например, путем ограничения общего объема ресурсов, доступных для инвестиций в оценку риска или в меры защиты или контрмеры) или косвенно (например, путем исключения деятельности, которая, хотя и предполагает относительно небольшие инвестиции в реагирование на риск, влечет за собой сокращение или отказ от инвестиций в устаревшие информационные системы или информационные технологии). Организации могут также обнаружить, что необходимость продолжать зависеть от унаследованных информационных систем может ограничить доступные организации варианты управления рисками. Ограничения могут также включать юридические, нормативные и/или договорные требования. Такие ограничения могут быть отражены в политике организации (например, ограничения на аутсорсинг, ограничения и/или требования для получения информации, которая собирается как часть мониторинга рисков). Культура организации может наложить косвенные ограничения на изменения в управлении (например, препятствуя переходу от децентрализованных к гибридным структурам управления) и на то, какие меры безопасности рассматривают организации как потенциальные общие меры безопасности. В частности, отношение организации к рискам информационных технологий, которые, например, способствуют широкой автоматизации и раннему принятию новых технологий, может ограничить степень предотвращения риска и, возможно, снизить риск, который может быть получен. Любые ограничения, связанные с культурой, которые ограничивают высшему руководителю/руководителю (например, ИТ-директору) видимость информационных систем организации, которые находятся вне их формальных полномочий (например, системы, связанные с предназначением) могут препятствовать общему пониманию сложности среды информационных систем и связанных рисков для организации. На Уровне 2, владельцы предназначения/деятельности интерпретирует ограничения в свете функций предназначения/ деятельности организации. Некоторые нормативные ограничения могут не применяться к конкретным функциям предназначения/деятельности (например, правила, которые относятся к международной деятельности, когда сфера предназначения/деятельности ограничена Соединенными Штатами). В качестве альтернативы могут применяться дополнительные требования (например, наложение договорных ограничений на процессы предназначения/деятельности, выполняемые совместно с другой организацией). На Уровне 3, владельцы информационных систем, поставщики общих мер безопасности и/или руководители программ интерпретируют ограничения, специфические в отношении к функциям общим для организации и для предназначения/ деятельности, относительно их систем и среды деятельности (например, требования, по обеспечению конкретных мер безопасности удовлетворяются через общие меры безопасности).

ДОПУСТИМЫЙ РИСК

**ЗАДАЧА 1-3:** Определение уровня допустимого риска для организации.

**Дополнительное Руководство:** Допустимый риск - уровень риска, который организации готовы принять для достижения стратегических целей и задач. Организации определяют допустимый риск, связанный с информационной безопасностью, в масштабах всей организации, учитывая все функции предназначения/деятельности. Организации могут использовать различные технологии для идентификации допустимого риска информационной безопасности (например, устанавливая зоны "вероятность-воздействие" в сфере деятельности или при помощи ряда представительных сценариев). Организации также определяют другие типы допустимых организационных и эксплуатационных рисков (например, финансовые риски, риски безопасности, риски соответствия нормативным требованиям или репетиционные риски). На Уровне 2, владельцы предназначения/деятельности могут иметь отличные от организации в целом допустимые риски. Ответственный за риски (функция) предоставляет организациям способы разрешения такого различия в допустимых рисках на Уровне 2. Уровень остаточного риска, принимаемый санкционирующими должностными лицами для информационных систем или унаследованных общих мер безопасности, находится в пределах допустимого риска организации, а не индивидуальных допустимых рисков этих санкционирующих должностных лиц. Кроме того, на Уровне 2 и Уровне 3 организации предоставляют руководство по оценке рисков для конкретных процессов предназначения/деятельности или информационных систем, фокусируясь на ближайшей эффективности предназначения/деятельности с более долгосрочным, стратегическим фокусом на допустимых рисках организации. Дополнительную информацию о допустимых рисках см. в разделе 2.3.3.

ПРИОРИТЕТЫ И КОМПРОМИССЫ

**ЗАДАЧА 1-4:** Определение приоритетов и компромиссов, учитываемых организацией при управлении рисками.

**Дополнительное Руководство:** Риски испытывают на разных уровнях, в различных формах и в различные периоды времени. На уровне 1, организации принимают компромиссные решения и устанавливают приоритеты для реагирования на такие риски. Организации, как правило, имеют множество приоритетов, которые иногда вступают в конфликт, что порождает потенциальный риск. Подходы, используемые организациями для управления портфелями рисков, отражают культуру организации, допустимость рисков, а также связанные с рисками допущения и ограничения. Эти подходы обычно воплощаются в стратегических планах, политике и дорожных картах организаций, которые могут указывать на предпочтения различных форм реагирования на риски. Например, организации могут быть готовы принять краткосрочный риск незначительной деградации деятельности для достижения долгосрочного снижения риска информационной безопасности. Однако такой компромисс может оказаться неприемлемым для одной особо важной функции предназначения/деятельности (например, требования реального времени во многих промышленных/процессных системах управления). Для этой высокоприоритетной области может потребоваться другой подход к повышению безопасности, включая применение компенсирующих мер безопасности.

***Результаты и последующие условия***

Результатом шага описания рисков является стратегия управления рисками, которая определяет, как организации намерены оценивать, реагировать на риски и мониторить их во времени. На шаге описания также создается набор политик, процедур, стандартов, руководств и ресурсов организации, охватывающих следующие темы: (i) область процесса управления рисками организации (например, охватываемые сущности организации; затрагиваемые функции предназначения/деятельности; порядок применения мероприятий по управлению рисками в рамках уровней управления рисками); (ii) руководство по оценке рисков, включая, например, характеристику источников угроз, источников информации об угрозах, представительных событий угроз (в частности тактики, технологий и процедур противника), когда рассматривать и как оценивать угрозы, источники информации об уязвимостях, используемые методики оценки рисков и предположения о рисках; (iii) руководство по реагированию на риски, включая, например, допустимые риски, используемые концепции реагирования на риски, альтернативные издержки, компромиссы, последствия реагирования, иерархия полномочий и приоритеты; (iv) руководство по мониторингу рисков, включая, например, руководство по анализу контролируемых факторов рисков для определения изменений в рисках, а также частоту, методы и отчетность по мониторингу; (v) другие ограничения и ограничения на выполнение работ по управлению рисками; и (vi) приоритеты и компромиссы организации. Результаты шага описания рисков служат входными данными для шагов оценки рисков, реагирования на риски и мониторинга рисков.

## 3.2 ОЦЕНКА РИСКОВ

Оценка рисков позволяет определить, расставить приоритеты и оценить риски для деятельности организации (т.е., её предназначения, функций, имиджа и репутации), активов организации, людей, других организаций и нации, следующие из эксплуатации и использования информационных систем.[62] При оценке рисков используются результаты оценки угроз и уязвимостей для определения и оценки рисков с точки зрения вероятности их возникновения и потенциального негативного воздействия (т.е. величины ущерба) на организации, активы и людей. Оценка рисков может проводиться на любом из уровней управления рисками, с различными целями и полезностью получаемой информации. Например, оценки рисков, проводимые на Уровне 1 или Уровне 2, сосредоточены на деятельности организации,

[62] Проект Специальной публикации NIST 800-30, Версия 1, содержит руководство по проведению оценок риска (включая инкрементные или дифференциальные оценки рисков) на всех трёх уровнях многоуровневого подхода к управлению рисками.

активах и людях – как в комплексе по всем направлениям предназначения/деятельности, так и только на тех оценках, которые являются частными для конкретного направления предназначения/ деятельности. Оценки рисков для всей организации могут основываться исключительно на предположениях, ограничениях, допустимых рисках, приоритетах и компромиссах, установленных на шаге описания рисков (полученные в основном в ходе мероприятий Уровня 1) или могут быть основаны на оценках рисков, проведенных по нескольким направлениям предназначения/деятельности (в основном на основе мероприятий Уровня 2). Оценки рисков, проведенные на одном уровне, могут быть использованы для уточнения/улучшения информации об угрозах, уязвимостях, вероятностях и воздействиях, используемой в оценках, проводимых на других уровнях. Степень возможности повторного использования информации, полученной в результате оценки рисков, определяется схожестью функций предназначения/деятельности и степенью автономии, которой обладают подразделения или субкомпоненты организации по отношению к материнским организациям. Децентрализованные организации могут рассчитывать на проведение большего количества мероприятий по оценке рисков на Уровне 2 и, как следствие, могут иметь большую потребность во взаимодействии в рамках Уровня 2 для выявления сквозных угроз и уязвимостей. Децентрализованные организации могут также извлечь пользу из оценок рисков на Уровне 1 и, в частности, определения первоначального набора источников угроз и уязвимостей. Оценки рисков для всей организации обеспечивают некоторую начальную приоритизацию рисков для лиц, принимающих решения, которые должны учитывать их при переходе к шагу реагирования на риски.

Организации получают значительную пользу от проведения оценки рисков как части общего для организации процесса управления рисками. Однако, после завершения оценки рисков организациям целесообразно потратить некоторое время на поддержание этих оценок в актуальном состоянии. Поддержание актуальности оценок рисков требует поддержки со стороны шага мониторинга рисков (например, наблюдение за изменениями в информационных системах и среде эксплуатации или анализ результатов мониторинга для поддержания осведомленности о рисках). Постоянное обновление оценок рисков дает множество потенциальных преимуществ, таких как своевременная, актуальная информация, которая позволяет высшему руководству/руководителям осуществлять управление рисками практически в режиме реального времени. Поддержание оценок рисков также снижает будущие затраты на оценку и сопровождает текущие усилия по мониторингу рисков. Организации могут решить, что проведение комплексных оценок рисков как способ поддержания текущих оценок рисков не представляет достаточной ценности. В таких ситуациях организации рассматривают возможность проведения инкрементных и/или дифференциальных оценок рисков. При инкрементных оценках риска рассматривается только новая информация (например, влияние использования новой информационной системы на риски для предназначения/деятельности), тогда как при дифференциальных оценках рисков рассматривается, как изменения влияют на определение рисков в целом. Инкрементные или дифференциальные оценки рисков полезны, если организациям требуется более целенаправленный анализ рисков, они стремятся к расширенному пониманию рисков или желают получить расширенное понимание рисков по отношению к функциям предназначения/деятельности.

## ШАГ 2: ОЦЕНКА РИСКОВ

### *Входные данные и предварительные условия*

Входные данные для шага оценки рисков от шага описания рисков включают, например: (i) приемлемая методология оценки рисков; (ii) широта и глубина анализа, используемые при оценке рисков; (iii) уровень детализации, требуемый для описания угроз; (iv), нужно ли/как оценивать внешних поставщиков услуг; и (v) нужно ли/как агрегировать результаты оценки рисков от различных подразделений организации или функций предназначения/деятельности для организации в целом. Ожидания организации относительно методологий оценки риска, методов и/или процедур определяются в значительной степени структурами управления, допустимым риском, культурой, доверием и процессами жизненного цикла. Перед проведением оценок рисков организации должны осознать фундаментальные причины их проведения и что составляет адекватную глубину и широту оценок. Предположения о рисках, ограничения рисков, допустимые риски и приоритеты/компромиссы, определенные на шаге описания риска, определяют, как организации используют оценки рисков - например, локальное применение оценок рисков на каждом из уровней управления рисками (т.е., управление, процессы предназначения/деятельности, информационные системы) или глобальное применение оценок рисков во всей организации. Оценки рисков могут быть проведены организациями даже тогда, когда некоторые входные данные от шага описания рисков не были получены или не были созданы предварительные условия. Однако в таких ситуациях качество результатов оценки рисков может пострадать. В дополнение к шагу описания рисков, шаг оценки рисков может получать входные данные от шага мониторинга рисков, особенно во время выполнения предназначения и на шаге эксплуатации/сопровождения жизненного цикла разработки системы (например, когда организации обнаруживают

новые угрозы или уязвимости, требующие немедленной переоценки рисков).Шаг оценки рисков может также получать входные данные от шага реагирования на риски (например, когда организации рассматривают риски применения новых технологических решений в качестве альтернативы мерам по снижению риска). По мере разработки планов действий на шаге реагирования на риски, может потребоваться дифференциальная оценка рисков для оценки различий, которые каждый план действий вносит в общее определение рисков.

### *Действия*

ИДЕНТИФИКАЦИЯ УГРОЗ И УЯЗВИМОСТЕЙ

**ЗАДАЧА 2-1:** Определение угроз и уязвимостей в информационных системах организации и среде, в которой эти системы функционируют.

**Дополнительное Руководство:** Идентификация угроз требует изучения источников угроз и событий. Для изучения источников и событий угроз организации определяют информацию о возможностях, намерения и целях угроз из всех доступных источников. Организации могут использовать ряд источников информации об угрозах на стратегическом или тактическом уровнях. Информация об угрозах, полученная на любом уровне, может быть использована для обоснования или уточнения действий, связанных с риском, на любом другом уровне. Например, конкретные угрозы (т.е. их тактики, методы и процедуры), выявленные в ходе оценки угроз на Уровне 1, могут непосредственно повлиять на решения по процессам предназначения/ деятельности и проекту архитектуры на Уровне 2. Конкретная информация об угрозах, полученная на Уровнях 2 и 3, может использоваться организациями для уточнения информации об угрозах, полученной в ходе первоначальных оценок угроз, проведенных на уровне 1.

Идентификация уязвимостей осуществляется на всех уровнях. Уязвимости, связанные с управлением организацией (например, непоследовательные решения об относительных приоритетах процессов предназначения/деятельности, выбор несовместимых реализаций мер безопасности), а также уязвимости, связанные с внешними зависимостями (например, электроэнергия, цепочки поставок, телекоммуникации), наиболее эффективно выявляются на Уровне 1. Однако в большей части выявление уязвимостей происходит на Уровнях 2 и 3. На Уровне 2 чаще всего выявляются уязвимости, связанные с процессами и архитектурой (например, уязвимости или недостатки, которые можно использовать, в процессах предназначения/ деятельности, архитектурах предприятия/информационной безопасности, включая встроенные архитектуры информационной безопасности). На уровне 3 основное внимание уделяется уязвимостям информационных систем. Эти уязвимости обычно обнаруживаются в аппаратных, программных и микропрограммных компонентах информационных систем или в среде, в которой системы функционируют. Другие области потенциальных уязвимостей включают уязвимости, связанные с определением, применением/реализацией и мониторингом процессов, процедур и услуг, относящихся к управленческим, эксплуатационным и техническим аспектам информационной безопасности. Уязвимости, связанные с проектом архитектуры и процессами предназначения/деятельности, могут оказать большое влияние на способность организаций успешно выполнять функции предназначения и деятельности из-за потенциального воздействия на многочисленные информационные системы и среду предназначения. Уточненные оценки уязвимостей, проведенные на Уровнях 2 и 3, передаются персоналу организации, ответственному за более стратегическую оценку рисков. Оценки уязвимости, проводимые на уровнях 2 и 3, позволяют оценить дополнительные сопутствующие переменные, такие как местоположение, близость к другим активам с высоким риском (физическим или логическим), а также ресурсные соображения, связанные со средой деятельности. Конкретная информация по среде деятельности, позволяет получить более полезные и действенные результаты оценки. Выявление уязвимостей может быть выполнено на уровне отдельных слабых мест/недостатков или на уровне первопричины. Выбирая между подходами, организации учитывают, является ли общей целью выявление каждого конкретного случая или симптома проблемы, или понимание глубинных коренных причин проблем. Понимание конкретных слабостей или недостатков, которые можно использовать, полезно при первичном выявлении проблемы или при необходимости быстрого устранения. Такое конкретное понимание также предоставляет организациям необходимые источники информации для последующей диагностики потенциальных коренных причин проблем, особенно системных.

Организации с более развитыми архитектурами предприятий (включая встроенные архитектуры информационной безопасности) и зрелыми процессами жизненного цикла имеют результаты, которые могут быть использованы для предоставления информации процессам оценки рисков. Предположения, ограничения, допустимость, приоритеты и компромиссы в отношении рисков, используемые при разработке архитектуры предприятия и встроенной архитектуры информационной безопасности, могут быть полезными источниками информации для начальных действий, по оценке рисков. Оценки рисков, проводимые для поддержки разработки архитектур сегментов или решений, также могут служить источниками информации для идентификации угроз и уязвимостей. Еще одним фактором, влияющим на выявление угроз и уязвимостей, является культура организации. Организации, которые поощряют свободное и открытое общение, а также отказ от наказания за распространение негативной информации, как правило, способствуют большей открытости со стороны лиц, работающих в этих организациях. Зачастую персонал организаций, работающий на Уровнях 2 и 3, обладает ценной информацией и может внести значимый вклад в выявление угроз и уязвимостей. Культура организаций влияет на готовность персонала передавать информацию о потенциальных угрозах и уязвимостях, что в конечном итоге влияет на качество и количество выявленных угроз/уязвимостей.

ОПРЕДЕЛЕНИЕ РИСКОВ

**ЗАДАЧА 2-2:** Определение рисков для деятельности и активов организации, людей, других организаций и нации, в случае использования выявленными угрозами выявленных уязвимостей.

**Дополнительное Руководство:** Организации определяют риски с учётом вероятности того, что известные угрозы используют известные уязвимости, а также результирующих последствий или негативного воздействия (т.е. величины ущерба), в случае их использования. Организации используют информацию об угрозах и уязвимостях вместе с информацией о вероятности и последствиях/воздействии для качественного или количественного определения рисков. Организации могут использовать различные подходы, для определения вероятности использования уязвимостей угрозами. Определение вероятности может быть основано либо на предположениях об угрозах, либо на фактической информации об угрозах (например, исторические данные о кибератаках, исторические данные о землетрясениях или конкретная информация о возможностях, намерениях и целях противника). При наличии конкретной и достоверной информации об угрозах (например, типы кибератак, тенденции кибератак, частота атак) организации могут использовать эмпирические данные и статистический анализ для определения более конкретных вероятностей возникновения угроз. На оценку вероятности также может повлиять то, как проводилась идентификация уязвимостей - на уровне отдельных слабых мест или недостатков, или на уровне первопричины. Относительная легкость/сложность использования уязвимостей, изощренность противников и характер среды деятельности влияют на вероятность использования уязвимостей угрозами. Организации могут характеризовать неблагоприятные воздействия по целям безопасности (например, потеря конфиденциальности, целостности или доступности). Однако для обеспечения максимальной полезности неблагоприятное воздействие выражается в терминах функций предназначения, деятельности и заинтересованных сторон или переводится в них.

*Определение рисков и неопределенность*

Определение рисков требует анализа информации, связанной с угрозами, уязвимостями, вероятностью и воздействием. Организациям также необходимо изучить уязвимости предназначения/деятельности и угрозы, для которых не существует средств защиты и/или контрмер. Характер исходных данных, предоставляемых на этом шаге (например, общие, конкретные, стратегические, тактические), напрямую влияет на тип выходных данных или определение рисков. Достоверность и точность определения рисков зависят от актуальности, точности, полноты и целостности информации, собранной для поддержки процесса оценки рисков. Кроме того, компоненты результата оценки рисков, которые влияют на достоверность и точность определения рисков, также влияют на величину неопределенности, связанной с этими определениями и последующими определениями рисков. Организации также должны учитывать дополнительные сведения, связанные с предполагаемыми временными рамками, связанными с конкретными рисками. Временные горизонты, связанные с потенциальными угрозами, могут определять будущую реакцию на риски (например, риск может не вызывать беспокойства, если временной горизонт риска находится в отдаленном будущем).

Руководство организации по определению риска в условиях неопределенности указывает, как комбинации вероятности и воздействия объединяются в определение уровня риска или значимости/рейтинга риска. Организациям необходимо понимать тип и объем неопределенности, связанной с решениями о рисках, чтобы определения рисков были понятны. На шаге описания рисков организации могут предоставить руководство по анализу рисков и определению рисков при наличии высокой степени неопределенности. Неопределенность вызывает особую озабоченность, когда при оценке рисков рассматриваются постоянные развивающиеся угрозы, для которых может потребоваться анализ взаимодействующих уязвимостей, общий объем знаний ограничен, а прошлое поведение могло быть не спрогнозированным.

Хотя определение угроз и уязвимостей часто применяется к функциям предназначения и деятельности, конкретные требования, связанные с функциями предназначения/деятельности, включая условия деятельности, могут привести к различным результатам оценки. Различные функции предназначения, деятельности и условия деятельности могут привести к различиям в применимости конкретной рассматриваемой информации об угрозах и вероятности потенциального ущерба, наносимого угрозами. Понимание компонента угроз при оценке рисков требует понимания конкретных угроз, с которыми сталкиваются конкретные функции предназначения или деятельности. Такая осведомленность об угрозах включает в себя понимание возможностей, намерений и целей конкретных противников. Допустимый риск для организаций и базовые убеждения, связанные с тем, как формируется допустимый риск (включая культуру внутри организаций), могут формировать восприятие воздействия и вероятности в контексте выявленных угроз и уязвимостей.

Даже при установлении четких критериев, на оценку рисков влияют культура организации, личный опыт и накопленные знания лиц, проводящих оценку. В результате оценщики рисков могут прийти к различным выводам на основе одной и той же информации. Такое разнообразие точек зрения может обогатить процесс оценки рисков и предоставить лицам, принимающим решения, больший объем информации и потенциально меньшее количество предубеждений. Однако такое разнообразие может также привести к противоречивым оценкам рисков. Определенные организацией и применяемые процессы обеспечивают средства для выявления противоречий практик и включают процессы для выявления и устранения таких противоречий.

***Результаты и последующие условия***

Результатом шага оценки рисков является определение рисков для деятельности организации (т.е. предназначения, функций, имиджа и репутации), активов организации, людей, других организаций и нации. В зависимости от подхода, который используют организации, до сведения лиц, принимающих решения, ответственных за реагирование на риски, могут быть доведены либо общий риск для организации, либо исходные данные, использованные для определения рисков. В некоторых ситуациях между шагом оценки рисков и шагом реагирования на риски происходят повторяющиеся циклы, пока не будут достигнуты конкретные

цели. В зависимости от порядка действий, выбранного на шаге реагирования на риски, может сохраняться некоторый остаточный риск. При определенных обстоятельствах уровень остаточного риска может вызвать повторную оценку рисков. Такая переоценка обычно бывает инкрементной (оценивается только новая информация) и дифференциальной (оценивается, как новая информация меняет общее определение риска).

Совокупность результатов оценки рисков на всех трех уровнях позволяет управлять портфелями рисков, принимаемых организациями. Выявленные риски, общие для более чем одной функции предназначения/деятельности в организации, могут также стать источником для будущих действий по оценке на Уровне 1, таких как анализ первопричин. Получение лучшего понимания причин, по которым определенные риски являются более распространенными или частыми, помогает лицам, принимающим решения, выбирать меры реагирования на риски, направленные на решение основных (или коренных) проблем, вместо того, чтобы сосредотачиваться только на поверхностных вопросах, связанных с существованием рисков. Результаты оценки рисков могут также определять будущие решения по проектированию и разработке архитектуры предприятия (включая встроенную архитектуру информационной безопасности) и информационных систем организации. Степень уязвимости функций предназначения/деятельности к ряду выявленных угроз и относительная легкость, с которой эти уязвимости могут быть использованы, вносят свой вклад в информацию о рисках, предоставляемую высшим руководителям/руководителям.

Результаты шага оценки рисков могут быть полезными исходными данными для шагов описания рисков и мониторинга рисков. Например, определение рисков может привести к пересмотру допустимого уровня риска организации, установленного на шаге определения рисков. Организации также могут использовать информацию, полученную на шаге оценки рисков, для информирования шага мониторинга рисков. Например, оценки рисков могут включать рекомендации по мониторингу конкретных элементов рисков (например, источников угроз), чтобы при преодолении определенных пороговых значений предыдущие результаты оценки рисков могли быть пересмотрены и обновлены, в случае необходимости. Конкретные пороговые значения, установленные в рамках программ мониторинга рисков, также могут служить основой для переоценки рисков. Если организации устанавливают критерии в рамках шага описания рисков для случаев, когда результаты оценки рисков не являются основанием для реагирования на риски, то результаты оценки могут быть поданы непосредственно на шаг мониторинга рисков в качестве источника исходных данных.

## 3.3 РЕАГИРОВАНИЕ НА РИСКИ

Реагирование на риски заключается в определении, оценке, принятии решений и реализации соответствующих планов действий[63], чтобы принять, избежать, снизить, разделить или передать риски для деятельности и активов организации, людей, других организаций и нации, возникающие в результате эксплуатации и использования информационных систем. Определение и анализ альтернативных направлений действий обычно происходит на Уровне 1 или Уровне 2. Это связано с тем, что альтернативные направления действий (т.е. потенциальные меры реагирования на риски) оцениваются с точки зрения ожидаемых последствий для всей организации и способности организации продолжать успешно выполнять функции предназначения и деятельности организации. Решения о применении мер реагирования на риски в масштабах всей организации обычно принимаются на Уровне 1, хотя эти решения принимаются на основе информации о рисках, полученной на нижних уровнях. На Уровне 2 альтернативные планы действий оцениваются с точки зрения ожидаемого воздействия на функции предназначения/деятельности организации, соответствующие процессы предназначения/деятельности, поддерживающие функции предназначения/деятельности, и требования к ресурсам. На Уровне 3 альтернативные планы действий оцениваются с точки зрения жизненного цикла разработки системы или максимального количества времени, доступного для реализации выбранного(ых) плана(ов) действий. Диапазон потенциальных реакций на риск является основным фактором, определяющим, на каком уровне будет осуществляться деятельность - на Уровне 1, Уровне 2 или Уровне 3. На принятие решений по рискам влияет допустимый риск для организации, определённый в рамках деятельности по описанию рисков на Уровне 1. Организации могут принимать решения о рисках на любом из уровней управления рисками с различными целями и полезностью получаемой информации.

### ШАГ 3: РЕАГИРОВАНИЕ НА РИСКИ

#### *Входные данные и предварительные условия*

Исходные данные, полученные на шагах оценки и описания рисков, включают: (i) идентификацию источников угроз и угрожающих событий; (ii) идентификацию уязвимостей, которые могут быть использованы; (iii) оценки потенциальных

[63] *План действий* - это поэтапное по времени или зависящее от ситуации сочетание мер реагирования на риски. *Меры реагирования* на риски - это конкретные действия, предпринимаемые в ответ на выявленные риски. Меры реагирования на риски могут управляться отдельно и могут включать, например, внедрение мер безопасности для снижения рисков, принятие политики безопасности для избегания рисков или принятия рисков в определенных обстоятельствах, а также соглашения организации для распределения или передачи риска.

последствий и/или воздействий, если угрозы используют уязвимости; (iv) оценки вероятности того, что угрозы используют уязвимости; (v) определение рисков для деятельности организации (т.е. предназначения, функций, имиджа и репутации), активов организации, людей, других организаций и нации; (vi) руководство по реагированию на риски, из стратегии управления рисками организации (см. Приложение H); и (vii) общие указания организации и руководство по соответствующему реагированию на риски. В дополнение к шагам оценки риска и описания риска, шаг реагирования на риск может получать входные данные от шага мониторинга риска (например, когда организации сталкиваются с нарушением или компрометацией своих информационных систем или среды эксплуатации, что требует немедленного реагирования для устранения инцидента и снижения дополнительного риска, возникшего в результате этого события). Шаг реагирования на риск может также получать входные данные от шага описания риска (например, когда от организаций требуется развернуть новые средства защиты и контрмеры в своих информационных системах на основе требований безопасности в новом законодательстве или политике OMB). Шаг описания риска также непосредственно формирует ограничения на ресурсы, связанные с выбором соответствующего плана действий. Дополнительные предварительные условия, установленные на шаге описания риска, могут включать: (i) ограничения, основанные на архитектуре и предыдущих инвестициях; (ii) предпочтения и допуски организации; (iii) ожидаемая эффективность снижения рисков (включая то, как эффективность измеряется и контролируется); и (iv) временной горизонт для рисков (например, текущий риск, прогнозируемый риск - то есть риск, который, как ожидается, возникнет в будущем на основе результатов оценки угроз или запланированных изменений в функциях предназначения/деятельности, архитектуре предприятия (включая архитектуру информационной безопасности) или аспектах соблюдения правовых или нормативных требований).

### *Действия*

ОПРЕДЕЛЕНИЕ МЕР РЕАГИРОВАНИЯ НА РИСКИ

**ЗАДАЧА 3-1:** Определение альтернативных планов действий в ответ на риски, определенные в ходе оценки рисков.

**Дополнительное Руководство:** Организации могут реагировать на риски различными способами. К ним относятся: (i) принятие риска; (ii) предотвращение риска; (iii) снижение риска; (iv) распределение риска; (v) передача риска; или (vi) сочетание вышеперечисленного. План действий - это поэтапное по времени или зависящее от ситуации сочетание мер по реагированию на риски. Например, в чрезвычайной ситуации организации могут принять риск, связанный с нефильтрованным подключением к внешнему поставщику услуг связи в течение ограниченного времени; затем избежать риска, прервав подключение; снизить риск в ближайшей перспективе путем применения мер безопасности для поиска вредоносных программ или свидетельств несанкционированного доступа к информации, имевших место в период нефильтрованного подключения; и, наконец, снизить риск в долгосрочной перспективе путем применения мер для более безопасной работы с такими подключениями.

*Принятие риска*

Принятие риска - это соответствующая реакция на риск, когда выявленный риск находится в пределах допустимого риска организации. Организации могут принять риск, считающийся низким, умеренным или высоким, в зависимости от конкретных ситуаций или условий. Например, организации с центрами обработки данных, расположенными в северо-восточной части США, могут принять риск землетрясений на основании известной вероятности землетрясений и уязвимости центров обработки данных к повреждениям в результате землетрясений. Организации принимают тот факт, что землетрясения возможны, но, учитывая редкость крупных землетрясений в этом регионе страны, считают, что устранять такой риск нерентабельно, то есть организации определяют, что риск, связанный с землетрясениями, является низким. С другой стороны, организации могут принять значительно больший риск (умеренный/высокий) в связи с настоятельными потребностями предназначения, деятельности или эксплуатации. Например, федеральные агентства могут решить поделиться очень чувствительной информацией с сотрудниками службы быстрого реагирования, которые обычно не имеют доступа к такой информации в связи с необходимостью остановить готовящиеся террористические атаки, даже если эта информация сама по себе не является быстро теряющей ценность в отношении риска потери конфиденциальности. Организации обычно принимают решения относительно общего уровня приемлемого риска и видов приемлемого риска с учетом приоритетов организации и компромиссов между: (i) ближайшими потребностями предназначения/деятельности и потенциальными долгосрочными последствиями для предназначения/деятельности; и (ii) интересами организации и потенциальными последствиями для людей, других организаций и нации.

*Предотвращение риска*

Предотвращение риска может быть подходящей реакцией на риск, когда выявленный риск превышает допустимый риск организации. Организации могут осуществлять определенные виды деятельности или использовать определенные виды информационных технологий, которые приводят к неприемлемому риску. В таких ситуациях предотвращение риска предполагает принятие конкретных мер по устранению деятельности или технологий, которые являются основой риска, или по пересмотру или изменению места этих видов деятельности или технологий в процессах предназначения/деятельности организации, чтобы предотвратить потенциально неприемлемый риск. Например, организации, планирующие использовать сетевые соединения между двумя доменами, могут определить путем оценки рисков, что существует неприемлемый риск при установлении таких соединений. Организации могут также определить, что реализация эффективных мер защиты и контрмер (например, междоменных решений) нецелесообразна в данных обстоятельствах. Таким образом, организации решают предотвратить риск путем устранения электронных или сетевых соединений и использования "воздушного зазора" с процессами ручного соединения (например, передачи данных с помощью вторичных устройств хранения).

*Снижение риска*

Снижение риска, или уменьшение риска, - это соответствующая реакция на риск для той части риска, которую нельзя принять, предотвратить, разделить или передать. Альтернативные варианты снижения риска зависят от: (i) уровня управления рисками и

объема решений по реагированию на риск, назначенных или делегированных должностным лицам организации на этом уровне (определяются структурами управления организации); и (ii) стратегии управления рисками организации и соответствующих стратегий реагирования на риск. Средства, используемые организациями для снижения риска, могут включать комбинацию мер реагирования на риск на всех трех уровнях. Например, снижение риска может включать общие меры безопасности на Уровне 1, реорганизацию процессов на Уровне 2 и/или новые или улучшенные управленческие, эксплуатационные или технические меры защиты или контрмеры (или некоторую комбинацию всех трех мер) на Уровне 3. Другим примером потенциального риска, требующего снижения, может служить ситуация, когда противник получает доступ к мобильным устройствам (например, портативным компьютерам или персональным цифровым помощникам) во время путешествий пользователей. Возможные меры по снижению риска включают, например, политики организации, запрещающие транспортировку мобильных устройств в определенные регионы мира, или процедуры получения пользователями чистых мобильных устройств, которые никогда не разрешается подключать к сетям организации.

*Распределение или передача риска*

Распределение риска или передача риска - это подходящий ответ на риск, когда организации хотят и имеют средства переложить обязанности по риску и ответственность на другие организации. Передача риска переносит все обязанности по риску или ответственность с одной организации на другую (например, использование страхования для передачи риска от конкретных организаций к страховым компаниям). Распределение риска перекладывает часть обязанностей по риску или ответственности на другие организации (обычно организации, обладающие более высокой квалификацией для решения проблемы риска). Важно отметить, что передача риска не снижает ни вероятность наступления опасных событий, ни их последствия в виде ущерба для деятельности и активов организации, людей, других организаций или нации. Распределение риска может представлять собой распределение обязанностей или распределение ответственности за другие, адекватные меры реагирования на риск, такие как предотвращение последствий. Поэтому концепция передачи риска менее применима в государственном секторе (например, в федеральных, государственных и местных органах власти), чем в частном секторе, поскольку ответственность организаций обычно устанавливается законодательством или политикой. Таким образом, самостоятельная передача риска организациями государственного сектора (как, например, приобретение страховки), как правило, невозможна. Распределение рисков часто происходит, когда организации определяют, что для устранения риска требуется опыт или ресурсы, которые лучше предоставить другим организациям. Например, выявленный риск может заключаться в физическом проникновении через периметр и кинетических атаках со стороны террористических групп. Организация решает установить партнерские отношения с другой организацией, совместно использующей физический объект, чтобы взять на себя совместную ответственность за устранение риска от кинетических атак.

ОЦЕНКА АЛЬТЕРНАТИВ

**ЗАДАЧА 3-2:** Оценка альтернативных планов действий по реагированию на риски.

**Дополнительное Руководство:** Оценка альтернативных планов действий может включать: (i) ожидаемую эффективность в достижении желаемой реакции на риски (и как эффективность измеряется и контролируется); и (ii) ожидаемую осуществимость реализации, включая, например, влияние на предназначение/деятельность, политические, юридические, социальные, финансовые, технические и экономические соображения. Экономические соображения включают затраты в течение ожидаемого периода времени, в течение которого будет осуществляться план действий (например, затраты на закупку, интеграцию в процессы организации на Уровне 1 и/или Уровне 2, информационные системы на Уровне 3, обучение и обслуживание). Во время оценки альтернативных направлений действий можно четко определить компромисс между краткосрочным повышением эффективности или результативности предназначения/деятельности и долгосрочным риском нанесения ущерба предназначению/деятельности из-за компрометации информации или информационных систем, которые обеспечивают эту краткосрочную выгоду. Например, организации, обеспокоенные возможностью компрометации мобильных устройств (например, ноутбуков) во время командировок сотрудников, могут оценить несколько вариантов действий, включая: (i) предоставление пользователям, отправляющимся в зоны повышенного риска, чистых ноутбуков; (ii) извлечение жестких дисков из ноутбуков и работа с CD или DVD; или (iii) проведение детальной оценки ноутбуков, прежде чем разрешить подключение к сетям организации. Первый вариант очень эффективен, поскольку возвращаемые ноутбуки никогда не подключаются к сетям организации. Хотя второй вариант гарантирует, что жесткие диски не могут быть повреждены, он не совсем эффективен, поскольку все еще существует вероятность того, что аппаратные устройства (например, материнские платы) могли быть скомпрометированы. Эффективность третьего варианта ограничена способностью организаций обнаружить потенциальную возможность внедрения вредоносного ПО в аппаратное обеспечение, микропрограмму или программное обеспечение. Таким образом, он является наименее эффективным из трех вариантов. С точки зрения предназначения и деятельности, третий вариант является наилучшей альтернативой, поскольку пользователи имеют доступ к стандартным конфигурациям ноутбуков, включая все приложения и вспомогательные данные, необходимые для выполнения задач, поддерживающих функции предназначения и деятельности. Такие приложения и данные будут недоступны в случае выбора первого или второго вариантов. В конечном счете, оценка плана действий производится на основе оперативных требований, включая требования информационной безопасности, необходимые для обеспечения успеха предназначения/деятельности в ближайшей и долгосрочной перспективе. Бюджетные ограничения, соответствие стратегиям управления инвестициями, гражданские свободы и защита конфиденциальности - вот некоторые из важных элементов, которые организации учитывают при выборе соответствующих действий. В тех случаях, когда организации определяют только один план действий, то оценка сосредоточена на том, является ли этот план действий адекватным. Если план действий считается неадекватным, то организациям необходимо доработать определенный план действий для устранения недостатков или разработать другой план действий (см. Задача 3-1).

В целом, для каждого плана действий осуществляется компромисс между риском и реакцией на риск, чтобы предоставить информацию, необходимую для: (i) выбора между направлениями действий; и (ii) оценки направлений действий с точки зрения эффективности реагирования, затрат, влияния на предназначение/деятельность и любых других факторов, которые считаются

важными для организаций. Как часть компромисса между риском и реакцией на риск рассматривается вопрос конкурирующих ресурсов. С точки зрения организации, это означает, что организации рассматривают, могут ли затраты (например, деньги, персонал, время) на реализацию данного плана действий негативно повлиять на другие функции предназначения или деятельности, и если да, то в какой степени. Это необходимо, поскольку организации имеют ограниченные ресурсы для использования и множество конкурирующих функций предназначения/деятельности по многим элементам организации. Поэтому организации оценивают общую ценность альтернативных планов действий в отношении функций предназначения/деятельности и потенциального риска для каждого элемента организации. Организации могут решить, что независимо от конкретной функции предназначения/деятельности и обоснованности связанного с ней риска, что существуют более важные функции предназначения/деятельности, которые сталкиваются с более значительными рисками и, следовательно, имеют больше прав на ограниченные ресурсы.

РЕШЕНИЯ ПО РЕАГИРОВАНИЮ НА РИСКИ

**ЗАДАЧА 3-3:** Выбор соответствующего плана действий по реагированию на риски.

**Дополнительное Руководство:** Принятие решений о наиболее подходящем плане действий включает в себя определенную форму расстановки приоритетов. Некоторые риски могут вызывать большее беспокойство, чем другие риски. В этом случае может потребоваться направить больше ресурсов на устранение рисков с более высоким приоритетом, чем на другие риски с более низким приоритетом. Это не обязательно означает, что риски с более низким приоритетом не будут рассматриваться. Скорее, это может означать, что на риски с более низким приоритетом может быть направлено меньше ресурсов (по крайней мере, на начальном шаге), или что риски с более низким приоритетом будут рассмотрены позже. Ключевой частью процесса принятия решения о рисках является признание того, что независимо от принятого решения, все еще остается определенная степень остаточного риска, который необходимо устранить. Организации определяют приемлемую степень остаточного риска на основе допустимого риска для организации и допустимостью риска для конкретных лиц, принимающих решения. На процесс принятия решений влияют некоторые более неосязаемые концепции, связанные с риском (например, допустимость риска, доверие и культура). Конкретные убеждения и подходы, принятые в организациях в отношении этих концепций, связанных с риском, влияют на план действий, выбираемый лицами, принимающими решения.

РЕАЛИЗАЦИЯ РЕАГИРОВАНИЯ НА РИСКИ

**ЗАДАЧА 3-4:** Реализация плана действий, выбранного для реагирования на риски.

**Дополнительное Руководство:** После выбора плана действий организации реализуют соответствующие меры реагирования на риски. Учитывая размер и сложность некоторых организаций, фактическая реализация мер реагирования на риски может быть сложной. Некоторые меры реагирования на риски носят тактический характер (например, применение исправлений для выявленных уязвимостей в информационных системах организации) и могут быть реализованы довольно быстро. Другие меры реагирования могут быть более стратегическими по своей природе и отражать решения, на реализацию которых требуется гораздо больше времени. Поэтому организации применяют и адаптируют, если это необходимо для конкретного плана действий по реагированию на риски, соображения по реализации мер реагирования на риски в стратегиях реагирования на риски (часть стратегии управления рисками, разработанной на шаге описания рисков). См. Приложение H, Стратегии реагирования на риски.

### *Результаты и последующие условия*

Результатом шага реагирования на риски является реализация выбранных действий с учетом: (i) лиц или элементов организации, ответственных за выбранные меры реагирования на риски, и определение критериев эффективности (т.е. формулирование показателей и пороговых значений, по которым можно судить об эффективности мер реагирования на риски); (ii) зависимости каждой выбранной меры реагирования на риски от других мер реагирования на риски; (iii) зависимости выбранных мер реагирования на риски от других факторов (например, от реализации других запланированных информационно-технологических мер); (iv) сроки реализации мер по реагированию на риски; (v) планы мониторинга эффективности мер реагирования на риски; (vi) определение триггеров мониторинга рисков; и (vii) промежуточные меры реагирования на риски, выбранные для реализации, если необходимо. Также осуществляется постоянное общение и обмен информацией, связанной с рисками, с отдельными лицами или элементами организации, на которые влияют меры реагирования на риски (включая потенциальные действия, которые могут потребоваться от этих лиц или элементов организации).

В дополнение к шагу мониторинга рисков, результаты шага реагирования на риски могут быть полезными исходными данными для шагов описания рисков и оценки рисков. Например, возможно, что анализ, проводимый во время оценки альтернативных вариантов действий, может поставить под сомнение некоторые аспекты стратегии реагирования на риски, которая является частью стратегии управления рисками, разработанной на шаге описания рисков. В таких случаях организации используют эту информацию для информирования на шаге описания рисков с принятием соответствующих мер для пересмотра стратегии управления рисками и связанной с ней стратегии реагирования на риски. В ходе оценки альтернативных планов действий по реагированию на риски организации могут также определить, что некоторые аспекты оценки рисков являются неполными или неверными. Эта информация может быть использована для информирования на шаге оценки рисков, что может привести к дальнейшему анализу или переоценке рисков.

## 3.4 МОНИТОРИНГ РИСКОВ

Мониторинг рисков предоставляет организациям средства для: (i) проверки *соблюдения требований*;[64] (ii) определения текущей *эффективности* мер реагирования на риски; и (iii) выявления влияющих на риск *изменений* в информационных системах и среде деятельности организации. Анализ результатов мониторинга дает организациям возможность поддерживать осведомленность о возникающем риске, выявлять необходимость пересмотра других шагов процесса управления рисками и инициировать мероприятия по улучшению процесса по мере необходимости.[65] Организации используют инструменты, методы и процедуры мониторинга рисков для повышения осведомленности о рисках, помогая высшим руководителям/руководителям лучше понимать текущий риск для деятельности и активов организации, людей, других организаций и нации. Организации могут внедрять мониторинг рисков на любом из уровней управления рисками с различными целями и полезностью получаемой информации. Например, деятельность по мониторингу на Уровне 1 может включать текущие оценки угроз и того, как изменения в пространстве угроз могут повлиять на деятельность на Уровнях 2 и 3, включая архитектуры предприятий (со встроенными архитектурами информационной безопасности) и информационные системы организации. Деятельность по мониторингу на Уровне 2 может включать, например, анализ новых или текущих технологий, используемых или рассматриваемых для будущего использования организациями, для выявления уязвимостей и/или недостатков этих технологий, которые могут повлиять на успех предназначения/деятельности. Мероприятия по мониторингу на Уровне 3 сосредоточены на информационных системах и могут включать, например, автоматизированный мониторинг стандартных параметров конфигурации продуктов информационных технологий, сканирование уязвимостей и текущую оценку мер безопасности. В дополнение к принятию решений о соответствующих мероприятиях по мониторингу на всех уровнях управления рисками, организации также решают, как будет проводиться мониторинг (например, автоматизированные или ручные подходы) и частоту проведения мероприятий по мониторингу на основе, например, частоты изменения развернутых элементов управления безопасностью, критических пунктов планов действий и этапов их выполнения, а также допустимого риска.

### ШАГ 4: МОНИТОРИНГ РИСКОВ

***Входные данные и предварительные условия***

Входные данные для этого шага включают стратегии реализации выбранных планов действий для реагирования на риски и фактическую реализацию выбранных планов действий. В дополнение к шагу реагирования на риски, шаг мониторинга рисков может получать входные данные от шага описания рисков (например, когда организации становится известно о постоянной развивающейся угрозе, отражающей изменение предположений об угрозах, это может привести к изменению частоты последующих действий по мониторингу). Шаг описания рисков также непосредственно определяет ограничения по ресурсам, связанные с разработкой и внедрением стратегии мониторинга в масштабах организации. В некоторых случаях результаты шага оценки рисков могут стать полезными входными данными для шага мониторинга рисков. Например, пороговые условия оценки риска (например, вероятность использования уязвимостей угрозами) могут быть входными данными к шагу мониторинга риска. В свою очередь, организации могут проводить мониторинг, чтобы определить, выполняются ли такие пороговые условия. Если пороговые условия выполнены, такая информация может быть использована на шаге оценки рисков, где она может служить основой для инкрементной, дифференциальной оценки рисков или общей переоценки рисков для организации.

***Действия***

СТРАТЕГИЯ МОНИТОРИНГА РИСКОВ

**ЗАДАЧА 4-1:** Разработка стратегии мониторинга рисков для организации, включающей цель, тип и частоту мероприятий по мониторингу.

[64] Проверка соответствия гарантирует, что организации внедрили требуемые меры реагирования на риски и что требования информационной безопасности, вытекающие и прослеживаемые из функций предназначения/деятельности организации, федерального законодательства, директив, правил, политик и стандартов/руководств, выполнены.

[65] Проект специальной публикации NIST 800-137 содержит руководство по мониторингу информационных систем организации и среды функционирования.

**Дополнительное руководство:** Организации реализуют программы мониторинга рисков: (i) для проверки того, что требуемые меры реагирования на риски реализованы и что требования информационной безопасности, вытекающие из и прослеживаемые к функциям предназначения/деятельности организации, федерального законодательства, директив, нормативных документов, политики и стандартов/руководств, выполнены (*мониторинг соблюдения требований*); (ii) для определения текущей эффективности мер реагирования на риски после реализации мер (*мониторинг эффективности*); и (iii) для выявления изменений в информационных системах организации и среде, в которой функционируют системы, которые могут повлиять на риски (*мониторинг изменений*), включая изменения в целесообразности текущей реализации мер реагирования на риски. Определение цели программ мониторинга рисков непосредственно влияет на средства, используемые организациями для проведения мониторинга, и на то, где проводится мониторинг (т.е. на каких уровнях управления рисками). Организации также определяют тип мониторинга, который будет применяться, включая подходы, основанные на автоматизации, или подходы, основанные на процедурных/ручных действиях с вмешательством человека. Наконец, организации определяют, как часто проводится мониторинг, балансируя между ценностью, получаемой от частого мониторинга, и потенциальными сбоями в работе, например, из-за прерывания процессов предназначения/деятельности, снижения операционной пропускной способности во время мониторинга и переключения ресурсов с деятельности на мониторинг. Стратегии мониторинга, разработанные на Уровне 1, влияют и задают направление для аналогичных стратегий, разрабатываемых на Уровнях 2 и 3, включая мероприятия по мониторингу, связанные с системой управления рисками на уровне информационной системы.

*Мониторинг соблюдения требований*

Мониторинг соблюдения требований применяется чтобы гарантировать, что организации осуществляют необходимые меры реагирования на риски. Это включает обеспечение того, что меры реагирования на риски, выбранные и реализованные организациями в ответ на описание рисков, полученное в результате оценки рисков, реализованы правильно и работают так, как предполагалось. Неспособность реализации мер реагирования на риски, выбранных организациями, может привести к тому, что организации будут продолжать подвергаться выявленным рискам. Мониторинг соблюдения требований является самым простым видом мониторинга, поскольку обычно существует конечный набор мер реагирования на риски, применяемых организациями, как правило, в форме мер безопасности. Такие меры обычно четко определены и сформулированы как результат шага реагирования на риски. Более сложной частью мониторинга соблюдения требований является оценка того, насколько правильно (и в некоторых случаях постоянно) реализуются меры реагирования на риски. Мониторинг соблюдения требований также включает, по мере возможности, анализ того, почему не удалось добиться соблюдения требований. Причины несоблюдения требований могут быть самыми разными: от того, что люди не смогли правильно выполнить свою работу, до того, что мера реагирования на риски не сработала должным образом. Если мониторинг указывает на нарушение соблюдения требований, то необходимо вернуться к шагу реагирования в процессе управления рисками. Ключевым элементом обратной связи на шаге реагирования являются результаты мониторинга соблюдения требований, указывающие на причину несоблюдения требований. В некоторых случаях несоблюдение требованиям может быть устранено простым повторным внедрением тех же мер реагирования на риски с небольшими изменениями или без них. Но в других случаях несоблюдение требований является более сложным (например, выбранные меры реагирования на риски слишком трудно реализовать или меры не функционируют так, как ожидалось). В таких случаях организациям может потребоваться вернуться к шагам оценки и принятия решений на шаге реагирования на риски, чтобы разработать другие меры реагирования на риски.

*Мониторинг эффективности*

Мониторинг эффективности используется организациями для определения того, были ли внедренные меры реагирования на риски действительно эффективными в снижении идентифицированных рисков до желаемого уровня. Хотя мониторинг эффективности отличается от мониторинга соблюдения требований, неспособность достичь желаемого уровня эффективности может быть признаком того, что меры реагирования на риски были внедрены неправильно или не работают так, как предполагалось. Определение эффективности мер реагирования на риски, как правило, является более сложной задачей, чем определение того, были ли эти меры реализованы правильно и действуют ли они в соответствии с поставленной целью (т.е. отвечают ли они установленным требованиям соответствия). Меры реагирования на риски, принятые правильно и действующие в соответствии с планом, не гарантируют эффективного снижения риска. В первую очередь это связано с: (i) сложностью среды деятельности, которая может порождать непредвиденные последствия; (ii) последующими изменениями в уровнях риска или связанных с ним факторах риска (например, угрозах, уязвимостях, воздействиях или вероятности); (iii) несоответствующими или неполными критериями, установленными в качестве результата шага реагирования на риски; и (iv) изменениями в информационных системах и среде деятельности после внедрения мер реагирования на риски. Это особенно актуально, когда организации пытаются определить, были ли достигнуты более стратегические результаты, и для более динамичной среды деятельности. Например, если желаемым результатом для организаций является снижение восприимчивости к постоянным развивающимся угрозам, это может быть трудно измерить, поскольку эти типы угроз по определению очень трудно обнаружить. Даже когда организациям удается установить критерии эффективности, часто бывает трудно получить критерии, поддающиеся количественной оценке. Поэтому вопрос о том, являются ли внедренные меры по реагированию на риски в конечном итоге эффективными, может стать предметом субъективного суждения. Более того, даже если количественно измеримые критерии эффективности предоставлены, может быть трудно определить, удовлетворяет ли предоставленная информация критериям. Если организации определят, что меры реагирования на риски неэффективны, то может возникнуть необходимость вернуться к шагу реагирования на риски. Как правило, при недостаточной эффективности организации не могут просто вернуться к реализации части шага реагирования на риски. Поэтому, в зависимости от причины отсутствия эффективности, организации пересматривают все части шага реагирования на риски (т.е. разработку, оценку, принятие решения и реализацию) и, возможно, шаг оценки рисков. Эти действия могут привести к тому, что организации разработают и внедрят совершенно новые меры реагирования на риски.

*Мониторинг изменений*

В дополнение к мониторингу соблюдения требований и мониторингу эффективности организации отслеживают изменения в информационных системах организации и средах, в которых функционируют эти системы. Мониторинг изменений в информационных системах и средах функционирования не связан напрямую с предыдущими мерами реагирования на риски, но, тем не менее, он важен для обнаружения изменений, которые могут повлиять на риски для деятельности и активов организации, людей, других организаций и нации. Как правило, такой мониторинг позволяет обнаружить изменения в условиях, которые могут подорвать предположения о рисках (сформулированные на шаге описания рисков).

- *Информационная система:* В информационных системах организации (включая оборудование, программное обеспечение и микропрограммное обеспечение) могут происходить изменения, которые могут привнести новые риски или изменить существующие риски. Например, обновления программного обеспечения операционной системы могут устранить возможности безопасности, которые существовали в более ранних версиях, тем самым внося новые уязвимости в информационные системы организации. Другим примером является обнаружение новых уязвимостей системы, которые выходят за рамки имеющихся инструментов и процессов для устранения таких уязвимостей (например, уязвимости, для которых не существует установленных средств защиты).
- *Среды функционирования:* Среда, в которой функционируют информационные системы, также может измениться таким образом, что это приведет к появлению новых рисков или изменению существующих рисков. Среда и эксплуатационные соображения включают, но не ограничиваются функциями предназначения/деятельности, угрозами, уязвимостями, процессами предназначения/деятельности, средствами, политикой, законодательством и технологиями. Например, может быть принято новое законодательство или нормативные акты, которые налагают дополнительные требования на организации. Это изменение может повлиять на допустимый риск, установленный организациями. Другим примером является изменение среды угроз, которое предоставляет информацию о новых тактиках, методах, процедурах или увеличении технических возможностей противников. Организации могут столкнуться с сокращением доступных ресурсов (например, персонала или финансирования), что в свою очередь приводит к изменению приоритетов. Организации также могут столкнуться с изменениями в собственниках сторонних поставщиков, что может повлиять на риск цепочки поставок. Изменение предназначения может потребовать от организаций пересмотреть основные предположения о рисках. Например, организация, в задачи которой входит сбор информации об угрозах возможных внутренних террористических атак и обмен такой информацией с соответствующими федеральными правоохранительными и разведывательными органами, может изменить сферу своей деятельности таким образом, что организация будет отвечать за обмен частью информации с местными службами быстрого реагирования. Такое изменение может повлиять на предположения относительно ресурсов безопасности, которые могут иметь в своем распоряжении такие пользователи. Изменения в технологии могут также повлиять на базовые предположения о рисках, установленные организациями. В отличие от других типов изменений, технологические изменения могут быть совершенно независимыми от организаций, но все же влиять на риски, которые организации должны учитывать. Например, улучшение вычислительной мощности может подорвать предположения о том, что представляет собой достаточно надежное средство аутентификации (например, количество факторов аутентификации) или криптографический механизм.

*Автоматизированный мониторинг в сравнении с ручным*

В целом, организации могут проводить мониторинг как автоматизированными, так и ручными методами. Если автоматизированный мониторинг возможен, его следует использовать, поскольку он, как правило, быстрее, эффективнее и экономичнее, чем ручной мониторинг. Автоматизированный мониторинг также менее подвержен человеческим ошибкам. Однако не для всех видов мониторинга можно использовать преимущества автоматизации. Мониторинг, проводимый на Уровне 3, как правило, поддается автоматизации, если отслеживаемая деятельность основана на информационных технологиях. Такая деятельность обычно может быть обнаружена, отслежена и проконтролирована путем установки соответствующего программного обеспечения, аппаратных средств и/или встроенного программного обеспечения. Для обеспечения того, чтобы автоматизированные процессы, процедуры и/или механизмы, поддерживающие деятельность по мониторингу, предоставляли необходимую информацию, такие процессы, процедуры и механизмы должны быть соответствующим образом проверены, обновлены и проконтролированы. Мониторинг соблюдения требований может быть поддержан автоматизацией, когда проверяемые меры по снижению риска основаны на информационных технологиях (например, установка брандмауэров или проверка параметров конфигурации на настольных компьютерах). Такая автоматизированная проверка часто может проверить, установлены ли меры по снижению риска и правильно ли они установлены. Аналогичным образом, контроль эффективности также может поддерживаться автоматизацией. Если пороговые условия для определения эффективности мер по снижению риска заранее определены, то автоматизация может поддерживать такой мониторинг эффективности. Хотя автоматизация может быть вспомогательным средством для Уровней 1 и 2, в целом автоматизация не дает существенного представления о деятельности, не связанной с информационными технологиями, которая более распространена на этих более высоких уровнях. Виды деятельности, которые, скорее всего, не выиграют от автоматизации, включают, например, использование нескольких поставщиков в цепочке поставок, изменяющиеся условия деятельности или оценка перспектив новых технических возможностей для поддержки функций предназначения/деятельности. Там, где автоматизированный мониторинг недоступен, организации используют ручной мониторинг и/или анализ.

*Частота мониторинга*

Частота мониторинга рисков (автоматизированного или ручного) определяется функциями предназначения/деятельности организаций и способностью организаций использовать результаты мониторинга для повышения уровня ситуационной осведомленности. Повышение уровня ситуационной осведомленности о состоянии безопасности информационных систем и среды деятельности организации помогает организациям лучше понимать риски. Частота мониторинга также определяется другими факторами, например: (i) предполагаемой частотой изменений в информационных системах и среде деятельности организации; (ii) потенциальным воздействием риска, если он не будет должным образом устранен с помощью соответствующих мер реагирования; и (iii) степенью изменения пространства угроз. На частоту мониторинга также может влиять тип проводимого

мониторинга (т.е. автоматизированные или процедурные подходы). В зависимости от частоты мониторинга, требуемого организациями, в большинстве ситуаций мониторинг наиболее эффективен и рентабелен при использовании автоматизации. Мониторинг может обеспечить значительные преимущества, особенно в ситуациях, когда такой мониторинг ограничивает возможности противников закрепиться в организациях (либо через информационные системы, либо через среду, в которой функционируют эти системы). Когда организации используют ручной мониторинг, как правило, неэффективно проводить его с той частотой, которую позволяет автоматизация. В некоторых случаях редкий мониторинг не является серьезной проблемой. Например, функции предназначения/деятельности, средства, законодательство, политика и технологии имеют тенденцию меняться более постепенно и поэтому не требуют частого мониторинга. Вместо этого, такие типы изменений лучше подходят для мониторинга на основе условий/событий (например, если функции предназначения и/или деятельности меняются, то мониторинг таких изменений уместен для определения того, влияют ли эти изменения на риски).

МОНИТОРИНГ РИСКОВ

**ЗАДАЧА 4-2:** Осуществление постоянного мониторинга информационных систем и среды деятельности организации для проверки соответствия требованиям, определения эффективности мер реагирования на риски и выявления изменений.

**Дополнительное руководство:** После того как организации завершают разработку своих стратегий мониторинга, эти стратегии внедряются в масштабах всей организации. Поскольку существует много различных аспектов мониторинга, могут выполняться не все аспекты мониторинга, или они могут выполняться в разное время. Конкретные аспекты мониторинга, которые выполняются, в основном диктуются предположениями, ограничениями, допустимым риском и приоритетами/ компромиссами, установленными организациями на шаге описания рисков. Например, хотя организации могут хотеть проводить все виды мониторинга (т.е. соблюдения требований, эффективности и изменений), ограничения, налагаемые на организации, могут позволить только мониторинг соблюдения требований, который может быть легко автоматизирован на Уровне 3. Если можно поддерживать несколько аспектов мониторинга, результаты шага описания рисков помогают организациям определить степень акцента и уровень усилий, которые необходимо приложить к различным видам мониторинга.

Как отмечалось выше, не все мероприятия по мониторингу проводятся на одних и тех же уровнях, с одной и той же целью, в одно и то же время или с использованием одних и тех же методов. Однако важно, чтобы организации пытались координировать различные мероприятия по мониторингу. Координация деятельности по мониторингу облегчает обмен информацией, связанной с рисками, которая может быть полезна для организаций при раннем предупреждении, разработке информации о тенденциях или своевременном и эффективном распределении мер по реагированию на риски. Если мониторинг не координируется, то польза от него может быть снижена, что может подорвать общие усилия по выявлению и устранению рисков. По мере возможности организации осуществляют различные мероприятия по мониторингу таким образом, чтобы максимизировать общую цель мониторинга, не ограничиваясь целями конкретных мероприятий по мониторингу. Результаты мониторинга рисков применяются при проведении дополнительных оценок рисков для поддержания осведомленности о существующих рисках, для выявления изменений в рисках и для указания необходимости повторного рассмотрения других шагов процесса управления рисками, если это необходимо.

### *Результаты и последующие условия*

Результатом шага мониторинга рисков является информация, полученная путем: (i) проверки того, что требуемые меры реагирования на риски реализованы и что требования информационной безопасности, вытекающие из и прослеживаемые к функциям предназначения/деятельности организации, федерального законодательства, директив, нормативных документов, политики и стандартов/руководств, удовлетворены; (ii) определения текущей эффективности мер реагирования на риски; и (iii) выявления изменений в информационных системах и средах деятельности организации. Результаты шага мониторинга рисков могут стать полезными исходными данными для шагов описания рисков, оценки рисков и реагирования на риски. Например, результаты мониторинга соблюдения требований могут потребовать от организаций повторного рассмотрения части реализации шага реагирования на риски, в то время как результаты мониторинга эффективности могут потребовать от организаций повторного рассмотрения всего шага реагирования на риски. Результаты мониторинга изменений в информационных системах и средах деятельности могут потребовать от организаций повторного обращения к шагу оценки рисков. Результаты шага мониторинга рисков могут также служить для шага описания рисков (например, когда организации обнаруживают новые угрозы или уязвимости, которые влияют на изменения в предположениях организации о рисках, допустимых рисках и/или приоритетах/компромиссах).

## ПРИЛОЖЕНИЕ А

# ССЫЛКИ

ЗАКОНЫ, ПОЛИТИКИ, ДИРЕКТИВЫ, ИНСТРУКЦИИ, СТАНДАРТЫ И РУКОВОДЯЩИЕ ПРИНЦИПЫ

### ЗАКОНОДАТЕЛЬСТВО

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

### ПОЛИТИКИ, ДИРЕКТИВЫ, ИНСТРУКЦИИ

1. Committee on National Security Systems (CNSS) Instruction 4009, National Information Assurance (IA) Glossary, April 2010.
2. Committee on National Security Systems (CNSS) Instruction 1253, Security Categorization and Control Selection for National Security Systems, October 2009.
3. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, Management of Federal Information Resources, November 2000.

### СТАНДАРТЫ

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.
3. ISO/IEC 15408:2005, Common Criteria for Information Technology Security Evaluation, 2005.

### РУКОВОДСТВА

1. National Institute of Standards and Technology Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, February 2006.
2. National Institute of Standards and Technology Special Publication 800-30, Revision 1, Guide for Conducting Risk Assessments, (Projected Publication Spring 2011).
3. National Institute of Standards and Technology Special Publication 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010.
4. National Institute of Standards and Technology Special Publication 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009.
5. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans, June 2010.
6. National Institute of Standards and Technology Special Publication 800-59, Guideline for Identifying an Information System as a National Security System, August 2003.

7. National Institute of Standards and Technology Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.

8. National Institute of Standards and Technology Special Publication 800-70, Revision 1, National Checklist Program for IT Products--Guidelines for Checklist Users and Developers, September 2009.

9. National Institute of Standards and Technology Special Publication 800-137, Initial Public Draft, Information Security Continuous Monitoring for Federal Information Systems and Organizations, December 2010.

## ПРИЛОЖЕНИЕ B

# ГЛОССАРИЙ

ОБЩИЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В данном приложении приведены определения терминов по безопасности, используемых в Специальной публикации 800-39. Термины в глоссарии соответствуют терминам, используемым в комплексе стандартов и руководств по безопасности, связанных с FISMA, разработанных NIST. Если не указано иное, все термины, используемые в данной публикации, также соответствуют определениям, содержащимся в Инструкции CNSS 4009 "Национальный глоссарий по информационному доверию (IA)".

| | |
|---|---|
| Adequate Security<br>Адекватная безопасность<br>[Циркуляр OMB A-130, Приложение III] | Безопасность, соизмеримая с риском и величиной ущерба, возникающего в результате потери, неправильного использования или несанкционированного доступа к информации или ее модификации. |
| Advanced persistent threat<br>Постоянная развивающаяся угроза | Противник, который обладает высоким уровнем компетентности и существенными ресурсами, которые позволяют ему создавать возможности для достижения его целей при использовании множественных векторов атаки (например, кибернетическая, физическая и радиоэлектронное подавление). Эти цели, как правило, включают создание и расширение плацдармов в инфраструктуре информационных технологий намеченных организаций с целью утечки информации, подрыва или воспрепятствования критическим аспектам предназначения, программ или организации; или размещение их, чтобы выполнить эти цели в будущем. Постоянная развивающаяся угроза: (i) неоднократно преследует свои цели в течение длительного периода времени; (ii) приспосабливается к усилиям защитников сопротивляться ей; и (iii) определяет, как поддерживать уровень взаимодействия, необходимый для выполнения её целей. |
| Agency<br>Агентство | См. *Executive Agency.* |
| Assessment<br>Оценка | См. *Security Control Assessment*. |
| Assessor<br>Оценщик | См. *Security Control Assessor.* |
| Assurance<br>Доверие<br>[CNSSI 4009] | Мера уверенности в том, что средства, методы, процедуры обеспечения безопасности и архитектура информационной системы точно представляют и осуществляют политику безопасности. |
| [NIST SP 800-53] | Основания для уверенности в том, что набор мер безопасности, предусмотренных в информационной системе, эффективен при их применении. |
| Assurance Case<br>Кейс доверия<br>[Институт программной инженерии, университет Карнеги-Меллона] | Структурированный набор аргументов и совокупности свидетельств, показывающий, что информационная система удовлетворяет определенным утверждениям относительно заданного показателя качества. |
| Authentication<br>Аутентификация<br>[FIPS 200] | Проверка идентификационных данных пользователя, процесса или устройства, обычно как предпосылка для предоставления доступа к ресурсам в информационной системе. |

| | |
|---|---|
| Authenticity<br>Аутентичность | Свойство, определяющее подлинность и возможность проверки и доверия; уверенность в достоверности передачи, сообщения или автора сообщения. См. *Authentication.* |
| Authorization (to operate)<br>Санкционирование (для применения) | Официальное управленческое решение, принимаемое высшим должностным лицом организации для разрешения применения информационной системы и явного принятия рисков в отношении деятельности организации (включая предназначение, функции, имидж или репутацию), активов организации, людей, других организаций и нации, на основе реализации согласованного набора мер безопасности. |
| Authorization Boundary<br>Граница санкционирования<br>[NIST SP 800-37] | Все компоненты информационной системы, которая санкционирована для применения санкционирующим должностным лицом, исключая отдельно санкционированные системы, с которыми соединена информационная система. |
| Authorizing Official<br>Санкционирующее должностное лицо<br>[CNSSI 4009] | Высшее (федеральное) должностное лицо или руководитель с полномочиями по официальному принятию на себя ответственности за применение информационной системы при допустимом уровне риска в отношении деятельности организации (включая предназначение, функции, имидж или репутацию), активов организации, людей, других организаций и нации. |
| Availability<br>Доступность<br>[44 U.S.C., Sec. 3542] | Обеспечение своевременного и надежного доступа к информации и её использования. |
| Chief Information Officer<br>Директор по информации<br>[PL 104-106, Раздел 5125 (b)] | Должностное лицо агентства, ответственное за:<br>(i) предоставление консультаций и другой помощи руководителю исполнительного агентства и другому высшему управленческому персоналу агентства, чтобы гарантировать, что информационные технологии приобретаются и информационные ресурсы управляются в соответствии с законами, правительственными распоряжениями, директивами, политиками, нормативными актами и приоритетами, установленными руководителем агентства;<br>(ii) разработку, поддержание и содействие внедрению соответствующей и интегрированной архитектуры информационных технологий для агентства; и<br>(iii) содействие эффективной и рациональной разработке и использованию всех основных процессов управления информационными ресурсами агентства, включая совершенствование рабочих процессов агентства. |
| Chief Information Security Officer<br>Директор по информационной безопасности | См. *Senior Agency Information Security Officer.* |
| Classified National Security Information<br>Классифицированная информация по национальной безопасности [CNSSI 4009] | Информация, которая была определена в соответствии с Правительственным распоряжением 13526 или любым предшествующим распоряжением как требующая защиты от несанкционированного раскрытия и помеченная для указания ее классифицированного статуса, когда она находится в документальной форме. |

| | |
|---|---|
| Common Control<br>Общая мера безопасности<br>[NIST SP 800-37] | Мера безопасности, которая является наследуемой одной или более информационными системами организации. См. *Security Control Inheritance*. |
| Common Control Provider<br>Поставщик общих мер безопасности<br>[NIST SP 800-37] | Должностное лицо организации, ответственное за разработку, реализацию, оценку и мониторинг общих мер безопасности (то есть, мер безопасности, наследуемых информационными системами). |
| Compensating Security Controls<br>Компенсирующие меры безопасности<br>[CNSSI 4009] | Управленческие, эксплуатационные и/или технические меры (т.е. защитные меры или контрмеры), используемые организацией вместо рекомендованных мер безопасности в низком, умеренном или высоком базовых наборах, которые обеспечивают эквивалентную или сопоставимую защиту информационной системы. |
| Confidentiality<br>Конфиденциальность<br>[44 U.S.C., Sec. 3542] | Сохранение установленных ограничений на доступ к информации и её раскрытие, включая средства для защиты персональной приватной и служебной информации. |
| Course of Action (Risk Response)<br>План действий (реагирования на риски) | Комбинация мер реагирования на риски с разбивкой по времени или в зависимости от ситуации. |
| Cyber Attack<br>Кибератака<br>[CNSSI 4009] | Атака, через киберпространство, направленная на использование предприятием киберпространства с целью нарушения, выведения из строя, уничтожения или злонамеренного управления вычислительной средой/инфраструктурой; либо нарушения целостности данных или похищения контролируемой информации. |
| Cyber Security<br>Кибербезопасность<br>[CNSSI 4009] | Способность защищать или оборонять использование киберпространства от кибератак. |
| Cyberspace<br>Киберпространство<br>[CNSSI 4009] | Глобальная область в информационной среде, состоящая из взаимозависимой сети инфраструктур информационных систем включая Интернет, телекоммуникационные сети, компьютерные системы и встроенные процессоры и контроллеры. |
| Defense-in-Breadth<br>Широкая защита<br>[CNSSI 4009] | Спланированный, систематизированный набор мультидисциплинарных мероприятий, направленный на выявление, управление и снижение риска использования уязвимостей на каждой стадии жизненного цикла системы, сети или субкомпонента (проектирование и разработка; производство; упаковка; сборка; системная интеграция; поставка; эксплуатация; поддержка; и ликвидация системы, сети или продукта). |
| Defense-in-Depth<br>Эшелонированная защита | Стратегия информационной безопасности, объединяющая людей, технологии и оперативные возможности для создания разнообразных барьеров на нескольких уровнях и для различных предназначений организаций. |

| | |
|---|---|
| Enterprise<br>Предприятие<br>[CNSSI 4009] | Организация с определенным предназначением/целью и определенными границами, использующая информационные системы для выполнения этого предназначения, и с ответственностью за управление собственными рисками и результатами деятельности. Предприятие может включать все или некоторые из следующих аспектов деятельности: приобретение, управление программами, управление финансами (например, бюджетами), людские ресурсы, безопасность, а также информационные системы, информацию и управление предназначением. См. *Организация*. |
| Enterprise Architecture<br>Архитектура предприятия<br>[CNSSI 4009] | Описание всего набора информационных систем предприятия: как они настроены, как они интегрированы, как они взаимодействуют с внешней средой на границе предприятия, как они работают для поддержки предназначения предприятия, и как они вносят вклад в общую безопасность предприятия. |
| Environment of Operation<br>Среда функционирования<br>[NIST SP 800-37] | Физическое окружение, в котором информационная система обрабатывает, хранит и передаёт информацию. |
| Executive Agency<br>Исполнительное агентство<br>[41 U.S.C., Sec. 403] | Исполнительный департамент, определенный в 5 U.S.C., Раздел 101; военный департамент, определенный в 5 U.S.C., Раздел 102; независимое учреждение, как определено в 5 U.S.C., Раздел 104 (1); и корпорация, полностью находящаяся в собственности Правительства, полностью попадающая под действие 31 U.S.C., Глава 91. |
| Federal Agency<br>Федеральное агентство | См. *Executive Agency.* |
| Federal Information System<br>Федеральная информационная система<br>[40 U.S.C., Sec. 11331] | Информационная система, которая используется или управляется исполнительным агентством, подрядчиком исполнительного агентства или другой организацией от имени исполнительного агентства. |
| Hybrid Security Control<br>Гибридная мера безопасности<br>[NIST SP 800-53] | Мера безопасности, которая реализована в информационной системе частично как общая мера безопасности и частично как специфичная для системы мера безопасности. См. *Common Control* и *System-Specific Security Control*. |
| Individuals<br>Физические лица | Объект оценки, включающий людей, применяющих спецификации, механизмы или мероприятия. |
| Industrial Control System<br>Промышленная система управления | Информационная система, используемая для управления промышленными процессами, такими как производство, обработка продукции, выпуск и распределение. Промышленные системы управления включают системы диспетчерского контроля и сбора данных, используемые для управления территориально распределенными активами, а также распределенные системы управления и небольшие системы управления, использующие контроллеры с программируемой логикой для управления локальными процессами. |
| Information<br>Информация<br>[CNSSI 4009] | Любое сообщение или представление знаний, таких как факты, данные или мнения на любом носителе или в любой форме, включая текстовую, числовую, графическую, картографическую, описательную или аудиовизуальную. |
| [FIPS 199] | Частный случай типа информации. |

| | |
|---|---|
| Information Owner<br>Владелец информации<br>[CNSSI 4009] | Должностное лицо с установленными законом или исполнительными полномочиями для указанной информации и ответственностью за установление мер безопасности по ее созданию, классификации, сбору, обработке, распространению и ликвидации. |
| Information Resources<br>Информационные ресурсы<br>[44 U.S.C., Sec. 3502] | Информация и связанные ресурсы, такие как персонал, оборудование, фонды и информационные технологии. |
| Information Security<br>Информационная безопасность<br>[44 U.S.C., Sec. 3542] | Защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, разрушения, модификации или уничтожения, с целью обеспечения конфиденциальности, целостности и доступности. |
| Information Security Architecture<br>Архитектура информационной безопасности | Встроенная, неотъемлемая часть архитектуры предприятия, которая описывает структуру и поведение процессов безопасности предприятия, систем информационной безопасности, персонала и подразделений организации, демонстрируя их соответствие предназначению и стратегическим планам предприятия. |
| Information Security Program Plan<br>План Программы информационной безопасности<br>[NIST SP 800-53] | Формальный документ, содержащий описание требований безопасности для программы информационной безопасности всей организации и описывающий меры управления программой и имеющиеся или планируемые общие меры безопасности для удовлетворения этим требованиям. |
| Information Steward<br>Управляющий информацией<br>[CNSSI 4009] | Должностное лицо агентства с установленными законом или исполнительными полномочиями для указанной информации и ответственностью за установление мер безопасности для ее создания, сбора, обработки, распространения и уничтожения. |
| Information System<br>Информационная система<br>[44 U.S.C., Sec. 3502] | Дискретный набор информационных ресурсов, организованных для сбора, обработки, поддержки, использования, обмена, распространения или ликвидации информации. |
| Information System Boundary<br>Границы информационной системы | См. *Authorization Boundary*. |
| Information System Owner<br>(or Program Manager)<br>Владелец информационной системы (или руководитель программы) | Должностное лицо, ответственное в целом за приобретение, разработку, интеграцию, модификацию или эксплуатацию и поддержку информационной системы. |
| Information System Resilience<br>Устойчивость информационной системы | Способность информационной системы: (i) продолжать работать в неблагоприятных условиях или при воздействии, даже если она находится в деградированном или ослабленном состоянии, сохраняя основные эксплуатационные возможности; и (ii) восстанавливаться до эффективного эксплуатационного состояния в сроки, соответствующие потребностями предназначения. |
| Information System Security Officer<br>Сотрудник безопасности информационной системы<br>[CNSSI 4009] | Физическое лицо, на которое высшим должностным лицом по информационной безопасности агентства, санкционирующим должностным лицом, должностным лицом администрации или владельцем информационной системы возложена ответственность за поддержание соответствующей безопасности применения информационной системы или программы. |

| | |
|---|---|
| Information Security Risk<br>Риск информационной безопасности | Риск для деятельности организации (включая предназначение, функции, имидж, репутацию), активов организации, людей, других организаций и нации в связи с возможностью несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения информации и/или информационных систем. |
| Information System-Related Security Risks<br>Риски безопасности, связанные с информационной системой | Риски, возникающие в результате потери конфиденциальности, целостности, или доступность информации или информационных систем и которые учитывают воздействие на организацию (включая активы, предназначение, функции, имидж или репутацию), людей, другие организации и нацию. См. *Риск*. |
| Information Technology<br>Информационная технология<br>[40 U.S.C., Sec. 1401] | Любое оборудование, взаимосвязанная система или подсистема оборудования, которое используется в автоматизированном получении, хранении, манипулировании, управлении, перемещении, контроле, отображении, коммутации, взаимообмене, передаче или приеме данных или информации исполнительным агентством. Для целей предыдущего предложения, оборудование используется исполнительным агентством, если оборудование используется исполнительным агентством непосредственно или используется подрядчиком по контракту с исполнительным агентством, который: (i) требует использования такого оборудования; или (ii) требует использования в значительной степени такого оборудования при исполнении услуги или поставке продукта. Термин «информационная технология» включает компьютеры, вспомогательное оборудование, программное обеспечение, встроенное микропрограммное обеспечение, и подобные процедуры, услуги (включая услуги поддержки) и связанные с ними ресурсы. |
| Information Type<br>Тип информации<br>[FIPS 199] | Конкретная категория информации (например, приватная, медицинская, служебная, финансовая, следственная, чувствительная для подрядчика, управления безопасностью), определенная организацией или, в некоторых случаях, конкретным законом, Правительственным распоряжением, директивой, политикой или нормативным документом. |
| Integrity<br>Целостность<br>[44 U.S.C., Sec. 3542] | Защита против неправомерной модификации или уничтожения информации, включающая обеспечение неотказуемости и аутентичности информации. |
| Management Controls<br>Управленческие меры безопасности<br>[FIPS 200] | Меры безопасности (т.е. меры защиты или контрмеры) для информационной системы, которые направлены на управление рисками и управление безопасностью информационной системы. |

| | |
|---|---|
| National Security System<br>Система национальной безопасности<br>[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, применение или использование которой включает разведывательную деятельность; включает криптологические работы, связанные с национальной безопасностью; включает руководство и управление вооруженными силами; включает оборудование, которое является неотъемлемой частью оружия или системы оружия; или является критически важной для непосредственного выполнения военных или разведывательных задач (исключая системы, которые должны использоваться для стандартных административных и деловых приложений, например, приложения для расчёта заработной платы, финансов, логистики и управления персоналом); или: (ii) постоянно защищена процедурами, установленными для информации, которая была специально определена критериями, установленными Правительственным распоряжением или законом конгресса, как классифицированная в интересах национальной обороны или внешней политики. |
| Operational Controls<br>Эксплуатационные меры безопасности<br>[FIPS 200] | Меры безопасности (т.е. меры защиты или контрмеры) для информационной системы, которые в основном реализуются и выполняются людьми (в отличие от систем). |
| Organization<br>Организация<br>[FIPS 200, уточненный] | Сущность любого размера, сложности или положения в организационной структуре (например, федеральное агентство или, в соответствующих случаях, любой из его оперативных элементов). |
| Plan of Action and Milestones<br>План действий и вехи<br>[Меморандум OMB 02-01] | Документ, определяющий задачи, которые необходимо выполнить. В нем подробно описываются ресурсы, необходимые для выполнения элементов плана, этапы выполнения задач и запланированные даты завершения этапов. |
| Reciprocity<br>Соглашение о взаимности<br>[CNSSI 4009] | Взаимное соглашение между участвующими организациями о принятии оценок безопасности друг друга для повторного использования ресурсов информационной системы и/или о принятии оцененных позиций безопасности друг друга для обмена информацией. |
| Resilience<br>Устойчивость | См. *Information System Resilience*. |
| Risk<br>Риск<br>[CNSSI 4009] | Мера степени, до которой сущности угрожают потенциальные обстоятельства или события и, как правило, является функцией от: (i) негативных последствий, которые возникнут в случае наступления обстоятельства или события; и (ii) вероятности наступления.<br>[Примечание: Риски безопасности, связанные с информационной системой, - это риски, которые возникают в результате потери конфиденциальности, целостности или доступности информации или информационных систем и отражают потенциальные негативные последствия для деятельности организации (включая предназначение, функции, имидж или репутацию), активов организации, людей, других организаций и нации]. |

| | |
|---|---|
| Risk Assessment<br>Оценка рисков | Процесс определения рисков для деятельности организации (включая предназначение, функции, имидж, репутацию), активов организации, людей, других организаций и нации, следующих из применения информационной системы.<br><br>Часть управления рисками, включающая анализ угроз и уязвимостей, и учитывающая их снижение, обеспечиваемое существующими или планируемыми мерами безопасности. Синоним анализа рисков. |
| Risk Executive (Function)<br>Ответственный за риски (функция)<br>[CNSSI 4009] | Лицо или группа лиц в организации, которые помогают обеспечить, чтобы: (i) связанные с риском рассмотрения безопасности для отдельных информационных систем, включая решения о санкционировании для этих систем, рассматривались с точки зрения всей организации относительно общих стратегических целей и задач организации по выполнению её функций предназначения и деятельности; и (ii) управление риском для отдельных информационных систем было последовательным в рамках организации, отражало допустимый риск для организации и рассматривалось наряду с другими рисками организации, влияющими на успех её предназначения/деятельности. |
| Risk Management<br>Управление рисками<br>[CNSSI 4009, уточненный] | Программа и поддерживающие процессы по управлению рисками информационной безопасности для деятельности организации (включая предназначение, функции, имидж и репутацию), активов организации, людей, других организаций и нации, включающие: (i) установление контекста для работ, связанных с рисками; (ii) оценку рисков; (iii) реагирование на риски после их определения; и (iv) мониторинг рисков в последующее время. |
| Risk Mitigation<br>Сокращение риска<br>[CNSSI 4009] | Определение приоритетов, оценка и внедрение соответствующих мер/контрмер по снижению риска, рекомендованных в процессе управления рисками. |
| Risk Monitoring<br>Мониторинг рисков | Постоянное поддержание осведомленности о среде рисков организации, программе управления рисками и связанных действий для поддержки принятия решений относительно рисков. |
| Risk Response<br>Реагирование на риски | Принятие, предотвращение, снижение, распределение или передача рисков для деятельности организации (то есть, предназначения, функций, имиджа или репутации), активов организации, людей, других организаций или нации. |
| Risk Response Measure<br>Мера реагирования на риск | Конкретное действие, предпринятое в ответ на выявленный риск. |
| Root Cause Analysis<br>Анализ первопричин | Системный подход, основанный на принципах, для выявления глубинных причин, связанных с определенным набором рисков. |
| Security Authorization (to operate)<br>Санкционирование безопасности (для применения) | См. *Authorization (to operate)*. |

| | |
|---|---|
| Security Categorization<br>Категорирование безопасности | Процесс определения категории безопасности для информации или информационной системы. Методологии категорирования безопасности описаны в Инструкции CNSS 1253 для систем национальной безопасности и в Публикации FIPS 199 для систем, не относящихся к национальной безопасности. |
| Security Control Assessment<br>Оценка мер безопасности<br>[CNSSI 4009, Уточненный] | Проверка или оценка управленческих, эксплуатационных и технических мер безопасности для определения степени, до которой эти меры безопасности реализованы правильно, применяются как предназначено и дают желаемый результат относительно удовлетворения требованиям безопасности для информационной системы или организации. |
| Security Control Assessor<br>Оценщик мер безопасности | Лицо, группа лиц или организация, ответственные за проведение оценки мер безопасности. |
| Security Control Baseline<br>Базовый набор мер безопасности<br>[CNSSI 4009] | Набор минимальных мер безопасности, определенных для информационной системы с низким, умеренным или высоким уровнем воздействия. |
| Security Control Enhancement<br>Улучшение мер безопасности | Утверждение о возможности обеспечения безопасности для: (i) встраивания дополнительной, но связанной функциональности в базовую меру безопасности; и/или (ii) усиления базовой меры безопасности. |
| Security Control Inheritance<br>Наследование мер безопасности<br>[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, не являющимися ответственными за систему или приложение; сущностями, внутренними или внешними по отношению к организации, в которой находятся система или приложение. См. *Common Control*. |
| Security Controls<br>Меры безопасности<br>[FIPS 199, CNSSI 4009] | Управленческие, эксплуатационные и технические меры безопасности (т.е. меры защиты или контрмеры), предписанные для информационной системы с целью защиты конфиденциальности, целостности и доступности системы и ее информации. |
| Security Impact Analysis<br>Анализ воздействия на безопасность<br>[NIST SP 800-37] | Анализ, проводимый должностным лицом организации для определения степени, в которой изменения в информационной системе влияют на состояние безопасности системы. |
| Security Objective<br>Цель безопасности<br>[FIPS 199] | Конфиденциальность, целостность или доступность. |
| Security Plan<br>План обеспечения безопасности | Формальный документ, содержащий обзор требований безопасности для информационной системы или программы информационной безопасности и описание имеющихся или планируемых мер безопасности для выполнения этих требований.<br>См. *System Security Plan* или *Information Security Program Plan.* |
| Security Policy<br>Политика безопасности<br>[CNSSI 4009] | Набор критериев для предоставления услуг безопасности. |

| | |
|---|---|
| Security Requirements<br>Требования безопасности<br>[FIPS 200] | Требования, предъявляемые к информационной системе, которые вытекают из применимых законов, Правительственных распоряжений, директив, политики, стандартов, инструкций, нормативных документов, процедур или потребностей целей предназначения/деятельности организации для обеспечения конфиденциальности, целостности и доступности обрабатываемой, хранимой или передаваемой информации. |
| Senior Agency Information Security Officer<br>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 выступающее в качестве основного связующего звена Директора по информации с санкционирующими должностными лицами агентства, владельцами информационных систем и сотрудниками безопасности информационных систем.<br>Примечание: организации, подчиненные федеральным агентствам, могут использовать термин Высшее должностное лицо по информационной безопасности или Директор по информационной безопасности, чтобы обозначить людей, занимающих должности с обязанностями, аналогичными Высшему должностному лицу агентства по информационной безопасности. |
| Senior Information Security Officer<br>Высшее должностное лицо по информационной безопасности | См. *Senior Agency Information Security Officer*<br>. |
| Subsystem<br>Подсистема | Основное подразделение или компонент информационной системы, состоящее из информации, информационных технологий и персонала, которое выполняет одну или несколько конкретных функций. |
| System<br>Система | См. *Information System*. |
| System Security Plan<br>План обеспечения безопасности системы<br>[NIST SP 800-18] | Формальный документ, который представляет обзор требований безопасности для информационной системы и описывает реализованные или планируемые меры безопасности для удовлетворения этим требованиям. |
| System-Specific Security Control<br>Мера безопасности, специфичная для системы<br>[NIST SP 800-37] | Мера безопасности для информационной системы, которая не определялась как общая мера безопасности или часть гибридной меры безопасности, которая должна быть реализована в информационной системе. |
| Tailoring<br>Адаптация<br>[NIST SP 800-53, CNSSI 4009] | Процесс, посредством которого базовый набор мер безопасности изменяется путем: (i) применения руководства по уточнению состава мер безопасности; (ii) спецификации компенсирующих мер безопасности, если это необходимо; и (iii) спецификации определенных организацией параметров в мерах безопасности с помощью явных утверждений о назначении и выборе. |
| Tailored Security Control Baseline<br>Адаптированный базовый набор мер безопасности | Набор мер безопасности, являющийся результатом применения руководства по адаптации к базовому набору мер безопасности. См. *Tailoring*. |

| | |
|---|---|
| Technical Controls<br>Технические меры безопасности<br>[FIPS 200] | Меры безопасности (т.е. меры защиты или контрмеры) для информационной системы, которые в основном реализуются и выполняются информационной системой с помощью механизмов, содержащихся в аппаратных, программных или микропрограммных компонентах системы. |
| Threat<br>Угроза<br>[CNSSI 4009] | Любое обстоятельство или событие, способное негативно повлиять на деятельность организации (включая предназначение, функции, имидж или репутацию), активы организации, людей, другие организации или нацию через информационную систему посредством несанкционированного доступа, уничтожения, раскрытия, модификации информации и/или отказа в обслуживании. |
| Threat Assessment<br>Оценка угрозы<br>[CNSSI 4009] | Процесс формальной оценки степени угрозы для информационной системы или предприятия и описания характера угрозы. |
| Threat Source<br>Источник угрозы<br>[CNSSI 4009] | Намерение и метод, направленные на преднамеренное использование уязвимости, или ситуация и метод, которые могут случайно использовать уязвимость. |
| Trustworthiness<br>Доверенность<br>[CNSSI 4009] | Атрибут человека или предприятия, который обеспечивает уверенность других в квалификации, возможностях и надежности этого субъекта для выполнения конкретных задач и возложенных на него обязанностей. |
| Vulnerability<br>Уязвимость<br>[CNSSI 4009] | Недостаток информационной системы, процедур безопасности системы, внутренних мер безопасности или реализации, который может быть использован источником угрозы. |
| Vulnerability Assessment<br>Оценка уязвимостей<br>[CNSSI 4009] | Систематизированное исследование информационной системы или продукт для определения адекватности мер безопасности, выявления недостатков безопасности, предоставления данных, на основании которых можно прогнозировать эффективность предлагаемых мер безопасности и подтверждения адекватности таких мер после реализации. |

## ПРИЛОЖЕНИЕ C

# АКРОНИМЫ

ОБЩИЕ СОКРАЩЕНИЯ

| | |
|---|---|
| APT | Advanced Persistent Threat (Постоянная развивающаяся угроза) |
| CIO | Chief Information Officer (Директор по информации) |
| CNSS | Committee on National Security Systems (Комитет по системам национальной безопасности) |
| COTS | Commercial Off-The-Shelf (Коммерческий готовый продукт) |
| DoD | Department of Defense (Министерство обороны) |
| FIPS | Federal Information Processing Standards (Федеральные стандарты по обработке информации) |
| FISMA | Federal Information Security Management Act (Федеральный закон об управлении информационной безопасностью) |
| IA | Information Assurance (Информационное доверие) |
| ICS | Industrial Control System (Промышленная система управления) |
| IEC | International Electrotechnical Commission (Международная электротехническая комиссия) |
| ISO | International Organization for Standardization (Международная организация по стандартизации) |
| NIST | National Institute of Standards and Technology (Национальный институт стандартов и технологий) |
| NSA | National Security Agency (Агентство национальной безопасности) |
| ODNI | Office of the Director of National Intelligence (Офис директора национальной разведки) |
| OMB | Office of Management and Budget (Офис управления и бюджета) |
| POAM | Plan of Action and Milestones (План действий и основные вехи) |
| RMF | Risk Management Framework (Основы управления рисками) |
| SCAP | Security Content Automation Protocol (Протокол автоматизации содержания безопасности) |
| SP | Special Publication (Специальная публикация) |
| U.S.C. | United States Code (Свод законов Соединенных Штатов Америки) |

ПРИЛОЖЕНИЕ D

# РОЛИ И ОБЯЗАННОСТИ

КЛЮЧЕВЫЕ УЧАСТНИКИ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ

В следующих разделах описаны роли и обязанности[66] ключевых участников процесса управления рисками в организации.[67] Учитывая, что организации имеют совершенно разное предназначение и структуры, могут существовать различия в названиях ролей, связанных с управлением рисками, и в том, как конкретные обязанности распределяются между сотрудниками организации (например, несколько человек выполняют одну роль или один человек выполняет несколько ролей).[68] Однако основные функции остаются неизменными. Применение процесса управления рисками на трех уровнях управления рисками, описанных в данной публикации, является гибким, что позволяет организациям эффективно достигать цели конкретных задач в рамках их соответствующих структур организаций для наилучшего управления рисками.

## D.1 РУКОВОДИТЕЛЬ АГЕНТСТВА (ГЛАВНЫЙ ИСПОЛНИТЕЛЬНЫЙ ДИРЕКТОР)

*Руководитель агентства* (или главный исполнительный директор) - это высшее должностное лицо или руководитель высшего уровня в организации, несущий общую ответственность за обеспечение информационной безопасности, соизмеримой с риском и величиной ущерба (т.е. воздействия) для деятельности и активов организации, людей, других организаций и нации в результате несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения: (i) информации, собираемой или хранимой агентством или от его имени; и (ii) информационных систем, используемых или эксплуатируемых агентством или подрядчиком агентства или другой организацией от имени агентства. Руководители агентств также несут ответственность за обеспечение того, что: (i) процессы управления информационной безопасностью интегрированы с процессами стратегического и оперативного планирования; (ii) старшие должностные лица организации обеспечивают информационную безопасность информации и информационных систем, которые поддерживают деятельность и активы, находящихся под их управлением; и (iii) организация имеет обученный персонал, достаточный для оказания помощи в соблюдении требований информационной безопасности в соответствующем законодательстве, политике, директивах, инструкциях, стандартах и руководствах. Посредством разработки и внедрения строгой политики руководитель агентства устанавливает приверженность организации информационной безопасности и действия, необходимые для эффективного управления рисками и защиты функций предназначения/деятельности, выполняемых организацией. Руководитель агентства устанавливает соответствующую ответственность за информационную безопасность и обеспечивает активную поддержку и надзор за мониторингом и совершенствованием программы информационной безопасности. Приверженность высшего руководства информационной безопасности устанавливает уровень должной осмотрительности в организации, который способствует созданию климата для успешного выполнения предназначения и деятельности.

## D.2 ОТВЕТСТВЕННЫЙ ЗА РИСКИ (ФУНКЦИЯ)

*Ответственный за риски (функция)* - это человек или группа лиц в организации, которая обеспечивает более комплексный подход во всей организации к управлению рисками. Ответственный за риски (функция) служит общим ресурсом по управлению рисками для высших руководителей/руководителей, владельцев предназначения/деятельности, директоров по информации, директоров по информационной

[66] Роли и обязанности, описанные в данном приложении, соответствуют ролям и обязанностям, связанными с Основами управления рисками в Специальной публикации NIST 800-37.

[67] Организации могут определить другие роли (например, управляющий объектами, менеджер по персоналу, системный администратор) для поддержки процесса управления рисками.

[68] Когда один человек выполняет несколько ролей в процессе управления рисками, необходимо гарантировать, что он сохраняет надлежащий уровень независимости и не имеет конфликта интересов.

безопасности, владельцев информационных систем, поставщиков общих мер безопасности, архитекторов предприятия, архитекторов информационной безопасности, инженеров информационных систем/безопасности, менеджеров/сотрудников по безопасности информационных систем и любых других заинтересованных сторон, заинтересованных в успехе предназначения/деятельности организаций. Ответственный за риски (функция) координирует свои действия с высшими руководителями/руководителями для того, чтобы:

- установить роли и обязанности по управлению рисками;
- разработать и внедрить *стратегию организации по управлению рисками*, которая определяет и предоставляет информацию для решений организации по рискам (включая то, как риски описываются, оцениваются, осуществляется реагирование и отслеживание во времени);
- управлять информацией об угрозах и уязвимостях в отношении информационных систем организации и сред, в которых функционируют эти системы;
- создавать общие для организации форумы для рассмотрения всех видов и источников риска (включая агрегированный риск);
- определять риски организации на основе совокупных рисков от эксплуатации и использования информационных систем и соответствующих сред функционирования;
- обеспечивать надзор за деятельностью по управлению рисками, осуществляемой организациями, для обеспечения последовательных и эффективных решений, основанных на оценке рисков;
- развивать более глубокое понимание рисков в связи со стратегическим видением организаций и их комплексных операций;
- создавать эффективные механизмы и служить координационным центром для передачи и обмена информацией, связанной с рисками, между ключевыми заинтересованными сторонами внутри организаций и за их пределами;
- определять степень автономии подчиненных организаций, разрешенную вышестоящими организациями в отношении определения, оценки, реагирования и мониторинга рисков;
- содействовать сотрудничеству и взаимодействию между уполномоченными должностными лицами, включая действия по санкционированию безопасности, требующие совместной ответственности (например, совместные/расширенные санкционирования);
- обеспечивать, чтобы решения по санкционированию безопасности учитывали все факторы, необходимые для успеха предназначения и деятельности; и
- обеспечивать, чтобы совместная ответственность за поддержку функций предназначения и деятельности организации с использованием внешних провайдеров получила необходимую обзорность и была возложена на соответствующие органы, принимающие решения.

Ответственный за риски (функция) не предполагает ни конкретной организационной структуры, ни формальной ответственности, закрепленной за каким-либо одним человеком или группой в организации. Руководители агентств или организаций могут решить оставить ответственного за риски (функция) или делегировать эту функцию. От ответственного за риски (функция) требуется сочетание навыков, опыта и взглядов для понимания стратегических целей и задач организаций, функций предназначения/деятельности организации, технических возможностей и ограничений, а также ключевых полномочий и указаний, определяющих деятельность организации. Для обеспечения такого необходимого сочетания, роль ответственного за риски (функция) может выполняться одним человеком или отделом (при поддержке экспертного персонала) или специально созданной группой (например, советом по рискам, исполнительным руководящим комитетом, советом исполнительного руководства). Ответственный за риски (функция) вписывается в структуру управления организации таким образом, чтобы способствовать эффективности и результативности.

## D.3 ДИРЕКТОР ПО ИНФОРМАЦИИ

*Директор по информации*[69] - это должностное лицо организации, ответственное за: (i) назначение старшего должностного лица по информационной безопасности; (ii) разработку и поддержание политики, процедур и методов управления информационной безопасностью для выполнения всех применимых требований; (iii) надзор за персоналом, несущим значимую ответственность за информационную безопасность, и обеспечение надлежащей подготовки этого персонала; (iv) оказание помощи старшим должностным лицам организации в отношении их обязанностей по обеспечению безопасности; и (v) в координации с другими старшими должностными лицами подготовку ежегодного отчета главе федерального агентства об общей эффективности программы информационной безопасности организации, включая ход выполнения корректирующих действий. Директор по информации при поддержке ответственного за риски (функция) и старшего должностного лица по информационной безопасности тесно сотрудничает с уполномоченными должностными лицами и их назначенными представителями, чтобы помочь обеспечить, что:

- общая для организации программа информационной безопасности эффективно реализуется, что приводит к адекватной безопасности всех информационных систем организации и среды функционирования этих систем;
- соображения информационной безопасности интегрированы в циклы программирования/ планирования/бюджетирования, архитектуры предприятия и жизненные циклы приобретения/разработки систем;
- информационные системы охвачены утвержденными планами безопасности и санкционированы на применение;
- мероприятия, связанные с информационной безопасностью, необходимые в рамках организации, выполняются эффективно, экономично и своевременно; и
- существует централизованная отчетность о соответствующей деятельности, связанной с информационной безопасностью.

Директор по информации и уполномоченные должностные лица также определяют на основе приоритетов организации соответствующее распределение ресурсов, предназначенных для защиты информационных систем, поддерживающих функции предназначения и деятельности организации. Для отдельных информационных систем директор по информации может быть назначен в качестве санкционирующего должностного лица или совместно санкционирующего должностного лица с другими старшими должностными лицами организации. Роль директора по информации имеет неотъемлемые полномочия правительства США и возлагается только на правительственный персонал.

## D.4 ВЛАДЕЛЕЦ/УПРАВЛЯЮЩИЙ ИНФОРМАЦИЕЙ

*Владелец/управляющий информацией* - это должностное лицо организации, обладающее законными, управленческими или оперативными полномочиями в отношении определенной информации и несущее ответственность за разработку политики и процедур, регулирующих ее создание, сбор, обработку, распространение и утилизацию.[70] В условиях совместного использования информации владелец/ управляющий информацией несет ответственность за установление правил надлежащего использования и защиты информации (например, правил поведения) и сохраняет эту ответственность, когда информация передается другим организациям или предоставляется им. Владелец/управляющий информацией обрабатываемой, хранимой или передаваемой информационной системой, может совпадать или не

[69] Если в организации нет официальной должности директора по информации, FISMA требует, чтобы соответствующие обязанности выполнялись сопоставимым должностным лицом организации.

[70] Федеральная информация является достоянием нации, а не конкретного федерального агентства или подчиненных ему организаций. Исходя из этого, многие федеральные агентства разрабатывают политику, процедуры, процессы и обучение, необходимые для прекращения практики владения информацией и внедрения практики управления информацией. Управление информацией - это тщательное и ответственное управление федеральной информацией, принадлежащей всей нации, независимо от того, какая сущность или источник является породителем, создателем или составителем информации. Управляющие информацией обеспечивают максимальный доступ к федеральной информации для элементов федерального правительства и его клиентов, уравновешенный обязательством защищать информацию в соответствии с положениями FISMA и любой связанной с безопасностью федеральной политикой, директивами, нормативными документами, стандартами и руководствами.

совпадать с владельцем системы. Одна информационная система может содержать информацию от нескольких владельцев/управляющих информацией. Владельцы/управляющие информацией предоставляют владельцам информационных систем сведения о требованиях безопасности и мерах безопасности для систем, в которых обрабатывается, хранится или передается информация.

## D.5 ВЫСШЕЕ ДОЛЖНОСТНОЕ ЛИЦО ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Высшее должностное лицо по информационной безопасности* - это должностное лицо организации, ответственное за: (i) выполнение обязанностей директора по информационной безопасности в соответствии с FISMA; и (ii) выполнение функций основного связующего звена между директором по информации и санкционирующими должностными лицами организации, владельцами информационных систем, поставщиками общих мер безопасности и сотрудниками по безопасности информационных систем. Высшее должностное лицо по информационной безопасности: (i) обладает профессиональной квалификацией, включая обучение и опыт, необходимыми для управления функциями программы информационной безопасности; (ii) выполняет обязанности по обеспечению информационной безопасности в качестве основной ответственности; и (iii) возглавляет отдел с предназначением и ресурсами для оказания помощи организации в достижении большей безопасности информации и информационных систем в соответствии с требованиями FISMA. Высшее должностное лицо по информационной безопасности (или вспомогательный персонал) может также выступать в качестве уполномоченных представителей санкционирующих должностных лиц или оценщиков мер безопасности. Роль высшего должностного лица по информационной безопасности имеет неотъемлемые полномочия правительства США и возлагается только на правительственный персонал.

## D.6 САНКЦИОНИРУЮЩЕЕ ДОЛЖНОСТНОЕ ЛИЦО

*Санкционирующее должностное лицо* - это высшее должностное лицо или руководитель, имеющий полномочия официально взять на себя ответственность за эксплуатацию информационной системы с приемлемым уровнем риска для деятельности и активов организации, людей, других организаций и нации.[71] Санкционирующие должностные лица обычно осуществляют бюджетный надзор за информационной системой или отвечают за операции по предназначению и/или деятельности, поддерживаемые системой. Через процесс санкционирования безопасности санкционирующие должностные лица несут *ответственность* за риски безопасности, связанные с функционированием информационной системы. Соответственно, санкционирующие должностные лица занимают руководящие должности с уровнем полномочий, соответствующим пониманию и принятию таких рисков безопасности, связанных с информационной системой. Санкционирующие должностные лица также утверждают планы безопасности, меморандумы о соглашении или взаимопонимании, планы действий и основные вехи, а также определяют, требуют ли значительные изменения в информационных системах или среде функционирования пересанкционирования. Санкционирующие должностные лица могут отказать в санкционировании применения информационной системы или, если система функционирует, приостановить применение, если существуют неприемлемые риски. Санкционирующие должностные лица координируют свою деятельность с ответственным за риски (функция), директором по информации, высшим должностным лицом по информационной безопасности, поставщиками общих мер безопасности, владельцами информационных систем, сотрудниками по безопасности информационных систем, оценщиками мер безопасности и другими заинтересованными сторонами в процессе санкционирования безопасности. С ростом сложности процессов предназначения/деятельности, партнерских соглашений и использования внешних/общих услуг, возможно, что в конкретной информационной системе могут присутствовать несколько санкционирующих должностных лиц. В этом случае между санкционирующими должностными лицами заключаются соглашения, которые документируются в плане безопасности. Санкционирующие должностные лица отвечают за обеспечение выполнения всех действий и функций, связанных с санкционированием безопасности, которые делегированы их уполномоченным представителям. Роль санкционирующего должностного лица имеет неотъемлемые полномочия правительства США и возлагается только на правительственный персонал.

[71] Ответственность санкционирующих должностных лиц, описанная в FIPS 200, была расширена в Специальной публикации NIST 800-53, чтобы включить риски для других организаций и нации.

## D.7 УПОЛНОМОЧЕННЫЙ ПРЕДСТАВИТЕЛЬ САНКЦИОНИРУЮЩЕГО ДОЛЖНОСТНОГО ЛИЦА

*Уполномоченный представитель санкционирующего должностного лица* - это должностное лицо организации, которое действует от имени санкционирующего должностного лица для координации и проведения необходимой повседневной деятельности, связанной с процессом санкционирования безопасности. Уполномоченные представители санкционирующего должностного лица могут быть уполномочены санкционирующими должностными лицами принимать определенные решения в отношении планирования и обеспечения ресурсами процесса санкционирования безопасности, утверждения плана обеспечения безопасности, утверждения и мониторинга выполнения планов действий и основных вех, а также оценки и/или определения риска. Уполномоченный представитель также может быть призван подготовить окончательный пакет санкционирования, получить подпись санкционирующего должностного лица на документе о санкционировании и передать пакет санкционирования соответствующим должностным лицам организации. Единственное действие, которое не может быть делегировано санкционирующим должностным лицом уполномоченному представителю - это принятие решения о санкционировании и подписание соответствующего документа о санкционировании (т.е. принятие риска для деятельности и активов организации, людей, других организаций и нации).

## D.8 ПОСТАВЩИК ОБЩИХ МЕР БЕЗОПАСНОСТИ

*Поставщик общих мер безопасности* - это лицо, группа или организация, ответственные за разработку, внедрение, оценку и мониторинг общих мер безопасности (т.е. мер безопасности, унаследованных информационными системами).[72] Поставщики общих мер безопасности отвечают за: (i) документирование определенных организацией общих мер безопасности в *плане безопасности* (или эквивалентном документе, предписанном организацией); (ii) обеспечение того, чтобы требуемые оценки общих мер безопасности проводились квалифицированными оценщиками с соответствующим уровнем независимости, определенным организацией; (iii) документирование результатов оценки в *отчете об оценке безопасности*; и (iv) *составление плана действий и вех* для всех мер безопасности, имеющих недостатки или дефекты. Планы безопасности, отчеты об оценке безопасности, планы действий и вех для общих мер безопасности (или обзор такой информации) предоставляются владельцам информационных систем, *наследующим* эти меры безопасности, после того, как информация рассматривается и утверждается высшим должностным лицом или руководителем, ответственным за надзор за этими мерами безопасности.

## D.9 ВЛАДЕЛЕЦ ИНФОРМАЦИОННОЙ СИСТЕМЫ

*Владелец информационной системы* - это должностное лицо организации, ответственное за закупку, разработку, интеграцию, модификацию, эксплуатацию, обслуживание и утилизацию информационной системы.[73] Владелец информационной системы отвечает за удовлетворение оперативных интересов сообщества пользователей (т.е. лиц, которые зависят от информационной системы для выполнения предназначения, деятельности или эксплуатационных требований) и за обеспечение соответствия требованиям информационной безопасности. В координации с ответственным за безопасность информационной системы, владелец информационной системы отвечает за разработку и поддержание плана безопасности и обеспечивает развертывание и эксплуатацию системы в соответствии с согласованными мерами безопасности. В координации с владельцем/управляющим информацией владелец информационной системы также отвечает за принятие решения о том, кто имеет доступ к

[72] Организации могут иметь несколько поставщиков общих мер безопасности в зависимости от того, как распределены обязанности по информационной безопасности в масштабах организации. Поставщики общих мер безопасности могут также быть владельцами информационных систем, если общие меры безопасности находятся в информационной системе.

[73] *Владелец информационной системы* выступает в качестве координатора информационной системы. В этом качестве владелец информационной системы выступает и как владелец, и как центральная точка контакта между процессом санкционирования и владельцами компонентов системы, включая, например: (i) приложения, сети, серверы или рабочие станции; (ii) владельцев/управляющих информацией, обрабатываемой, хранимой или передаваемой системой; и (iii) владельцев функций предназначения и деятельности, поддерживаемых системой. Некоторые организации могут называть владельцев информационных систем менеджерами программ или владельцами деятельности/активов.

системе (и с какими типами привилегий или правами доступа)[74], и обеспечивает, чтобы пользователи системы и вспомогательный персонал прошли необходимое обучение по вопросам безопасности (например, инструктаж по правилам поведения). На основании указаний уполномоченного должностного лица владелец информационной системы информирует соответствующих должностных лиц организации о необходимости проведения санкционирования безопасности, обеспечивает наличие необходимых ресурсов для этой работы и предоставляет оценщику мер безопасности требуемый доступ к информационной системе, информацию и документацию. Владелец информационной системы получает результаты оценки безопасности от оценщика мер безопасности. После принятия соответствующих мер по уменьшению или устранению уязвимостей владелец информационной системы собирает пакет разрешений и передает его санкционирующему должностному лицу или уполномоченному представителю для принятия решения.[75]

## D.10 СОТРУДНИК БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

*Сотрудник безопасности информационной системы*[76] - это лицо, ответственное за обеспечение надлежащего оперативного уровня безопасности информационной системы и работающее в тесном сотрудничестве с владельцем информационной системы. Сотрудник безопасности информационной системы также выступает в качестве главного консультанта по всем вопросам, техническим и иным, связанным с безопасностью информационной системы. Сотрудник по безопасности информационной системы обладает подробными знаниями и опытом, необходимыми для управления аспектами безопасности информационной системы и во многих организациях на него возлагается ответственность за повседневные действия по обеспечению безопасности системы. Эта ответственность может также включать, но не ограничиваться, физическую и экологическую защиту, безопасность персонала, обработку инцидентов, обучение и информирование по вопросам безопасности. Сотрудник безопасности информационной системы может быть призван оказать помощь в разработке политики и процедур безопасности и обеспечить соблюдение этих политик и процедур. В тесной координации с владельцем информационной системы сотрудник безопасности информационной системы часто играет активную роль в мониторинге системы и среды ее функционирования, включая разработку и обновление плана безопасности, управление и контроль изменений в системе, а также оценку влияния этих изменений на безопасность.

## D.11 АРХИТЕКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

*Архитектор информационной безопасности* - это лицо, группа лиц или организация, ответственные за обеспечение того, чтобы требования информационной безопасности, необходимые для защиты функций предназначения/деятельности организации, были адекватно учтены во всех аспектах архитектуры предприятия, включая эталонные модели, архитектуры сегментов и решений, а также результирующие информационные системы, поддерживающие процессы предназначения и деятельности. Архитектор информационной безопасности служит связующим звеном между архитектором предприятия и инженером по безопасности информационных систем, а также координирует работу с владельцами информационных систем, поставщиками общих мер безопасности и сотрудниками по безопасности информационных систем по распределению мер безопасности между системно-специфическими, гибридными или общими мерами безопасности. Кроме того, архитекторы информационной безопасности в тесной координации с сотрудниками по безопасности информационных систем консультируют

[74] Ответственность за принятие решения о том, кто имеет доступ к конкретной информации в информационной системе (и с какими типами привилегий или прав доступа), может лежать на владельце/управляющем информации.

[75] В зависимости от того, как организация организовала свою деятельность по санкционированию безопасности, санкционирующее должностное лицо может назначить лицо, отличное от владельца информационной системы, для составления и сбору информации для пакета санкционирования безопасности. В этой ситуации назначенное лицо должно координировать действия по составлению и сбору информации с владельцем информационной системы.

[76] Организации могут также определить роль *руководителя по безопасности информационной системы* или *руководителя по информационной безопасности* с аналогичными обязанностями, как у сотрудника по безопасности информационной системы, или с обязанностями по надзору за программой информационной безопасности. В этих ситуациях сотрудники по безопасности информационных систем могут, по усмотрению организации, подчиняться непосредственно руководителям по безопасности информационных систем или руководителям по информационной безопасности.

санкционирующих должностных лиц, директоров по информации, высших должностных лиц по информационной безопасности и ответственных за управление рисками (функции) по ряду вопросов, связанных с безопасностью, включая, например, установление границ информационной системы, оценку серьезности недостатков и дефектов в информационной системе, планы действий и вехи, подходы к снижению рисков, предупреждения о безопасности и потенциальные негативные последствия уязвимостей.

## D.12 ИНЖЕНЕР ПО БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

*Инженер по безопасности информационной системы* - это лицо, группа лиц или организация, ответственные за проведение мероприятий по обеспечению безопасности информационной системы. Инженерия безопасности информационной системы - это процесс, который фиксирует и уточняет требования информационной безопасности и обеспечивает эффективную интеграцию требований в компоненты информационных технологий продуктов и информационных систем посредством целенаправленного формирования архитектуры, проектирования, разработки и конфигурирования безопасности. Инженеры по безопасности информационных систем являются неотъемлемой частью команды разработчиков (например, интегрированной проектной группы), проектирующих и разрабатывающих информационные системы организации или модернизирующих унаследованные системы. Инженеры по безопасности информационных систем используют лучшие практики при внедрении мер безопасности в информационной системе, включая методологии разработки программного обеспечения, принципы проектирования систем/безопасности, безопасное проектирование, безопасную архитектуру и методы безопасного кодирования. Инженеры по безопасности систем координируют свою деятельность, связанную с безопасностью, с архитекторами информационной безопасности, высшими должностными лицами по информационной безопасности, владельцами информационных систем, поставщиками общих мер безопасности и сотрудниками по безопасности информационных систем.

## D.13 ОЦЕНЩИК МЕР БЕЗОПАСНОСТИ

*Оценщик мер безопасности* - это лицо, группа лиц или организация, ответственные за проведение комплексной оценки управленческих, эксплуатационных и технических мер безопасности, используемых в информационной системе или наследуемых ею, для определения общей эффективности этих мер (т.е. степени, в которой меры безопасности внедрены правильно, работают по назначению и дают желаемый результат в отношении выполнения требований безопасности системы). Оценщики мер безопасности также дают оценку серьезности недостатков или дефектов, обнаруженных в информационной системе и среде ее функционирования, и рекомендуют корректирующие действия для устранения выявленных уязвимостей. В дополнение к вышеперечисленным обязанностям оценщики мер безопасности готовят окончательный отчет об оценке безопасности, содержащий результаты и выводы по итогам оценки. Перед началом оценки мер безопасности оценщик проводит оценку плана обеспечения безопасности, чтобы убедиться, что план содержит набор мер безопасности для информационной системы, которые отвечают заявленным требованиям безопасности.

Необходимый уровень независимости оценщика определяется конкретными условиями оценки мер безопасности. Например, когда оценка проводится в поддержку решения о санкционировании или продлении санкционирования, санкционирующее должностное лицо четко определяет степень независимости, требуемую в соответствии с федеральной политикой, директивами, стандартами и руководствами. Независимость оценщика является важным фактором: (i) сохранения беспристрастного и непредвзятого характера процесса оценки; (ii) определения достоверности результатов оценки безопасности; и (iii) обеспечения получения санкционирующим должностным лицом максимально объективной информации для принятия обоснованного, основанного на рисках решения о санкционировании. Владелец информационной системы и поставщик общих мер безопасности полагаются на опыт в области безопасности и техническое суждение оценщика, чтобы: (i) оценить меры безопасности, используемые в информационной системе и наследуемые ею, используя процедуры оценки, указанные в плане оценки безопасности; и (ii) предоставить конкретные рекомендации по устранению недостатков или дефектов в мерах безопасности и устранению выявленных уязвимостей.

## ПРИЛОЖЕНИЕ E

# ЗАДАЧИ ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ

СВОДКА ЗАДАЧ ДЛЯ ШАГОВ В ПРОЦЕССЕ УПРАВЛЕНИЯ РИСКАМИ

| ЗАДАЧА | ОПИСАНИЕ ЗАДАЧИ |
|---|---|
| **Шаг 1: Описание рисков** | |
| **ЗАДАЧА 1-1** ПРЕДПОЛОЖЕНИЯ О РИСКАХ | Определение допущений, которые влияют на то, как оцениваются, осуществляется реагирование и контролируются риски в организации. |
| **ЗАДАЧА 1-2** ОГРАНИЧЕНИЯ ПО РИСКАМ | Определение ограничений на проведение мероприятий по оценке рисков, реагированию на риски и мониторингу рисков в организации. |
| **ЗАДАЧА 1-3** ДОПУСТИМЫЙ РИСК | Определение уровня допустимого риска для организации. |
| **ЗАДАЧА 1-4** ПРИОРИТЕТЫ И КОМПРОМИСЫ | Определение приоритетов и компромиссов, учитываемых организацией при управлении рисками. |
| **Шаг 2: Оценка рисков** | |
| **ЗАДАЧА 2-1** ОПРЕДЕЛЕНИЕ УГРОЗ И УЯЗВИМОСТЕЙ | Определение угроз и уязвимостей информационных систем организации и сред, в которых работают эти системы. |
| **ЗАДАЧА 2-2** ОПРЕДЕЛЕНИЕ РИСКОВ | Определение рисков для деятельности и активов организации, людей, других организаций и нации, если выявленные угрозы используют выявленные уязвимости. |
| **Шаг 3: Реагирование на риски** | |
| **ЗАДАЧА 3-1** ОПРЕДЕЛЕНИЕ РЕАКЦИИ НА РИСКИ | Определение альтернативных вариантов действий в ответ на риски, определенные в ходе оценки рисков. |
| **ЗАДАЧА 3-2** ОЦЕНКА АЛЬТЕРНАТИВ | Оценка альтернативных планов действий по реагированию на риски. |
| **ЗАДАЧА 3-3** РЕШЕНИЯ ПО РЕАГИРОВАНИЮ НА РИСК | Выбор соответствующего план действий по реагированию на риски. |
| **ЗАДАЧА 3-4** РЕАЛИЗАЦИЯ РЕАГИРОВАНИЯ НА РИСК | Реализация выбранного плана действий по реагированию на риски. |
| **Шаг 4: Мониторинг рисков** | |
| **ЗАДАЧА 4-1** СТРАТЕГИЯ МОНИТОРИНГА РИСКОВ | Разработка стратегии мониторинга рисков для организации, включающей цель, тип и частоту мероприятий по мониторингу. |
| **ЗАДАЧА 4-2** МОНИТОРИНГ РИСКОВ | Осуществление постоянного мониторинга информационных систем и среды деятельности организации для проверки соответствия требованиям, определения эффективности мер реагирования на риски и выявления изменений. |

**ПРИЛОЖЕНИЕ F**

# МОДЕЛИ УПРАВЛЕНИЯ

ПОДХОДЫ К УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Для удовлетворения потребностей организации можно использовать три подхода к управлению информационной безопасностью: (i) централизованный подход; (ii) децентрализованный подход; или (iii) гибридный подход. Полномочия, ответственность и право принятия решений, связанных с информационной безопасностью и управлением рисками, различаются в каждом подходе к управлению. Соответствующая структура управления для организации зависит от многих факторов (например, потребности предназначения/деятельности; специфика и размер организации; географическое распределение деятельности, активов и людей в организации; и допустимый риск). Структура управления информационной безопасностью должна согласовываться с другими структурами управления (например, управления информационными технологиями) для обеспечения совместимости с установленной практикой управления в организации и повышения ее общей эффективности.

### *Централизованное управление*

В централизованных структурах управления полномочия, ответственность и право принятия решений возлагаются исключительно на центральные органы. Эти центральные органы устанавливают соответствующие политики, процедуры и процессы для обеспечения участия всей организации в разработке и реализации стратегий управления рисками и информационной безопасности, принятия решений по рискам и информационной безопасности, а также создания механизмов взаимодействия между организациями и внутри организаций. Централизованный подход к управлению требует сильного, хорошо информированного центрального руководства и обеспечивает последовательность в организации. Централизованные структуры управления также предоставляют меньшую автономию для подчиненных организаций, которые являются частью головной организации.

### *Децентрализованное управление*

В децентрализованных структурах управления информационной безопасностью полномочия, ответственность и право принятия решений возлагаются и делегируются отдельным подчиненным организациям в рамках головной организации (например, отделения/компоненты в исполнительном департаменте федерального правительства или бизнес-подразделения в корпорации). Подчиненные организации устанавливают свои собственные политики, процедуры и процессы для обеспечения участия (части) организации в разработке и внедрении стратегий управления рисками и информационной безопасности, принятии решений по рискам и информационной безопасности, а также создании механизмов взаимодействия внутри организации. Децентрализованный подход к управлению информационной безопасностью позволяет совмещать подчиненные организации с различными потребностями предназначения/деятельности и средой деятельности за счет последовательности в организации в целом. Эффективность такого подхода значительно повышается за счет обмена информацией о рисках между подчиненными организациями с учётом того, чтобы ни одна подчиненная организация не могла передать риск другой без ее информированного согласия. Также важно обмениваться информацией, связанной с рисками, с вышестоящими организациями, поскольку решения о рисках, принимаемые подчиненными организациями, могут оказывать влияние на организацию в целом.

### *Гибридное управление*

В гибридных структурах управления информационной безопасностью полномочия, ответственность и право принятия решений распределяются между центральным органом и отдельными подчиненными организациями. Центральный орган устанавливает политику, процедуры и процессы для обеспечения участия всей организации в части стратегий управления рисками, информационной безопасности и

решений, затрагивающих всю организацию (например, решений, связанных с общей инфраструктурой или общими службами безопасности). Подчиненные организации аналогичным образом устанавливают соответствующие политики, процедуры и процессы для обеспечения их участия в части стратегий и решений по управлению рисками и информационной безопасности, которые специфичны для их потребностей предназначения/деятельности и условий деятельности. Гибридный подход к управлению требует сильного, хорошо информированного руководства для организации в целом и для подчиненных организаций, и обеспечивает последовательность в организации по тем аспектам риска и информационной безопасности, которые влияют на всю организацию.

## ПРИЛОЖЕНИЕ G

# МОДЕЛИ ДОВЕРИЯ

ПОДХОДЫ К УСТАНОВЛЕНИЮ ДОВЕРЕННЫХ ОТНОШЕНИЙ

Следующие модели доверия описывают способы, с помощью которых организации могут добиться уровня доверия, необходимого для формирования партнерских отношений, сотрудничества с другими организациями, обмена информацией или получения услуг информационной системы/безопасности. Ни одна модель доверия не является по своей сути лучше любой другой модели. Скорее, каждая модель предоставляет организациям определенные преимущества и недостатки, основанные на их обстоятельствах (например, структура управления, допустимый риск, критичность/чувствительность процессов предназначения и деятельности организаций).

### *Подтвержденное доверие*

В *модели подтвержденного доверия* одна организация получает совокупность свидетельств относительно действий другой организации (например, политики информационной безопасности организации, ее деятельности и решений, связанных с рисками) и использует эти свидетельства для установления уровня доверия с другой организацией. Примером подтвержденного доверия является ситуация, когда одна организация разрабатывает приложение или информационную систему и предоставляет свидетельства (например, план безопасности, результаты оценки) второй организации, которые подтверждают утверждения первой организации о том, что приложение/система отвечает определенным требованиям безопасности и/или включает соответствующие меры безопасности из Специальной публикации NIST 800-53. Подтвержденное доверие может быть недостаточным, то есть свидетельства, предлагаемые первой организацией второй организации, могут не полностью удовлетворять требованиям доверия или ожиданиям доверия второй организации. Чем больше свидетельств предоставляется между организациями, а также чем выше качество таких свидетельств, тем большая степень доверия может быть достигнута. Доверие связано со степенью прозрачности между двумя организациями в отношении деятельности и решений, связанных с рисками и информационной безопасностью.

### *Прямое историческое доверие*

В *модели прямого исторического доверия* достижения, продемонстрированные организацией в прошлом, особенно в ее деятельности и решениях, связанных с рисками и информационной безопасностью, могут способствовать и помочь установить уровень доверия с другими организациями. Хотя подтверждённые модели доверия предполагают, что организация предоставляет требуемый уровень свидетельств, необходимых для установления доверия, получение таких свидетельств не всегда возможно. В таких случаях доверие может основываться на других решающих факторах, включая исторические отношения организации с другой организацией или ее недавний опыт работы с другой организацией. Например, если одна организация работала со второй организацией в течение многих лет, выполняя какую-либо деятельность, и не имела негативного опыта, первая организация может быть готова доверить второй организации работу по другой деятельности, даже если у организаций нет общего опыта в этой конкретной деятельности. Прямое историческое доверие имеет тенденцию накапливаться со временем, причем более позитивный опыт способствует повышению уровня доверия между организациями. И наоборот, негативный опыт может привести к снижению уровня доверия между организациями.

### *Опосредованное доверие*

В *модели опосредованного доверия* организация устанавливает уровень доверия с другой организацией на основе заверений, предоставленных некой третьей стороной, которой доверяют взаимно. Существует несколько типов моделей опосредованного доверия, которые могут быть использованы. Например, две

организации, пытающиеся установить доверенные отношения, могут не иметь прямой истории доверия между двумя организациями, но иметь доверенные отношения с третьей организацией. Третья сторона, которой доверяют обе организации, выступает посредником в установлении доверенных отношений между двумя организациями, тем самым помогая установить необходимый уровень доверия. Другой тип опосредованного доверия включает в себя концепцию транзитивности доверия. В этом примере одна организация устанавливает доверенные отношения со второй организацией. Независимо от первых доверенных отношений, вторая организация устанавливает доверенные отношения с третьей организацией. Поскольку первая организация доверяет второй организации, а вторая организация доверяет третьей организации, между первой и третьей организациями теперь установлены доверенные отношения (иллюстрирующие концепцию переходного доверия между организациями)[77].

### *Мандатное доверие*

В *модели мандатного доверия* организация устанавливает уровень доверия с другой организацией на основании конкретного мандата, выданного третьей стороной, обладающей властью.[78] Этот мандат может быть установлен соответствующим органом власти посредством исполнительных указов, директив, нормативных документов или политики (например, меморандум главы агентства, предписывающий всем подчиненным организациям принимать результаты оценок безопасности, проведенных любой подчиненной организацией в рамках агентства). Мандатное доверие также может быть установлено, когда некоторая организационная структура назначается авторитетным источником для предоставления информационных ресурсов, включая продукты, системы или услуги информационных технологий. Например, организация может быть наделена ответственностью и полномочиями по выдаче сертификатов инфраструктуры открытых ключей (PKI) для группы организаций.

### *Гибридное доверие*

В целом, описанные выше модели доверия не являются взаимоисключающими. Каждая из моделей доверия может использоваться независимо как отдельная модель или в сочетании с другой моделью. В организации может использоваться несколько моделей доверия (например, на различных шагах жизненного цикла разработки системы). Кроме того, поскольку организации часто бывают большими и разнообразными, возможно, что подчиненные организации в рамках головной организации могут независимо использовать различные модели доверия при установлении доверенных отношений с потенциальными организациями-партнерами (включая подчиненные организации). Структура управления организации может устанавливать конкретные условия того, как различные модели доверия используются в организации взаимодополняющим образом.

### *Пригодность различных моделей доверия*

Модели доверия могут быть использованы на различных уровнях в рамках подхода к управлению рисками, описанного в данной публикации. Ни одна из моделей доверия не является по своей сути лучше или хуже других. Однако некоторые модели могут лучше подходить для определенных ситуаций, чем другие. Например, модель подтвержденного доверия, поскольку она требует свидетельств технического характера (например, успешно проведенные тесты), вероятно, лучше всего подходит для применения на Уровне 3. Напротив, модель прямого исторического доверия, в которой значительное внимание уделяется прошлому опыту, больше подходит для применения на Уровнях 1 или 2. Модели опосредованного и мандатного доверия обычно больше ориентированы на управление и, следовательно, лучше всего подходят для применения на уровне 1. Однако некоторые реализации модели мандатного доверия, например, требование доверять источнику сертификата PKI, больше

[77] В модели опосредованного доверия первая организация, как правило, не имеет представления о характере доверенных отношений между второй и третьей организациями.

[78] Авторитетная организация однозначно принимает на себя риски, которые будут нести все организации, на которые распространяется мандат, и несет ответственность за решения, связанные с рисками, навязанные этой организацией.

ориентированы на уровень 3. Аналогично, хотя модель опосредованного доверия в основном ориентирована на уровень 1, ее реализация может быть более ориентирована на информационную систему или уровень 3. Примером такого применения может быть использование сервисов аутентификации, которые подтверждают подлинность или идентичность компонента или сервиса информационной системы.

Характер конкретного сервиса информационных технологий также может повлиять на пригодность и применимость различных моделей доверия. Модель подтвержденного доверия является более традиционной моделью для подтверждения доверия к продукту, системе или сервису информационных технологий. Однако эта модель доверия лучше всего работает в ситуациях, когда существует определенная степень контроля между сторонами (например, контракт между правительством и внешним поставщиком услуг) или когда есть достаточно времени для получения и проверки свидетельств, необходимых для установления доверенных отношений. Подтвержденное доверие является неоптимальной моделью для ситуаций, когда две стороны являются равными и/или когда решения о доверии в отношении совместно используемых/предоставляемых услуг должны приниматься быстро из-за очень динамичного и быстрого характера запрашиваемых/предоставляемых услуг (например, сервис-ориентированные архитектуры).

**ПРИЛОЖЕНИЕ H**

# СТРАТЕГИИ РЕАГИРОВАНИЯ НА РИСКИ

ОТ ЗАЩИТЫ ГРАНИЦ К ГИБКОЙ ОБОРОНЕ

Организации разрабатывают *стратегии управления рисками* в рамках шага описания риска в процессе управления рисками, описанного в третьей главе. Стратегии управления рисками касаются того, как организации намерены оценивать риски, реагировать на риски и контролировать риски, делая явными и прозрачными представления о рисках, которые организации обычно используют при принятии инвестиционных и операционных решений. В рамках стратегий управления рисками организации также разрабатывают *стратегии реагирования на риски*. Практические реалии, с которыми сегодня сталкиваются организации, делают стратегии реагирования на риски крайне необходимыми - реалии потребности в эффективности предназначения/деятельности, предлагаемой информационными технологиями, отсутствия доверия к имеющимся технологиям и растущего осознания противниками возможности достижения своих целей по нанесению ущерба путем компрометации информационных систем организации и сред, в которых эти системы работают. Высшие руководители/руководители современных организаций сталкиваются с почти неразрешимой дилеммой - информационные технологии, необходимые для успеха предназначения/деятельности, могут быть теми же технологиями, с помощью которых противники приводят к провалу предназначения/деятельности. Разработанные и внедренные организациями стратегии реагирования на риски предоставляют этим высшим руководителям/руководителям (т.е. лицам, принимающим решения в организациях) практические, прагматичные пути решения этой дилеммы. Четко определенные и сформулированные стратегии реагирования на риски помогают гарантировать, что высшие руководители/руководители берут на себя ответственность за реагирование на риски организации и в конечном итоге несут *ответственность* и *подотчетность* за решения, связанные с рисками, понимая, признавая и открыто принимая возникающие в результате этого риски для предназначения/деятельности.

Как описано во второй главе, существует пять основных типов реагирования на риск: (i) принять; (ii) избежать; (iii) снизить; (iv) поделиться; и (v) передать.[79] Хотя каждый тип реагирования может иметь соответствующую стратегию, должна существовать общая стратегия выбора из основных типов реагирования. Ниже рассматривается общая стратегия реагирования на риски и стратегия для каждого типа реагирования. Кроме того, представлены конкретные стратегии снижения рисков, включая описание того, как такие стратегии могут быть реализованы в организациях.

## H.1 ОБЩИЕ СТРАТЕГИИ РЕАГИРОВАНИЯ НА РИСКИ

Стратегии реагирования на риски определяют: (i) лиц или подкомпоненты организации, ответственных за выбранные меры реагирования на риск и определение критериев эффективности (т.е. формулировка показателей и пороговых значений, по которым можно судить об эффективности мер реагирования на риски); (ii) зависимости выбранных мер реагирования на риски от других мер реагирования на риски; (iii) зависимости выбранных мер реагирования на риски от других факторов (например, реализации других запланированных мер в области информационных технологий); (iv) сроки реализации мер реагирования на риски; (v) планы мониторинга эффективности мер реагирования на риски; (vi) определение условий мониторинга рисков; и (vii) промежуточные меры реагирования на риски, выбранные для реализации, если это необходимо. Стратегии реализации мер реагирования на риски могут включать промежуточные меры, которые организации решают реализовать. Общая стратегия реагирования на риски обеспечивает подход организации к выбору между основными мерами реагирования на риски для данной ситуации по рискам. Решение о *принятии* риска должно соответствовать заявленному допустимому риску для организации. Тем не менее, все еще существует необходимость в четко определенном, установленном

[79] Между основными реакциями на риск существует дублирование. Например, совместный риск - это риск, который принимается каждой стороной в соглашении о совместном использовании, а избегание риска можно рассматривать как уменьшение риска до нуля. Тем не менее, при таком понимании дублирования есть смысл рассмотреть каждый из пяти типов реагирования на риск отдельно.

пути организации для выбора одной или комбинации реакций на риск: принятие, избегание, снижение, распределение или передача. Организации часто попадают в ситуации, когда риск больше, чем хотят принять назначенные высшие руководители/руководители. Вероятно, потребуется некоторое принятие риска. Возможно, удастся избежать риска, разделить или передать риск, и, вероятно, возможно некоторое снижение риска. Избегание риска может потребовать выборочной реорганизации процессов предназначения/деятельности организации и отказа от некоторых преимуществ, получаемых от использования информационных технологий в масштабах всей организации, возможно, даже тех, которые организации воспринимают как необходимые преимущества. Снижение риска требует затрат ограниченных ресурсов и может быстро стать экономически неэффективным из-за прагматических реалий степени снижения риска, которая может быть реально достигнута. Наконец, распределение и передача рисков также имеют последствия, некоторые из которых если и не являются неприемлемыми, то могут быть нежелательными. Стратегии реагирования на риски в организациях позволяют высшим руководителям/руководителям принимать решения на основе рисков в соответствии с целями, задачами и более широкими перспективами организации.

## H.2 СТРАТЕГИИ ПРИНЯТИЯ РИСКОВ

*Стратегии принятия рисков* организации являются важным дополнением к заявлениям организации о допустимом риске. Цель установления допустимого риска организации заключается в том, чтобы четко и недвусмысленно обозначить предел риска - то есть, как далеко готовы зайти организации в отношении принятия риска для деятельности организации (включая предназначение, функции, имидж и репутацию), активов организации, людей, других организаций и страны. Однако операции в реальном мире редко бывают настолько простыми, чтобы сделать такие заявления о допустимом риске конечным условием для принятия решений о принятии рисков.

## H.3 СТРАТЕГИИ ПРЕДОТВРАЩЕНИЯ РИСКОВ

Из всех стратегий реагирования на риски, *стратегии предотвращения риск*ов организации могут быть ключом к достижению адекватного реагирования на риски. Прагматические реалии доверенности информационных технологий, доступных для использования в рамках общих ограничений ресурсов, делают разумное использование этих технологий, возможно, значительным, если не самым значительным ответом на риски. Разумное использование информационных технологий, составляющих информационные системы организации, по сути, является формой предотвращения риска - то есть организации изменяют способ использования информационных технологий, чтобы изменить характер понесенного риска (т.е. предотвратить риск). Однако такие подходы могут находиться в большом противоречии с желаниями организации, а в некоторых случаях и с мандатом на полную автоматизацию процессов предназначения/деятельности. Организации активно решают эту дилемму, чтобы: (i) высшие руководители/руководители (и другие должностные лица организации, принимающие решения на основе рисков) несли ответственность только за то, на что они в состоянии повлиять; и (ii) лица, принимающие решения, могли принимать сложные решения о рисках, которые на самом деле могут отвечать наилучшим интересам организации.

## H.4 СТРАТЕГИИ РАСПРЕДЕЛЕНИЯ И ПЕРЕДАЧИ РИСКОВ

*Стратегии распределения рисков* и *стратегии передачи рисков* организации являются ключевыми элементами в принятии решений о рисках для конкретных функций предназначения/деятельности организации на Уровне 2 или информационных систем организации на Уровне 3. Стратегии распределения и передачи рисков учитывают и используют все преимущества снижения рисков путем распределения/ передачи потенциального воздействия на другие внутренние элементы организации или на другие внешние организации, что позволяет доказать, что некоторые другие организации на самом деле полностью (передача) или частично (распределение) ответственны за риск и несут за него ответственность. Для того чтобы распределение рисков или передача рисков были эффективными мерами реагирования на риски, необходимо, чтобы воздействие на локальную среду (например, на процессы предназначения/ деятельности или информационные системы) было устранено в ходе

распределения или передачи рисков (т.е. внимание должно быть сосредоточено на успехе предназначения/деятельности, а не на возложении вины). Кроме того, деятельность по распределению и передаче рисков должна осуществляться в соответствии с внутри- и межорганизационной динамикой и реалиями (например, специфика организации, управление, допустимый риск). Это объясняет, почему стратегии распределения/передачи рисков особенно важны для того, чтобы распределение и/или передача были жизнеспособным вариантом реагирования на риск.

## H.5 СТРАТЕГИИ СНИЖЕНИЯ РИСКА

*Стратегии снижения рисков* организации отражают точку зрения организации на то, какие меры по снижению рисков должны быть использованы и где они должны быть применены, чтобы снизить риски информационной безопасности для деятельности и активов организации, людей, других организаций и нации. Стратегии снижения рисков являются основным связующим звеном между программами управления рисками организации и программами информационной безопасности, причем первые охватывают все аспекты управления рисками, а вторые в основном являются частью компонента реагирования на риски в процессе управления рисками. Эффективные стратегии снижения риска учитывают общее размещение и распределение мер по снижению риска, степень предполагаемого снижения риска и охватывают меры по снижению риска на Уровне 1 (например, общие меры безопасности), на Уровне 2 (например, архитектура предприятия, включая встроенную архитектуру информационной безопасности, и учитывающие риск процессов предназначения/деятельности) и на Уровне 3 (меры безопасности в отдельных информационных системах). Стратегии снижения рисков организации отражают следующее:

- Процессы предназначения/деятельности разрабатываются с учетом потребностей в защите информации и требований информационной безопасности;[80]
- Архитектуры предприятий (включая встроенные архитектуры информационной безопасности) разрабатываются с учетом реально достижимых мер по снижению рисков;
- Меры по снижению рисков реализуются в рамках информационных систем организации и сред функционирования посредством мер защиты/контрмер (т.е. мер безопасности) в соответствии с архитектурой информационной безопасности; и
- Программы, процессы и меры защиты/контрмеры информационной безопасности являются очень гибкими и подвижными в отношении реализации, признавая разнообразие функций предназначения и деятельности и динамичную среду, в которой работают организации.[81]

Организации разрабатывают стратегии снижения рисков на основе стратегических целей и задач, требований предназначения и деятельности, а также приоритетов организации. Стратегии обеспечивают основу для принятия основанных на рисках решений по информационной безопасности, связанных с информационными системами и применяемых к ним в организации. Стратегии снижения рисков необходимы для обеспечения адекватной защиты организаций от растущих угроз для информации, обрабатываемой, хранимой и передаваемой информационными системами организации. Характер угроз и динамичная среда, в которой работают организации, требуют гибких и масштабируемых мер защиты, а также решений, которые могут быть адаптированы к быстро меняющимся условиям. Эти условия включают, например, появление новых угроз и уязвимостей, развитие новых технологий, изменения в требованиях предназначения/деятельности и/или изменения в среде деятельности. Эффективные стратегии снижения рисков поддерживают цели и задачи организаций и установленные приоритеты предназначения/деятельности, тесно связаны с архитектурой предприятия и архитектурой информационной безопасности и могут действовать на протяжении всего жизненного цикла разработки систем.

[80] Помимо потребностей в защите информации, определяемых предназначением/деятельностью, требования к информационной безопасности поступают из различных источников (например, федеральное законодательство, политика, директивы, правила и стандарты).

[81] Динамические среды деятельности характеризуются, например, постоянными изменениями людей, процессов, технологий, физической инфраструктуры и угроз.

Традиционные стратегии снижения рисков в отношении угроз от кибератак сначала полагались почти исключительно на монолитную *защиту границ*. Эти стратегии предполагали, что противник находится за пределами некоторого установленного оборонительного периметра, а целью организаций является отражение атаки. Основным направлением статической пограничной защиты была защита от проникновения продуктов информационных технологий и информационных систем, используемых организацией, а также любые дополнительные меры защиты и противодействия, применяемые в средах, в которых работают продукты и системы. Признание того, что границы информационных систем являются проницаемыми или пористыми, привело к тому, что частью стратегии снижения рисков стала защита в глубину, полагающаяся на механизмы обнаружения и реагирования для устранения угроз внутри защитного периметра. В современном мире, характеризующемся *постоянными развивающимися угрозами*,[82] необходима более комплексная стратегия снижения рисков - стратегия, сочетающая традиционную защиту границ с *гибкой защитой*.

Гибкая защита предполагает, что небольшой процент угроз от целенаправленных кибератак будет успешным путем компрометации информационных систем организации через цепочку поставок[83] путем поражения первоначальных мер защиты и контрмер (т.е. мер безопасности), внедренных организациями, или путем использования ранее не выявленных уязвимостей, для которых не были созданы средства защиты. В этом сценарии противники действуют внутри защитных периметров, установленных организациями, и могут иметь значительный или полный контроль над информационными системами организации. Гибкая защита использует концепцию *устойчивости информационных систем*, то есть способность систем работать во время атаки, даже в деградированном или ослабленном состоянии, и быстро восстанавливать оперативные возможности для основных функций после успешной атаки. Концепция устойчивости информационной системы может быть применена и к другим классам угроз, включая угрозы от нарушений в окружающей среде и/или человеческие ошибки бездействия/действия. Наиболее эффективные стратегии снижения рисков используют сочетание пограничной защиты и гибкой обороны в зависимости от характеристик угрозы.[84] Эта стратегия двойной защиты иллюстрирует две важные концепции информационной безопасности, известные как "*эшелонированная защита*"[85] и "*широкая защита*".[86]

***Информация имеет ценность и должна быть защищена. Информационные системы (включая людей, процессы и технологии) являются основными средствами, используемыми для обработки, хранения и передачи такой информации, что позволяет организациям выполнять свои предназначения в различных условиях деятельности и в конечном итоге быть успешными.***

---

[82] *Постоянная развивающаяся угроза* - это противник, обладающий продвинутым уровнем знаний и значительными ресурсами, которые позволяют ему создавать возможности для достижения своих целей, используя многочисленные направления атак (например, кибер-, физические и обманные). Эти цели обычно включают создание/расширение плацдармов в информационно-технологической инфраструктуре целевых организаций с целью утечки информации, подрыва или препятствования критическим аспектам предназначения, программы или организации; или позиционирование себя для выполнения этих целей в будущем. Постоянная развивающаяся угроза: (i) преследует свои цели неоднократно в течение длительного периода времени; (ii) адаптируется к усилиям защитников противостоять ей; и (iii) определяет поддержание уровня взаимодействия, необходимого для выполнения своих целей.

[83] Проект межведомственного отчета NIST 7622 содержит руководство по управлению рисками цепочки поставок.

[84] Характеристики угрозы включают возможности, намерения и информацию о цели.

[85] *Эшелонированная защита* - это стратегия информационной безопасности, объединяющая людей, технологии и операционные возможности для создания переменных барьеров на нескольких уровнях и предназначениях организации.

[86] *Широкая защита* - это спланированный, систематический комплекс междисциплинарных мероприятий, направленных на выявление, управление и снижение риска использования уязвимостей на каждом шаге жизненного цикла системы, сети или субкомпонента (проектирование и разработка системы, сети или продукта; производство; компановка; сборка; системная интеграция; распространение; эксплуатация; техническое обслуживание; и вывод из эксплуатации).