Обновляемая подборка материалов
для проведения лекционных занятий по дисциплине

Б1.В.ДВ.07.01
«Введение в теорию управления рисками информационной безопасности»

Комаров Игорь Иванович

2018

Раздел 1. Концептуальные основы управления рисками ИБ.

Назначение пособия и задачи изучения дисциплины. Связь с другими дисциплинами..

Настоящее учебное пособие предназначено для поддержки изучения курса «Управление рисками информационной безопасности», который является обязательным для изучения в рамках подготовки магистрантов по программе 090900.68 "Управление информационной безопасностью" направления 090900 «Информационная безопасность».

Подготовка по направлению осуществляется на факультете «Компьютерные технологии и управление» (КТиУ), базовая кафедра – «Безопасные информационные технологии» (БИТ).

Для успешного освоения дисциплины облучающийся должен владеть:

знаниями базовых положений теории информации и математической статистики; принципов функционирования и использования программно-аппаратных средств обеспечения информационной безопасности и инженерно-технических средств защиты информации, способов организации дистанционного взаимодействия компьютерных систем, элементов криптографической защиты информации;

умениями осуществлять поиск информации во встроенных справочных системах и больших слабоструктурированных информационных массивах, в том числе в сети Интернет, анализировать и оценивать на качественном уровне ресурсоемкость задач, решаемых компьютерными системами, читать и анализировать коды неизвестных программ на одном из формальных языков, работать с нормативно-правовыми документами в области информационной безопасности;

навыками работы на ЭВМ с использованием интерфейсов командной строки и WIMP; одним из языков программирования высокого уровня, профессиональной терминологией, навыками безопасного использования технических средств в профессиональной деятельности.

Содержание дисциплины является логическим развитием дисциплин Философия (на основе базовой подготовки магистранта), Основы информационной безопасности, Организационно-правовые механизмы обеспечения информационной безопасности, Программно-аппаратные средства информационной безопасности, Организация защищенного документооборота.

Изучение значительной части материала может быть поддержано путем параллельного освоения дисциплины «Математическое моделирование объектов и систем» и дисциплины по выбору «Технические средства противодействия промышленному шпионажу».

Целью освоения дисциплины является достижение следующих результатов образования:

знания на уровне представлений: о системной сложности задачи управления рисками ИБ; теоретических и технико-экономических противоречиях системы управления рисками ИБ; о возможности выполнения отдельных этапов комплекса задач управления рисками ИБ с использованием формальных математических моделей; основных тенденциях и перспективах развития систем управления рисками ИБ;

знания на уровне воспроизведения: источники рисков информационной безопасности; цели и задачи управления рисками ИБ; методологии и стандарты оценки и управления рисками ИБ, их классификацию; руководящие документы в области оценки рисков ИБ; содержание технического задания на разработку компонента инструментального средства управления рисками ИБ; факторы, влияющие на определение стоимости активов и ущербов от реализации рисков способы, модели и способы оценки стоимости активов и рисков;

знания на уровне понимания: о роли и месте задачи управления рисками в комплексной системе информационной безопасности; о потенциальных возможностях инструментальных сред анализа и управления рисками информационной безопасности; о критериях выбора инструментальных средств управления рисками ИБ;

умения теоретические: формулировать предложения по реструктуризации объекта информатизации с точки зрения снижения рисков ИБ; производить сведение отдельных этапов задачи управления рисками к математическим оптимизационным задачам; производить обоснованный выбор методов и средств для решения отдельных задач управления рисками ИБ;

умения практические: проводить количественную оценку рисков ИБ, оценивать эффективность функционирования системы управления рисками ИБ; оценивать выполнение требований руководящих документов и методологических стандартов к системе управления рисками ИБ; формировать перечень мероприятий по созданию системы управления рисками ИБ, уметь выбирать инструментальные средства для выполнения задач управления рисками ИБ;

навыки: использования одного из математических пакетов для решения задач управления рисками ИБ; самостоятельного информационного поиска в массивах открытой документации; работы с руководящими документами и стандартами; владения профессиональной терминологией; безопасного использования технических средств в профессиональной деятельности; обеспечения ИБ личного информационного пространства.

На материале дисциплины базируются курсы, завершающие подготовку выпускника: Управление информационной безопасностью, Комплексное обеспечение информационной безопасности. Кроме того, материал дисциплины может найти свое применение в ходе выполнения научно-исследовательской работы и магистерской диссертации.

Проблема терминологической неоднозначности.

В силу высокой динамики области информационной безопасности в ходе изучения дисциплины перед обучающимся ставиться задача самостоятельного обзора источников информации по предмету курса и составления актуализированного аннотированного списка информационных источников, в основу которого можно положить материал приложения 1 [?!!]. Условно все информационные ресурсы можно разделить на несколько групп:

– 1) нормативно-правовые источники, к числу которых, в первую очередь, следует отнести обязательные и рекомендуемые к выполнению официальные документы (законы, приказы, руководящие документы, инструкции, методические рекомендации и т.п.), а также стандарты различного статуса (государственные, межгосударственные, отраслевые, ведомственные, корпоративные);

– 2) научные научно-практические, и научно-популярные публикации, к которым можно отнести результаты научных исследований (монографии, статьи, отчеты, тезисы и информационные сообщения), содержащие объективные данные о достижениях в области курса и смежных областях;

– 3) официальные, в том числе – маркетинговые, материалы компаний – поставщиков решений, товаров и услуг в области информационной безопасности (декларируемые характеристики продукции и услуг, отчеты, коммерческие предложения, материалы как встроенных, так и сетевых справочных систем и руководств, данные служб поддержки);

– 4) учебные материалы различного статуса и назначения;

– 5) материалы профессионального сообщества специалистов в области информационной безопасности вообще и управления рисками в частности (тематические сайты, форумы и блоги).

Наибольшую опасность для успешной реализации проектов несёт в себе использование устаревших (измененных или утративших силу) документов перовой группы, а также ошибочных или недостоверных данных, которые могут оказаться в любом источнике остальных групп нашей классификации. Поэтому принятие принципиально важных решений в области управления рисками должно базироваться на фактах, полученных из источников, имеющих достаточную степень доверия.

Множественность и неоднозначность формулировок базовых понятий в области информационной безопасности и управления рисками, вызванная использованием документов из различных источников (в том числе вольных переводов иноязычных текстов) определила необходимость формирования глоссария, приведенного в приложении 2, использование которого позволяет не только однозначно определиться с содержанием конкретного понятия, но и выяснить контекст его употребления, получить дополнительные характеристики системы взглядов лица, его употребляющего.

Место рисков информационной безопасности в общей системе рисков проекта.

Для корректного системного определения понятия риска, обсуждаемого в данном курсе, а также методов и средств, используемых для управления им, требуется ограничить область исследования.

Пусть мы обсуждаем деятельность *коммерческого* предприятия, основной задачей которого является получение максимальной прибыли (Пр) в рамках действующих условий функционирования (ограничений) (Огр) во множестве всех доступных для анализа сфер деятельности предприятия, в том числе собственных ресурсов. Пусть в рамках априорного описания условий функционирования у предприятия имеется план (пл) оптимальных[1] (рациональных) действий:

$$\begin{cases} \text{Пр}_{\text{пл}} \to \max \\ \text{Огр}_{\text{пл}} \cong const \end{cases}. \qquad (1)$$

Примером проекции этих общих соображений на этап проектирования технологического объекта может служить рисунок (рис. 1) из ГОСТ Р 51901.4-2005 (Менеджмент риска. Руководство по применению при проектировании), отображающий возможность воздействия множества конкретных условий функционирования на процесс производства конечного продукта.

Поскольку условия функционирования имманентно изменчивы, то имеет место некоторая *неопределенность* развития условий функционирования. Причем, любая неопределенность в развитии любой из сфер, взаимодействующей с нашим коммерческим предприятием, может иметь одну из трёх степеней влияния на результат реализации плана – размер прибыли: положительное влияние – прибыль увеличивается, отрицательное влияние – прибыль уменьшается, нейтральное – на прибыль не влияет.

[1] Вопросы оптимальности (рациональности) решений исследуются в рамках научного направления кибернетики «Теория оптимального управления» и связанных с нею дисциплин. Для ознакомления с ними можно рекомендовать источники ?!!.

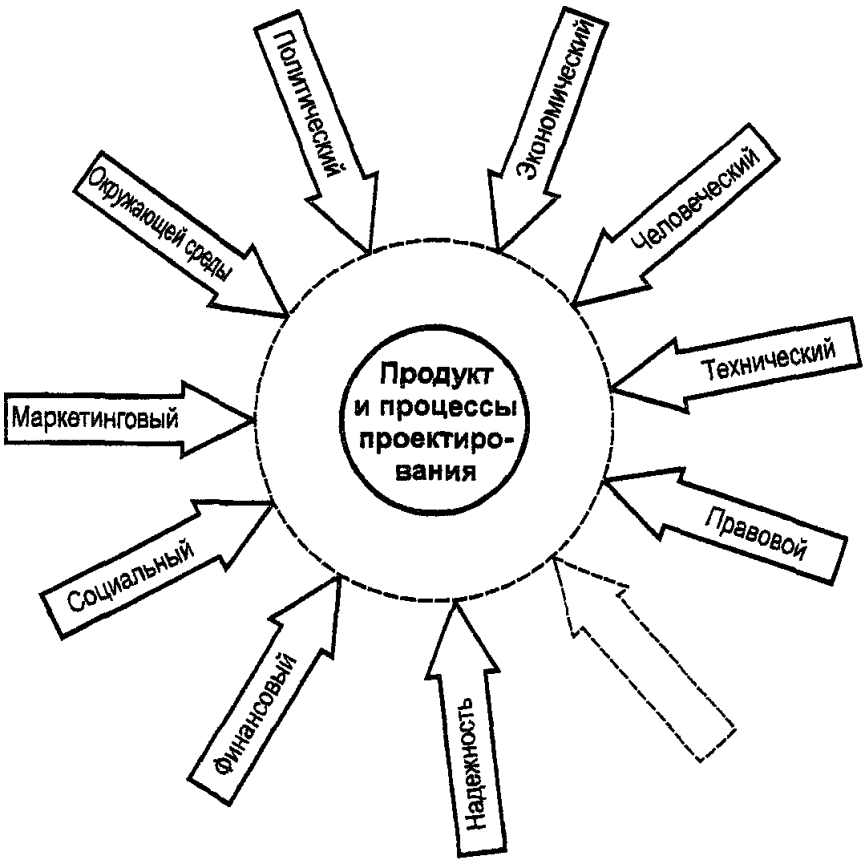


Рисунок 1. Множество условий функционирования определяющее неопределенность результата процесса

Таким образом мы получаем более формальную интерпретацию интуитивно понятного определения риска – как негативного последствия некоторого нежелательного события. Однако в стандартах понятие риска имеет более строгую формулировку со ссылками на другие термины. Считаем целесообразным привести достаточно обширную цитату (таблица 1) из ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения».

Таблица 1. Фрагмент определения базовых понятий в ГОСТ Р 51897-2011

1 Термины, относящиеся к риску	перевод	
1.1 **риск**: Следствие влияния неопределенности на достижение поставленных целей[1].	en	risk
	fr	risque
Примечание 1 — Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и/или негативное).		

[1] В соответствии с ФЗ «О техническом регулировании» от 27.12.2002 № 184-ФЗ «риск — это вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда».

Примечание 2 — Цели могут быть различными по содержанию (в области экономики, здоровья, экологии и т. п.) и назначению (стратегические, общеорганизационные, относящиеся к разработке проекта, конкретной продукции и процессу).
Примечание 3 — Риск часто характеризуют путем описания возможного события (3.5.1.3) и его последствий (3.6.1.3) или их сочетания.
Примечание 4 — Риск часто представляют в виде последствий возможного события (включая изменения обстоятельств) и соответствующей вероятности.
Примечание 5 — Неопределенность — это состояние полного или частичного отсутствия информации, необходимой для понимания события, его последствий и их вероятностей.

2 Термины, относящиеся к менеджменту риска		
2.1 **менеджмент риска**: Скоординированные действия по руководству и управлению организацией в области риска (1.1).	en	risk management
	fr	management du risque
2.1.1 **структура менеджмента риска**: Взаимосвязанные элементы, которые обеспечивают реализацию принципов и организационные меры, применяемые при проектировании, разработке, внедрении, мониторинге (3.8.2.1), анализе и постоянном улучшении менеджмента риска (2.1) организации.	en	risk management framework
	fr	cadre organisationnel de management du risque

Примечание 1 — Принципы отражают политику, цели, полномочия и обязательства в области менеджмента риска (2.1).
Примечание 2 — Организационные меры включают в себя планы, взаимоотношения, подотчетность, ресурсы, процессы и действия.
Примечание 3 — Структура менеджмента риска должна быть интегрирована в общую стратегию, политику и практическую деятельность организации.

2.1.2 **политика в области менеджмента риска**: Заявление высшего руководства об общих намерениях, руководящих принципах и направлениях деятельности организации в области менеджмента риска (2.1).	en	risk management policy
	fr	politique de management du risque
2.1.3 **план менеджмента риска**: Краткое, схематичное описание деятельности и мероприятий в пределах структуры менеджмента риска (2.1.1), устанавливающих подход, элементы менеджмента и ресурсы, применяемые для менеджмента риска (2.1).	en	risk management plan
	fr	plan de management du risque

Примечание 1 — Элементы менеджмента обычно включают в себя процедуры,

методы, распределение ответственности, последовательность действий и сроки их исполнения. Примечание 2 — План менеджмента риска может быть применен к конкретной продукции, процессу и проекту, к части или всей организации.

В контексте уяснения задачи управления риском целесообразно обратиться к части первой широко известных «Общих критериев» – ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1 Введение и общая модель.

В ней при описании общего контекста безопасности приводится следующая мнемосхема (рис. ?!!2), позволяющая определить взаимосвязь основных понятий безопасности.

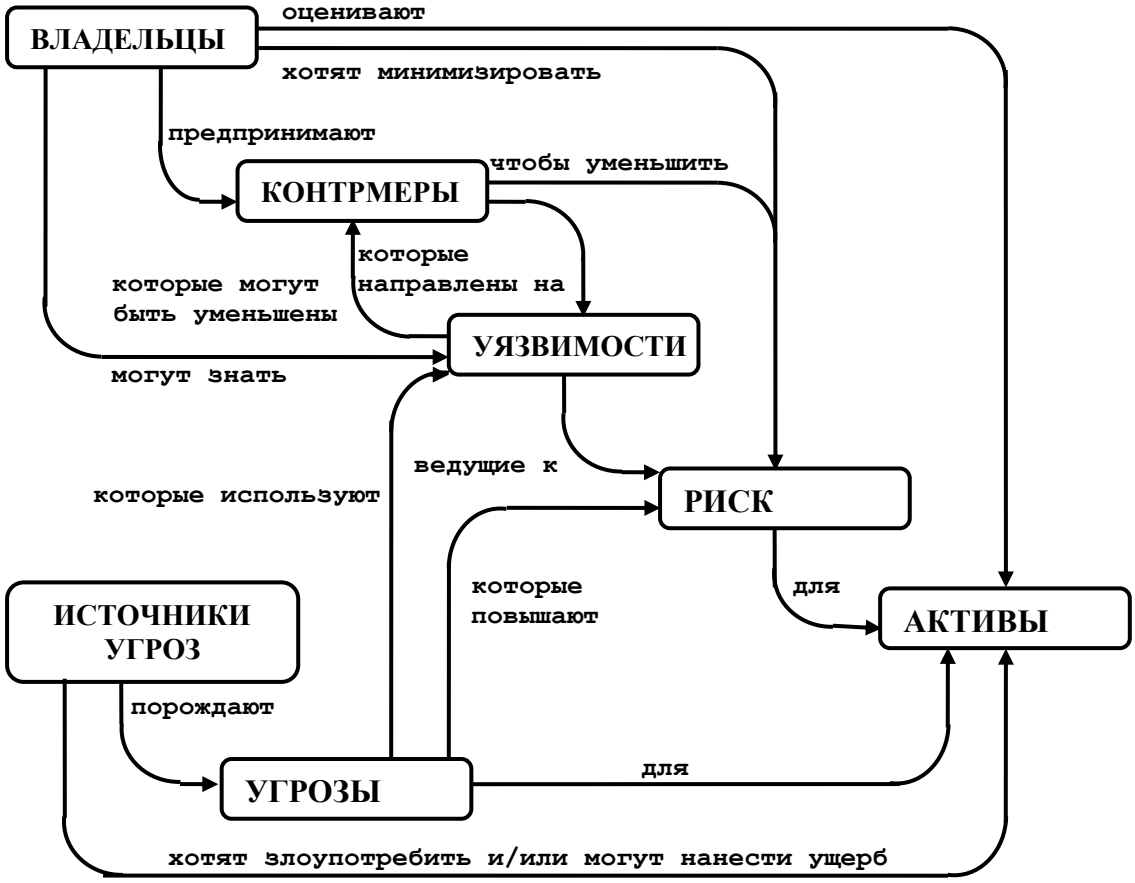


Рисунок 2 – Понятия безопасности и их взаимосвязь

Предложим иную графическую интерпретацию роли и места рисков информационной безопасности в виде следующей матрицы взаимовлияний (рис. 3).

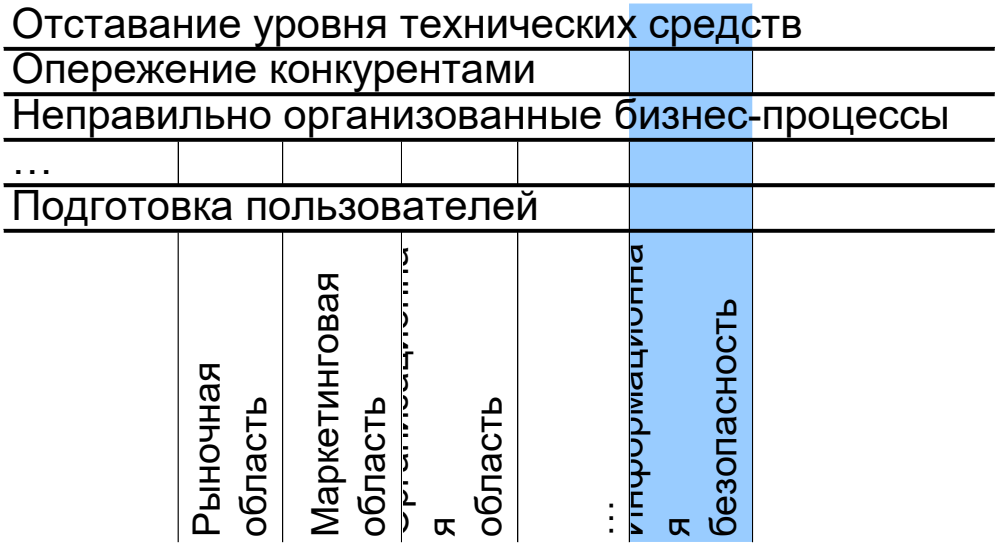


Рисунок 3. Влияние информационной безопасности
на факторы риска коммерческого предприятия.

Действительно, информационная безопасность оказывает влияние на все виды обеспечения производственного цикла, как внутри предприятия, так и его окружения. Например, нарушение требования конфиденциальности относительно конкретных параметров бизнес-плана предприятия позволит конкурентам заблаговременно изменить собственные планы и выработать контрмеры, а нарушение целостности информационного обеспечения бизнеса может привести к невозможности выполнения компонентов технологических цепочек, что делает невозможным реализацию основных миссий предприятия.

Источники и условия реализаций рисков информационной безопасности.

Конкретизация понятия риска на область информационной безопасности требует дополнительных обоснований. А именно: широко используемое в теории и практике информационной безопасности понятие «модель угроз» предполагает описание возможных нарушений информационной безопасности в виде кортежа, характеризующего в общем виде возможность и последствия негативного события в области информационной безопасности. Адаптированное обобщение такого кортежа, соответствующего рисунку 3 из документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008 г. представлена в таблице 2.

Таблица 2 Адаптированная форма представления модели угроз

Источник угрозы	Уязвимость	Способ реализации угрозы	Объект воздействия	Деструктивное воздействие

A	B	C	D	E
субъект или объект	*недостатки ИС*	*конкретный набор действий (атака)*	*элементы ИС*	*нарушаемые требования ИБ*

Аналогичное по смыслу определение приводится и в документе «Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения СТО БР ИББС-1.0-2010» (принят и введен в действие Распоряжением Банка России от 21.06.2010 N Р-705):

«Модель угроз информационной безопасности; модель угроз ИБ: описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба»

Следствием этих формализаций является вывод о необходимости наличия совокупности всех элементов кортежа для возникновения нежелательного события, а, значит и негативных последствий.

В качестве дополнительной иллюстрации зависимостей понятий информационной безопасности можно привести несколько модифицированную мнемосхему, предложенную А.К. Гультяевым (рис. 4).

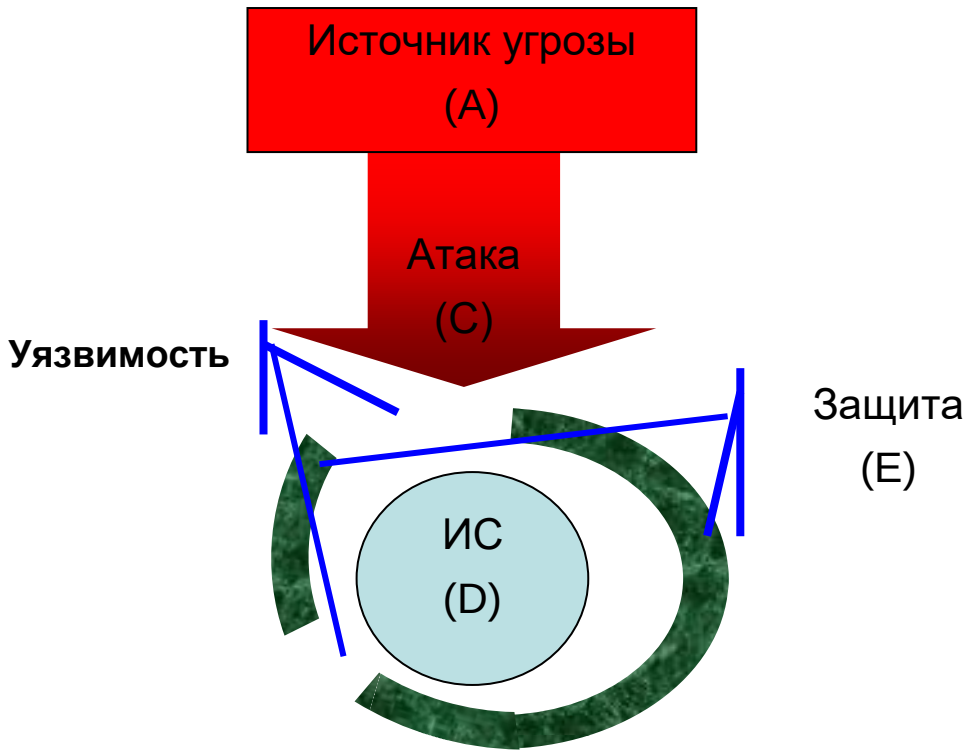


Рисунок 4. Взаимосвязь элементов кортежа
описания угрозы информационной безопасности

Действительно, для того, чтобы возник негативный эффект, связанный с нарушением правил информационной безопасности (E), последние должны быть определены; должен присутствовать объект атаки (D) – элемент информационной системы; должна присутствовать реализуемая последовательность действий (C) (как умышленная - атака, так и случайная - инцидент), направленная на эксплуатацию конкретной уязвимости (B) – недостатка ИС, причем эти действия инициируются источником угрозы (A).

Очевидно, что в зависимости от объекта атаки (D), её реализуемости (C) и результатов (E) степень негативных последствий будет различной. Не рассматривая пока способы, методы и средства оценки негативных последствий, определим общую зависимость между упомянутыми понятиями. Традиционно для этого используется понятие **величина риска** (R), под которым будем понимать количественное значение произведения некоторым образом полученной оценки негативных последствий (D) (ущерба, англ. damage) и вероятности его возникновения (P_D):

$$R = D * P_D . \quad (2)$$

Естественно, что это выражение может быть применено к любому из видов ущербов, однако не стоит забывать, что реализация той или иной угрозы может вызвать несколько негативных последствий, о чем, кстати, имеется явное упоминание в ГОСТ Р 51897 «Менеджмент риска. Термины и определения» версии от 2002 года.

Тогда логично, что общая оценка рисков информационной безопасности по всем угрозам для системы в целом определяется:

$$R_s = \sum_{i=1...n} D_i * P_i \quad (3)$$

где R_s – искомая оценка рисков информационной системы в целом; D_i – оценка рисков i-го вида; P_i – вероятность возникновения нежелательного события i – го вида; n – общее число таких событий.

Обсуждая методологическую роль выражений (2) и (3), следует понимать, что их практическое использование возможно только в условиях наличия количественного выражения значений P_i и D_i, что само по себе является нетривиальной задачей.

Например, обсуждая вопрос выполнения условий реализации рисков, как совокупности всех взаимосвязанных компонентов кортежа, описывающего угрозу, следует (в том числе, но не только) проанализировать факторы, которые могут оказать воздействие на информационную безопасность информационной системы. Качество самостоятельного перечисления таких факторов чрезвычайно сильно зависит от уровня подготовки исполнителя не только в

узкой области информационной безопасности, но и в целом ряде смежных областей, касающихся как предметной области объекта информатизации, так и всех видов его обеспечения.

В качестве средства, позволяющего повысить качества (оперативность, достоверность, объективность и т.п.) обсуждаемой процедуры следует упомянуть классификацию факторов, воздействующих на информацию, изложенную в ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». В разделе 5 упомянутого документа приводится перечисление классификационных признаков и задается иерархия факторов. Так все перечисленные «воздействующие или могущие воздействовать на безопасность защищаемой информации и подлежащие учету при организации защиты информации» [цитата ГОСТ] факторы, «по признаку отношения к природе возникновения» могут быть отнесены к объективным или субъективным; по отношению к обсуждаемому объекту информатизации – внутренними или внешними.

Система классификации, определяемая п.п. 5.3, имеет иерархическую структуру и включает: подклассы, группы, подгруппы, виды и подвиды.

Например, п.п. 6.1.1.2.а.2 (выделен заливкой в листинге 1) указывает на необходимость анализа факторов, происходящих из внутренне присущей техническому средству возможности излучать акустические сигналы, связанные с речевой коммуникацией (например, данные оперативной командной связи, распространяемые по системе громкоговорителей).

Листинг 1. Фрагмент классифицирующего описания факторов, воздействующих на информацию, согласно ГОСТ Р 51275-2006.

```
6.1 Перечень объективных факторов, воздействующих на
безопасность защищаемой информации
    6.1.1 Внутренние факторы
       6.1.1.1 Передача сигналов:
          а) по проводным линиям связи;
          б) по оптико-волоконным линиям связи;
          в) в диапазоне радиоволн и в оптическом
             диапазоне длин волн.
       6.1.1.2 Излучения сигналов, функционально присущие
          техническим средствам ОИ:
           а) излучения акустических сигналов:
                1) сопутствующие работе технических
                 средств обработки и передачи информации;
                2) сопутствующие произносимой или
                воспроизводимой ТС речи;
             б) электромагнитные излучения и поля:
                1) излучения в радиодиапазоне;
                2) излучения в оптическом диапазоне.
```

Таким образом, эта и другие подобные модели упорядочивания системы знаний об элементах угроз, не просто имеющих место, но, самое главное, – актуальных для информационной системы, играют важную методологическую роль, связанную с фиксацией и распространением лучшего опыта, применение которого повышает вероятность формирования адекватных контрмер за счет уменьшения ошибок анализа риска.

Несколько забегая вперед, можно заметить, что методической основой программных средств поддержки процесса управления рисками является именно этот подход – максимальное использование зафиксированного опыта, полнота применения которого контролируется с помощь формальных алгоритмических средств.

Управление рисками информационной безопасности как сложная задача.

Очевидно, что каждая ИС в каждый конкретный момент времени характеризуются конкретными значениями P_i, D_i и n, а, значит и R_s. В соответствии с идеологией, иллюстрируемой рисунком 2, естественным желанием владельцев информационных активов является минимизация рисков, для чего предпринимаются определенные контрмеры в рамках системы управления информационной безопасностью (СУИБ). Однако эти контрмеры являются затратами, роль и место которых в бизнесе очевидны далеко не всем. В таком случае принято апеллировать к принципу разумной достаточности: *невозможно и нецелесообразно устранить все угрозы информационной безопасности ИС, следует свести их к приемлемому уровню* (рис. 5?!!).

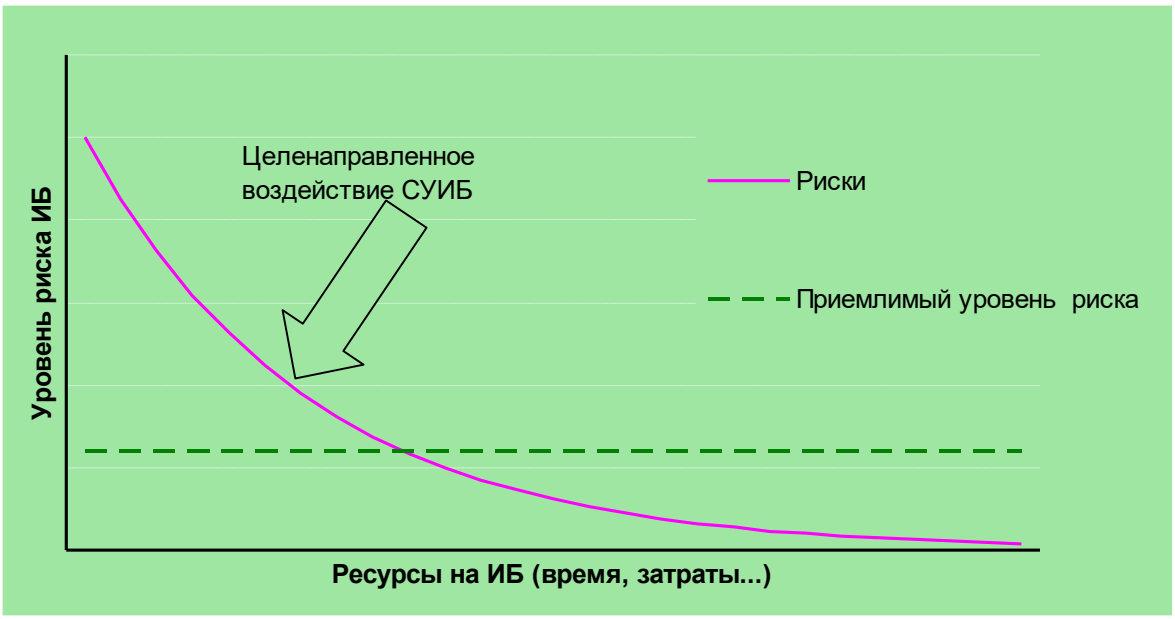


Рисунок 5. Роль СУИБ в управлении рисками

Касаясь вопроса определения уровня приемлемого риска, следует учесть зависимость (рис. 6), приводимую в монографии Герасименко В.А. и

Малюк А.А Основы защиты информации М.: Инкомбук, 1997. Как видно на графике, динамика зависимостей далеко не линейная: на начальном этапе отношение стоимостей защитных мероприятий и уменьшения ожидаемого ущерба много меньше единицы, что говорит о высокой эффективности капиталовложений, однако с приближением к точке оптимума эффективность снижается. После точки оптимума дополнительные капиталовложения уже превышают размер ожидаемого ущерба, а суммарные затраты снова возрастают, причем стопроцентная защищенность не достигается в принципе.

Рисунок 6 Идеализированный график соотношения
«затраты на защиту - ожидаемые потери»

На основании изложенных соображений определим общую постановку задачи управления рисками. В силу сложности взаимосвязи множества факторов и процессов задача управления рисками информационной безопасности относится к классу сложных задач. Далеко не всегда имеется возможность нахождения такой комбинации решений, методов и средств по управлению рисками, которые имеют наибольшую маргинальную стоимость – то есть, с наибольшей скоростью снижают уровень рисков. Причем эта сложность имеет как теоретическое, так и практическое происхождение.

С точки зрения теории задача управления рисками может быть отнесена к классу *динамических нелинейных целочисленных стохастических* задач. То есть, имеют место:

– *динамически* изменяющиеся цели, зависимости и ограничения в анизотропном пространстве событий;

– *нелинейные* функциональные зависимости между взаимосвязанными элементами;

– *целочисленные* значения элементов анализируемой системы, определяемые их физической сущностью;

– *стохастический* характер проистекающих процессов и низкая достоверность прогностических данных, не подкрепляемых апостериорно.

Более того, при дальнейшем изучении выражений (4.а), (4.б), и (5) следует помнить, что в общем случае формализованное описание цели производиться не *функцией* заданного вида, устанавливающей однозначное соответствие между набором входных параметров и результатом, а *функционалом*, сам вид которого может изменяться в зависимости от условий.

Варианты постановки задачи управления рисками информационной безопасности.

Таким образом, вышеизложенные требования и условия решения задачи управления рисками относят её к классу сложных задач. Как правило, сложные задачи в универсальной своей постановке не имеют практического применения либо из-за теоретических ограничений, либо из-за трудности реализации. Современные подходы к решению таких задач базируются на достижениях теории систем и системного анализа и состоят в сведении к типовым задачам, решаемость которых доказана в заданной системе ограничений. Рассмотрим интерпретацию задачи управления рисками информационной безопасности в виде задач оптимального управления – то есть формирования такого комплекса взаимосвязанных управленческих воздействий, которые обеспечат наилучшее в некотором смысле решение[1]

Как и любая оптимизационная задача[2], она имеет двойственную постановку, причем конкретный вид определяется априори заданными условиями и предпочтениями. Традиционно оптимизационные задачи описываются двумя взаимосвязанными компонентами:

– целевой функцией, нахождение заданного (в том числе неизвестного минимального или максимального) значения которой и дает искомое решение;

– и системой ограничений, которые задают область определения целевой функции (то есть, множество допустимых решений). Ограничения могут накладываться на каждый из аргументов целевой функции.

В условиях, когда организация имеет заранее выделенные «неотнимаемые» ресурсы для решения задачи управления рисками и стремится в рамках имеющихся ресурсов минимизировать риски, постановка задачи будет иметь вид:

найти такую управляющую последовательность (М) (или в терминологии п.п. 2.1 Таблицы 1 «скоординированные действия по руководству и управлению организацией в области риска») в результате выполнения которой общий риск

---

[1] Дополнительную информацию по этому вопросу следует получать в специализированных источниках. Например, классическом труде Вентцель Е.С. Введение в исследование операций – М.: Советское радио, 1964, а также в большом количестве открытых ресурсов.

2 В рамках курса используются ссылки на учебное пособие Акулич И.Л. Математическое программирование в примерах и задачах: Учеб. пособие. – 2-е изд. испр. и доп. – М.: Высшая школа, 1993.

Систематизированное изложение фундаментальных положений теоретической кибернетики можно получить в двухтомнике Кузин Л.Т. Основы кибернетики Том 1. Математические основы кибернетики, Том 2 Основы кибернетических моделей.

системы (R_{sM}) при использовании этого управления (M) примет минимально возможное значение, а суммарная стоимость защитных мер (C_{prM}), предусмотренных управлением M, не превысит заданного значения:

$$\begin{cases} R_{sM} \xrightarrow{M} \min \\ \sum C_{prM} \le const \end{cases}. \qquad (4.а)$$

В данном случае целевой функцией является функция получения значения риска, цель – её минимизации, а системой ограничений – совокупность требований по непревышению стоимости ресурсов.

В условиях, когда в организации задается заранее известный уровень риска, который не должен быть превышен, следует определить минимально достаточные ресурсы для решения этой задачи. Тогда имеет место следующая формулировка:

найти такую управляющую последовательность (M) в результате выполнения которой общий риск системы (R_{sM}) при использовании этого управления (M) не превысит заданного значения, а суммарная стоимость защитных мер (C_{prM}), предусмотренных управлением M, примет минимально возможное значение:

$$\begin{cases} R_{sM} \le const \\ \sum C_{prM} \xrightarrow{M} \min \end{cases}. \qquad (4.б)$$

Здесь целевой функцией является функция получения стоимости защитных мероприятий, цель – её минимизация, а ограничением является значение остаточного риска.

Если же на момент постановки задачи нет жесткого определения ни суммарной стоимости защитных ресурсов, ни уровня приемлемого риска, то постановка задачи должна обеспечивать нахождение глобального экстремума функции совокупных потерь, представленной на рисунке 6. Эта точка помечена как «оптимальный уровень», и представляет теоретический минимум. Обобщенная постановка задачи будет иметь вид:

$$\begin{cases} R_{sM} + C_{prM} \xrightarrow{M} \min \\ R_{sM} \le const_R \\ \sum C_{prM} \le const_c \end{cases}, \qquad (5)$$

где дополнительно введённые $const_C$ и $const_R$ обозначают максимально допустимые ограничения на риск и затраты по управлению им.

Более того, задачи в данных формулировках существуют не изолировано и должны интерпретироваться с учетом основной цели предприятия, обозначенной в выражении (1). Обеспечение информационной безопасности деятельности предприятия является таким же производственным процессом, как и производство товаров и услуг в рамках основной миссии. Однако до настоящего времени существуют воззрения на эту область деятельности как на исключительно «убыточный цех». Это связано, прежде всего, с тем, что определение роли и степени влияния уровня информационной безопасности на достижение главных целей предприятия является еще одной из нетривиальных задач, подходы к решению которой будут обсуждаться ниже. Кроме того, имеется психологический аспект: не произошедшие инциденты не замечаются, а расходы на безопасность видны каждому руководителю.

Место задачи управления рисками в цикле Деминга по управлению информационной безопасностью.

Определив в общем виде задачу управления рисками, приведем тезисный обзор моделей, описывающих её решение.

До недавнего времени одним из самых известных подходов к моделированию управленческих процессов являлся, так называемый, «Цикл Деминга» или «Цикл Деминга-Шухарта». Он получил известность после успешного применения при модернизации послевоенной Японии в 50-х годах XX в.

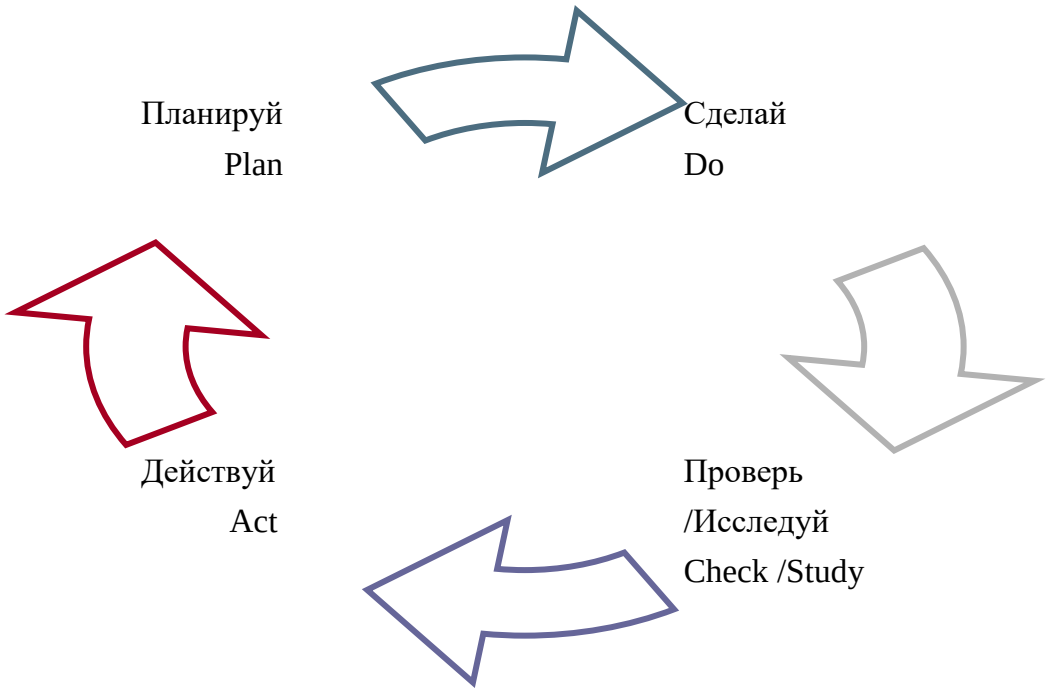


Рисунок 6.а Цикл Деминга

Основное содержание и последовательность действий при реализации управленческого решения, изображенных на рисунке 6.а дополнительных комментариев не требуют[1].

Для наших же целей следует знать, что имеются ещё два названия этой модели управления:

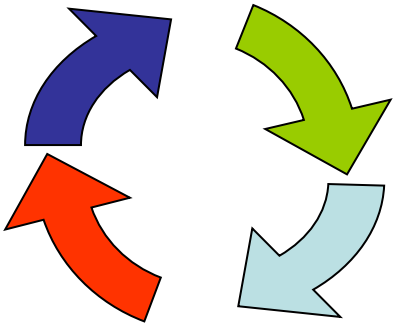
– PDCA: Plan (Планируй) –Do(Сделай) –*Check (Проверь)* –Act (Действуй);

– PDSA: Plan (Планируй) –Do(Сделай) – *Study (Исследуй)* –Act (Действуй).

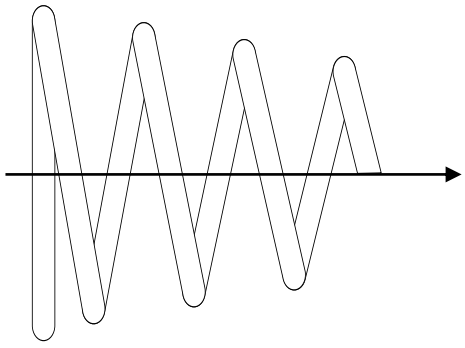
Как видно, они отличаются третьими компонентами выделенными курсивом. Содержательное же отличие этих двух циклов управленческой деятельности состоит в том, что в первом случае (модель PDCA) этап *Check* – проверка – производиться по заранее заданным показателям и критериям, что возможно только при достаточно высокой стабильности процессов.

В модели же PDSA этап проверки заменяется этапом исследования. Предметом исследования является оценка степени или динамики достижения цели выполняемого цикла. Необходимость процесса исследования определяется тем, что в изменяющихся условиях деятельности заранее заданные показатели и критерии могут уже не соответствовать условиям обстановки, а, значит, и не характеризовать степень её достижения. Более того, сам способ проверки может быть изменен. В любом случае результаты этого этапа должны обеспечить подготовку следующего этапа – действия.

Мнемоническим образом модели PDCA может стать цикл на плоскости (рис. 6.б.1), тогда как модель PDSA приобретает, как минимум, ещё одно измерение (время, условия и т.п.) и может быть представлена спиралью (рис. 6.б.2).



1) «Плоский» цикл PDCA



2) Трехмерная спираль PDSA

Рисунок 6.б Мнемосхема ,отображающая различия моделей PDCA и PDSA

В контексте задачи управления рисками информационной безопасности цикл Деминга может использоваться на двух уровнях:

Во-первых, с точки зрения управления (менеджмента) информационной безопасностью в целом. И тогда задача управления рисками «размазывается» по этапам. Вот как интерпретируется процессный подход к организации

[1] Желающим получить дополнительную информацию по этому вопросу можно рекомендовать открытый ресурс http://deming.ru/TeorUpr/PDSA.htm, содержащий материал книги Г. Нива «Пространство доктора Деминга» в переводе Ю.Т. Рубаника

системы менеджмента информационная безопасность в ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (рис.7). Причем в п.п. 4.1 этого стандарта имеется прямое указание на использование модели PDCA.

Второй уровень относиться к собственно задаче управления рисками. В этом случае каждый из этапов цикла Деминга по управлению рисками может быть представлен собственным циклом меньшего масштаба, что соответствует традиционному подходу декомпозиции сложной задачи.

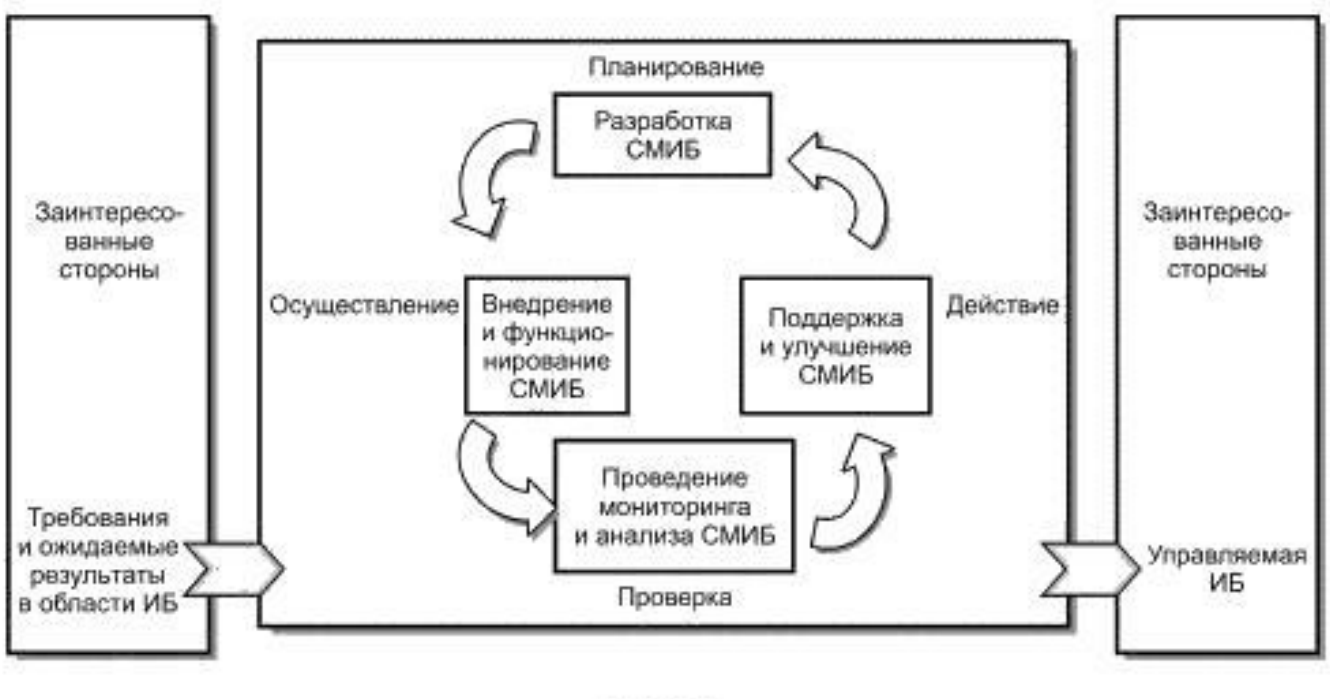


Рисунок 7. Организация менеджмента ИБ по модели PDCA
согласно требованиям ГОСТ Р ИСО/МЭК 27001-2006

В завершении обсуждения модели управления следует определить содержание каждого из этапов цикла Деминга. Для этого воспользуемся иллюстрацией (рис. 8), детализирующей изложения государственного стандарта.

Рисунок 8 Модель системы управления рисками
(Свиткин М. Формирование системы менеджмента риска компании // «Методы менеджмента качества», № 2 за 2010)

Значение терминов, используемых на схеме, раскрываются в упомянутом ранее стандарте (табл. 1).

Таблица 3. Определения понятий по ГОСТ Р ИСО/МЭК 27001—2006

Термин и его определение	Пер. на англ.
3.7 **система менеджмента информационной безопасности; СМИБ**: Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности. Примечание — Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.	information security management system; ISMS
3.8 **целостность**: Свойство сохранять правильность и полноту активов.	integrity
3.9 **остаточный риск**: Риск, остающийся после его обработки.	residual risk
3.10 **принятие риска**: Решение по принятию риска.	(risk acceptance

3.11 **анализ риска**: Систематическое использование информации для определения источников риска и количественной оценки риска.	risk analysis
3.12 **оценка риска**: Общий процесс анализа риска и его оценивания	risk assessment
3.13 **оценивание риска**: Процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости	risk evaluation
3.14 **менеджмент риска**: Скоординированные действия по руководству и управлению организацией в отношении риска. Примечание — Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникацию риска.	risk management
3.15 **обработка риска**: Процесс выбора и осуществления мер по модификации риска. Примечания: 1 Меры по обработке риска могут включать в себя избежание, оптимизацию, перенос или сохранение риска. 2 В настоящем стандарте термин «мера управления» (control) использован как синоним термина «мера» (measure).	risk treatment
3.16 **положение о применимости**: Документированное предписание, определяющее цели и меры управления, соответствующие и применимые к системе менеджмента информационной безопасности организации. Примечание — Цели и меры управления основываются на результатах и выводах процессов оценки и обработки рисков, на требованиях законодательных или нормативных актов, на обязательствах по контракту и бизнес -требованиях организации по отношению к информационной безопасности.	statement of applicability

В качестве примера точки зрения на структуру и задачи системы управления рисками информационной безопасности можно привести положения федерального закона N 161-ФЗ «О национальной платежной системе» от 27.06.2011 г.

Так п.п. 5.3 статьи 15 «Оператор платежной системы и требования к его деятельности» содержит однозначное указание на то, что «Оператор платежной

системы обязан … организовывать систему управления рисками в платежной системе в соответствии со статьей 28 настоящего Федерального закона, осуществлять оценку и управление рисками в платежной системе».

Подпункт 1.13 статьи 20 гласит, что: «Правилами платежной системы должны определяться: …система управления рисками в платежной системе, включая используемую модель управления рисками, перечень мероприятий и способов управления рисками».

А упомянутую выше статью 28, целиком посвященную вопросу системы управления рисками, считаем целесообразным привести в полном объеме.

Статья 28. Система управления рисками в платежной системе

1. В целях настоящего Федерального закона под системой управления рисками в платежной системе понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для бесперебойности функционирования платежной системы с учетом размера причиняемого ущерба.

2. Оператор платежной системы обязан определить одну из следующих используемых в платежной системе организационных моделей управления рисками в платежной системе:

1) самостоятельное управление рисками в платежной системе оператором платежной системы;

2) распределение функций по оценке и управлению рисками между оператором платежной системы, операторами услуг платежной инфраструктуры и участниками платежной системы;

3) передача функций по оценке и управлению рисками оператором платежной системы, не являющимся кредитной организацией, расчетному центру.

3. Система управления рисками должна предусматривать следующие мероприятия:

1) определение организационной структуры управления рисками, обеспечивающей контроль за выполнением участниками платежной системы требований к управлению рисками, установленных правилами платежной системы;

2) определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;

3) доведение до органов управления оператора платежной системы соответствующей информации о рисках;

4) определение показателей бесперебойности функционирования платежной системы в соответствии с требованиями нормативных актов Банка России;

5) определение порядка обеспечения бесперебойности функционирования платежной системы в соответствии с требованиями нормативных актов Банка России;

6) определение методик анализа рисков в платежной системе, включая профили рисков, в соответствии с требованиями нормативных актов Банка России;

7) определение порядка обмена информацией, необходимой для управления рисками;

8) определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;

9) определение порядка изменения операционных и технологических средств и процедур;

10) определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;

) определение порядка обеспечения защиты информации в платежной системе.

4. Способы управления рисками в платежной системе определяются оператором платежной системы с учетом особенностей организации платежной системы, модели управления рисками, процедур платежного клиринга и расчета, количества переводов денежных средств и их сумм, времени окончательного расчета.

5. Система управления рисками может предусматривать следующие способы управления рисками:

1) установление предельных размеров (лимитов) обязательств участников платежной системы с учетом уровня риска;

2) создание гарантийного фонда платежной системы;

3) управление очередностью исполнения распоряжений участников платежной системы;

4) осуществление расчета в платежной системе до конца рабочего дня;

5) осуществление расчета в пределах предоставленных участниками платежной системы денежных средств;

6) обеспечение возможности предоставления кредита;

7) использование безотзывных банковской гарантии или аккредитива;

8) другие способы управления рисками, предусмотренные правилами платежной системы.

6. Правилами платежной системы может быть предусмотрено создание оператором платежной системы коллегиального органа по управлению рисками в платежной системе, в состав которого включаются ответственные за управление

рисками представители оператора платежной системы, операторов услуг платежной инфраструктуры, участников платежной системы. В состав органа по управлению рисками по согласованию с Банком России могут быть включены представители Банка России с правом совещательного голоса.
7. В функциональные обязанности и компетенцию органа управления рисками входят:
1) установление критериев оценки системы управления рисками, включая системный риск, и проведение указанной оценки;
2) формирование предложений и рекомендаций по итогам проведения оценки системы управления рисками.
8. Система управления рисками значимой платежной системы должна предусматривать создание органа управления рисками значимой платежной системы, указанного в части 6 настоящей статьи, и использование не менее двух способов управления рисками, указанных в пунктах 1 - 7 части 5 настоящей статьи.

Как видно, законодательный акт содержит явные указания на организационные и технологические аспекты реализации системы управления рисками. Это относится и к моделям управления рисками (п.п. 2), и к мероприятиям (п.п. 3), и к конкретным способам управления рисками (п.п. 5).

Модели динамики стоимости информации.

С лингвистической точки зрения ключевым понятием термина «управление рисками информационной безопасности» является глагол. А это значит, что его имманентным признаком является время – одно из пространств в которых развивается процесс. Соответственно, для осознанного влияния на этот процесс следует иметь представление о временны’х характеристиках затрагиваемых элементов.

В зависимости от физической сущности процессов информационного взаимодействия можно выделить несколько типовых моделей изменения стоимости информации во времени. Дадим им обоснование и графическую интерпретацию (рис. 9):

1. Ступенчатая – характеризуется относительно высоким уровнем стоимости до определенного момента времени (t_x), после которого происходит резкий спад и уход в область информационного шума. Указанная зависимость может быть формально описана выражением:

$$\begin{cases} C_t \cong C_0, \text{ при } t \le t_x \\ C_t \cong C_{ост}, \text{ при } t > t_x \end{cases}, \quad (6)$$

где C_t – стоимость информации на момент времени t;

C_0 – стоимость информации в начальный момент времени;

$C_{ост}$ – остаточная стоимость информации;

t – параметр времени.

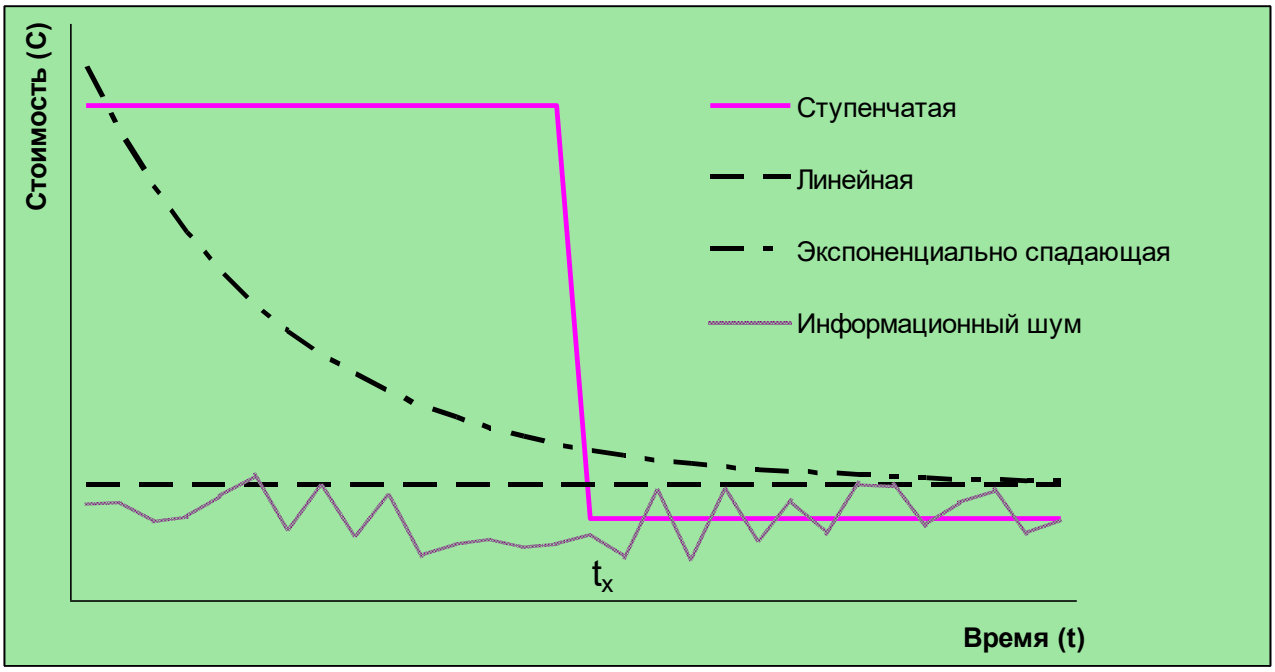


Рисунок 8 Графическая интерпретация моделей стоимости информации

Примером такого поведения стоимости информации является тендерная (конкурсная) процедура при получении контрактов или особые виды аукционов. Действительно, практический интерес для участника торгов представляет информация об условиях контракта конкурентов только до момента прекращения приема документов или вскрытия заявок). То есть до того момента, когда ещё можно изменить параметры собственные предложений. По окончании приема (вскрытия) заявок информация, как правило, становиться публичной и представляет ценность, разве что для анализа результатов обсуждаемой процедуры. В любом случае – она не ограничивается в распространении.

2. Экспоненциально спадающая – изменяется по закону

$$C_t = C_0 * e^{-k*t} + C_{const}, \quad (7)$$

где дополнительно введены:

k – коэффициент, характеризующий скорость падения стоимости информации;

C_{const} – константа определяющая ценность информации после интенсивного спада (пьедестал стоимости).

Высокая начальная стоимость информации характеризует степень её социальной значимости. А при высокой значимости будут предприниматься попытки овладения ею: как путем получения доступа через владельца, так и путем повторной её генерации (проведения собственных исследований, экспериментов, привлечения экспертов и т.п.)

По такому закону изменяется, например, стоимость новостных сообщений, которые очень быстро из высокоценных превращаются в объекты, создающие информационный шум.

2. Линейная – стоимость информации изменяется по линейному закону:

$$C_t = -k * t * C_0 + C_{const}, \tag{8}$$

На графике приведен случай, когда k=0, то есть на длительном интервале времени практически не изменяется ($C_t \approx C_0 \approx C_{const}$). Такая модель характеризует информацию «длительного использования», например, правила внутреннего распорядка стандартного учреждения или основные законы естественных наук. Относительно невысокая их стоимость определяется невысоким интересом, тогда как в противном случае, будут предприняты попытки получить доступ к ней, и события будут развиваться по моделям 1 или 2.

При анализе реальной ситуации следует понимать, что рассмотренные идеальные модели могут не в полной мере отражать суть происходящих процессов. Тогда имеет смысл использовать интервальное описание стоимости информации, предлагающее для каждого временного отрезка свою модель изменения стоимости (рис. 9). Например:

$$\begin{cases} C_t = C_0, \text{ при } t \le t_1 \\ C_t = C_0 * e^{-k*t} + C, \text{ при } t_1 < t \le t_2, \\ C_t = C_{ост}, \text{ при } t > t_3 \end{cases} \tag{9}$$

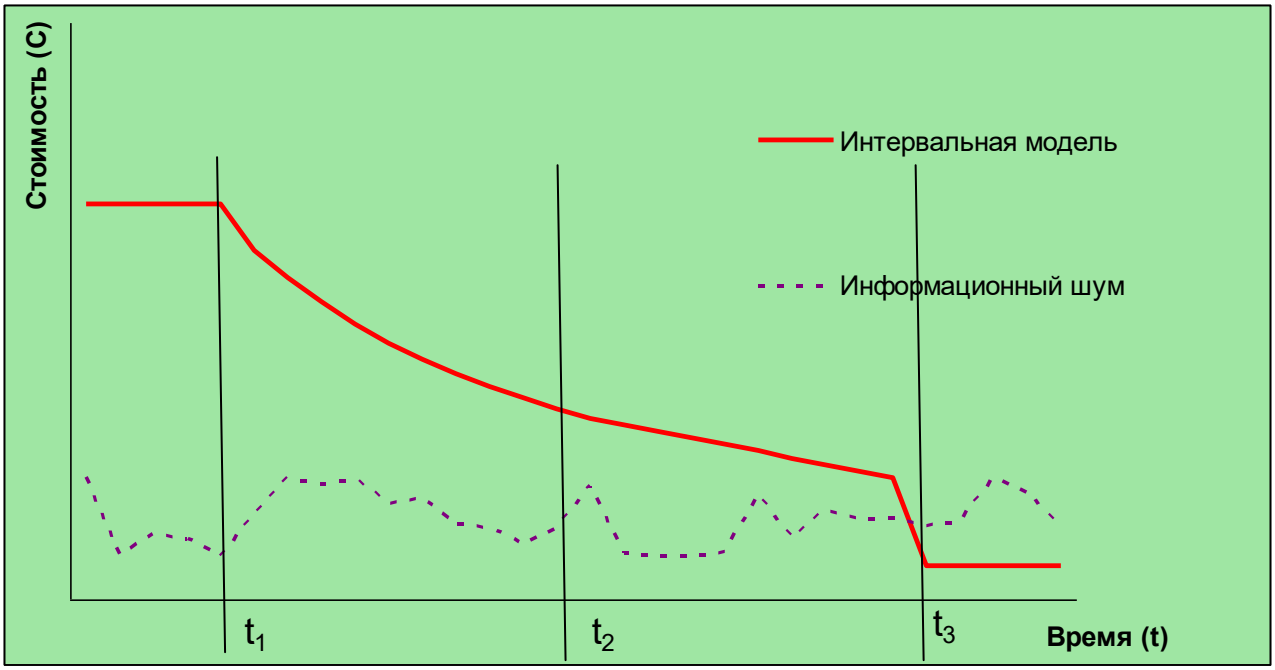


Рисунок 9. Графическая интерпретация
интервальной модели стоимости информации

Подходы к определению ценности (стоимости) информации.

Получение оценки стоимости информации на практике может быть реализовано с использование нескольких подходов.

Наиболее простой – *оценка стоимости фактических затрат*, которые были произведены для получения оцениваемой информации. Естественно, эти затраты могут иметь различную природу: от конкретного значения суммы выплаты автору патента или now-how за право его использования до оценки суммарной стоимости владения научно-исследовательской лаборатории, результатом интеллектуальной деятельности которой стал способ производства, защищенный упомянутым патентом.

Недостатком этого способа является то, что оценивается стоимость получения оцениваемой информации, но не оценивается степень её влияния на производственный процесс и на рынок в целом.

Касательно последнего пункта следует вспомнить «функциональное» определение коммерческой тайны согласно пункту 2 статьи 3 Федерального закона РФ от 29 июля 2004 г. N 98-ФЗ О коммерческой тайне (в действующей редакции).

```
Статья 3. Основные понятия, используемые в настоящем
Федеральном законе
…
2) информация, составляющая коммерческую тайну (секрет
производства), - сведения любого характера
(производственные, технические, экономические,
```

организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

Ведь именно «неизвестность третьим лицам» представляет конкурентное преимущество.

Оценка степени влияния на производственный процесс так же не может производиться этим способом.

Иллюстративный пример: «Сколько может стоить утерянный пароль администратора «подвисшего» сервера в разгар подготовки годовой отчетности?». Затраты на его формирование – практически нулевые, затраты на сохранение – незначительны, а ущерб от нарушения работоспособности процедур, как минимум равен себестоимости труда организации, во время которой имел место вынужденный простой.

Перейдем от оценки стоимости к оценке ценности информации (и предложим любознательному читателю самостоятельно уяснить различия этих оценок.)

Оценка ценности информации по Стратоновичу[1] возможна в следующих условиях. Пусть:

1) есть четкая формулировка цели, которую следует достигнуть;
2) возможна объективная оценка достижения цели;
3) имеется возможность получения оценки **затрат** на достижение цели;
4) цель может быть достигнута различными способами, в отношении которых верны утверждения 1-3.

Понимая информацию, как средство способствующее достижению цели, можно выделить способы и использованием и без использования оцениваемой информации.

Тогда ценность информации определяется *как разность между затратами на достижение цели без использования этой информации* ($C_{без\,\inf}$) *и с её использованием* ($C_{с\,\inf}$):

$$C_{\inf} = C_{без\,\inf} - C_{с\,\inf}. \qquad (10.а)$$

[1] Стратонович Р.Л. О ценности информации // Изв. АН СССР. Техническая кибернетика. 1965. N 5. С.3□12.

Иногда при определении ценности информации учитывают затраты на её синтез и обслуживание ($C_{\text{обсл}}$):

$$C_{\text{inf}} = C_{без\ \text{inf}} - (C_{с\,\text{inf}} + C_{\text{обсл}}), \qquad (10.б)$$

Еще одна трактовка этого подхода принадлежит Е.С. Вентцель[1]: когда эффективность каких-либо мероприятий можно оценить численно, приращение эффективности (т.е. разность между эффективностью проведения мероприятий до и после получения информации об условиях, в которых они будут проходить) характеризует важность и ценность полученного сообщения.

Вероятностная оценка ценности информации возможна в следующих условиях. Пусть:

1) есть четкая формулировка цели, которую следует достигнуть;
2) возможна объективная оценка достижения цели;
3) имеется возможность получения оценки **вероятности** достижение цели;
4) цель может быть достигнута различными способами, в отношении которых верны утверждения 1-3.

Вероятностный способ определения меры ценности информации для достижения цели, предложенный М.М. Бонгартом (см там же), применим только в условиях, когда известны вероятности достижения цели с использованием ($P_{\text{с inf}}$) и без использования оцениваемой информации ($P_{\text{без inf}}$):

$$C_{\text{inf}} = \log_2 \frac{P_{\text{с inf}}}{\text{P}_{\text{без inf}}}, \qquad (11)$$

Для устранение ряда недостатков вероятностного подхода В.И. Корогодиным введена другая интерпретация данных вероятностных оценок достижения цели для определения ценности информации:

$$C_{\text{inf}} = \frac{P_{\text{с inf}} - \text{P}_{\text{без inf}}}{1 - \text{P}_{\text{без inf}}} \qquad (12)$$

Экспертный метод оценки стоимости информации – базируется на системе оценок, получаемых по результатам обработки субъективных заключений. Подходы к реализации экспертных процедур обсуждаются во втором разделе пособия.

Дополнительную информацию особенностях применения перечисленных подходов в органах государственной власти можно найти в статье А.Д. Данилова «Ценность информации и технологии «электронного

[1] Академический толковый словарь. открытый доступ :http://dic.academic.ru/dic.nsf/enc_philosophy/ /7453/ТЕОРИЯ

правительства» в трудах VIII Всероссийской объединенной конференции «Технологии информационного общества — Интернет и современное общество» (IST/IMS-2005).

За рамками рассмотрения курса остается вопрос метрологического обеспечения задач управления рисками информационной безопасности. На самом деле вопрос измерений в области менеджмента информационной безопасности и определения степени доверия к их результатам заслуживает особого обсуждения.

Рассмотрению этого вопроса с позиции лучших практик посвящен ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.

Примером встраивания процесса измерений в общий цикл PDCA, предусмотренный ГОСТ Р ИСО/МЭК 27001-2006 (см. выше) является утверждение этой же модели в обсуждаемом стандарте (рис. 10).

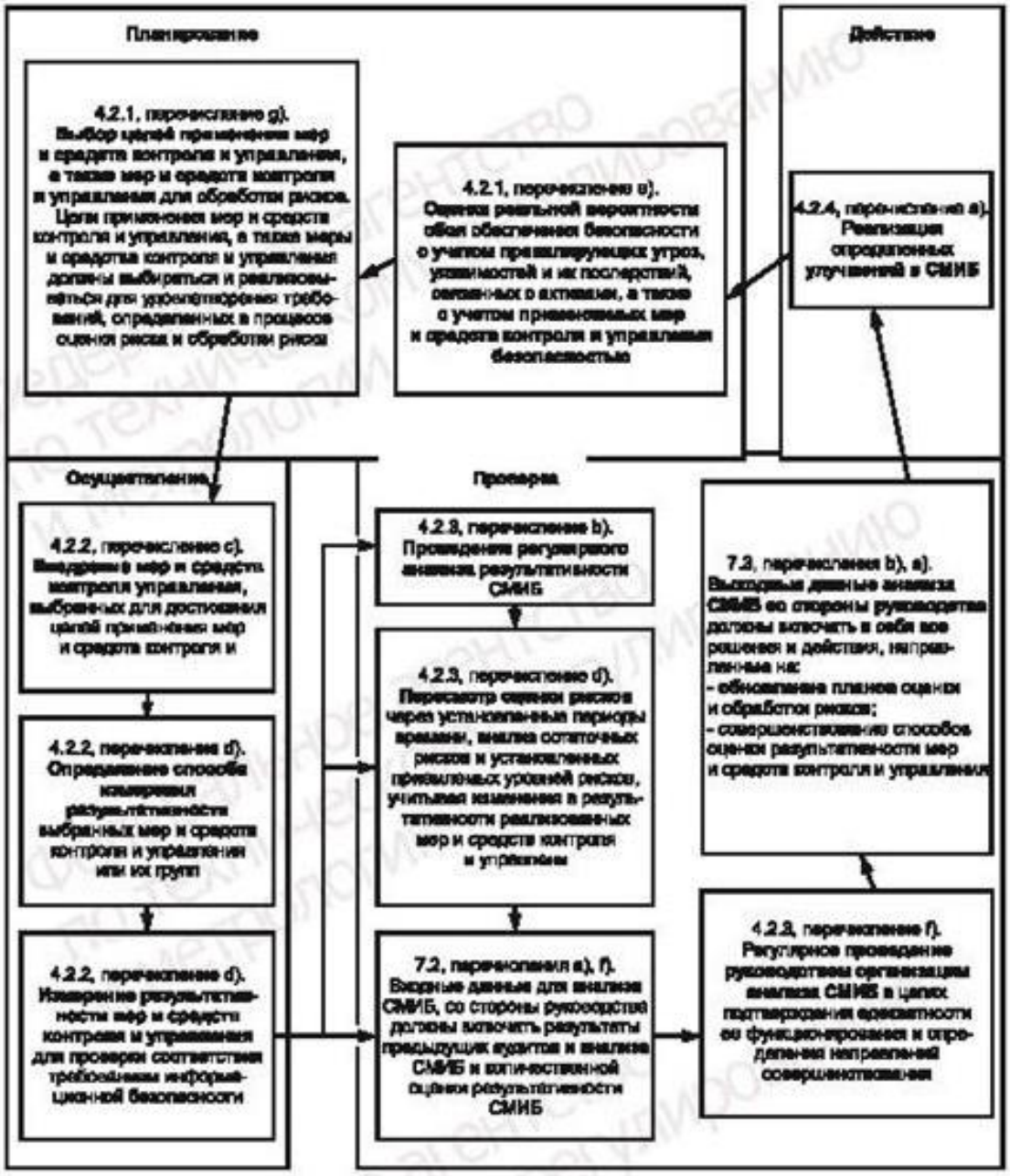


Рисунок 10. Взаимосвязь деятельности, связанной с измерениями в цикле PDCA (?!! изменить рисунок)

Раздел 2. Методологии оценки рисков ИБ.

Понятие и классификация методологий оценки рисков ИБ, их сравнительная характеристика. Критерии выбора методологии оценки рисков ИБ

Как было показано в первом разделе, нахождение оптимального (рационального) решения задачи управления рисками информационной безопасности в любой из постановок (4.а), (4.б), (5) относится к классу сложных задач, как с научно-методической, так и практической точек зрения. Попытки объединения теоретических достижений и лучших практик реализуются в виде стандартов.

Современный этап стандартизации характеризуется высокой активность всех заинтересованных сторон – от инициативных членов сообщества профессионалов до государственных структур, которые в силу своего предназначения обязаны заниматься регулированием обсуждаемой темы. На практике это приводит к регулярным обновлениям и изменениям нормативно-правовой базы.

Российская действительность не является исключением: анализ прилагаемого (Прил. 1) списка нормативно-правовых источников позволяет сделать заключение о высокой динамике обновления документов, часть из которых является переводами международных стандартов.

Вместе с тем, в области безопасности информационных технологий имеется ряд особенностей, которые следует учитывать при использовании этих документов:

– терминологическая неоднозначность (см. прил. 2 Глоссарий терминов в области информационной безопасности), вызванный:

а) различием толкований в официальных переводах и практикой употребления терминов в профессиональном сообществе, характеризующейся калькированием и интерпретацией на более ранних этапах;

б) различием толкований в различных версиях одного и того же документа: сравните, например, определения понятий, связанных с риском информационной безопасности в ГОСТ Р 51897-2002 (Менеджмент риска. Термины и определения) и в версии этого же документа от 2011 года;

в) влиянием на терминологию необходимости согласовывать их значение со множеством значений во взаимосвязанных документах из смежных областей;

– необходимость выполнения обязательных требований руководящих органов в критически важной сфере обеспечения информационной безопасности;

– необходимостью прозрачного взаимодействия с поставщиками программных и аппаратных средств (вызванной импортной зависимостью российского информационно-телекоммуникационного сектора), а также с интеграторами и партнерами в области высокотехнологичных информационных технологий (инициированного перерастанием границ

киберпространства за территориальные пределы и ведением межнациональных проектов);

– существующие информационные системы и технологии, а, значит и средства управления рисками создавались предыдущие годы и, естественно, с использованием норм, практик и теорий прошлых этапов; не все системы управления рисками информационной безопасности могут быть безболезненно модернизированы (впрочем, не всегда это и требуется);

– однозначно декларируемого приоритета российских национальных стандартов в случае противоречия с международными.

Как видно, многие из этих факторов стимулируют противоречивые тенденции в деятельности специалиста в области информационной безопасности и управления рисками в частности. Выход из сложившегося многообразия противоречивых тенденций, норм и правил может быть сформирован на основе понимания общеметодологических концепций данного вопроса.

Систему взглядов на изучаемый вопрос можно представить следующей мнемосхемой (Таблица 11):

Таблица 4. Иерархия и области применения и документированных практик.

Когда применяются	**Направления деятельности** ***(примеры)***		
	методологические	**организационные**	**технические**
Применять, если: –соответствуют задаче; –требует иностранный партнер; – если нет ограничений в РФ.	международные и иностранные стандарты, *в том числе на этапе обсуждения (RFC)*		
	COBIT, ERM COSO	ISO/IEC 17799 BS 7799-3:2006	ISO15408 (CC)
Преимущественно применять, если: – требует госзаказчик, ведомство (партнер); – если нет ограничений регулирующих органов.	отечественные стандарты, *в том числе ведомственные*		
	ГОСТ Р 50922 СТО БР ИББС-1.0-2010	ГОСТ Р ИСО/МЭК 17799	ОСТ Р ИСО / МЭК 15408 (ОК) ГОСТ Р 51275
Применять обязательно согласно требованиям к виду деятельности. В добровольном порядке, если соответствует задаче.	Обязательные к применению нормы и правила (законы, приказы, инструкции, методические рекомендации)		
	Закон РФ от 21.07.1993 N 5485-1 "О государственной тайне"	Инструкция о порядке допуска должностных лиц и гр. РФ к ГТ (Пост. Пр. РФ от 6.01.10 г. N 63)	РД. СВТ. Защита от НСД

В общем случае

?!! http://binni45.lghost.ru/index.files/page0008.htm

В результате рассмотрения и обобщения действующих, предлагаемых и возможных схем оценки риска ИБ АС, ИТ и организаций можно выделить несколько типовых подходов по решению задач по затрагиваемой проблеме.

1 Первый подход направлен на оценку рисков от реализации предполагаемых угроз с учетом наносимого при этом ущерба. В процессе оценки рисков должны быть рассмотрены все возможные угрозы, вероятности возникновения угроз $P_у$ и последствия реализации угроз в виде определенного ущерба $У_щ$ применительно к конкретной организации или эксплуатируемой ею АС или ИТ. В результате такого рассмотрения для определенного количества угроз, наносящих основной ущерб, (актуальных угроз) принимается решение о необходимости введения барьеров с технической или организационной основой их реализации. При этом остаются угрозы, относительно которых не принято решение о применении защитных мер, и вследствие этого возможен некий ущерб в случае их реализации, что определяет риск. Например, в стандарте ГОСТ Р ИСО/МЭК 15408 данный тип риска определяется как "остаточный риск". Основные этапы первого подхода по оценке риска представлены на рисунке 1.

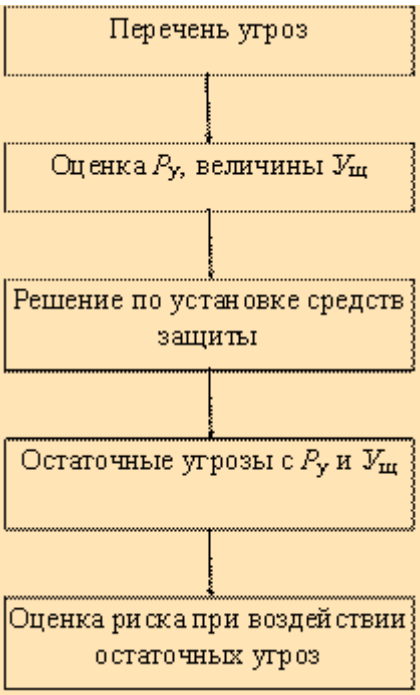


Рисунок 1 - Первый подход оценки рисков

2 Второй подход направлен на оценку влияния отклонений в конкретных организациях, АС или ИТ от установленного образца, требования к которому закреплены в нормативных документах. При этом предполагается, что при разработке или выборе нормативного документа были рассмотрены все или основные угрозы и их последствия с учетом выработанных политик безопасности в сообществе. Основные этапы второго подхода по оценке риска представлены на рисунке 2.

Таким образом, риск при рассмотрении данного подхода есть оценка степени отклонения от принятых требований ИБ с учетом их важности и влияния на бизнес-деятельность организации.

Типовым примером применения данного подхода можно считать применение в качестве нормативного документа международного стандарта ISO/IEC 17799 и измерение отклонений от требований данного стандарта на основе, например использования вопросных модулей продукта "COBRA" для оценки рисков.

Безусловно, данный подход менее трудоемок при его использовании по сравнению с рассмотренным первым подходом, но его применение возможно только в случае разработки такого нормативного документа или принятия какого-либо из известных документов действительно обеспечивающего формирование всех требований, позволяющих при их реализации защититься от всех или основных известных угроз. В связи с использованием оценок на более высоком уровне точность оценки риска будет более низкой, чем при использовании первого подхода.

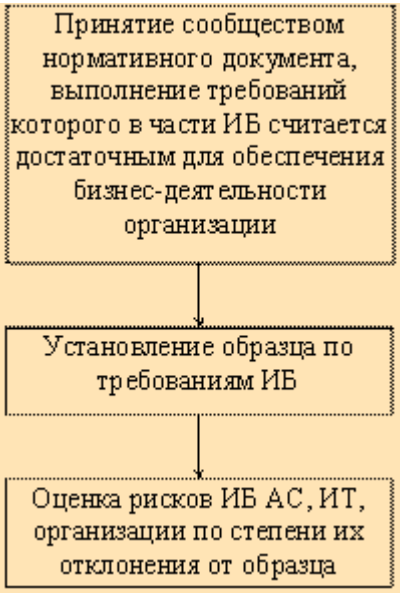
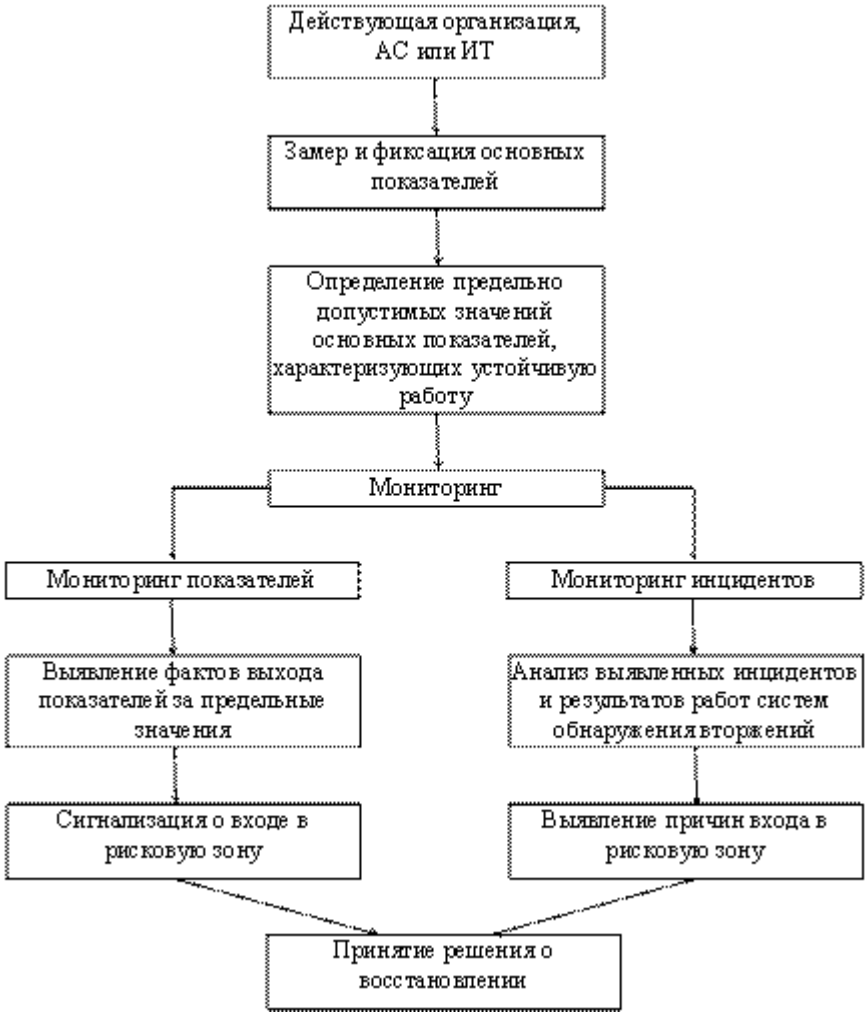


Рисунок 2 - Второй подход оценки рисков

Итак, **третий подход** ориентирован на оценку рисков ИБ АС, ИТ или организации в условиях реального функционирования в динамически изменяемой среде. Так как оценка выполнимости заложенных при разработке требований ИБ становится недостаточной, то возможный подход может быть направлен на оценку реального состояния организации, АС или ИТ по их функционированию в некоторой устойчивой зоне.

Указанный подход базируется на непрерывном мониторинге АС, определении состояния ее параметров и обнаруженных инцидентов ИБ, определении уровня стабильности АС. При выходе параметров функционирования системы за установленные нормы должен формироваться сигнал о переходе АС в состояние повышенного риска (или аномальное состояние), а на основании анализа инцидентов - определение возможных причин, породивших вход АС в эту рисковую зону. Такой подход в технической литературе называется "обнаружение аномалий" - в противовес "обнаружению вторжений". При обнаружении аномалий выявляются и обрабатываются неизвестные событии и таким образом накапливаются знания о динамических изменениях в системе и ее среде. При обнаружении вторжений, как правило, используются имеющиеся знания относительно сценариев возможных вторжений (атак). Оба указанных подхода могут органично дополнять друг друга.



Четвертый Метод базируется на принципах, заключающихся в том, что на этапе разработки известны все источники опасностей и их основные характеристики. Например, для оценки защищенности системы от опасных программно-технических воздействий для угроз, порожденных случайными и преднамеренными источниками, определяется частота их воздействия и среднее время воздействия. Считается, что при работоспособности всех заложенных средств зашиты, систему можно считать полностью защищенной, а незащищенность порождается только некачественной работой средств защиты.

Данный подход по оценке рисков по своему сценарию близок как к первому, так и второму подходу. К первому подходу его приближает процесс оценки, начиная с перечня угроз, а ко второму - наличие требований по РД, которые можно считать образцом. Основным отличием подхода является ориентация на существующую статистику появления угроз. Метод более ориентирован не на поиск оптимальных путей обеспечения информационной безопасности, а на оценку выполнения существующих общих требований по защите, определенных действующими документами, и расчете значений риска в виде вероятности нахождения системы в безопасном состоянии, которая определяется в пределах $0,95 \le P_p \le 0,99$ и в полной мере ориентирован на оценку надежности работы с учетом факторов, связанных с ИБ.

Данный подход применим в условиях возможностей определения всего перечня угроз, точных значений по вероятностям их появления и интервалу воздействия, а так же уверенности в том, что защита от выбранного перечня угроз гарантирует требуемый уровень информационной безопасности.

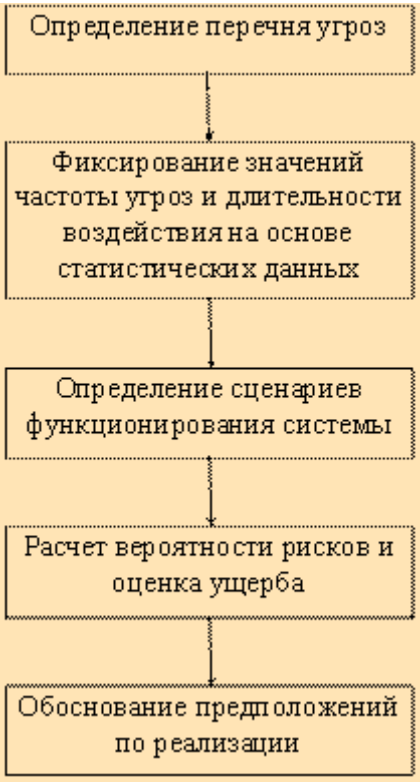


Рисунок 4 – Четвертый подход оценки рисков

© Olivier1961 http://commons.wikimedia.org/w/index.php?title=File:COSO-02.svg&page=1&uselang=ru

Обычно Концептуальные основы управления рисками организаций представляются в виде «Магического куба ERM COSO», показывающего взаимосвязь Целей (верхняя грань куба), Компонентов (горизонтальные ряды) и Подразделений организации (вертикальные ряды)ERM COSO (Enterprise Risk Management — Integrated Framework Committee of Sponsoring Organizations of the Treadway Commission)

Перечень продуктов, методов и способов оценки рисков

Наименование	Статус	Техническая основа оценки	Результат оценки
URSIT (метод)	Принят для оценки рисков ИТ финансовых организаций и провайдеров ИТ-услуг для надзорных органов США	Принят ФРС США и учитывает специфику банковского дела при оценка ИТ финансовых организаций и провайдеров ИТ-услуг для банковской сферы	Выявление организаций и провайдеров услуг с высоким риском с целью усиления к ним мер надзорного характера
OCTAVE (метод)	Рекомендации, разработанные Институтом Разработки Программного обеспечения Carnegie для широкого применения	Самоуправляемая сводной группой анализа оценка рисков ИБ организаций	Выявление организацией рисков ИБ в виде рисков конфиденциальности, целостности и доступности активов ИТ
ISO TR 13569 (пример подхода)	Технический отчет, принятый техническим комитетом ИСО 68 "Банковские и связанные с ними финансовые услуги"	В первичной основе рекомендован для применения в банковской сфере. Содержит пример применения для банковского сообщества одного из методов оценки рисков, определенных в 3-части ISO/IEC 13335	Детализированная оценка рисков: - денежной потери; - потерь производительности; - системных затруднений, - при использовании АС и ИТ в банковской сфере
COBIT (пример подхода)	Принят Фондом Аудита и Контроля Информационных систем	Определены 34 процесса и соответственно целей контроля ИТ организации не привязанные к области деятельности организации. Один из процессов планирования и организации 9 определяет обобщенный процесс оценки рисков.	Содержит общие рекомендации по оценке рисков на этапе планирования применения в организации систем ИТ
MARION(метод)	Разработан Банковской комиссией Франции, рекомендательно принят для оценки состояния информационных систем кредитный организаций	Документ принят в качестве основы для оценки рисков ИБ для ИС кредитных организаций Франции по 25 областям по 4-х бальной шкале для каждой области	Выявление наиболее проблемных областей для возможной последующей проработки этих направлений.
CRAMM (программный продукт)	Метод анализа и контроля рисков, принят Центральным Агентством по Компьютерам и Телекоммуникациям (ССТА) Великобритании в поддержку стандарта BS7799	Как метод принят в Великобритании для оценки рисков в различных отраслях деятельности	Оценка рисков ИБ организации при обработке критической информации
ISO/IEC 17799 (философия)	Международный стандарт	Используется отдельными методами оценки рисков в качестве образца "нулевого риска", где риск означает степень отклонения от образца	При признании такого подхода используется как руководство к действию по тем областям ИБ, где выявлены существенные отклонения от ISO/IEC 17799

ISO/IEC 13335 (пример подхода)	Технический отчет ИСО и МЭК	Определяет в 3 части 4 различных подхода к оценке рисков безопасности ИТ, методологически подобных тем, что реализованы в CRAMM	Оценка риска организаций и ИТ по одному из приведенных в отчете методов оценки рисков
COBRA	(программный продукт)	Оценка рисков как степень отклонения от образца - международного стандарта ISO/IEC 17799	Степень отклонения от положений (рекомендаций) ISO/IEC 17799
РД 4.25.01 93	Действует в России	Документ ориентирован на оценку состоятельности и качества продукции, для оценки риска, может быть использован только методологически	Оценка состоятельности и качества выпускаемой продукции на основе сравнения с выбранным ближайшим аналогом (образцом), определяет степень отклонения от образца
Принципы менеджмента риска для электронных банковских услуг (Базельский комитет по банковскому надзору)	Рекомендован международной банковской организаций для применения в банковских структурах.	Ориентирован на банковскую специфику и рассматривает вопросы безопасности при использовании ИТ в банковских организациях	На результат оценки непосредственно не ориентирован
ГОСТ Р ИСО/МЭК 15408 2002 (пример подхода)	Введен в действие в России с начала 2004 г.	Общетехнический стандарт по безопасности ИТ, где показаны место и роль оценок рисков к общей концепции безопасности ИТ. Для практики рекомендует руководствоваться положениями ISO/IEC 13335	Включение в ПЗ и ЗБ актуальных угроз безопасности ИТ и выбор необходимых функциональных требований и требований доверия безопасности ИТ

Комплекс стандартов, имеющих с своем составе стандарты систем менеджмента типов А, Б и В, рекомендуется рассматривать как семейство стандартов менеджмента. Например, для систем менеджмента информационной безопасности к 2010 г. уже фактически сформировалось семейство стандартов СМИБ, отвечающее требованиям Руководства ISO 72 (см. рис. 30).

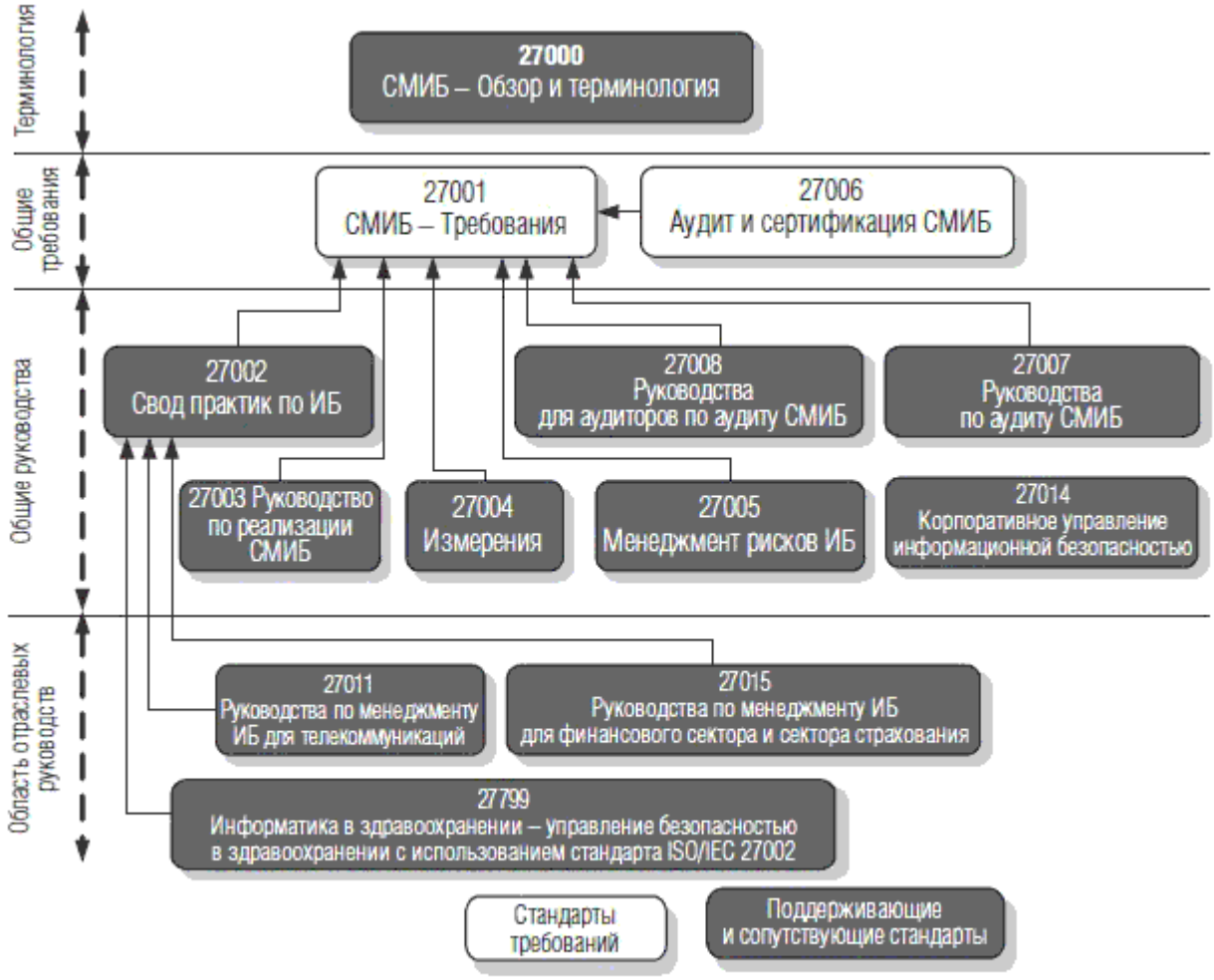


Рис. 30. Семейство стандартов СМИБ

формализации формирования

ГОСТ Р ИСО/МЭК 18044 – 2007 Информационная технология Методы и средства обеспечения безопасности МЕНЕДЖМЕНТ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ISO/IEC TR 18044:2004 Information technology— Security techniques — Information security incident management

ГОСТ Р ИСО МЭК 27006-2008 ?!! можно ли давать рисунок ?!!

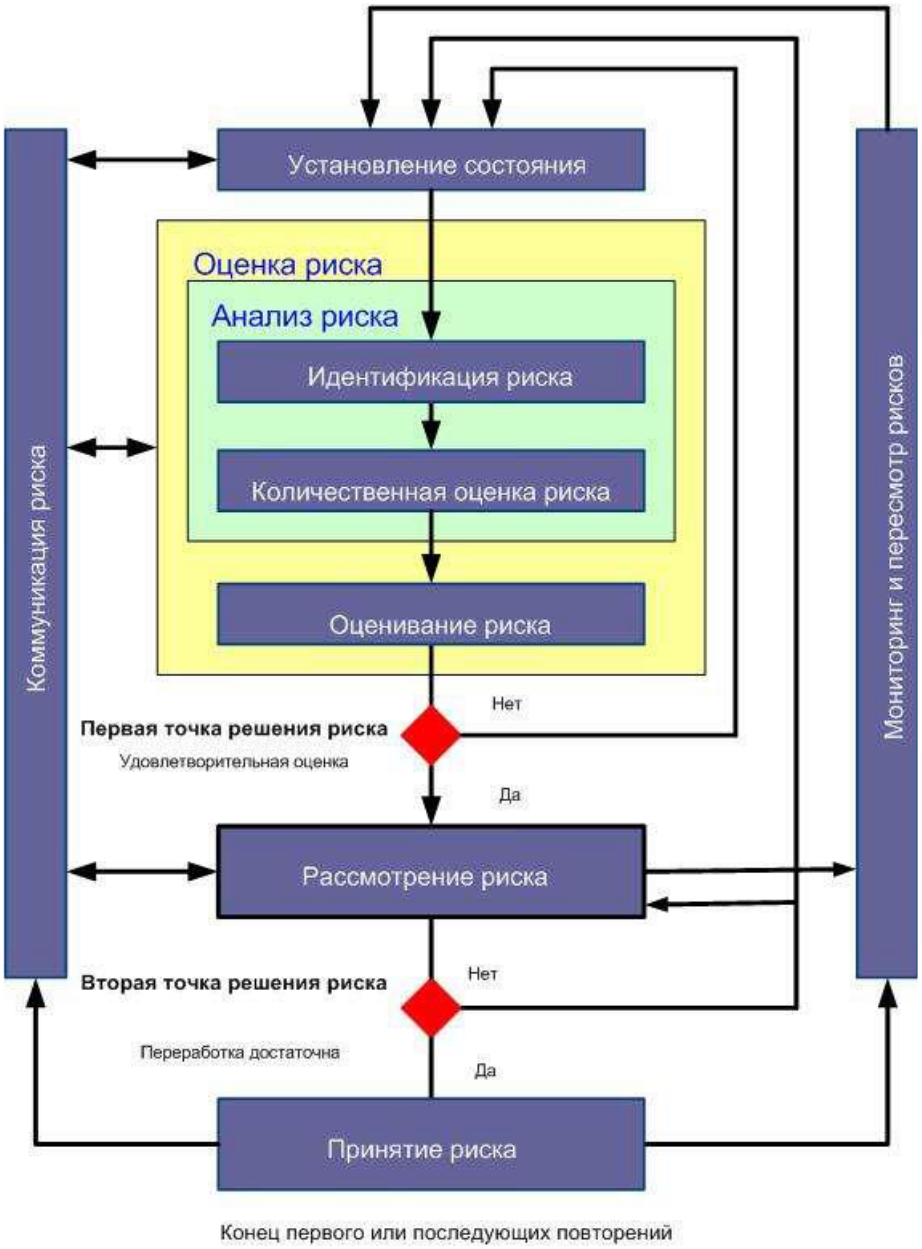


Рисунок 1. Процесс управления риском информационной безопасности

Раздел 3. Введение в математические основы управления рисками ИБ

Постановка математической задачи оптимального управления. Классификация задач оптимального управления. Математическое программирование. Формы и средства использования стандартных математических моделей для решения задачи управления рисками ИБ.

Экспертные оценки www.aup.ru/books/m157/3_4_1.htm

Теоретические занятия (1 лекция) -2 часа.
Лекция 2..

ГОСТ Р 51901-2002 Управление надежностью. Анализ риска технологических систем (Dependability management. Risk analysis of technological systems):

Таблица 1 — Перечень наиболее распространенных методов, используемых при анализе риска

Метод	Описание и применение	Ссылка
Анализ «дерева событий»	Совокупность приемов идентификации опасности и анализа частот, в которых используется индуктивный подход с целью перевода различных инициирующих событий в возможные исходы	А.4 приложения А
Анализ видов и последствий отказов, а также Анализ видов, последствий и критичности отказов	Совокупность приемов идентификации главных источников опасности и анализа частот, с помощью которых анализируются все аварийные состояния данной единицы оборудования на предмет их влияния как на другие компоненты, так и на систему в целом	А.2 приложения А; МЭК 60812 [1]
Анализ «дерева неисправностей»	Совокупность приемов идентификации опасности и анализа частот нежелательного события, с помощью которых определяются все пути его реализации. Используется графическое изображение	А.3 приложения А; МЭК 61025 [2]
Исследование опасности и связанных с ней проблем	Совокупность приемов идентификации фундаментальной опасности, при помощи которых оценивается каждая часть системы с целью обнаружения того, могут ли происходить отклонения от назначения конструкции и какие последствия это может повлечь	А.1 приложения А
Анализ влияния человеческого фактора	Совокупность приемов анализа частот в области воздействия людей на показатели работы системы, при помощи которых определяется влияние ошибок человека на надежность	А.6 приложения А

Окончание таблицы 1

Метод	Описание и применение	Ссылка
Предварительный анализ опасности	Совокупность приемов идентификации опасности и анализа частот, используемых на ранней стадии проектирования с целью идентификации опасностей и оценки их критичности	А.5 приложения А
Структурная схема надежности	Совокупность приемов анализа частот, на основе которых создается модель системы и ее резервов для оценки надежности системы	МЭК 61078 [3]

Таблица 2 — Перечень дополнительных методов, используемых при анализе риска

Метод	Описание и применение
Классификация групп риска по категориям	Классификация видов риска по категориям в порядке приоритетности групп риска
Ведомости проверок	Составление перечней типовых опасных веществ и/или источников потенциальных аварий, которые нуждаются в рассмотрении. С их помощью можно оценивать соответствие законам и стандартам
Общий анализ отказов	Метод, предназначенный для определения того, возможен ли случайный отказ (авария) ряда различных частей или компонентов в рамках системы, и оценки его вероятного суммарного эффекта
Модели описания последствий	Оценка воздействия события на людей, имущество или окружающую среду. Используются как упрощенные аналитические подходы, так и сложные компьютерные модели
Метод Делфи	Способ комбинирования экспертных оценок, которые могут обеспечить проведение анализа частоты, моделирования последствий и/или оценивания риска
Индексы опасности	Совокупность приемов по идентификации/оценке опасности, которые могут быть использованы для ранжирования различных вариантов системы и определения менее опасных вариантов
Метод Монте-Карло и другие методы моделирования	Совокупность приемов анализа частоты, в которых используется модель системы для оценки вариаций в исходных условиях и допущениях
Парные сопоставления	Способ оценки и ранжирования совокупности рисков путем попарного сравнения
Обзор данных по эксплуатации	Совокупность приемов, которые могут быть использованы для выявления потенциально проблемных областей, а также для анализа частоты, основанного на данных об авариях, данных о надежности и прочее
Анализ скрытых процессов	Метод выявления скрытых процессов и путей, которые могли бы привести к наступлению непредвиденных событий

Практические занятия (1 занятие)- 2 часа.

Практическое занятие 3. Решение оптимизационных задач (на примере задачи линейного программирования). Сведение практических задач управления рисками к стандартным задачам математического программирования. Графическая интерпретация задачи линейного программирования. Средства автоматизации оптимизационных задач.

Мизов А. С., Шевяхов М. Ю. Некоторые подходы к оценке информационных рисков с использованием нечётких множеств Электронный журнал «Системный анализ в науке и образовании» Выпуск №1, 2010 год

Лабораторный практикум - 4 часа, 1 работа.

Реализация этапов задачи управления рисками методами математического программирования.

Используемое оборудование: аппаратная платформа: процессор AMD Athlon 64 X2 Dual Core 4200+ 2,21 ГГц, оперативная память 2 ГГБ, жёсткий диск 160 ГГБ, Видеоадаптер NVIDIA GeForce 8500 GT, сетевая плата, монитор, клавиатура, мышь.

Управление самостоятельной работой студента.

Консультации по изучению дополнительных материалов, выполнению комплексного итогового проекта. Консультации по вопросам подготовки, выполнения и защиты лабораторного практикума.

Раздел 4. Инструментальные средства поддержки решения задач управления рисками ИБ.

Сравнительный анализ инструментальных средств управления рисками.

Критерии выбора инструментальных средств управления рисками.

Практические занятия (1 занятие)- 2 часа.

Практическое занятие 4.

Опыт ведущих компаний по управлению рисками ИБ. Перспективы развития методов и средств управления рисками ИБ.

Лабораторный практикум - 4 часа, 1 работа.

есть демоверсия RMI.rar и с сайта http://www.srisks.ru/ РискМенеджер

Компания Digital Security есть презентация dsoffice_presentation.zip и данный не сайте http://www.dsec.ru/products/grif/ о продукте Гриф и Кондор

Подробнее о продуктах Computer Associates CA Technologies http://www.interface.ru/home.asp?artId=60&vId=13

Исследование возможностей инструментальных средств управления рисками ИБ. Разработка ТЗ на разработку компонента инструментального средства управления рисками ИБ.

Используемое оборудование: аппаратная платформа: процессор AMD Athlon 64 X2 Dual Core 4200+ 2,21 ГГц, оперативная память 2 ГГБ, жёсткий диск 160 ГГБ, Видеоадаптер NVIDIA GeForce 8500 GT, сетевая плата, монитор, клавиатура, мышь.

Управление самостоятельной работой студента.

Консультации по самостоятельному изучению дополнительных материалов, интеграции и отладке итогового приложения, формированию пояснительной записки, представлению итогового приложения, подготовке к экзамену.

Приложение 1.Источники информации по курсу:

нормативно-правовые:

1. Федеральный закон N 98-ФЗ «О коммерческой тайне» от 29 июля 2004 г.
2. Федеральный закон N 161-ФЗ «О национальной платежной системе» от 27.06.2011 г.
3. Доктрина информационной безопасности Российской Федерации // Российская газета. — 2000. — 28 сентября. № 187.
4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (выписка) Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.
5. ГОСТ Р 50.1.053-2005 Информационная технология. Основные термины и определения в области технической защиты информации
6. ГОСТ Р 50779.10—2000 «Статистические методы. Вероятность и основы статистики. Термины и определения» (ISO 3534-1 Statistics — Vocabulary and symbols — Part 1: General statistical terms and terms used in probability1)
7. ГОСТ Р 50922- 2006 Защита информации ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ
8. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
9. ГОСТ Р 51897-2011 (взамен 2002) Менеджмент риска. Термины и определения.
10. ГОСТ Р 51898—2002 «Аспекты безопасности. Правила включения в стандарты». (Руководство ИСО/МЭК 51:1999 ISO/IEC Guide 51 Safety aspects — Guidelines for their inclusion in standards)
11. ГОСТ Р 51901.4- 2005 (МЭК 62198:2001) Руководство по применению при проектировании (IEC 62198:2001 Project risk management - Application guidelines (MOD)
12. ГОСТ Р 51901-2002 Управление надежностью. Анализ риска технологических систем (Dependability management. Risk analysis of technological systems)
13. ГОСТ Р 52069.0-2003 Защита информации. Система стандартов. Основные положения.
14. ГОСТ Р 53633.0-2009 Информационные технологии. Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Общая структура бизнес-процессов
15. ГОСТ Р 53633.1-2009 Информационные технологии. Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Декомпозиция и описание процессов. Процессы уровня 2 eTOM.

Основная деятельность. Управление взаимоотношениями с поставщиками и партнерами

16. ГОСТ Р 53633.2-2009 Информационные технологии. Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Декомпозиция и описание процессов. Процессы уровня 2 eTOM. Основная деятельность. Управление и эксплуатация ресурсов
17. ГОСТ Р 53633.3-2009 Информационные технологии. Сеть управления электросвязью. Расширенная схема деятельности организации связи (eTOM). Декомпозиция и описание процессов. Процессы уровня 2 eTOM. Основная деятельность. Управление взаимоотношениями с клиентами
18. ГОСТ Р ИСО 31000-2010 Менеджмент риска Принципы и руководство
19. ГОСТ Р ИСО 9000—2008 «Системы менеджмента качества. Основные положения и словарь». (ISO 9000:2005 Qualitymanagement systems — Fundamentals and vocabulary)
20. ГОСТ Р ИСО/МЭК 12207-2010 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств
21. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
22. ГОСТ Р ИСО/МЭК 15288:2002 Информационная технология. Системная инженерия. Процессы жизненного цикла систем
23. ГОСТ Р ИСО/МЭК 15288-2005 Информационная технология. Системная инженерия. Процессы жизненного цикла систем
24. ГОСТ Р ИСО/МЭК 15408-1.2002. Раздел 4.
25. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
26. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
27. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
28. ГОСТ Р ИСО/МЭК 15504-1-2009 Информационная технология. Оценка процессов. Часть 1. Концепция и словарь

29. ГОСТ Р ИСО/МЭК 15504-2-2009 Информационная технология. Оценка процессов. Часть 2. Проведение оценки
30. ГОСТ Р ИСО/МЭК 15504-3-2009 Информационная технология. Оценка процессов. Часть 3. Руководство по проведению оценки
31. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
32. ГОСТ Р ИСО/МЭК 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
33. ГОСТ Р ИСО/МЭК 20000-1-2010 Информационная технология. Менеджмент услуг. Часть 1. Спецификация
34. ГОСТ Р ИСО/МЭК 20000-2-2010 Информационная технология. Менеджмент услуг. Часть 2. Кодекс практической деятельности
35. ГОСТ Р ИСО/МЭК 27001-2006 Название: Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (Information technology. Security techniques. Information security management systems. Requirements)
36. ГОСТ Р ИСО/МЭК 27002-2005 Информационные технологии. Свод правил по управлению защитой информации
37. ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения
38. ГОСТ Р ИСО/МЭК 27005:2008 Информационные технологии. Методы защиты. Менеджмент рисков информационной безопасности
39. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
40. ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности
41. ГОСТ Р ИСО/МЭК 27033-1-2011 Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей
42. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
43. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

44. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

45. ГОСТ Р ИСО/МЭК ТО 16326-2002 Программная инженерия. Руководство по применению ГОСТ Р ИСО/МЭК 12207 при управлении проектом

46. СТО БР ИББС-1.0-2010 Стандарт Банка России Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. Ппринят и введен в действие Распоряжением Банка России от 21.06.2010 N Р-705

основная литература:

47. Андрианов В.В., Курило А.П. Обеспечение информационной безопасности бизнеса. – М.: Альпина Паблишер, 2010 г.

монографии и учебные пособия:

48. Александров А. Комплексное управление информационными рисками // BYTE Россия. - 2004.- 10 июня.

49. Анин Б. Ю. Защита компьютерной информации — СПб: БХВ-Петербург, 2000 г. 384 стр.

50. Астахов А.М. Аудит безопасности ИС // Конфидент 2003. № 1 (49). С. 63 -67.

51. Афанасьев В.Н., Постников А.И. Информационные технологии в управлении предприятием. — М.: МИЭМ, 2003. — 143 с.

52. Баранов А.П., Борисенко Н.П., Зегжда П.Д., Корт С.С., Ростовцев А.Г. Математические основы информационной безопасности: Пособие. Орел: ВИПС, 1997.-354 с.

53. Буянова И. С. Современная система управления информационной безопасностью с новым стандартом ISO/1EC 27001:2005, 2006 г. Код доступа: http://www.traectoria.ru

54. Галатенко В.А. Основы информационной безопасности. Интернет-университет информационных технологий ИНТУИТ.ру. 2004. - 280с.

55. Герасименко В.А., Малюк А.А Основы защиты информации М.: Инкомбук, 1997

56. Гузик С. Стандарты CobiT// Jet Info №1 2003 г.

57. Данилин Н.С. Основы построения единой автоматизированной системы ГТК РФ.-М.: РТА, 1997.

58. Домарев, В.В. Безопасность информационных технологий. Системный подход. М.: Изд-во «DiaSoft», 2004. - 992 стр.

59. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему. Ч. 1. СПб.: Мир и семья, 1997.

60. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем.- М.: Горячая линия Телеком, 2000. - 452 с.

61. Ивлев В., Попова Т. Вип-костинг средство для функционально-стоимостного анализа бизнес-процессов// Менеджмент сегодня №5, 2002 г.

62. Ивушкин А. Аализ рисков информационной безопасности http://taxpravo.ru/analitika/statya-131560-analiz_riskov_informatsionnoy_bezopasnosti

63. Информационные технологии в бизнесе / под ред. М. Желены. СПб: Питер, 2002.-1120 стр.

64. Кащеев Р. Balanced Scorecard: новое заклинание или стратегия управления?// электронный журнал «Финансы.Яи» март 2003 г. Код доступа: http://www.finansy.ru

65. Кляшторная О. Оценка ИТ-проектов. Что выбрать?// Директор ИС №6, 2003 г.

66. Кузнецов Н.А., Кульба В.В., Микрин Е.А. и др. Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. / отв. ред. Н.А. Кузнецов, В.В. Кульба; Ин-т проблем передачи ин-форм. РАН. -М.: Наука, 2006. Т. 1. - 495 с.

67. Курило А.П., Ухлинов Л.М. Проектирование систем контроля доступа к ресурсам сетей ЭВМ. -М.: МИФИ, 1997.

68. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH.- СПб.: БХВ-Петербург, 2003. 736 с.

69. Липаев В. В. Экономика производства сложных программных продуктов М.: СИНТЕГ, 2008 г. 432 стр.

70. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учеб. пособие для вузов. — М.: Горячая линия — Телеком, 2004. 280 с.

71. Медведовский И.Д. ISO 17799: Эволюция стандарта в период 2002 2005, 2005 г. Код доступа: http://www.dsec.ru/

72. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через INTERNET. М.: НПО «Мир и семья- 95», 1997.

73. Мизов А. С., Шевяхов М. Ю. Некоторые подходы к оценке информационных рисков с использованием нечётких множеств Электронный журнал «Системный анализ в науке и образовании» Выпуск №1, 2010 год

74. Найман Э. Л. Путь к финансовой свободе: Профессиональный подход к трейдингу и инвестициям. 3-е издание М.:АЛЬПИНА 2007 г. - 480 стр.

75. Некрасова Е. Информационная система предприятия: эффекты или эффективность?// СЮ №1 2003 г.

76. Нестеров Д. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft Интернет-Университет Информационных Технологий, http://www.intuit.ru/department/itmngt/riskanms/

77. Норенков И. П. Подходы к проектированию автоматизированных систем// электронный журнал «Наука и образование» №6 2005 г. Код доступа: http://teclmomag.edu.ru

78. Носаков. В. Создание комплексной системы управления информационной безопасностью // Jet Info №7 2006 г.

79. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность. М: ДМК Пресс, 2004. — 384с.

80. Симонов С.В. Анализ рисков, управление рисками. Jet Info, 2, 2003.

81. Симонов С.В. Современные концепции управления информационными рисками, (http://www.compulink.ru/security).

82. Трифаленков И., Зайцева Н. Функциональная безопасность корпоративных систем. // Открытые системы. — 2002. № 7 8.

83. Ухлинов Л.М. Управление безопасностью информации в автоматизированных системах. — М.: МИФИ, 1996.

84. Шиляев А. Эффективность инвестиций в информационные технологии: подходы к измерению и оценке//"Бизнес-образование", №2(15), 2003 г. сс. 155-172.

85. Щербакова О. Методы оценки и управления стоимостью компании, основанные на концепции экономической добавленной стоимости// Финансовый менеджмент №3, 2003 г.

86. Ярочкин В.И., Бузанова Я.В. Аудит безопасности фирмы: теория и практика : учеб. пособие для вузов. М.: Академический Проект; Королев: Парадигма, 2005. - 352 с.

источники на английском языке:

87. BS 7799-2:2002 Information security management. Specification with guidance for use UK: BSI, 2002 г. - 38 стр.

88. FIPS Pub 199:2004 Standards for Security Categorization of Federal Information and Information Systems

89. FIPS Pub 200:2006 Minimum Security Requirements for Federal Information and Information Systems

90. ISO 10241 International terminology standards — Preparation and layout
91. ISO 10241-1:2011 «Terminological entries in standards — Part 1: General requirements and examples of presentation».
92. ISO 31000:2009 Riskmanagement — Principles and guidelines
93. ISO 704 Terminology work — Principles and methods
94. ISO 860 Terminology work — Harmonization of concepts and terms
95. ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management
96. ISO/IEC 18028-1:2006 Information technology — Security techniques — IT network security — Part :1 Network security management
97. ISO/IEC 18028-2:2006 Information technology — Security techniques — IT network security — Part :2 Network security architecture
98. ISO/IEC 18028-3:2005 Information technology — Security techniques — IT network security — Part :3 Securing communications between networks using security gateways
99. ISO/IEC 18028-4:2005 Information technology — Security techniques — IT network security — Part :4 Securing remote access
100. ISO/IEC 18028-5:2006 Information technology — Security techniques — IT network security — Part :5 Securing communications across networks using virtual private networks
101. ISO/IEC 18043:2006 Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems
102. ISO/IEC 21827:2002 Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)
103. ISO/IEC 27000:2009 Information technology - Security techniques - Information security management systems - Overview and vocabulary
104. ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements
105. ISO/IEC 27005:2008 «Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности»
106. ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management
107. ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management
108. ISO/IEC 27006:2007 «Информационные технологии. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью»

109. ISO/IEC 27006:2007 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

110. ISO/IEC FDIS 17799:2005 Information technology- Security techniques Code of practice for information security management

111. ISO/IEC FDIS 27001:2005 Information technology- Security techniques Information security management systems — Requirements

112. ISO/IEC Guide 2 Standardization and related activities — General vocabulary

113. ISO/IEC Guide 51 Safety aspects — Guidelines for their inclusion in standards

114. NIST SP 800-18:2006 Guide for Developing Security Plans for Federal Information Systems

115. NIST SP 800-30:2002 Risk Management Guide for Information Technology Systems

116. NIST SP 800-37:2008 Guide for Security Authorization of Federal Information Systems

117. NIST SP 800-53:2009 Recommended Security Controls for Federal Information Systems and Organizations

118. NIST SP 800-55:2008 Performance Measurement Guide for Information Security

119. NIST SP 800-60:2008 Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories

120. NIST SP 800-61:2008 Computer Security Incident Handling Guide

121. Risk Management Guide for Information Technology Systems. NIST, Special Publication 800-30.

Приложение 2. Глоссарий терминов в области ИБ

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующий стандарт:

ИСО/МЭК 17799:2005 Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **активы** (asset): Все, что имеет ценность для организации.

[ИСО/МЭК 13335-1:2004] [4]

3.2 **доступность** (availability): Свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

[ИСО/МЭК 13335-1:2004] [4]

3.3 **конфиденциальность** (confidentiality): Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса.

[ИСО/МЭК 13335-1:2004] [4]

3.4 **информационная безопасность;** ИБ (information security): Свойство информации сохранять конфиденциальность, целостность и доступность.

Примечание — Кроме того, данное понятие может включать в себя также и свойство сохранять аутентичность, подотчетность, неотказуемость и надежность.

[ИСО/МЭК 17799:2005]

3.5 **событие информационной безопасности** (information security event): Идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

[ИСО/МЭК ТО 18044:2004] [5]

3.6 **инцидент информационной безопасности** (information security incident): Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Примечание — Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

[ИСО/МЭК ТО 18044:2004] [5]

3.7 **система менеджмента информационной безопасности;** СМИБ (information security management system; ISMS): Часть общей системы менеджмента, основанная на использовании методов оценки бизнес-рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Примечание — Система менеджмента включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы.

3.8 **целостность** (integrity): Свойство сохранять правильность и полноту активов.

[ИСО/МЭК 13335-1:2004] [4]

3.9 **остаточный риск** (residual risk): Риск, остающийся после его обработки.

[Руководство ИСО/МЭК 73:2002] [6]

3.10 **принятие риска** (risk acceptance): Решение по принятию риска.

[Руководство ИСО/МЭК 73:2002] [6]

3.11 **анализ риска** (risk analysis): Систематическое использование информации для определения источников риска и количественной оценки риска.

[Руководство ИСО/МЭК 73:2002] [6]

3.12 **оценка риска** (risk assessment): Общий процесс анализа риска и его оценивания.
[Руководство ИСО/МЭК 73:2002] [6]
3.13 **оценивание риска** (risk evaluation): Процесс сравнения количественно оцененного риска с заданными критериями риска для определения его значимости.
[Руководство ИСО/МЭК 73:2002] [6]
3.14 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в отношении риска.

Примечание — Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникацию риска.

[Руководство ИСО/МЭК 73:2002] [6]
3.15 **обработка риска** (risk treatment): Процесс выбора и осуществления мер по модификации риска.
[Руководство ИСО/МЭК 73:2002] [6]

Примечания
1 Меры по обработке риска могут включать в себя избежание, оптимизацию, перенос или сохранение риска.
2 В настоящем стандарте термин «мера управления» (control) использован как синоним термина «мера» (measure).

3.16 **положение о применимости** (statement of applicability): Документированное предписание, определяющее цели и меры управления, соответствующие и применимые к системе менеджмента информационной безопасности организации.

Примечание — Цели и меры управления основываются на результатах и выводах процессов оценки и обработки рисков, на требованиях законодательных или нормативных актов, на обязательствах по контракту и бизнес-требованиях организации по отношению к информационной безопасности.

4 Система менеджмента информационной безопасности

4.1 Общие требования

Организация должна разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную СМИБ применительно ко всей деловой деятельности организации и рискам, с которыми она сталкивается. С учетом целей настоящего стандарта используемый процесс основан на применении модели PDCA, приведенной на рисунке 1.

4.2 Разработка системы менеджмента информационной безопасности. Управление системой менеджмента информационной безопасности

4.2.1 Разработка системы менеджмента информационной безопасности

Организация должна осуществить следующее:
a) определить область и границы действия СМИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий, в том числе детали и обоснование любых исключений из области ее действия (см. 1.2);
b) определить политику СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий, которая:
1) содержит концепцию, включающую в себя цели, основные направления и принципы действий в сфере ИБ;
2) принимает во внимание требования бизнеса, нормативно-правовые требования, а также договорные обязательства по обеспечению безопасности;
3) согласуется со стратегическим содержанием менеджмента рисков организации, в рамках которого будет разрабатываться и поддерживаться СМИБ;
4) устанавливает критерии оценки рисков [см. 4.2.1, перечисление c)];
5) утверждается руководством организации.

Примечание — Для целей настоящего стандарта политика СМИБ имеет приоритет перед политикой ИБ. Эти политики могут быть изложены в одном документе;

c) определить подход к оценке риска в организации, для чего необходимо:
1) определить методологию оценки риска, подходящую для СМИБ, которая должна соответствовать требованиям обеспечения деятельности организации и нормативно-правовым требованиям информационной безопасности;

ГОСТ 50922—2006 Защита информации. Основные термины и определения.

(рвёт текст?!!)

ГОСТ Р 50922-96

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ Защита информации ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1 **Защищаемая информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Примечание:

Собственником информации может быть - государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

2 **Защита информации** - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

3 **Защита информации от утечки** - деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации [иностранными] разведками.

4 **Защита информации от несанкционированного воздействия** защита информации от НСВ: Деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

5 **Защита информации от непреднамеренного воздействия** - деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

6 **Защита информации от разглашения** - деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

7 **Защита информации от несанкционированного доступа** - защита информации от НСД: Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Примечание:

Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

8 **Защита информации от [иностранной] разведки** - деятельность по предотвращению получения защищаемой информации [иностранной] разведкой.

9 **Защита информации от [иностранной] технической разведки** - деятельность по предотвращению получения защищаемой информации [иностранной] разведкой с помощью технических средств.

10 **Защита информации от агентурной разведки** - деятельность по предотвращению получения защищаемой информации агентурной разведкой.

11 **Цель защиты информации** - желаемый результат защиты информации.

Примечание:

Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и/или несанкционированного и непреднамеренного воздействия на информацию.

12 **Эффективность защиты информации** - степень соответствия результатов защиты информации поставленной цели.

13 **Показатель эффективности защиты информации** - мера или характеристика для оценки эффективности защиты информации.

14 **Нормы эффективности защиты информации** - значения показателей эффективности защиты информации, установленные нормативными документами.

3.2 Организация защиты информации

15 **Организация защиты информации** - содержание и порядок действий по обеспечению защиты информации.

16 **Система защиты информации** - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам,

установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

17 **Мероприятие по защите информации** - совокупность действий по разработке и/или практическому применению способов и средств защиты информации.

18 **Мероприятие по контролю эффективности защиты информации** - совокупность действий по разработке и/или практическому применению методов [способов] и средств контроля эффективности защиты информации.

19 **Техника защиты информации** - средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

20 **Объект защиты** - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

21 **Способ защиты информации** - порядок и правила применения определенных принципов и средств защиты информации.

22 **Категорирование защищаемой информации [объекта защиты]** - установление градаций важности защиты защищаемой информации [объекта защиты].

23 **Метод [способ] контроля эффективности защиты информации** - порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

24 **Контроль состояния защиты информации** - проверка соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

25 **Средство защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.

26 **Средство контроля эффективности защиты информации** - техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

27 **Контроль организации защиты информации** - проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

28 **Контроль эффективности защиты информации** - проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

29 **Организационный контроль эффективности защиты информации** - проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

30 **Технический контроль эффективности защиты информации** - контроль эффективности защиты информации, проводимой с использованием средств контроля.

ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения Это старые термины есть ГОСт 2011 года.

3.1.1 **риск:** Сочетание вероятности события и его последствий

Примечания

1 Термин «риск» обычно используют только тогда, когда существует возможность негативных последствий.

2 В некоторых ситуациях риск обусловлен возможностью отклонения от ожидаемого результата или события.

3 Применительно к безопасности см. [1]

3.1.2 **последствие:** Результат события

Примечания

1 Результатом события может быть одно или более последствий.

2 Последствия могут быть ранжированы от позитивных до негативных. Однако применительно к аспектам безопасности последствия всегда негативные.

3 Последствия могут быть выражены качественно или количественно

3.1.3 **вероятность:** Мера того, что событие может произойти.

Примечание - ГОСТ Р 50779.10 дает математическое определение вероятности: «действительное число в интервале от 0 до 1, относящееся к случайному событию». Число может отражать относительную частоту в серии наблюдений или степень уверенности в том, что некоторое событие произойдет. Для высокой степени уверенности вероятность близка к единице

3.1.4 **событие:** Возникновение специфического набора обстоятельств, при которых происходит явление.

Примечания

1 Событие может быть определенным или неопределенным.

2 Событие может быть единичным или многократным.

3 Вероятность, связанная с событием, может быть оценена для данного интервала времени

3.1.5 **источник:** Объект или деятельность с потенциальными последствиями.

Примечание - Применительно к безопасности источник представляет собой опасность (см. [1])

3.1.6 **критерии риска:** Правила, по которым оценивают значимость риска.

Примечание - Критерии риска могут включать в себя сопутствующие стоимость и выгоды, законодательные и обязательные требования, социально-экономические и экологические аспекты, озабоченность причастных сторон, приоритеты и другие затраты на оценку

3.1.7 **менеджмент риска:** Скоординированные действия по руководству и управлению организацией в отношении риска.

Примечание - Обычно менеджмент риска включает в себя оценку риска, обработку риска, принятие риска и коммуникацию риска

3.1.8 **система менеджмента риска:** Набор элементов системы менеджмента организации в отношении менеджмента риска.

Примечание - Элементы системы менеджмента риска могут включать в себя стратегическое планирование, принятие решений и другие процессы, затрагивающие риск

3.2 Термины, относящиеся к лицам или организациям, подвергающимся риску

3.2.1 **причастная сторона:** Любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска.

Примечания

1 Лицо, принимающее решение, также является причастной стороной.

2 Причастная сторона включает в себя заинтересованную сторону, но имеет более широкое значение, чем заинтересованная сторона

3.2.2 **заинтересованная сторона:** Лицо или группа лиц, заинтересованные в деятельности или успехе организации.

Примеры: потребители, владельцы, работники организации, поставщики, банкиры, ассоциации, партнеры или общество.

Примечание - Группа лиц может состоять из организации, ее части или нескольких организаций (ГОСТ Р ИСО 9000)

3.2.3 **осознание риска:** Набор ценностей и озабоченностей, в соответствии с которыми причастная сторона рассматривает конкретный риск.

Примечания

1 Осознание риска зависит от потребностей, результатов и знаний причастных сторон.

2 Осознание риска может отличаться от объективных данных.

3.2.4 **коммуникация риска:** Обмен информацией о риске или совместное использование этой информации между лицом, принимающим решение, и другими причастными сторонами.

Примечание - Информация может касаться существования, природы, формы, вероятности, тяжести, приемлемости, мероприятий или других аспектов риска

3.3 Термины, относящиеся к оценке риска

3.3.1 **оценка риска:** Общий процесс анализа риска и оценивания риска

3.3.2 **анализ риска:** Систематическое использование информации для определения источников и количественной оценки риска.

Примечания

1 Анализ риска обеспечивает базу для оценивания риска, мероприятий по снижению риска и принятия риска.

2 Информация может включать в себя исторические данные, результаты теоретического анализа, информированное мнение и касаться причастных сторон

3.3.3 **идентификация риска:** Процесс нахождения, составления перечня и описания элементов риска.

Примечания

1 Элементы риска могут включать в себя источники или опасности, события, последствия и вероятность.

2 Идентификация риска может также отражать интересы причастных сторон

3.3.4 **идентификация источников:** Процесс нахождения, составления перечня и описания источников.

Примечание - Применительно к безопасности идентификация источников представляет собой идентификацию опасностей (см. [1])

3.3.5 **количественная оценка риска:** Процесс присвоения значений вероятности и последствий риска.

Примечание - Количественная оценка риска может учитывать стоимость, выгоды, интересы причастных сторон и другие переменные, рассматриваемые при оценивании риска

3.3.6 **оценивание риска:** Процесс сравнения количественно оцененного риска с данными критериями риска для определения значимости риска.

Примечания

1 Оценивание риска может быть использовано для содействия решениям по принятию или обработке риска.

2 Применительно к безопасности см. [1]

3.4 Термины, относящиеся к обработке риска и управлению риском

3.4.1 **обработка риска:** Процесс выбора и осуществления мер по модификации риска.

Примечания

1 Термин «обработка риска» иногда используют для обозначения самих мер.

2 Меры по обработке риска могут включать в себя избежание, оптимизацию, перенос или сохранение риска

3.4.2 **управление риском:** Действия, осуществляемые для выполнения решений в рамках менеджмента риска.

Примечание - Управление риском может включать в себя мониторинг, переоценивание и действия, направленные на обеспечение соответствия принятым решениям

3.4.3 **оптимизация риска:** Процесс, связанный с риском, направленный на минимизацию негативных и максимальное использование позитивных последствий и, соответственно, их вероятности.

Примечания

1 С точки зрения безопасности оптимизация риска направлена на снижение риска.

2 Оптимизация риска зависит от критериев риска с учетом стоимости и законодательных требований

3.4.4 **снижение риска:** Действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском

3.4.5 **уменьшение** (последствия события): Ограничение любого негативного последствия конкретного события

3.4.6 **предотвращение риска:** Решение не быть вовлеченным в рискованную ситуацию или действие, предупреждающее вовлечение в нее.

Примечание - Решение может быть принято на основе результатов оценивания риска

3.4.7 **перенос риска:** Разделение с другой стороной бремени потерь или выгод от риска.

Примечания

1 Законодательные или обязательные требования могут ограничивать, запрещать или поручать перенос определенного риска.

2 Перенос риска может быть осуществлен страхованием или другими соглашениями.

3 Перенос риска может создавать новый риск или модифицировать существующий риск.

4 Перемещение источника не является переносом риска

3.4.8 **финансирование риска:** Предусмотрение финансовых средств на расходы по обработке риска и сопутствующие затраты.

Примечание - В некоторых отраслях финансирование риска относится только к субсидированию финансовых последствий, связанных с риском

3.4.9 **сохранение риска:** Принятие бремени потерь или выгод от конкретного риска.

Примечание - Сохранение риска не включает в себя обработку риска в результате страхования или перенос риска другими средствами

3.4.10 **принятие риска:** Решение принять риск.

Примечание - Принятие риска зависит от критериев риска

3.4.11 **остаточный риск:** Риск, остающийся после обработки риска.

(скачать документ MS Word, 102 Кб)

Руководящий документ
Защита от несанкционированного доступа к информации
Термины и определения

Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.

Настоящий руководящий документ устанавливает термины и определения понятий в области защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.

Установленные термины обязательны для применения во всех видах документации.

Для каждого понятия установлен один термин. Применение синонимов термина не допускается.

Для отдельных терминов даны (в скобках) краткие формы, которые разрешается применять в случаях, исключающих возможность их различного толкования.

Для справок приведены иностранные эквиваленты русских терминов на английском языке, а также алфавитные указатели терминов на русском и английском языках.

1. Термины и определения

Термин	Определение
1. Доступ к информации (Доступ) Access to information	Ознакомление с информацией, ее обработка, в частности, копирование модификация или уничтожение информации
2. Правила разграничения доступа (ПРД) Security policy	Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
3. Санкционированный доступ к информации Authorized access to information	Доступ к информации, не нарушающий правила разграничения доступа
4. Несанкционированный доступ к информации (НСД) Unauthorized access to information	Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Примечание. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем
5. Защита от несанкционированного доступа (Защита от НСД) Protection from unauthorized access	Предотвращение или существенное затруднение несанкционированного доступа
6. Субъект доступа (Субъект) Access subject	Лицо или процесс, действия которого регламентируются правилами разграничения доступа
7. Объект доступа (Объект) Access object	Единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа
8. Матрица доступа Access matrix	Таблица, отображающая правила разграничения доступа
9. Уровень полномочий субъекта доступа Subject privilege	Совокупность прав доступа субъекта доступа
10. Нарушитель правил разграничения доступа (Нарушитель ПРД) Security policy violator	Субъект доступа, осуществляющий несанкционированный доступ к информации
11. Модель нарушителя правил разграничения доступа (Модель нарушителя ПРД) Security policy violator’s model	Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа
12. Комплекс средств защиты (КСЗ) Trusted computing base	Совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации
13. Система разграничения	Совокупность реализуемых правил разграничения доступа в

доступа (СРД) Security policy realization	средствах вычислительной техники или автоматизированных системах
14. Идентификатор доступа Access identifier	Уникальный признак субъекта или объекта доступа
15. Идентификация Identification	Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
16. Пароль Password	Идентификатор субъекта доступа, который является его (субъекта) секретом
17. Аутентификация Authentication	Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности
18. Защищенное средство вычислительной техники (защищенная автоматизированная система) Trusted computer system	Средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты
19. Средство защиты от несанкционированного доступа (Средство защиты от НСД) Protection facility	Программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа
20. Модель защиты Protection model	Абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа
21. Безопасность информации Information security	Состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз
22. Целостность информации Information integrity	Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения)
23. Конфиденциальная информация Sensitive information	Информация, требующая защиты
24. Дискреционное управление доступом Discretionary access control	Разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту
25. Мандатное управление доступом Mandatory access control	Разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности
26. Многоуровневая защита Multilevel secure	Защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности
27. Концепция диспетчера доступа	Концепция управления доступом, относящаяся к абстрактной машине, которая посредничает при всех обращениях

Reference monitor concept	субъектов к объектам
28. Диспетчер доступа (ядро защиты) Security kernel	Технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа
29. Администратор защиты Security administrator	Субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации
30. Метка конфиденциальности (Метка) Sensitivity label	Элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте
31. Верификация Verification	Процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие
32. Класс защищенности средств вычислительной техники (автоматизированной системы) Protection class of computer systems	Определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации
33. Показатель защищенности средств вычислительной техники (Показатель защищенности) Protection criterion of computer systems	Характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники
34. Система защиты секретной информации (СЗСИ) Secret information security system	Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах
35. Система защиты информации от несанкционированного доступа (СЗИ НСД) System of protection from unauthorized access to information	Комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах
36. Средство криптографической защиты информации (СКЗИ) Cryptographic information protection facility	Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности
37. Сертификат защиты (Сертификат) Protection certificate	Документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных

38. Сертификация уровня защиты (Сертификация) Protection level certification	Процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите

2. Алфавитный указатель терминов на русском языке

Администратор защиты

по РС БР ИББС_2.2_2009

(http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf Настоящие рекомендации в области стандартизации не могут быть полностью или час_
тично воспроизведены, тиражированы и распространены в качестве официального издания без

разрешения Банка России.)

3.1. **Априорные защитные меры:** защитные меры, эксплуатация которых сокращает ка_
чественно или количественно существующие уязвимости объектов защиты информационных активов, тем самым снижая вероятность реализации соответствующих угроз ИБ (например, средства защиты от несанкционированного доступа).

3.2. **Апостериорные защитные меры:** защитные меры, эксплуатация которых сокра_
щает степень тяжести последствий нарушения свойств ИБ информационных активов (напри_
мер, средства резервного копирования и восстановления информации).

3.3. **Допустимый риск нарушения информационной безопасности:** риск нарушения ИБ, предполагаемый ущерб от которого организация БС РФ в данное время и в данной ситуа_
ции готова принять.

3.4. **Информационный актив:** информация с реквизитами, позволяющими ее иденти_
фицировать; имеющая ценность для организации БС РФ; находящаяся в распоряжении орга_
низации БС РФ и представленная на любом материальном носителе в пригодной для ее обра_
ботки, хранения или передачи форме.

3.5. **Источник угрозы информационной безопасности; источник угрозы ИБ:** объект или субъект, реализующий угрозы ИБ путем воздействия на объекты среды информационных активов организации БС РФ.

3.6. **Модель угроз информационной безопасности; модель угроз ИБ:** описание ис_
точников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); мас_
штабов потенциального ущерба.

3.7. **Обработка риска нарушения информационной безопасности:** процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ, или мер по переносу, принятию или уходу от риска.

3.8. **Объект среды информационного актива:** материальный объект среды использо_
вания и (или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).

3.9. **Остаточный риск нарушения информационной безопасности:** риск, остающий_
ся после обработки риска нарушения ИБ.

3.10. **Оценка риска нарушения информационной безопасности:** систематический и документированный процесс выявления, сбора, использования и анализа информации, позво_
ляющей провести оценивание рисков нарушения ИБ, связанных с использованием информа_
ционных активов организации БС РФ на всех стадиях их жизненного цикла.

3.11. **Риск:** мера, учитывающая вероятность реализации угрозы и величину потерь (ущер_
ба) от реализации этой угрозы.

3.12. **Риск нарушения информационной безопасности; риск нарушения ИБ1:** риск, связанный с угрозой ИБ.

3.13. **Угроза информационной безопасности; угроза ИБ:** угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов организа_
ции БС РФ.

3.14. **Ущерб:** утрата активов, повреждение (утрата свойств) активов и (или) инфраструк_
туры организации или другой вред активам и (или) инфраструктуре организации БС РФ, насту_

пивший в результате реализации угроз ИБ через уязвимости ИБ.

Примерные формы (шаблоны) документирования по рекомендациям СБ РФ
(оформить из первоисточника http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf)

РС БР ИББС_2.2_2009

Приложение 2

Примерная форма документирования перечня типов информационных активов области оценки рисков нарушения ИБ и их свойств ИБ

На примере заполнения:
тип информационного актива — “Информация ограниченного доступа” (далее — “ДСП информация”).
Примечание.
Свойства ИБ, поддержание которых необходимо обеспечивать в рамках СОИБ организации БС РФ для типа информационного актива, обозначаются
знаком “+”, остальные свойства ИБ — знаком “–”.

Тип информационного актива	**Свойства информационной безопасности**			
	конфиденциальность	**целостность**	**доступность**	**другие свойства ИБ (при необходимости)**
“ДСП информация”	+	+	+	–
…				
…				

Приложение 3

Примерная форма документирования перечня типов объектов среды

На примере заполнения:
тип информационного актива — “ДСП информация”.

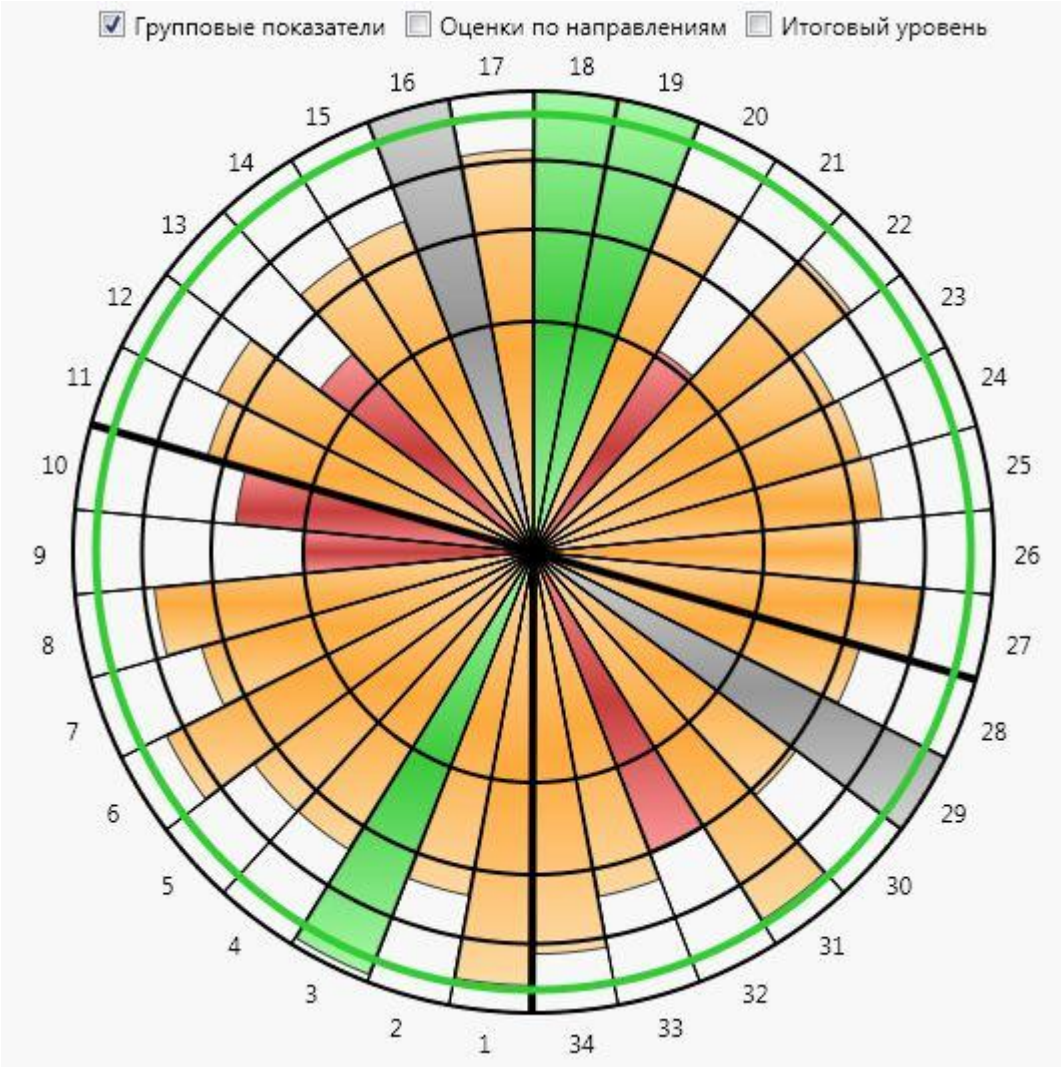
Тип информационного актива	**Уровни иерархии информационной инфраструктуры**	**Типы объектов среды**
“ДСП информация”	Физический уровень	Линии связи, аппаратные и технические средства, физические носители информации
	Сетевой уровень	Маршрутизаторы, коммутаторы, концентраторы
	Уровень сетевых приложений и сервисов	Программные компоненты передачи данных по компьютерным сетям (сетевые сервисы)
	Уровень операционных систем	Файлы данных с “ДСП информацией”
	Уровень систем управления базами данных	Базы данных с “ДСП информацией”
	Уровень банковских технологических приложений и сервисов	Прикладные программы доступа и обработки “ДСП информации”, бумажные носители
…		

Приложение 4

Примерная форма документирования данных и результатов оценки СВР угроз ИБ

На примере заполнения:
тип информационного актива — “ДСП информация”;
свойство ИБ — “Конфиденциальность”;
способ реализации угрозы — “Несанкционированное копирование”;
тип объекта среды — “Файлы данных с ДСП информацией”;
источники угроз — “Внутренний нарушитель” и “Внешний нарушитель”.
Примечание.
В ячейках “Оценка СВР угроз ИБ” требуется указать значение из следующего перечня: нереализуемая; минимальная; средняя; высокая; критическая.
[1] Степень детализации и порядок группировки для рассмотрения способов реализации угроз ИБ определяется организацией БС РФ.

Тип информац__			



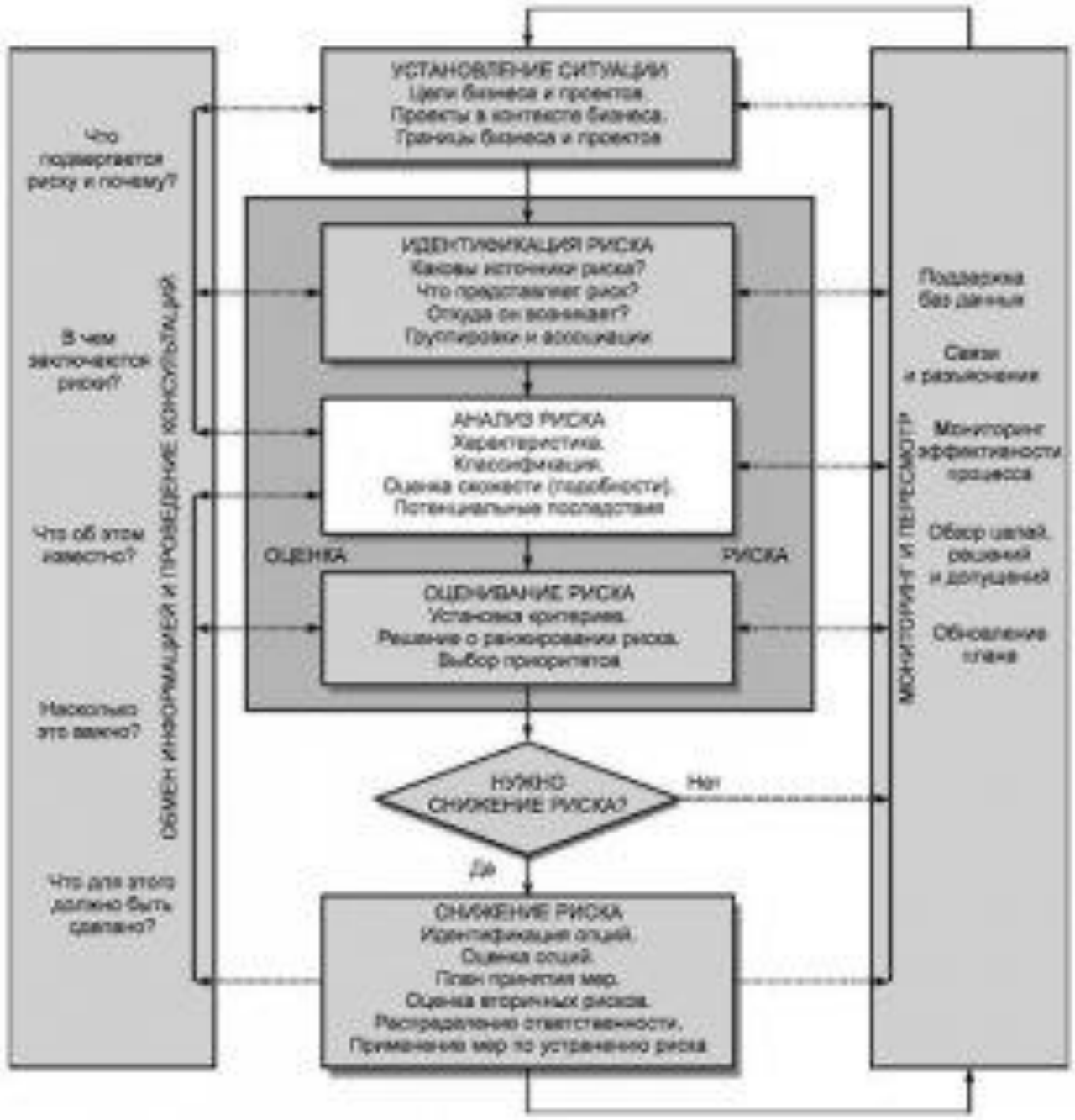
Описание	**English:** Compliance diagramm of the Russian Bank Information Security Standart STO BR IBBS **Русский:** Диаграмма соответствия организации требованиям СТО БР ИББС-1.0
Дата	20.04.2011
Источник	Bank Security Assessment Tool
Автор	LeetSoft

Остатки:

http://conf.sfu-kras.ru/sites/mn2012/thesis/s012/s012-095.pdf УДК 004.942 **АВТОМАТИЗИРОВАННАЯ СИСТЕМА УЧЕТА И АНАЛИЗА РИСКОВ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА Заболотникова А.Е., научные руководители ст. преподаватель каф. ИСТМ Лапина Е.В., доц. каф. ИСТМ Лапина Л.А.** ***Сибирский федеральный университет***

Задание контрмер. Выбор защитных мер для понижения риска осуществляется в соответствии с ГОСТ Р ИСО/МЭК ТО 13335-4-2007 и ГОСТ Р ИСО 15489-1-2007. Получение оценки снижения рисков основывается на

предположении, что вероятность успешной атаки на укрепленную систему задается соотношением 4: 3 Pnew = Pold*(«Старое_время» / «Новое_время»),



ГОСТ Р 52806-2007 Менеджмент рисков проектов ОБЩИЕ ПОЛОЖЕНИЯ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Менеджмент риска

РУКОВОДСТВО ПО ПРИМЕНЕНИЮ ПРИ ПРОЕКТИРОВАНИИ

Risk management.
Application guidelines in projects

Дата введения — 2006—02—01

1 Область применения

Настоящий стандарт применим для любого проекта технологического содержания. Он может также быть применен и к другим проектам.

Стандарт устанавливает общие положения менеджмента риска при проектировании, его подпроцессы и воздействующие факторы. Основными подпроцессами являются:

- определение ситуации, включая подтверждение целей проекта;
- идентификация риска;
- оценка риска, включая анализ и количественную оценку риска;
- обработка риска;
- исследование и мониторинг риска;
- обмен информацией по вопросам риска (включая консультации);
- обучение по проекту.

Настоящий стандарт распространяется на организационные требования процесса менеджмента риска на различных стадиях проектирования.

В некоторых ситуациях может быть нецелесообразно включать все положения настоящего стандарта в контракт. Соответственно требования настоящего стандарта следует рассматривать как формирующую часть контракта только по желанию сторон.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 27.310—95 Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения (*МЭК 60812:1985 «Методы анализа надежности систем. Метод анализа вида и последствий отказов (FMEA)», NEQ*)

ГОСТ Р ИСО 10006—2005 Системы менеджмента качества. Руководство по менеджменту качества при проектировании (*ИСО 10006:2003 «Системы менеджмента качества. Руководящие указания по менеджменту качества проектов», IDT*)

ГОСТ Р 51901.13—2005 (МЭК 61025:1990) Менеджмент риска. Анализ дерева неисправностей (*МЭК 61025:1990 «Анализ дерева неисправностей (FTA)», MOD*)

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

Издание официальное

При этом ГОСТ Р 51901.4-2005 «Менеджмент риска. Руководство по применению при проектировании» (http://vsegost.com/Catalog/54/5424.shtml) на странице IV дает явное указание, что этот стандарт не относиться к вопросам ИБ.