Специальная публикация Национального института стандартов и технологий 800-30

Руководство по управлению рисками для систем информационных технологий Рекомендации Национального института Стандартов и технологий

Расширенный реферат по материалам: NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems; Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary
TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

Деятельность Центра компетенции по электронному правительству при Американской Торговой Палате в России осуществляется при финансовой поддержке Агентства США по Международному развитию (USAID).

Содержание:

Phone: (095) 961 2136
E-mail: e-gov.office@amcham.ru

Использование эффективных процессов управления рисками, которые поддерживают принятие обоснованных решений, основанных на учете возможных рисков позволяют своевременно и эффективно адресовать все проблемы, связанные с угрозами безопасности критических национальных инфраструктур, с рентабельностью обеспечения безопасности и с необходимостью поддержания непрерывности деятельности. Управление рисками является одной из необходимых функций управления, которая не должна быть сведена к исключительно технической функции, связанной с эксплуатацией ИТ или выполнением персоналом требований по безопасности. Руководство организации, ответственное за инфраструктуру ИТ (например, Руководитель службы информационных систем (CIO), руководители агентств и подразделений) должны определить и гарантировать выполнение эффективной и всесторонней программы управления рисками, которая должна охватывать все сегменты предприятия и поддерживать осуществление его миссии.

Краткий обзор проблемы управления рисками

Риск является отрицательным следствием наличия уязвимости и характеризуется, во-первых, вероятностью возникновения негативного события и, во-вторых, последствиями при возникновении этого события. Управление риском представляет собой процесс идентификации риска, процесс оценки степени риска и процесс осуществления мероприятий, направленных на уменьшение риска до приемлемого уровня. Цель выполнения процессов управления риском состоит в том, чтобы дать возможность организации выполнить свою миссию или миссии за счет:
1) повышения безопасности ИТ-систем, которые хранят, обрабатывают или передают информацию в пределах и вне организации;
2) повышения информированности и осведомленности руководства относительно принятых решений по управлению риском для получения обоснованных объемов затрат, которые должны становиться неотъемлемой частью общего бюджета ИТ;
3) оказания помощи руководству в авторизации (или в аккредитации) своих систем ИТ на базе документированной поддержки результатами, вытекающими из выполнения процессов управления риском.

Управление риском охватывает решение трех задач: оценка (или определение) риска, уменьшение риска, окончательные оценки и выводы. Управление риском является процессом, который позволяет менеджерам ИТ сбалансировать эксплуатационные и экономические затраты предпринимаемых мер по защите и достигать улучшений в осуществлении миссии, обеспечивая защиту тех систем ИТ и тех данных, которые поддерживают выполнение миссии своих организаций. Необходимо напомнить, что этот процесс относиться не только к среде ИТ; в действительности проблемы риска возникают во всех сферах повседневной жизни людей и организаций. Достаточно привести примеры из области обеспечения домашней безопасности. Многие люди предпочитают домашние системы безопасности и готовы ежемесячно платить за их

обслуживание, чтобы быть уверенными, что эти системы реально обеспечат надежную защиту их собственности. Очевидно, что домовладельцы провели баланс между стоимостью установки системы, затратами на их контроль и ценностью их домашнего имущества и безопасности своей семьи.

Интеграция управления риском в жизненный цикл развития систем (System Development Life Cycle, SDLC).

Управление рисками является итеративным процессом и его действия происходят на каждой стадии жизненного цикла. Уменьшение отрицательного воздействия на организацию и потребность в нормальной базе для принятия решения составляют фундаментальные предпосылки для того, чтобы организации осуществляли процесс управления риска для своих систем по ИТ. Жизненный цикл ИТ-систем имеет пять основных стадий: инициирование, разработка (или приобретение), реализация, эксплуатация (или обслуживание), и вывод из эксплуатации (удаление, передача, списание и т.д.). В приводимой ниже таблице 1 обобщается деятельность по управлению риском, связанная с каждой стадией жизненного цикла ИТ-системы.

Таблица 1. Обобщенное представление действий по управлению риском, связанная с каждой стадией жизненного цикла ИТ-системы.

Стадии жизненного цикла	Характеристика стадии	Действия по управлению риском
Стадия 1 — Инициирование	Потребность в ИТ-системе сформулирована, цель и сфера действия ИТ-системы документально оформлены.	Для поддержки процессов разработки требований к системе, включая требования по безопасности и концепцию действий по обеспечению безопасности (стратегию) используются идентифицированные риски.
Стадия 2 — Разработка или приобретение	ИТ-система разработана, закуплена, запрограммирована, развита или перестроена.	Риски, идентифицированные в течение этой стадии могут использоваться, чтобы поддержать процессы анализа и исследования безопасности ИТ-системы; в некоторых случаях эти процессы могут привести необходимости замены архитектуры или проекта системы в течение разработки.
Стадия 3 — Реализация	Все установленные характеристики, возможности и особенности средств обеспечения безопасности ИТ-системы должны быть конфигурированы, осуществлены, протестированы и пройти верификацию.	Процессы управления риском направлены на оценку выполнения системой своих требований, в том числе, в пределах смоделированной окружающей среды предстоящей эксплуатации. Решения относительно идентифицированных рисков должны быть приняты до начала полной эксплуатации данной системы.
Стадия 4 — Эксплуатация или обслуживание	Система выполняет свои функции. В большинстве случаев система подвергается постоянным изменениям в виде появления дополнительных аппаратных средств ЭВМ и программного обеспечения, а также в виде изменений организационных процессов, политики и процедур.	Действия по управлению риском осуществляются в рамках проведения периодической переавторизации ИТ-системы (или ее переаккредитации), либо в тех случаях, когда в ИТ-системе производятся серьезные изменения, связанные с ее эксплуатацией или с окружающей средой ее использования (например, появляются новые интерфейсы системы).
Стадия 5 —	Эта стадия охватывает выведение из	Действия по управлению риском выполняются для

Выведение из эксплуатации	использования информации, аппаратных средств ЭВМ и программного обеспечения. Соответствующие действия могут включать перемещение, архивирование, удаление или уничтожение информации, а также удаление аппаратных средств ЭВМ и программного обеспечения.	тех компонентов системы, которые будут устраняться или заменяться. Эти действия должны быть направлены на то, чтобы гарантировать, что все процедуры с аппаратными средствами ЭВМ, с программным обеспечением, с оставшимися данными и с миграцией системы в целом проведены безопасными и систематизированными способами.

Методология оценки риска.

Оценка риска является первым процессом в методологии управления рисками. Организации используют оценку риска, чтобы определить степень потенциальной угрозы и связанного с ней риска от применения ИТ-системы в пределах всего своего жизненного цикла. Результаты этого процесса помогают идентифицировать соответствующие меры по управлению (контролю) за сокращением или устранением риска при выполнении мероприятий, направленных на уменьшение риска. Риск является функцией вероятности того, что данный источник угрозы, использует потенциальную уязвимость организации и закончится осуществлением воздействия этого неблагоприятного события на данную организацию. Чтобы определить вероятность будущего неблагоприятного события, потенциальные угрозы для ИТ-систем должны быть одновременно проанализированы с двух позиций: потенциальной уязвимости и наличия средств контроля (управления) в соответствующем месте ИТ-системы. Воздействие риска выражается степенью вреда, который мог бы быть вызван осуществлением данной угрозы для данного вида уязвимости.

Методология оценки риска охватывает девять главных шагов. Общая схема методологии оценки риска представлена на рисунке 1.

Исходные данные	Действия по оценке риска	Результаты
• Компьютерное оборудование • Программное обеспечение • Системные интерфейсы • Данные и информация • Люди • Миссия системы	**Шаг 1** **Характеристика системы**	• Границы системы • Функции системы • Критичность системы и данных • Чувствительность системы и данных
• История атак на систему • Данные от разведывательных агентств, NIPC, OIG, FedCIRC, СМИ	**Шаг 2** **Идентификация угроз**	• Формулировки угроз
• Отчеты по предыдущим оценкам рисков • Сообщения о различных аудитах • Требования к безопасности • Результаты тестирования безопасности	**Шаг 3** **Идентификация уязвимости**	• Перечень потенциальных точек уязвимости
• Текущее состояние контроля • Планируемые мероприятия по контролю	**Шаг 4** **Анализ контроля (управления)**	• Перечень текущих и планируемых мер по проведению контроля
• Мотивация источников угроз • Возможности угроз • Природа уязвимости • Текущее состояние контроля	**Шаг 5** **Определение вероятности (возможности)**	• Рейтинги возможности осуществления угроз
• Анализ воздействия на выполнение миссии • Оценка критичности активов • Критичность данных • Чувствительность данных	**Шаг 6** **Анализ воздействия**	• Рейтинги воздействия угроз
• Вероятность угрозы для эксплуатации • Размеры воздействия • Адекватность планируемых или текущих мер по контролю	**Шаг 7** **Определение риска**	• Риски и уровни допустимых рисков
	Шаг 8 **Рекомендации по контролю**	• Рекомендованные мероприятия по контролю
	Шаг 9 **Документальное оформление результатов**	• Отчет по оценке рисков

Рис.1. Общая схема методологии оценки риска

Далее кратко рассматривается содержание каждого шага методологии оценки риска.

Шаг 1- характеристика системы: первый шаг должен определить масштабы и сферу последующих действий, включая границу действия системы, информацию и ресурсы, которые составляют область ее воздействия и интересов. Сюда входят минимальные аппаратные средства ЭВМ и программное обеспечение, внутренние и внешние интерфейсы системы, используемые или произведенные системой информация и данные, действия персонала по поддержке системы, реализация системой интерфейсов и процессов пользователя, критические системы и данные, чувствительность данных и системы.

Шаг 2 – Идентификация угрозы: угроза представляет собой потенциал успешного осуществления негативного действия с использованием выявленной уязвимости. В свою очередь уязвимость эта та или иная слабость, которая может быть возникнуть случайно, либо окажется внесенной в систему преднамеренно по каким либо причинам. Ясно, что источник угрозы не представляет какого либо риска в тех случаях, когда уязвимость отсутствует. При определении вероятности осуществления угрозы следует рассматривать источники угроз, потенциально существующие уязвимости, а также имеющиеся средства контроля. Цель настоящего шага состоит в том, чтобы идентифицировать потенциальные источники угрозы и сформировать перечень потенциальных источников угроз, которые необходимо оценить применительно к исследуемым ИТ-системам. В таблице 2 приводится классификация возможных угроз со стороны людей с их мотивацией и угрожающими действиями.

Таблица 2. Классификация возможных угроз со стороны людей с их мотивацией и угрожающими действиями.

Источники угрозы	Мотивации	Угрожающие действия
Хакеры, взломщики	• Вызовы • Эгоцентризм, самомнение • Бунт, противодействие	• хакерство • социальная разработка (Social engineering) • вторжение или проникновение в систему • несанкционированный доступ к системе
Компьютерные преступники	• Разрушение информации • Незаконное раскрытие информации • Денежно-кредитные операции с целью получить выгоду • Несанкционированное изменение данных	• компьютерное преступление (например, киберпреследование) • мошеннический акт (например, переигрывание, имитирование или перехват) • информационное взяточничество • получение доступа путем обмана • вторжение в систему
Террористы	• Шантаж • Разрушение • Эксплуатация • Месть	• терроризм • информационная война • нападение на системы (например, невозможность распределенного обслуживания) • проникновение в систему • вмешательство в систему
Промышленный шпионаж (компании, иностранные правительства, интерес со стороны	• Получение конкурентоспособных преимуществ • Экономический шпионаж	• экономическая эксплуатация • кража информации • покушение на секретность персональных данных • социальная разработка • проникновение в систему

других правительственных ведомств)		• несанкционированный доступ в систему
Посвященные в систему люди (плохо обученные, обозленные, рассерженные, злонамеренные, небрежные, нечестные или уволенные служащие)	• Любопытство • Эгоцентризм • Получение данных • Денежно-кредитные устремления • Месть • Неумышленные ошибки и упущения (например, ввод ошибочных данных, ошибка программирования)	• нападение на служащих • шантаж • просмотр конфиденциальной внутренней информации • злоупотребление компьютером • мошенничество и воровство • информационное взяточничество • ввод фальсифицированных, искаженных данных • перехват данных • ввод злонамеренных кодов (например, вирусов, логических бомб, троянских коней) • продажа персональной информации • внесение дефектов в систему • вторжение в систему • создание саботажа со стороны системы • несанкционированный доступ в систему

Шаг 3 – Идентификация уязвимости: анализ угроз для ИТ-систем должен включать анализ уязвимостей, связанных с окружающей средой функционирования системы. Цель этого шага состоит в том, чтобы разработать перечень уязвимостей системы (как ее недостатков, так и выявленных слабостей), которыми могли бы воспользоваться потенциальные источники угроз. Приводимая ниже таблица 3 дает некоторые примеры пар: уязвимость / угроза.

Таблица 3. Некоторые примеры пар: уязвимость / угроза

Уязвимость	Источник угрозы	Угрожающее действие
Системные идентификаторы уволенных служащих не удалены из системы.	Уволенные служащие	Вхождение в сеть компании и доступ к данным, которые являются собственностью компании.
Брандмауэр компания позволяет идентифицированным гостям через средства сетевого теледоступа	Неавторизованные пользователи (например, хакеры, уволенные служащие, компьютерные	Использование сетевого теледоступа к XYZ серверу идентифицированными гостями.

вхождение на XYZ сервер.	преступники, террористы)	
Производитель идентифицировал существующие недостатки в системе безопасности, однако, новые решения не применены в системе.	Неавторизованные пользователи (например, хакеры, уволенные служащие, компьютерные преступники, террористы)	Получение несанкционированного доступа к чувствительным файлам системы, благодаря известным точкам уязвимости системы.

Точки уязвимости могут быть расположены в трех основных областях: область управления; область эксплуатации; область технических средств. В таблице 4 приведены критерии, предложенные для идентификации уязвимости в этих трех областях безопасности.

Таблица 4. Критерии идентификации уязвимости в трех основных областях безопасности.

Область безопасности	**Критерий безопасности**
Безопасность управления	• назначение ответственных; • поддержка непрерывности; • способность реагировать на возникающий инцидент; • периодический пересмотр обзор средств управления безопасности; • персональная ответственность и исследование предпосылок для появления уязвимости; • проведение оценки рисков; • обучение вопросам техники и безопасности; • разделение обязанностей; • авторизация и переавторизация системы; • планирование обеспечения безопасности системы и приложений.
Безопасность эксплуатации	• контроль загрязнения воздушной среды (дым, пыль, химикалии); • контроль за обеспечением качества электропитания; • доступ и распоряжение данными; • внешнее распределение и маркирование данных; • возможности физической защиты (например, помещений для компьютеров, центра данных, офиса и т.д.); • контроль влажности; • температурный контроль; • автоматизированные рабочие места, переносные компьютеры, автономные персональные компьютеры.

Техническая безопасность	• коммуникации (например, набор через клавиатуру, межсоединение систем, маршрутизаторы); • шифрование; • дискреционный (т.е. по усмотрению) контроль доступа; • идентификация и установление подлинности (аутентификация); • обнаружение вторжения; • повторное использование объекта; • системный аудит.

Шаг 4 – Анализ контроля (управления): цель этого шага состоит в том, чтобы проанализировать средства управления, которое было осуществлены или запланированы к реализации в организации с целью минимизировать или устранить вероятность (или саму возможность) осуществления угрозы с использованием уязвимости системы. При проведении оценки полной вероятности осуществления угрозы из за наличия потенциальной уязвимости окружающей среды необходимо учитывать состояние или планы развития средств управления и контроля за точками уязвимости.

Шаг 5 – Определение вероятности (возможности): Для получения полной вероятности того, что потенциальная уязвимость окружающей среды может быть использована для осуществления угрозы должна рассматриваться следующие доминирующие факторы: мотивации и возможности источника угрозы; характер и природа существующей уязвимости; наличие и показатели эффективности существующих средств контроля и управления. Возможны два вида оценок: количественная и качественная. Количественная оценка риска выражает возможность осуществления угрозы (ее вероятность), воздействие и риск в числовых величинах. Качественная оценка использует для выражения того или иного значения шкалу оценок *высокий, средний, низкий*. Если используемая количественная метрика оказывается недостаточно полной, точной или адекватной, то количественный подход имеет малые, либо вообще не имеет преимуществ перед качественным подходом, так как приходится использовать субъективную интерпретацию количественных характеристик. Поэтому сегодня большинство подходов начинают с использования качественных показателей ранжирования (*высокий, средний, низкий*) и присваивают диапазон значений каждому из трех показателей. В таблице 5 приведены качественные характеристики и их содержательные определения для каждого из трех уровней.

Таблица 5. Характеристика качественных уровней определения возможности осуществления угрозы

Уровень возможности	**Определение**
Высокий	Источник угрозы является высокоактивным и обладает

	достаточно высокими возможностями, в то время как управление предотвращением использования уязвимости для осуществления этой угрозы оказывается неэффективным.
Средний	Источник угрозы является достаточно активным и способным, однако средства управления, находящиеся на местах и обязанные воспрепятствовать использованию уязвимости действуют эффективно и могут противостоять угрозе.
Низкий	У источника угроз отсутствуют мотивации для осуществления угроз или они очень незначительны, а средства управления, находящиеся на местах, имеют возможность эффективно препятствовать использованию уязвимости для осуществления угроз.

Шаг 6 – Анализ воздействия (влияния): следующий важный шаг в измерении уровня риска должен определить степень неблагоприятности воздействия в случае успешного осуществления угрозы уязвимости. Неблагоприятное воздействие может быть описано с позиции потери или ухудшения любого, либо комбинации любых из трех следующих целей обеспечения безопасности: целостность, готовность и конфиденциальность. В таблице 6 дана качественная характеристика уровней воздействия в случае осуществления угрозы.

Таблица 6. Качественная характеристика уровней воздействия в случае осуществления угрозы

Уровень возможности	**Определение**
Высокий	Реализация угрозы через существующую в системе уязвимость: 1) может окончиться серьезными потерями дорогостоящих основных материальных активов или ресурсов; 2) может значительно нарушить, повредить или воспрепятствовать выполнению миссии организации, нанести вред репутации организации или ее интересам; 3) может закончиться человеческими жертвами или серьезным материальным ущербом.
Средний	Реализация угрозы через существующую в системе уязвимость: 1) может окончиться дорогостоящими потерями материальных активов или ресурсов; 2) может нарушить, повредить или воспрепятствовать выполнению миссии организации или нанести вред ее репутации или ее интересам; 3) может окончиться ущербом для людей.
Низкий	Реализация угрозы через существующую в системе

	уязвимость: 1) может окончиться потерей некоторых материальных активов или ресурсов; 2) может заметно затрагивать процесс выполнения миссии организации или ее репутацию и интересы.

Шаг 7 – Определение риска: цель этого шага состоит в том, чтобы оценить уровень риска ИТ-системы. Определение риска для любой конкретной пары угроза / уязвимость может быть выражено в виде следующих метрик:

- *Вероятность того, что данный источник угрозы попытается использовать и успешно преодолеет данную уязвимость;*
- *Величина воздействия, которое может возникнуть, если источник угрозы успешно использует данную уязвимость;*
- *Адекватность запланированной или существующей системы безопасности для сокращения или устранения риска.*

В таблице 7 показана матрица, позволяющие количественно оценить величину риска в зависимости от уровня возможности осуществления угрозы и от уровня воздействия этой угрозы.

Таблица 7. Матрица количественной оценки величины риска в зависимости от уровня возможности осуществления угрозы и от уровня воздействия этой угрозы.

Возможность осуществления угрозы	**Воздействие**		
	Низкая (10)	Средняя (50)	Высокая (100)
Высокая (1,0)	Низкая 10x1,0=10	Средняя 50x1,0=50	Высокая 50x1,0=100
Средняя (0,5)	Низкая 10x0,5=5	Средняя 50x0,5=25	Высокая 100x0,5=50
Низкая (0,1)	Низкая 10x0,1=1	Средняя 50x0,1=5	Высокая 100x0,1=10

В таблице 8 показан перечень соответствующих действий, которые предпринимаются в ответ на тот или иной уровень риска согласно количественным оценкам, приведенным в предыдущей таблице.

Таблица 8. Уровни риска и необходимые действия.

Уровень риска	**Определение риска и необходимые действия**
Высокий	Если средства наблюдение или обнаружения оценивают риск, как риск высокой степени, то возникает серьезная потребность в развертывании корректирующих мероприятий. При этом существующая система контроля может некоторое время

	использоваться, однако новые мероприятия по корректирующему плану должны быть введены в действие как можно скорее.
Средний	Если средства наблюдения оценивают риск, как риск средней степени, то корректирующие мероприятия и соответствующий план должны быть разработаны и введены в действие в пределах разумного периода времени.
Низкий	Если средства наблюдения описывают существующий риск как незначительный (риск низкого уровня), то соответствующие органы управления риском должны определить, требуются ли какие-либо корректирующие действия, либо можно принять обнаруженный уровень риска.

Шаг 8 – Рекомендации по контролю (управлению): В течение этого шага процесса создаются средства контроля и управления, которые могли бы смягчить или полностью устранить идентифицированные риски для поддержания соответствующих действий организации. Цель рекомендуемых средств управления состоит в том, чтобы уменьшить до приемлемого уровня риск для ИТ-систем и используемых данных. В число рассматриваемых факторов, которые необходимо учитывать при формировании рекомендаций по средствам управления и по альтернативным решениям для минимизации или устранения идентифицированных рисков, входят: эффективность рекомендуемых опций (например, совместимость систем), законодательство и регулирование, политика организации, особенности и воздействие эксплуатации, безопасность и надежность.

Шаг 9 – Документальное оформление результатов: После того, как оценка риска закончена (источники угрозы и уязвимости идентифицированы, получены оценки вероятностей рисков и сформированы рекомендации по средствам контроля и управления), полученные результаты должны быть официально представлены в виде отчета или инструктивных указаний. Отчет по оценкам риска должен быть предназначен для использования высшим уровнем руководства, владельцами миссии, лицами, которые принимают решения на политике, по процедурам, по бюджету, а также для эксплуатации системы и для управления изменениями. В отличие от исследовательских отчетов или отчетов аудиторов, цели которых состоят в поиске новых решений или в анализе существующих просчетов, отчеты по оценкам рисков не должны иметь обличительный характер, а, наоборот, они должны представлять систематический и аналитический подход к оценкам степени риска таким образом, чтобы высшее руководство организации могло получить полное понимание возможных рисков и их последствий и выделять достаточные ресурсы на их уменьшение и на исправление потенциальных потерь.

Уменьшение рисков.

Уменьшение рисков предполагает определение приоритетов, проведение оценок и реализацию соответствующих средств управления сокращением рисков, рекомендуемых в процессе проведения оценок рисков. Поскольку полное устранение риска, как правило не реально или не осуществимо, высшее руководство организации, менеджеры функциональных и бизнес-подразделений несут ответственность за то, чтобы реализовать ***наиболее подходящие средства управления и контроля*****,** позволяющие уменьшить риски для выполнения миссии до приемлемого уровня, **с *минимальным неблагоприятным воздействием*** на ресурсы организации и на выполнение миссии ***(рентабельное управление рисками).*** Уменьшение рисков является последовательной и систематизированной методологией, которая должна использоваться высшим руководством с целью уменьшения рисков для осуществления миссии. Уменьшение рисков может быть достигнуто применением любой из перечисленных ниже опций по уменьшению риска:

- ***Принятие риска (Risk Assumption).*** *Принимать потенциальный риск и продолжать использовать ИТ- системы, либо реализовать средства управления, позволяющее снизить риск до приемлемого уровня.*
- ***Предотвращение риска (Risk Avoidance).*** *Избегать рисков, устраняя причину риска и/или его последствия (например, воздержаться от использования некоторых функций системы, или закрыть систему, когда риски полностью идентифицированы).*
- ***Ограничение риска (Risk Limitation).*** *Ограничивать имеющийся риск, реализовав и применив средства управления, которые минимизируют неблагоприятное воздействие осуществления угрозы для уязвимости (например, использование поддерживающего, профилактического или детективного (тайного)контроля).*
- ***Планирование риска (Risk Planning).*** *Управлять риском, путем разработки плана действий по уменьшению риска, который может предусматривать введение определенных приоритетов, реализацию и проведение контроля.*
- ***Исследование и уведомление (Research and Acknowledgment).*** *Понизить риск возможных потерь, путем уведомления о наличии уязвимости или недостатков в системе и исследования средств контроля для исправления уязвимости.*
- ***Перенос риска (Risk Transference).*** *Переместить риск, используя другие опции, чтобы получить компенсации за возможные потери, например, путем страхования покупок.*

Общая последовательность действий в методология уменьшения рисков, которая, как рассмотренная выше методология оценки риска, является составной частью жизненного цикла развития ИТ-систем, приведена на рис.2 .

Исходные данные	Действия по уменьшению риска	Результаты
• Уровень риска, полученный по данным отчетов по оценке рисков	**Шаг 1** **Приоритеты действий**	• Проведение ранжирования действий, начиная с самого низкого уровня рисков
• Отчет по оценке рисков	**Шаг 2** **Оценка рекомендованных опций контроля**	• Перечень возможных мероприятий по контролю
	Шаг 3 **Проведение анализа на рентабельность** • **Воздействие реализации** • **Воздействие не реализации** • **Связанные затраты**	• Результаты анализа на уровень рентабельности
	Шаг 4 **Выбор средств контроля**	• Выбранные средства контроля
	Шаг 5 **Определение ответственности**	• Перечень ответственности должностных лиц
	Шаг 6 **Разработка плана реализации** • **Риски и соответствующие уровни рисков;** • **Распределенные по приоритетам действия;** • **Рекомендованные средства контроля;** • **Запланированные средства контроля;** • **Ответственность должностных лиц;** • **Исходные данные;** • **Требования по сопровождению.**	• План реализации
	Шаг 7 **Реализация выбранной системы контроля**	• Остаточный риск

Рис.2. Методология действий по уменьшению рисков

Анализ рентабельности и остаточный риск

Анализ рентабельности предлагаемых новых средств управления или усовершенствования существующих средств охватывает следующее:

- Определение воздействия осуществления новых или проведения усовершенствования существующих средств управления;
- Определение воздействия не осуществления нового или не проведения усовершенствования существующих средств управления
- Оценка затрат на выполнения перечисленных действий. Затраты могут включать (перечень не полный) следующее: закупки аппаратных средств ЭВМ и программного обеспечения, снижение эксплуатационной

эффективности, если характеристики системы или ее функциональные возможности будут уменьшены для увеличения безопасности, затраты на осуществление дополнительных видов политики и процедур, затраты на прием дополнительного персонала служащих, которые должны будут осуществлять предложенную политику, процедуры или услуги, затраты на обучение персонала, затраты на поддержание и на обслуживание.

- Оценка рентабельности реализации по сравнению с критичностью системы и данных, чтобы определить важность осуществления новых средств управления с учетом возникающих затрат и соответствующего воздействия осуществившегося риска.

Организации могут анализировать степень сокращения риска, связанного с новыми или усовершенствованными средствами управления с позиции уменьшения вероятности угрозы или степени воздействия, т.е. тех двух параметров, которые определяют уровень допустимого риска для осуществления миссии организации. ***Риск, остающийся после реализации нового средства управления или проведения усовершенствования существующего средства управления является остаточным риском.*** Фактически не существует ИТ-систем, которые были бы свободными от рисков и поэтому большинство реализуемых средств управления предназначены, главным образом для того, чтобы адресовать или уменьшить уровень рисков, в том числе и до нуля. Если остаточный риск не был уменьшен до приемлемого уровня, то цикл управления рисками должен быть повторен с целью нахождения путей дальнейшего понижения остаточного риска до приемлемого уровня. Уполномоченное должностное лицо, ответственное за ИТ-инфраструктуру в конечном итоге принимает решение о достижении приемлемого уровня риска, после чего им подписывается соответствующий документ, разрешающий использование всей системы при достигнутом уровне остаточного риска.

Ключевые факторы успешного управления рисками

Успешная программа управления рисками должна опираться на следующие факторы:

- наличие обязательств со стороны высшего руководства организации о предоставлении необходимых ресурсов и времени;
- полная поддержка и участие со стороны подразделения, ответственного за ИТ;
- компетентность специалистов, проводящих оценки риска; специалисты должны обладать опытом применения методологии оценки риска для отдельных участков и всей системы в целом, по идентификации рисков для выполнения миссии организации и по обеспечению рентабельных мер предосторожности, которые удовлетворяют имеющиеся потребности организации;
- достаточный уровень осведомленности и сотрудничество всех членов сообщества пользователей, которые должны строго следовать

установленным процедурам и выполнять все требования по контролю за соблюдением мер предосторожности по охране миссии своей организации;
- непрерывно продолжающееся определение и оценка IT-рисков, имеющих отношение к выполнению миссии.

Хотя известная Директива Офиса управления и бюджета А-130 устанавливает обязательность включения процессов управления рисками, тем не менее, управление риска должно выполняться и интегрироваться в жизненный цикл ИТ-систем не только в соответствии с требованиями Директивы А-130, но и потому, что управление рисками перешло в категорию «наилучшей практики» в качестве средства поддержки миссии организации.

Десять наиболее часто задаваемых вопросов относительно оценки риска

1. ***Как разница между качественной и количественной оценкой риска?***
   Количественная оценка риска выражает возможность осуществления угрозы (ее вероятность), воздействие и риск в числовых величинах, в то время как качественная оценка использует для выражения того или иного значения шкалу оценок *высокий, средний, низкий*. Главное преимущество количественного подхода состоит в том, что при этом получаются показатели, которое могут быть непосредственно использованы для анализа рентабельности. Однако, если используемая количественная метрика оказывается недостаточно полной, последовательной, точной и уместной, этот подход имеет малые, либо вообще не имеет преимуществ перед качественным подходом, так как приходится использовать субъективную интерпретацию количественных характеристик. Поэтому сегодня большинство подходов начинают с использования качественных показателей ранжирования (*высокий, средний, низкий*) и присваивают диапазон значений каждому из трех показателей.

2. ***Кто должен принимать участие в осуществлении оценок риска?***
   Для каждой конкретной системы (систем) группа по оценке риска должна включить, как минимум, следующих представителей: владелец (владельцы) системы, специалисты, представляющие безопасность ИТ-систем, операционные пользователи системы и персонал, который поддерживает работу ИТ-системы. Кроме того, руководство может добавить к этой группе любых других представителей и специалистов, участие которых оно считает полезным или необходимым.

3. ***Сколько времени должна продолжаться оценка рисков?***
   Период времени, необходимый для того, чтобы провести оценку риска изменяется в зависимости от масштабов и сложности анализируемой системы, а также от ответственности, количества и уровня

квалификации задействованных ресурсов. Обычно, оценка рисков несложной прикладной системы среднего объема может быть проведена в период времени до трех месяцев. Более сложные поддерживающие системы (сети, центры данных) или сложные приложения могут потребовать в среднем от шести до девяти месяцев.

4. ***Как часто должны проводиться оценки рисков?***
Каждая система в ходе разработки должна быть подвергнута оценке риска в процессе всего жизненного цикла вплоть до проведения ее сертификации и аккредитации. Системы, которые находятся в состоянии эксплуатации должны быть подвергнуты оценке риска каждый раз по мере появления серьезных изменений в функциональных возможностях или в ИТ-архитектуре. Согласно Директиве А-130 Офиса управления и бюджета каждое приложение или системы поддержки должны подвергаться оценке риска по крайней мере раз в каждые три года. Наконец, Акт по обеспечению безопасности правительственный информации (Government Information Security Reform Act, GISRA) от 2000 года требует, чтобы правительственные агентства проводили ежегодные обзоры своих программ безопасности, включая испытания систем. Ясно, что агентства могут вводить дополнительные уровни частоты проведения испытаний различных систем (например, предусмотреть большее количество испытаний для систем, критических по отношению к миссии организации).

5. ***Кому должен быть представлен заключительный отчет по результатам оценки риска?***
Заключительный отчет по результатам оценки риска должен быть представлен ответственному владельцу системы. Он должен использовать полученные результаты для того, чтобы принять обоснованные решения относительно готовности системы. Менеджер должен принять решение, либо о необходимости продолжения работ по усовершенствованию средств управления до получения удовлетворительного уровня риска, либо признать, что достигнутый уровень риска является приемлемым.

6. ***Каким образом можно определить количественные значения показателей риска?***
Определение риска может быть получено в соответствии со следующей формулой:

Вероятность угрозы * Воздействие Угрозы = Ожидаемый Риск

7. ***Каким образом оценить затраты по «неосязаемым» воздействиям?***
Определить величину затрат для неосязаемых факторов, типа доверия со стороны общества или репутация организации, достаточно трудно. Однако, анализируя случая воздействия на бизнес и на клиентов, вызванные, например, слабостями системы или потерями конфиденциальности, можно оценить потенциальное воздействие и

использовать специально ориентированные рабочие группы в качестве метода, который позволит провести адресование неосязаемых факторов.

8. Каким образом можно получить доступ к информации об источниках угрозы?

Информация об угрозах доступна из различных источников таких, как государственные и местные организации и учреждения, которые отслеживают угрозы со стороны природной и окружающей среды (например, метеорологические службы), а также местные предприятия коммунального обслуживания. Кроме того, информация об источниках угрозы со стороны людей доступна из федеральных и местных источников в правоохранительных учреждениях. Правительственные агентства могут также получать информацию из Офиса генерального инспектора (Office of Inspectors General, OIG), Национального Центра Защиты Инфраструктуры (National Infrastructure Protection Center, NIPC), Федерального центра по компьютерным инцидентам (Federal Computer Incident Responsible Center, FedCIRC), и других служб, отвечающих за критические компьютерные системы. Средства массовой информации также следует рассматривать как хороший источник информации. Наконец, Интернет обеспечивает большой ресурс для проведения исследований в этой области. Большинство поставщиков оценок риска имеет надежные и развернутые базы данных по различным источникам и видам угроз.

9. Какие существуют источники информации, относящейся к уязвимости?

Хорошими источниками информации, связанной с уязвимостью можно считать результаты ранее поведенных аудитов, предыдущие отчеты об оценках риска, отчеты Главного Контрольно-Финансового Управления (General Accounting Office, GAO), отчеты Офиса генерального инспектора (OIG), отчеты с анализом случаев мошенничества, ошибок и нарушений, допущенных системой, документация, содержащая требования по безопасности, Белые Книги в отраслях промышленности и другие доступные публикации. Ключевым ресурсом, доступным в Национальном институте стандартов и технологий NIST является инструмент ICAT, который может быть найден в http: // icat.nist.gov. Этот инструмент обеспечивает доступ к идентифицированным видам уязвимости систем и к информации относительно решений, позволяющих устранить эту уязвимость.

10. Каким образом эта методология может быть использована в случае совместной работы множества взаимодействующих систем?

Каждая система, вовлеченная во взаимодействие, в первую очередь должна пройти оценку риска самостоятельно. После того, как эта оценка закончена, должны быть определены возможности и масштабы взаимодействия всех систем в терминах интерфейсов системы, интерфейсов пользователя, возможностей по соединениям, потоков

данных / информации, а также дополнительных функциональных возможностей, которые будут осуществлены в результате этого взаимодействия. Используемые шаги остаются прежними, однако сложность и глубина анализа зависит от характера взаимодействия и от конкретной области интересов. Очевидно, что в целом усилия, требуемые для проведения таких оценок, значительно больше, чем для отдельных систем.