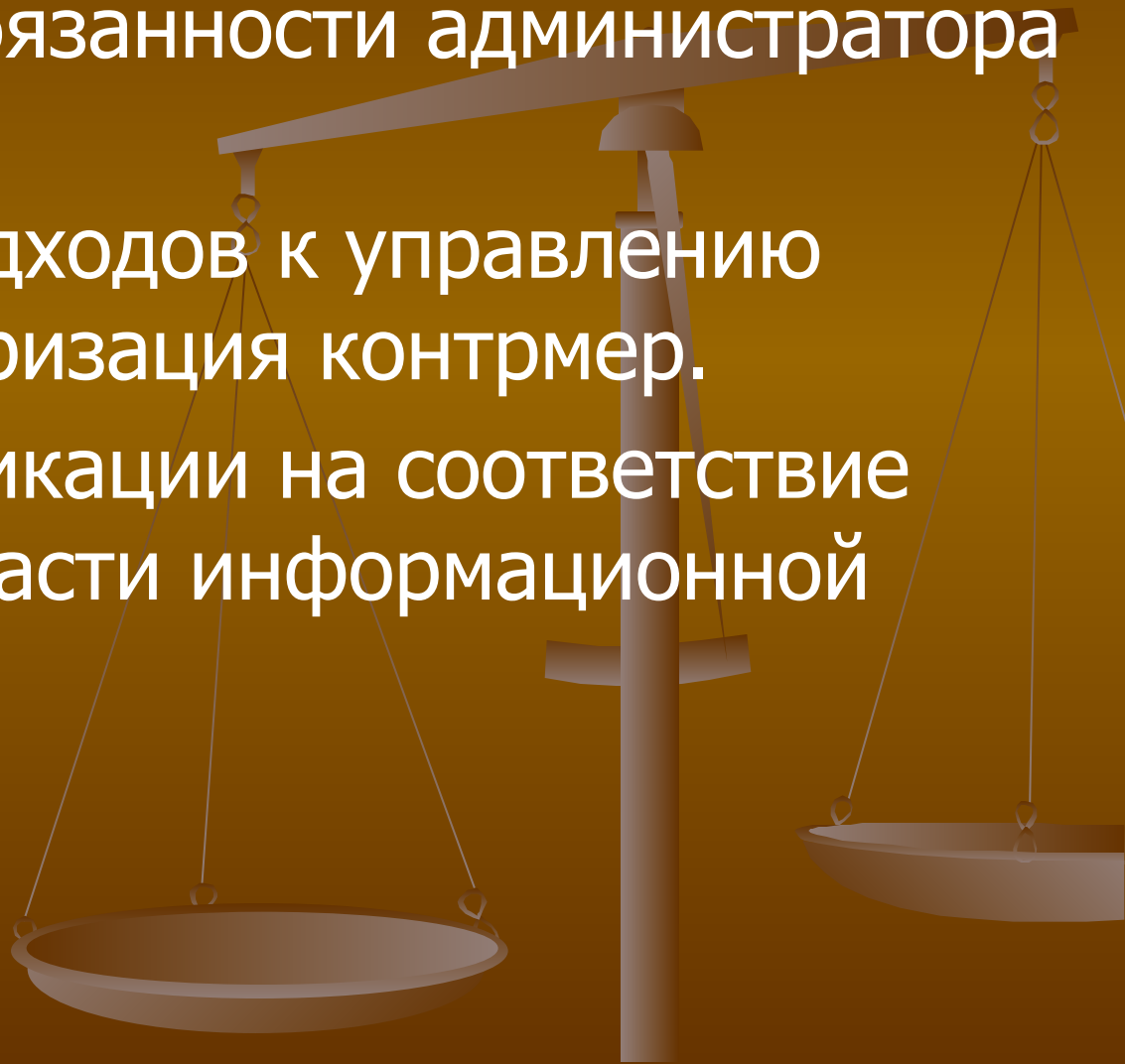
ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 2. Организационные меры обеспечения информационной безопасности компьютерных систем

Учебные вопросы

1. Роль задачи и обязанности администратора безопасности.
2. Определение подходов к управлению рисками, структуризация контрмер.
3. Порядок сертификации на соответствие стандартам в области информационной безопасности.



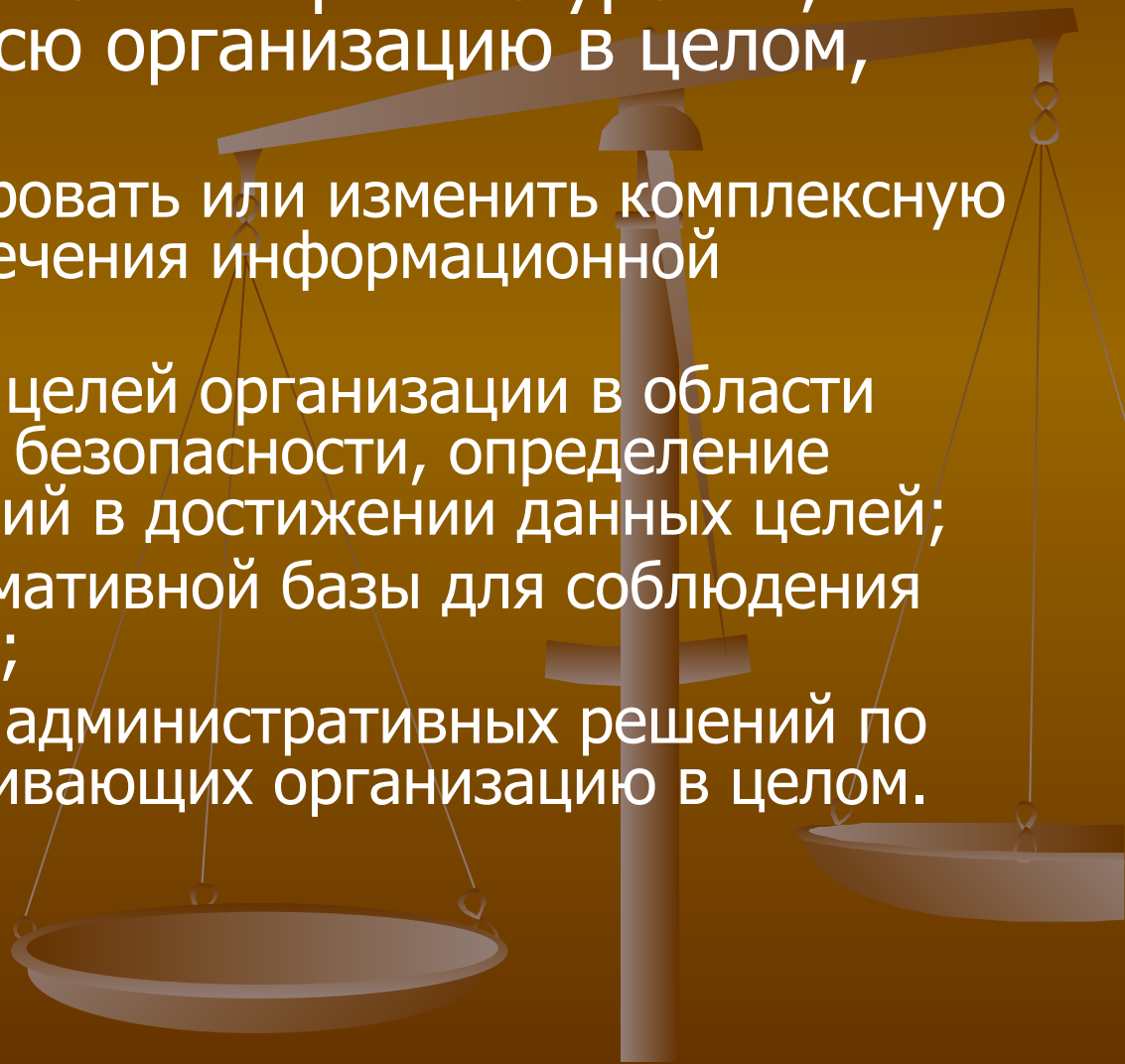
- **Администратор защиты** *(Security administrator)* — это субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации (по руководящему документу «Защита от несанкционированного доступа к информации: Термины и определения»).
- Администратор защиты — сотрудник, должностные обязанности которого подразумевают обеспечение штатной работы парка компьютерной техники, сети и программного обеспечения в организации.
- Администраторы защиты — это основные люди, которые противостоят атакам взломщиков и позволяют безопасно общаться внутри инфраструктуры компании, а также за её пределами. По сути администратор защиты тоже в какой-то мере компьютерный взломщик, так как он должен знать все те приемы взлома и обхода защиты (например брандмауэраАдминистраторы защиты — это основные люди, которые противостоят атакам взломщиков и позволяют безопасно общаться внутри инфраструктуры компании, а также за её пределами. По сути администратор защиты тоже в какой-то мере компьютерный взломщик, так как он должен знать все те приемы взлома и обхода защиты (например брандмауэра), которые применяют взломщики. Однако в большинстве организаций, в обязанности администратора защиты входит не только слежение за сетевой безопасностью организации, а также и другие сопутствующие проблемы: борьба с вирусами, настройка пользовательского программного обеспечения и прочее. Занимается администратор безопасности, соответственно, проблемами информационной безопасности. Работает, как правило, в аутсорсинговой компании либо крупной компании, корпорации. Особенно хорошо разбирается в протоколах шифрования и аутентификации и их практическом применении (VPNАдминистраторы защиты — это основные

Административный уровень защиты информации

- Под **административным уровнем** информационной безопасности относятся действия общего характера, предпринимаемые руководством организации к обеспечению защиты информации.
- Главная цель – формирование политики безопасности, отражающей подход организации к защите данных.
- Политика безопасности административного уровня – совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.
- Выработку политики безопасности и ее содержание рассматривают на трех горизонтальных уровнях детализации:
  - Верхний уровень – вопросы, относящийся к организации в целом;
  - Средний уровень – вопросы, касающиеся отдельных аспектов ИБ;
  - Нижний уровень – вопросы относящиеся к конкретным сервисам;

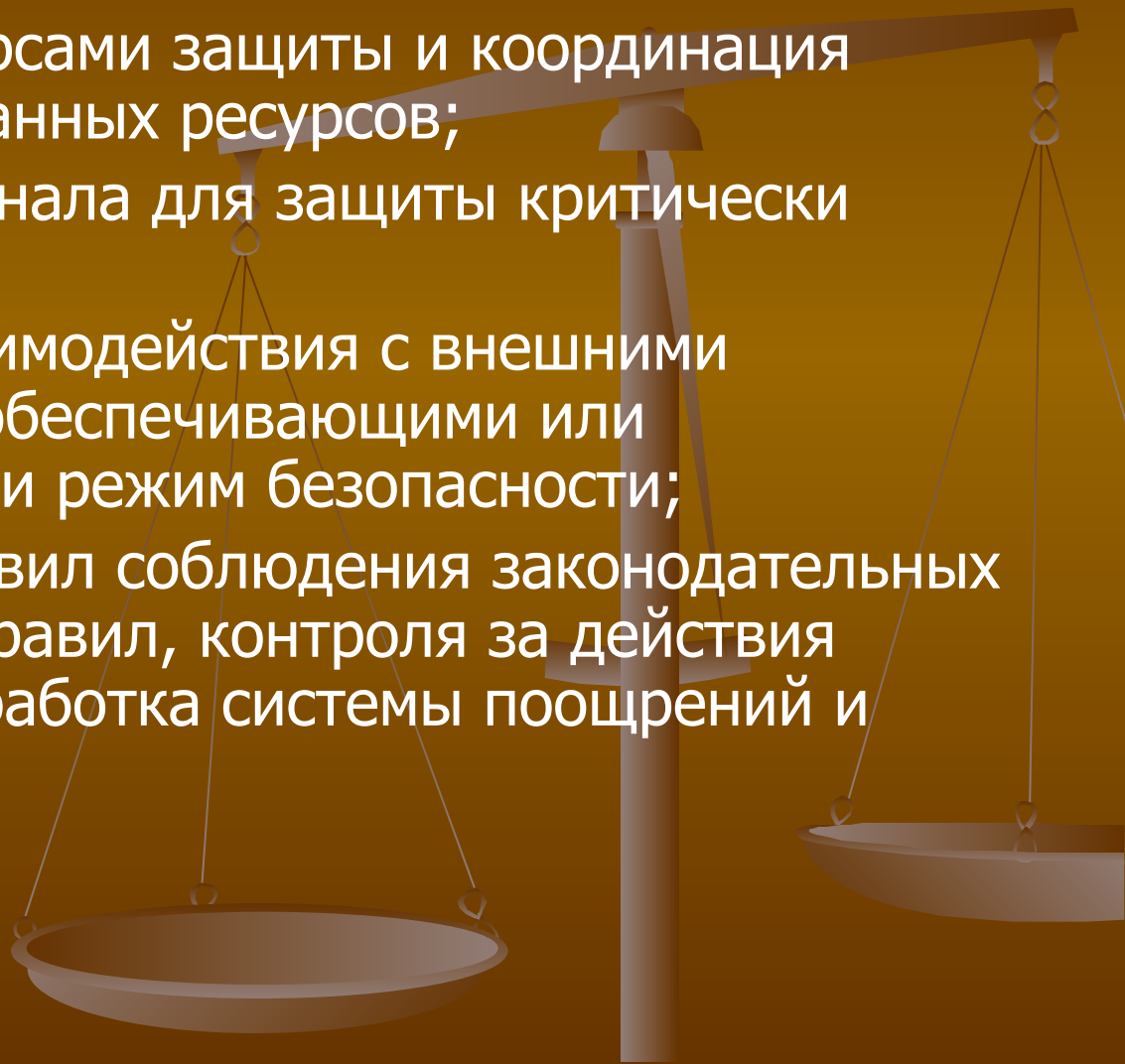
Политика безопасности верхнего уровня

- Политика безопасности верхнего уровня, затрагивающая всю организацию в целом, включает в себя:
  - решение сформировать или изменить комплексную программу обеспечения информационной безопасности;
  - формулирование целей организации в области информационной безопасности, определение общих направлений в достижении данных целей;
  - обеспечение нормативной базы для соблюдения законов и правил;
  - формулирование административных решений по вопросам, затрагивающих организацию в целом.



Политика безопасности верхнего уровня

- На данном уровне выносится:
  - управление ресурсами защиты и координация использования данных ресурсов;
  - выделение персонала для защиты критически важных систем;
  - определение взаимодействия с внешними организациями, обеспечивающими или контролирующими режим безопасности;
  - определение правил соблюдения законодательных и нормативных правил, контроля за действия сотрудников, выработка системы поощрений и наказаний.

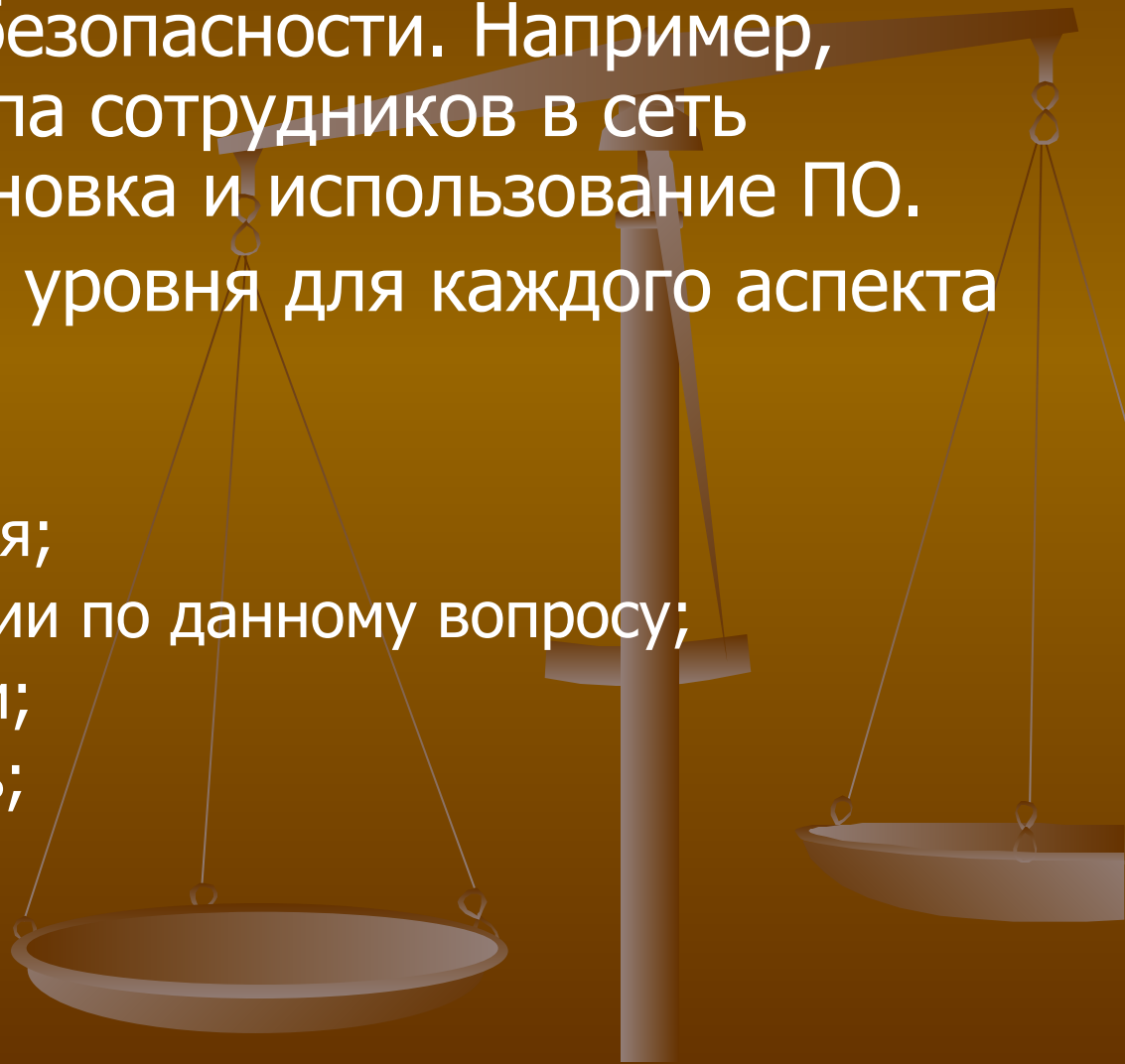


Рекомендации к политике безопасности верхнего уровня

- Британский стандарт BS 7799:1995 рекомендует следующие разделы в документ, характеризующий политику безопасности:
  - вводный, подтверждающий озабоченность руководства проблемами ИБ;
  - организационный, содержащий описание подразделений, ответственных за ИБ;
  - классификационный, описывающий имеющиеся ресурсы и уровень требуемый уровень защиты;
  - штатный, характеризующий меры безопасности применительно к персоналу;
  - раздел, относящийся к вопросам физической защиты;
  - раздел, относящийся к управлению компьютерами и сетями;
  - раздел, описывающий правила разграничения доступа к служебной информации;
  - раздел, характеризующий порядок разработки и сопровождения ИС;
  - раздел, описывающий меры, направленные на обеспечение непрерывности в работе;
  - юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству.

Политика безопасности среднего уровня

- К среднему уровню относят вопросы, относящиеся к отдельным аспектам информационной безопасности. Например, организация доступа сотрудников в сеть Интернет или установка и использование ПО.
- Политика среднего уровня для каждого аспекта должна освещать:
  - описание аспекта;
  - область применения;
  - позиция организации по данному вопросу;
  - роли и обязанности;
  - законопослушность;
  - точки контакта.

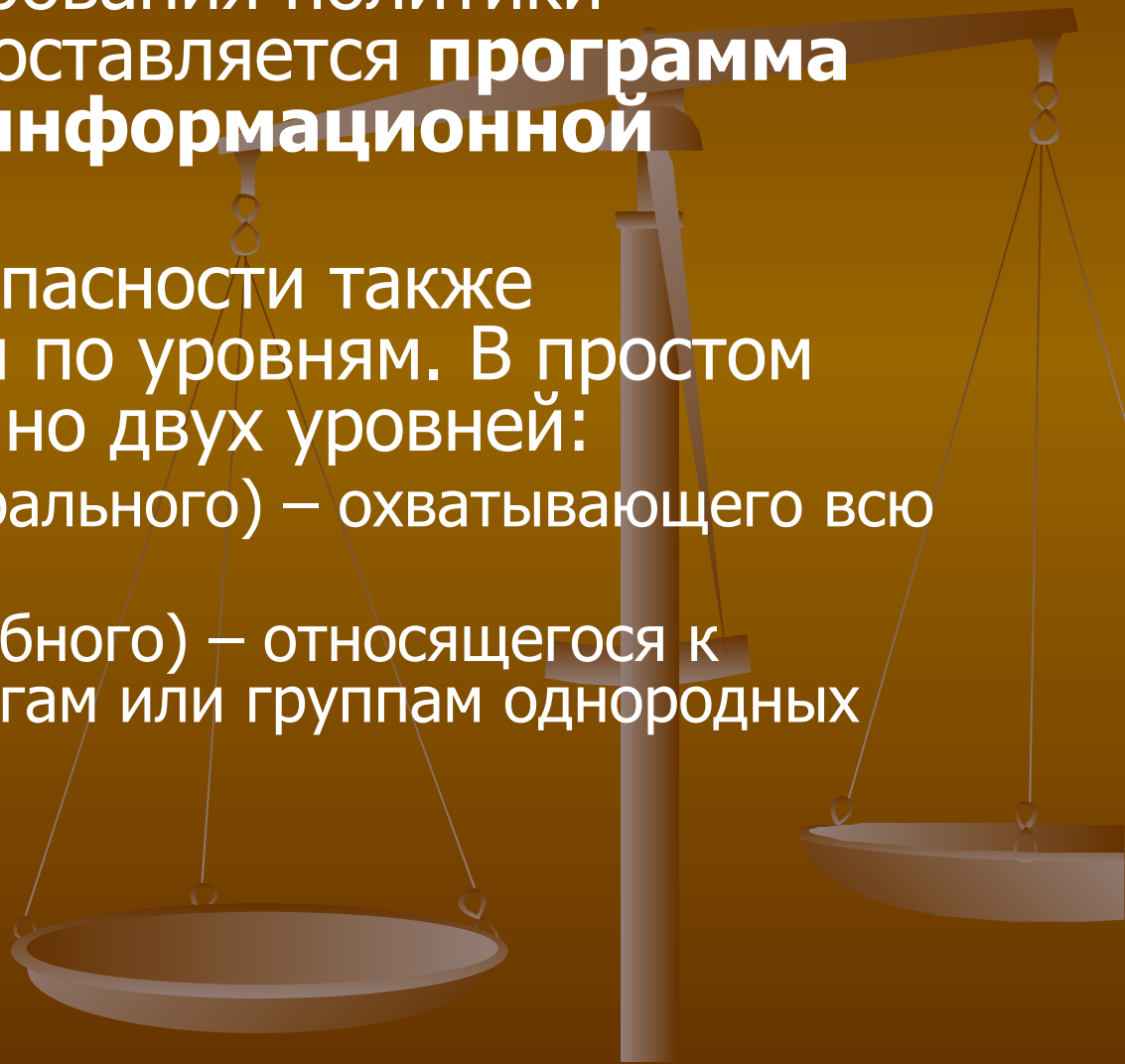


Политика безопасности нижнего уровня

- Политика безопасности нижнего уровня относится к работе конкретных информационных сервисов.
- Такая политика включает в себя два аспекта:
  - цели;
  - правила достижения заданных целей.
- Политика безопасности данного уровня быть выражена полно, четко и конкретно. Например, определять сотрудников, имеющих право на работу с конкретной информационной системой и данными.
- Из целей выводятся правила безопасности, описывающие кто, что и при каких условиях может выполнять те или иные процедуры с информационными сервисами.

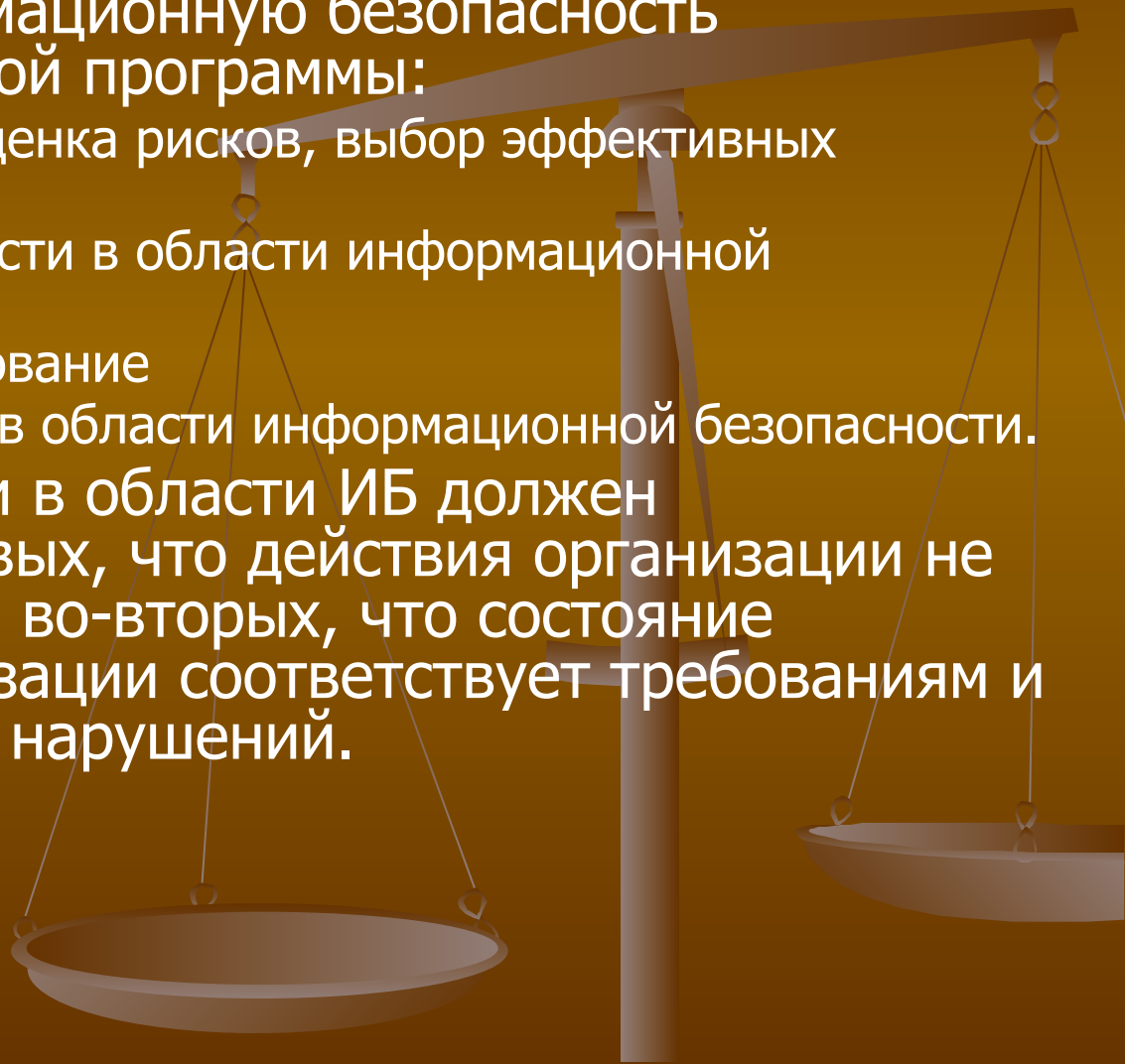
Административный уровень защиты информации

- После формулирования политики безопасности, составляется **программа обеспечения информационной безопасности**.
- Программа безопасности также структурируется по уровням. В простом случае достаточно двух уровней:
  - верхнего (центрального) – охватывающего всю организацию;
  - нижнего (служебного) – относящегося к отдельным услугам или группам однородных сервисов.



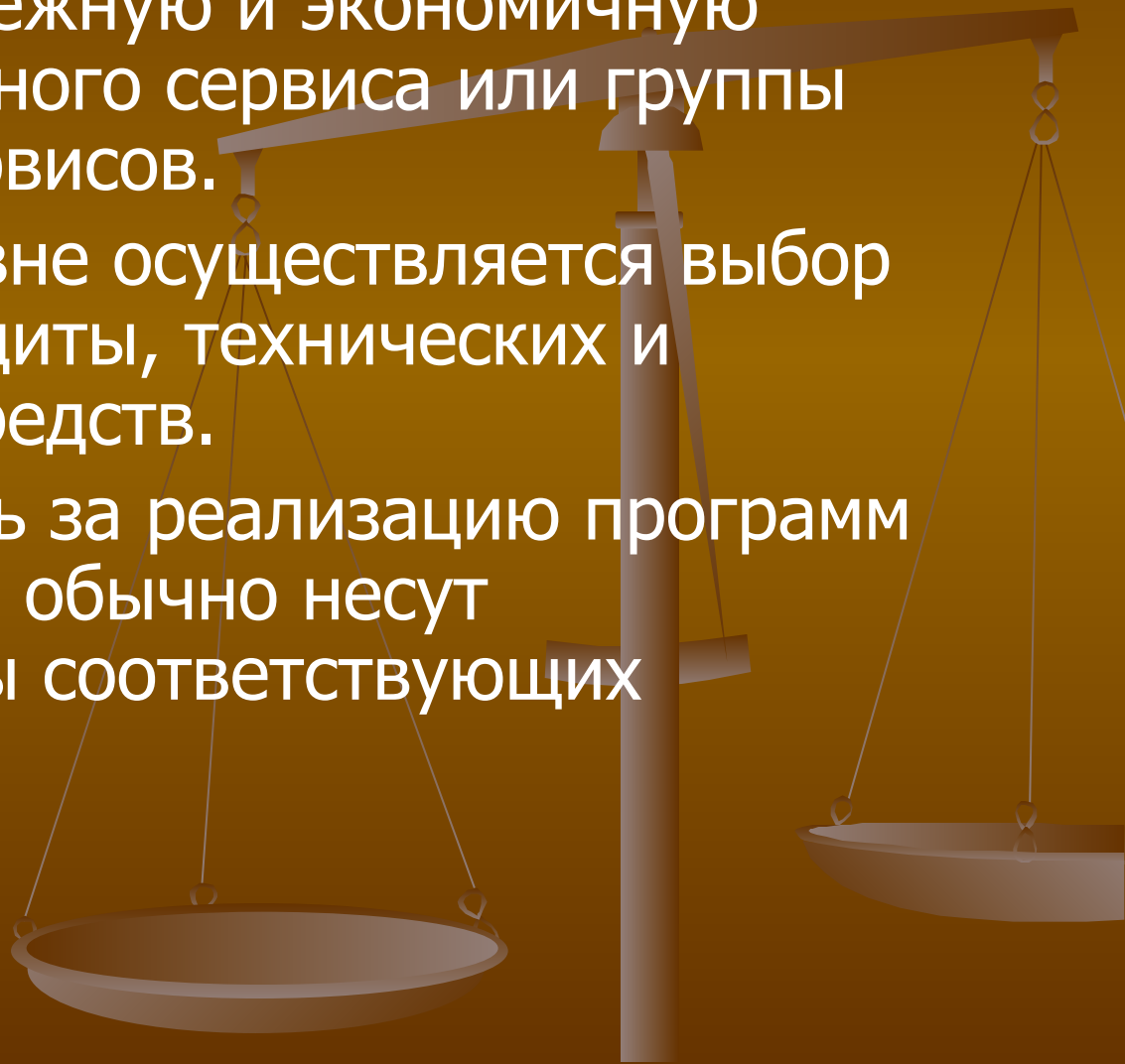
Программа верхнего уровня

- Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. Цели такой программы:
  - Управление рисками (оценка рисков, выбор эффективных решений);
  - Координация деятельности в области информационной безопасности
  - Стратегическое планирование
  - Контроль деятельности в области информационной безопасности.
- Контроль деятельности в области ИБ должен гарантировать, во-первых, что действия организации не противоречат законам, во-вторых, что состояние безопасности в организации соответствует требованиям и реагировать на случаи нарушений.



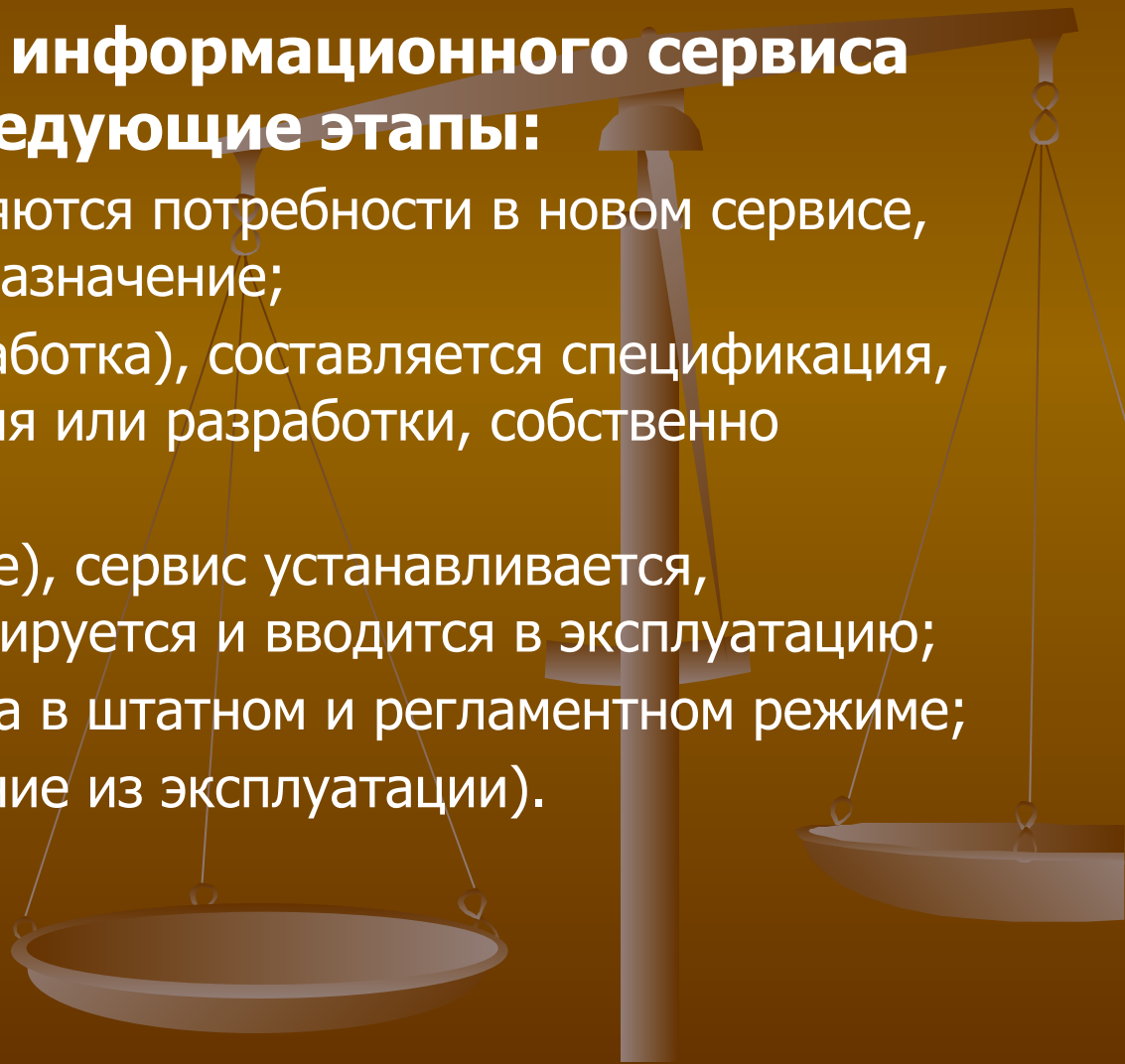
Программы служебного уровня

- Цель программы нижнего уровня – обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов.
- На нижнем уровне осуществляется выбор механизмов защиты, технических и программных средств.
- Ответственность за реализацию программ нижнего уровня обычно несут администраторы соответствующих сервисов.



Синхронизация программы безопасности с жизненным циклом системы

- **В жизненном цикле информационного сервиса можно выделить следующие этапы:**
  - **инициация**, определяются потребности в новом сервисе, документируется его назначение;
  - **приобретение** (разработка), составляется спецификация, варианты приобретения или разработки, собственно приобретение;
  - **установка** (внедрение), сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию;
  - **эксплуатация**, работа в штатном и регламентном режиме;
  - **утилизация** (выведение из эксплуатации).



Оценка критичности информационного сервиса

- Для обеспечения безопасной работы сервиса в рамках информационной системы на всех этапах жизненного цикла должны быть рассмотрены вопросы:
  - Какая информация предназначена для обслуживания?
  - Какие возможные последствия от реализации угроз ИБ а данном сервисе?
  - Каковы особенности данного сервиса?
  - Каковы характеристики персонала, имеющие отношения к информационной безопасности?
  - Каковы угрозы, по отношению к которым сервисы и информация наиболее уязвимы?
  - Каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?
- Результаты оценки критичности – отправная точка для составления спецификации.

2. Определение подходов к управлению рисками, структуризация контрмер.

- Безопасность информационных технологий (ИТ) и систем (ИС) является одной из главных составляющих проблемы обеспечения безопасности организации.
- Одним из важнейших аспектов реализации политики ИБ является анализ угроз, оценка их достоверности и тяжести вероятных последствий. Реально риск появляется там, где есть вероятность осуществления угрозы, при этом величина риска прямо пропорциональна величине этой вероятности (рис. 1).

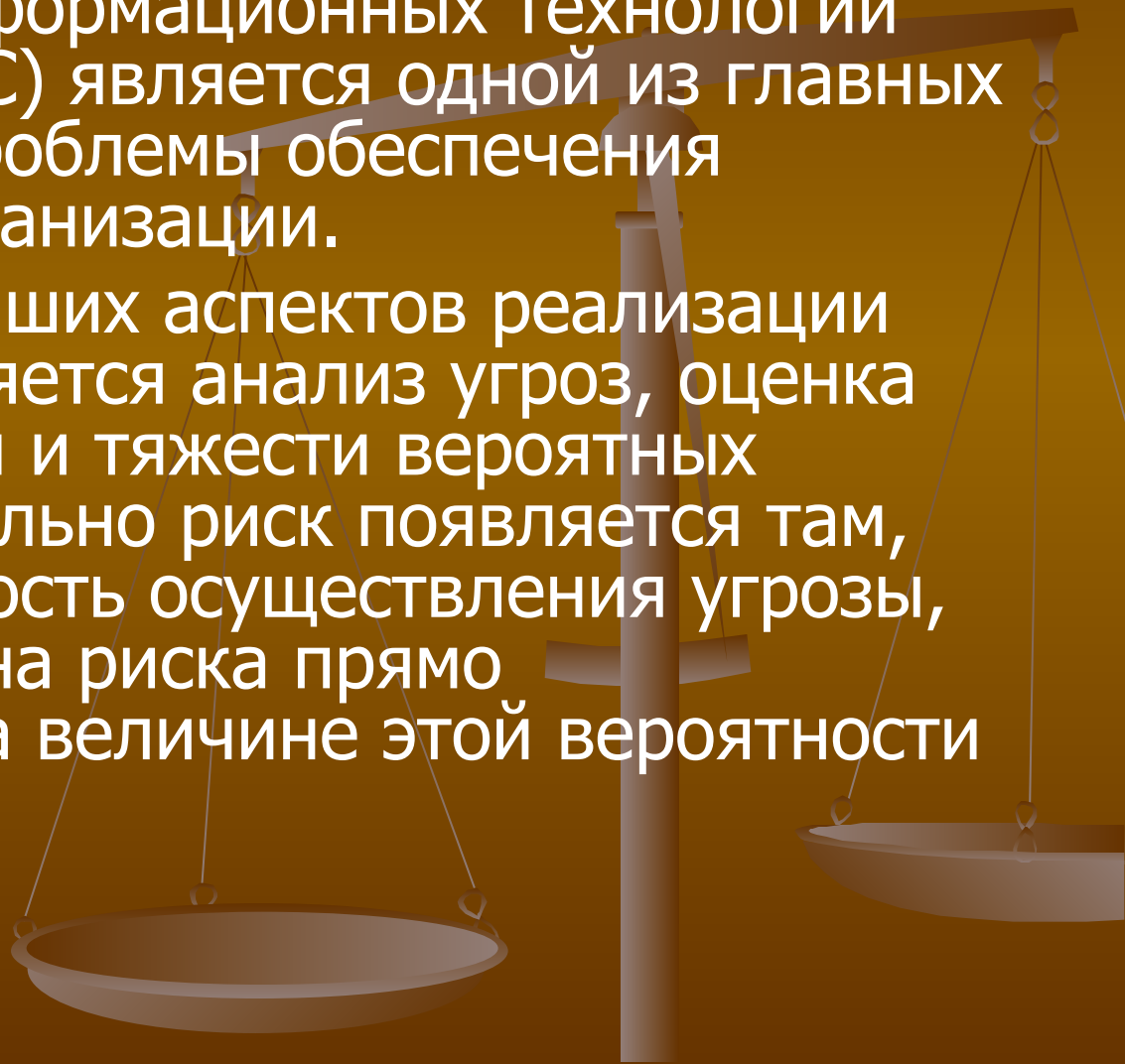


Рис. 1 Неопределенность как основа формирования риска

Целесообразно выявлять не только сами угрозы, но и источники их возникновения — это поможет правильно оценить риск и выбрать соответствующие меры нейтрализации.

- Для противодействия каждому способу нелегального входа нужны свои механизмы безопасности. После идентификации угрозы необходимо оценить вероятность ее осуществления и размер потенциального ущерба.
- Оценивая тяжесть ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдаленные, в частности подрыв репутации компании, ослабление её позиций на рынке и т. п.

- После проведения идентификации и анализа угроз, их возможных последствий имеется несколько подходов к управлению: оценка риска, уменьшение риска, уклонение от риска, изменение характера риска, принятие риска, выработка корректирующих мероприятий (**Рис. 2.**).

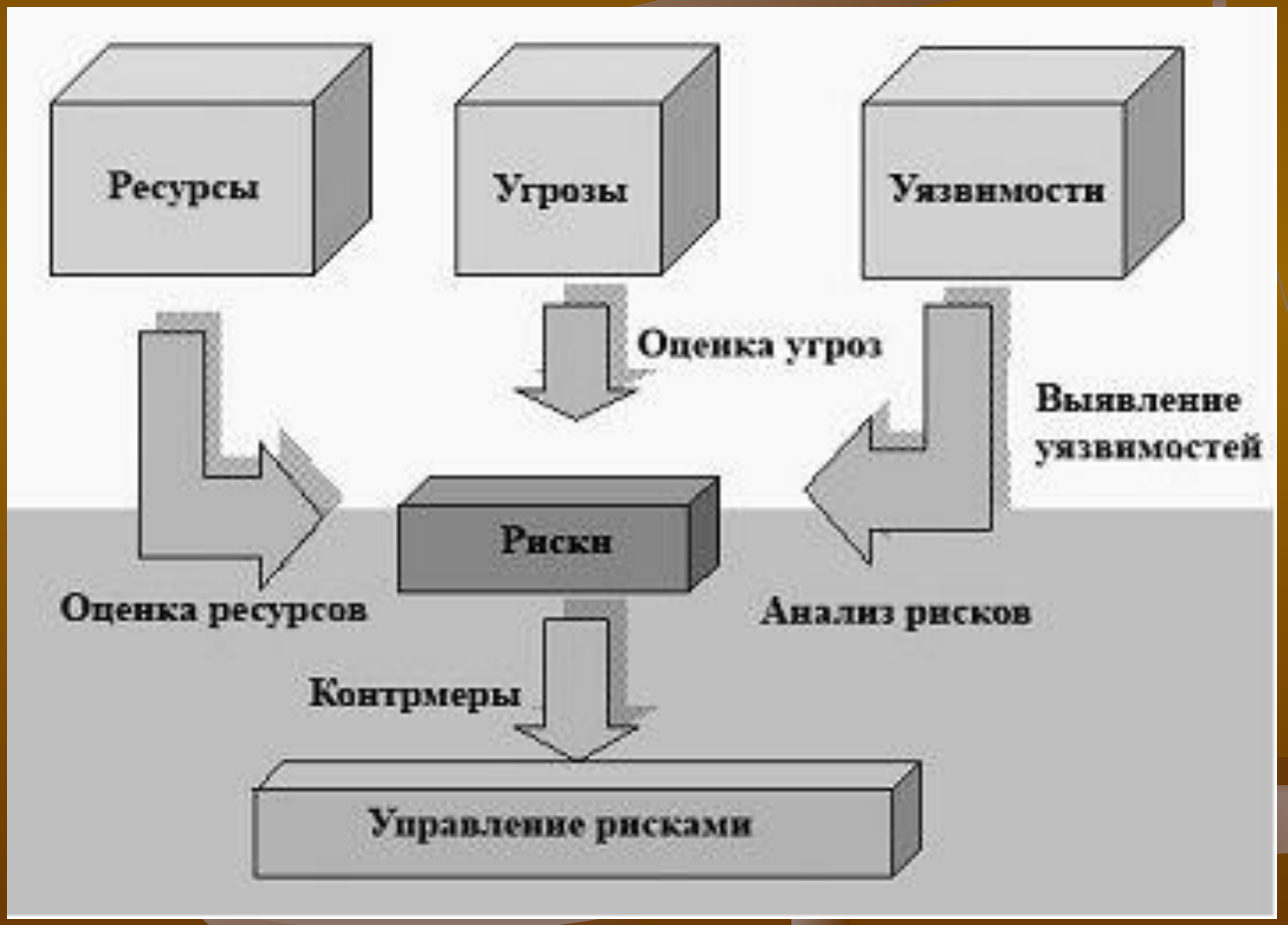


Рис. 2. Схема управления рисками

- При идентификации активов и информационных ресурсов, подлежащих защите, следует учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, в том числе текущий рейтинг и репутацию компании. Одним из главных результатов идентификации является получение детальной информационной структуры организации и способов ее использования.
- Выбор анализируемых объектов и степень детальности их рассмотрения — следующий шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру, для крупной — следует сосредоточиться на наиболее важных (критичных) сервисах. Если важных сервисов много, то выбираются те из них, риски для которых заведомо велики или неизвестны. Если информационной основой организации является локальная сеть, то в число аппаратных объектов следует включить компьютеры, периферийные устройства, внешние интерфейсы, кабельное хозяйство и активное сетевое оборудование.
- К программным объектам следует отнести операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, программы управления сетью и отдельными подсистемами. Важно зафиксировать в каких узлах сети хранится программное обеспечение, где и как используется. Третьим видом информационных объектов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, а также способы доступа к ним. Все это важно для оценки рисков и последствий нарушений информационной безопасности.

- Оценка рисков производится на основе накопленных исходных данных и оценки степени определенности угроз. Часто применяют такой метод, как умножение вероятности осуществления угрозы на величину предполагаемого ущерба. (Если для вероятности и ущерба использовать трехбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвертый — к среднему, два последних — к высокому. По этой шкале можно оценивать приемлемость рисков.)
- Если какие-либо риски оказались недопустимо высокими, необходимо реализовать дополнительные защитные меры.
- Технология оценки рисков должна сочетать формальные метрики и формирование реальных количественных показатели для оценки. С их помощью необходимо ответить на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства экономически выгодно использовать.
- **Методология снижения рисков**. Многие риски можно существенно уменьшить путем использования простых и недорогих контрмер. Например, грамотное (регламентированное) управление доступом снижает риск несанкционированного вторжения. От некоторых классов рисков можно уклониться — вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов. Некоторые риски не могут быть уменьшены до малой величины, однако после реализации стандартного набора контрмер их можно принять, постоянно контролируя остаточную величину риска.
- Оценка стоимости защитных мер должна учитывать не только прямые расходы на закупку оборудования и/или программного обеспечения, но и расходы на внедрение новинки, обучение и переподготовку персонала и т. д.
- Управление рисками является многоступенчатым итерационным процессом (рис. 3).

- **Методология снижения рисков**. Многие риски можно существенно уменьшить путем использования простых и недорогих контрмер. Например, грамотное (регламентированное) управление доступом снижает риск несанкционированного вторжения. От некоторых классов рисков можно уклониться — вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов. Некоторые риски не могут быть уменьшены до малой величины, однако после реализации стандартного набора контрмер их можно принять, постоянно контролируя остаточную величину риска.
- Оценка стоимости защитных мер должна учитывать не только прямые расходы на закупку оборудования и/или программного обеспечения, но и расходы на внедрение новинки, обучение и переподготовку персонала и т. д.
- Управление рисками является многоступенчатым итерационным процессом (рис. 3).

- **Методология снижения рисков**. Многие риски можно существенно уменьшить путем использования простых и недорогих контрмер. Например, грамотное (регламентированное) управление доступом снижает риск несанкционированного вторжения. От некоторых классов рисков можно уклониться — вынесение Web-сервера организации за пределы локальной сети позволяет избежать риска несанкционированного доступа в локальную сеть со стороны Web-клиентов. Некоторые риски не могут быть уменьшены до малой величины, однако после реализации стандартного набора контрмер их можно принять, постоянно контролируя остаточную величину риска (рис. 3.).

Рис. 3. Схема оценки и снижения рисков

- Оценка стоимости защитных мер должна учитывать не только прямые расходы на закупку оборудования и/или программного обеспечения, но и расходы на внедрение новинки, обучение и переподготовку персонала и т. д.
- Управление рисками является многоступенчатым итерационным процессом (рис. 4).

Рис. 4. Итерационный процесс управления рисками

Отработка рисков включает в себя ряд важных этапов, которые в обязательном порядке включаются в плановую работу по обеспечению информационной безопасности (рис. 5.).

Рис. 5. Этапы отработка риска

На практике методики управления рисками позволяют:

- создавать модели информационных активов организации с точки зрения безопасности;
- классифицировать и оценивать ценности активов;
- составлять списки наиболее значимых угроз и уязвимостей безопасности;
- ранжировать угрозы и уязвимости безопасности;
- оценивать и отрабатывать риски;
- разрабатывать корректирующие меры;
- обосновывать средства и меры контроля рисков;
- оценивать эффективность/стоимость различных вариантов защиты;
- формализовать и автоматизировать процедуры оценивания и управления рисками.

Применение соответствующих программных средств позволяет уменьшить трудоемкость проведения анализа рисков и выбора контрмер. В настоящее время разработано большое количество программных продуктов для анализа и управления рисками базового уровня безопасности. Примером достаточно простого средства является программный пакет BSS (Baseline Security Survey, UK).

- В основе методов, подобных CRAMM, лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит как для больших, так и для мелких организаций, как правительственного, так и коммерческого сектора.
- К сильным сторонам метода CRAMM относится следующее:

I. CRAMM является хорошо структурированным и широко опробованным методом анализа рисков, позволяющим получать реальные практические результаты;

II. программный инструментарий CRAMM может использоваться на всех стадиях проведения аудита безопасности ИС;

III. в основе программного продукта лежит достаточно объемная база знаний по контрмерам в области информационной безопасности, базирующаяся на рекомендациях стандарта BS 7799;

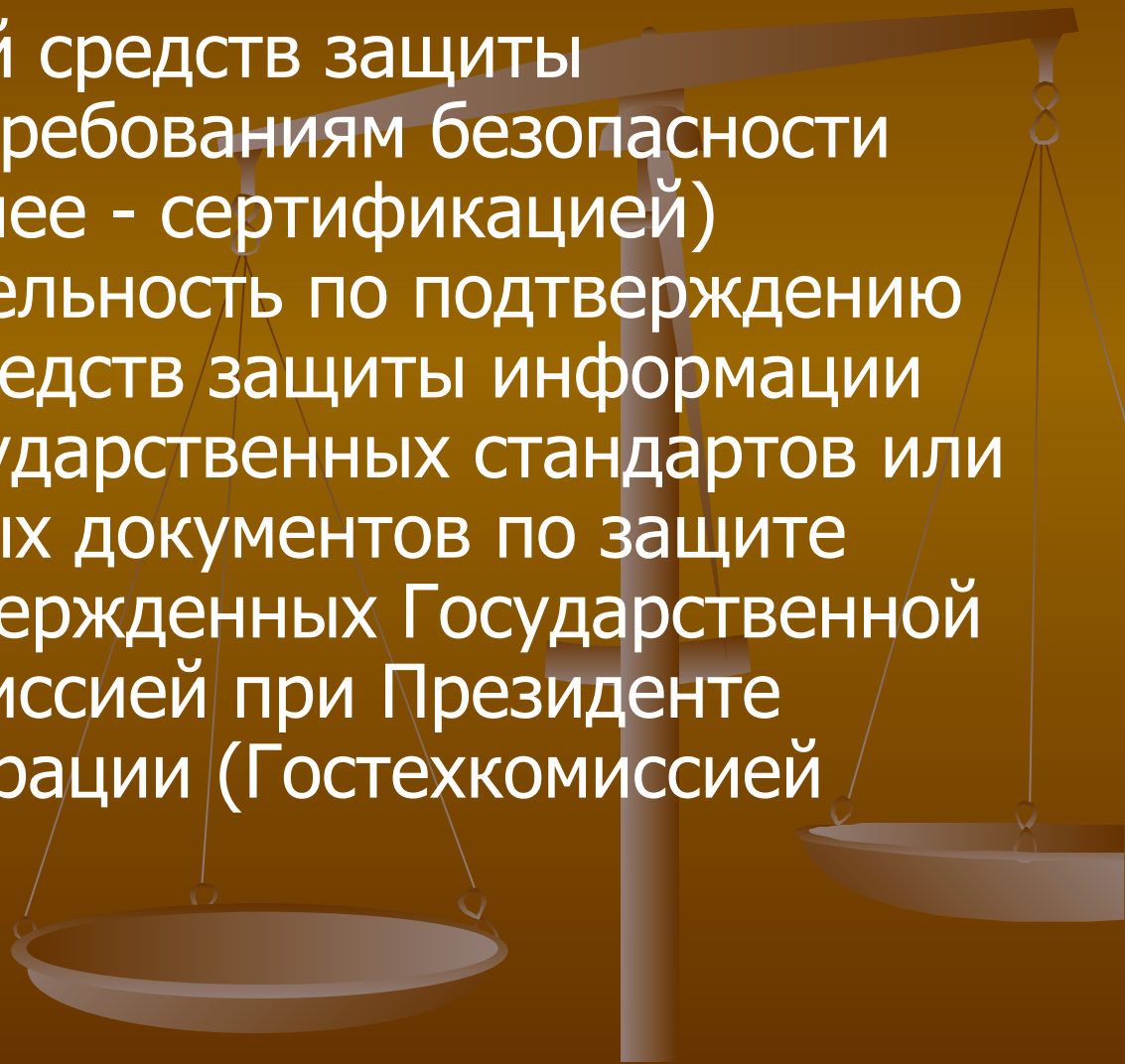
IV. гибкость и универсальность метода CRAMM позволяет использовать его для аудита ИС любого уровня сложности и назначения;

V. CRAMM можно использовать в качестве инструмента для разработки плана непрерывности бизнеса и политик информационной безопасности организации;

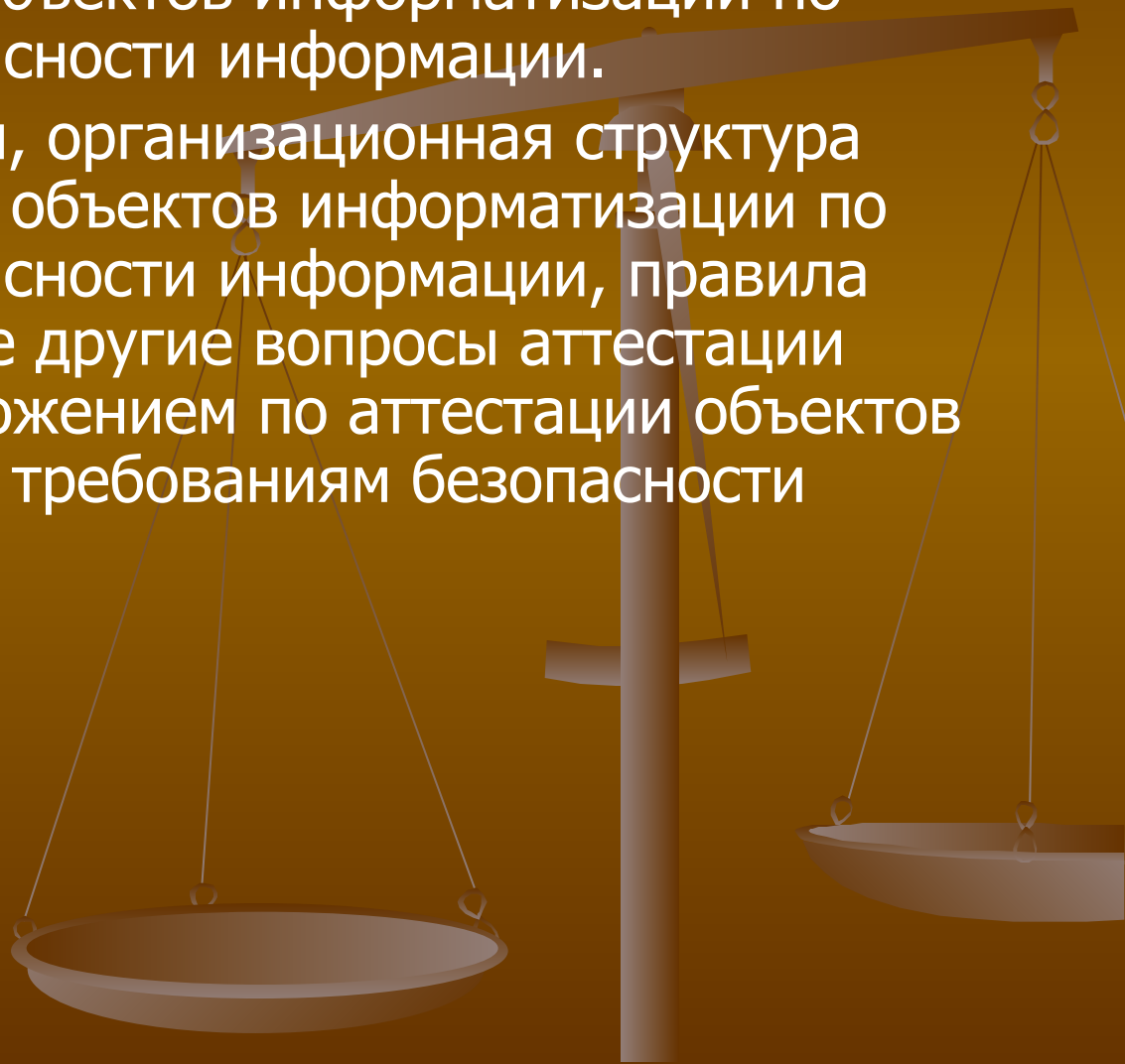
VI. CRAMM может использоваться в качестве средства документирования механизмов безопасности ИС.

3. Порядок сертификации на соответствие стандартам в области информационной безопасности.

Под сертификацией средств защиты информации по требованиям безопасности информации (далее - сертификацией) понимается деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией России).



- Система сертификации средств защиты информации по требованиям безопасности информации включает в себя аттестацию объектов информатизации по требованиям безопасности информации.
- Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации, правила проведения, а также другие вопросы аттестации определяются “Положением по аттестации объектов информатизации по требованиям безопасности информации”.



Целями создания системы сертификации являются:

- реализация требований статьи 28 Закона Российской Федерации “О государственной тайне”;
- реализация требований государственной системы защиты информации в Российской Федерации от технических разведок и от ее утечки по техническим каналам;
- создание условий для качественного и эффективного обеспечения потребителей сертифицированной техникой защиты информации;
- обеспечение национальной безопасности Российской Федерации в информационной сфере;
- содействие формированию рынка защищенных информационных технологий и средств их обеспечения;
- формирование и осуществление единой научно-технической и промышленной политики в информационной сфере с учетом современных требований по противодействию техническим разведкам и технической защите информации.

- Сертификация средств защиты информации осуществляется федеральным и аккредитованными органами по сертификации. Сертификационные испытания проводятся аккредитованными испытательными центрами (лабораториями) на их материально-технической базе. В отдельных случаях по согласованию с федеральным органом по сертификации (или органом по сертификации) допускается проведение испытаний на испытательной базе заявителя данного средства защиты информации.
- Правила аккредитации определяются действующим в системе “Положением об аккредитации испытательных центров (лабораторий) и органов по сертификации средств защиты информации”.
- Организационную структуру системы сертификации образуют:

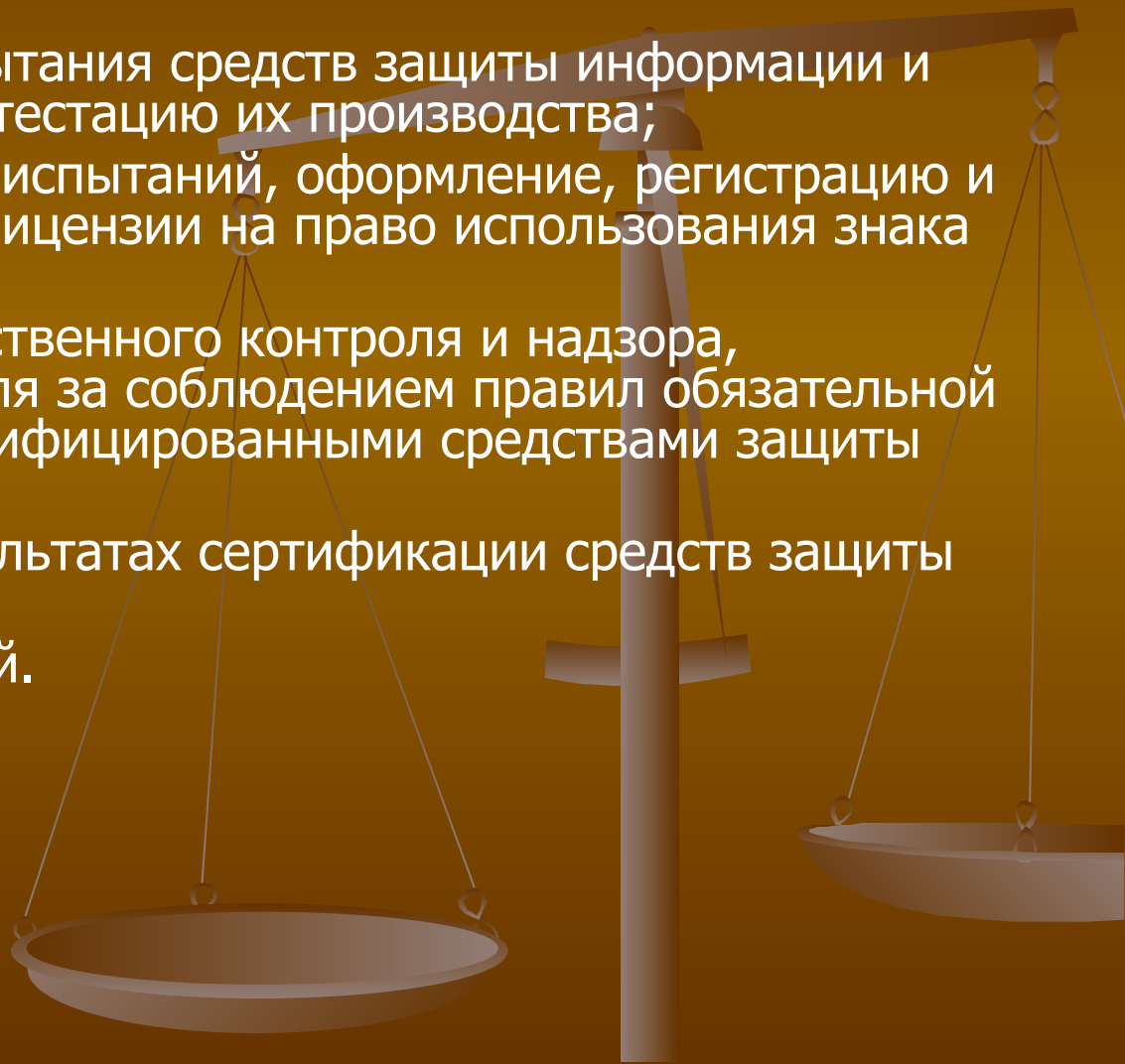
- федеральный орган по сертификации средств защиты информации (Гостехкомиссия России);
- центральный орган системы сертификации средств защиты информации;
- органы по сертификации средств защиты информации;
- испытательные центры (лаборатории);
- заявители.

Органы по сертификации средств защиты информации в пределах установленной области аккредитации:

- участвуют в определении схемы проведения сертификации средств защиты информации с учетом предложений заявителя;
- уточняют требования, на соответствие которым проводятся сертификационные испытания;
- рекомендуют заявителю испытательный центр (лабораторию);
- утверждают программы и методики проведения сертификационных испытаний;
- проводят экспертизу технической, эксплуатационной документации на средства защиты информации и материалов сертификационных испытаний;
- оформляют экспертное заключение по сертификации средств защиты информации и представляют их в федеральный орган по сертификации;
- организуют, при необходимости, предварительную проверку (аттестацию) производства сертифицируемых средств защиты информации;
- участвуют в аккредитации испытательных центров (лабораторий) и органов по аттестации объектов информатизации;
- организуют инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации и участвуют в инспекционном контроле за деятельностью испытательных центров (лабораторий);
- хранят документацию (оригиналы), подтверждающую сертификацию средств защиты информации;
- ходатайствуют перед федеральным органом по сертификации о приостановке или отмене действия выданных сертификатов;
- формируют и актуализируют фонд нормативных и методических документов, необходимых для сертификации, участвуют в их разработке;
- представляют заявителю необходимую информацию по сертификации.

Процедура сертификации включает:

- подачу и рассмотрение заявки на проведение сертификации (продление срока действия сертификата) средств защиты информации;
- сертификационные испытания средств защиты информации и (при необходимости) аттестацию их производства;
- экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия;
- осуществление государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации;
- информирование о результатах сертификации средств защиты информации;
- рассмотрение апелляций.



- По результатам контроля федеральный орган может приостановить или аннулировать действие сертификата и аттестата аккредитации, а орган по сертификации - ходатайствовать об этом. Решение об аннулировании действия сертификата принимается только в том случае, если в результате принятых незамедлительных мер не может быть восстановлено соответствие средств защиты информации установленным требованиям. Причинами, которые могут заставить принять такое решение, являются:
- изменение нормативных и методических документов по защите информации в части требований к средствам защиты информации, методам испытаний и контроля;
- изменение технологии изготовления, конструкции (состава), комплектности средств защиты информации и системы контроля их качества;
- невыполнение требований технологии изготовления, контроля и испытаний средств защиты информации;
- несоответствие сертифицированных средств защиты информации техническим условиям или формуляру, выявленное в ходе государственного или инспекционного контроля;
- отказ заявителя в допуске (приеме) лиц, уполномоченных осуществлять государственный контроль и надзор, инспекционный контроль за соблюдением правил сертификации и за сертифицированными средствами защиты информации.