ВОПРОСЫКЗАЧЕТУ

1. Охарактеризуйте место и роль автоматизированных систем в управлении бизнес-процессами.

Автоматизация на основе современных ИТ позволяет принимать решения более оперативно и обоснованно, учитывая при этом большой объем сведений, повышая качество и эффективность управления — управления чем бы то ни было — от отдельных узлов и агрегатов, деятельностью отдельных людей до технологических процессов на производстве, бизнес-процессов компаний, экономических и социально-политических процессов в обществе.

1. Какие факторы определяют актуальность проблемы защиты АС в современных условиях?

* Обострением противоречий между потребностями общества в расширении свободного обмена информацией и чрезмерными ограничениями на ее распространение и использование;
* расширением сферы применения ЭВМ;
* повышением уровня доверия к АСУ и обработки информации,;
* вовлечением в процесс информационного взаимодействия все большего числа людей и организаций;
* концентрацией больших объемов информации различного назначения;
* количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;
* отношением к информации как к товару информационных услуг;
* многообразием видов угроз и возникновением новых каналов несанкционированного доступа к информации;
* увеличением числа квалифицированных пользователей средствами вычислительной техники;
* возрастанием уязвимости субъектов;
* развитием рыночных отношений в сфере ИТ.

1. Перечислите особенности современных автоматизированных систем как объектов защиты.
   * территориальная разносность компонентов АС
   * широкий спектр способов представления, хранения и передачи информации
   * участие в процессе автоматизированной обработки информации большого количества пользователей и персонала;
   * непосредственный и одновременный доступ к ресурсам большого числа пользователей;
   * разнородность средств вычислительной техники и связи;
   * отсутствие специальных средств защиты в большинстве типов технических средств, широко используемых в АС.
2. Назовите причины обострения проблемы обеспечения информационной безопасности.

* расширение сферы применения СВТ и возросший уровень доверия к автоматизированным системам управления и обработки информации;
* переход к рыночным отношениям в области создания и предоставления информационных услуг;
* развитие и распространение информационно-телекоммуникационных сетей;
* распространение компьютерной грамотности в широких слоях населения из-за доступности СВТ и прежде всего ПК;
* отсутствие стройной и непротиворечивой системы законодательно-правового регулирования отношений в сфере накопления, использования и защиты информации;
* бурное развитие и широкое распространение компьютерных вирусов;
* наличие злоумышленников.

1. Почему проблема обеспечения безопасности АС относится к числу трудноразрешимых?

* Недостаточное понимание необходимости защиты используемых АС;
* Высокая степень неопределенности рисков при применении новейших АС;
* Сложность АС как объектов защиты;
* Необходимость комплексного подхода к защите АС с учетом их значительной зависимости от человеческого фактора;
* Сложность разрешения конфликтов интересов между различными категориями субъектов;
* Отставанием методов и средств защиты от развития информационных технологий, а также методов и средств нападения;
* Недостатком квалифицированных специалистов в сфере компьютерной безопасности и низким уровнем компьютерной культуры пользователей.

1. Что понимается под риском информационной безопасности? Каковы составляющие риска?

**Риск** — это оценка опасности определенной угрозы.

Риск выражает вероятностно-стоимостную оценку возможных потерь(ущерба)и характеризуется:

* Вероятностью успешной реализации угрозы;
* Стоимостью потерь(ущерба) в случае реализации угрозы.



1. В чем заключается анализ рисков и управление ими? Перечислите этапы анализа и управления.

Анализ рисков заключается в выявлении существующих угроз и оценке их опасности. На этапе анализа рисков выявляют все значимые угрозы, т. е. угрозы, характеризующиеся большой частотой реализации или приводящие к существенным потерям.

Управление рисками предполагает принятие мер защиты, направленных на снижение частоты успешной реализации угроз и/или ущерба в случае их реализации.

Основные этапы анализа рисков и управления ими:

* Определение границ системы и методологи и оценки рисков;
* Идентификация и оценка информационных ресурсов системы;
* Идентификация угроз и оценка вероятностей их реализации;
* Определение риска и выбор средств защиты;
* Внедрение средств защиты и оценка остаточного риска.

1. Каковы требования к методам оценки целесообразности затрат на обеспечение безопасности АС?

* Метод должен обеспечивать количественную оценку затрат на безопасность АС, используя качественные показатели оценки вероятностей событий и их последствий;
* Быть прозрачным с точки зрения пользователя и давать возможность вводить собственные эмпирические данные;
* Быть универсальным;
* Позволять моделировать ситуацию, при которой существует несколько контрмер, направленных на предотвращение определенных угроз.

1. Назовите категории затрат, связанных с безопасностью, АС; кратко

охарактеризуйте каждую категорию и перечислите статьи расходов для каждой из них.

1. Организационные затраты на формирование и поддержание звена управления Системой защиты:

* Формирование политики безопасности АС;
* Приобретение и внедрению эксплуатацию программно-технических средств;
* Приобретение и настройку средств защиты информации;
* Содержание персонала.

1. Затраты на контроль — определение и подтверждение достигнутого уровня защищенности ресурсов АС:

* Контроль реализации функций, обеспечивающих управление безопасностью АС;
* Организация взаимодействия между подразделениями для решения конкретных задач по обеспечению безопасности АС;
* Проведение аудита безопасности по каждой части АС;
* плановые проверки и испытания средств защиты информации;
* проверка навыков эксплуатации и средств защиты персоналом;
* внеплановые проверки и испытания;

1. Внутренние затраты на ликвидацию последствий нарушений политики безопасности АС

* Идентификация угроз безопасности АС;
* Поиск уязвимостей системы безопасности АС;
* Оплата труда специалистов, выполняющих работы по определению возможного ущерба и переоценке степени риска;
* Ликвидация последствий нарушения режима безопасности;
* Восстановление системы безопасности АС до соответствия требованиям политики безопасности;

1. Внешние затраты на ликвидацию последствий нарушения политики безопасности АС:

* Невыполнение обязательств перед государством и партнерами;
* Юридическое сопровождение и выплата компенсаций;
* Проведение дополнительных исследований и разработка новой рыночной стратегии;
* Заработная плата служащих, организационные и прочие расходы, непосредственно связанные с предупредительными мероприятиями;

1. Затраты на техническое обслуживание системы безопасности ИТ:

* Управление системой безопасности ИТ;
* Планирование системы безопасности ИТ;
* Изучение возможностей инфраструктуры по обеспечению безопасности ИТ;
* Проверка сотрудников на лояльность, выявление угроз безопасности ИТ;

1. Что понимается под безопасностью вообще и безопасностью АС в частности?

**Безопасность**—защищенность от возможного ущерба, наносимого при реализации угроз.

**Безопасность автоматизированной системы** — защищенность всех ее компонентов от разного рода нежелательных для соответствующих субъектов воздействий.

1. Дайте определение АС и безопасности АС.

**Автоматизированная система** обработки информации – организационно-техническая система, представляющая собой совокупность взаимосвязанных компонентов, объединенных по организационно-структурному, тематическому, технологическому или иным основаниям для выполнения автоматизированной обработки информации в целях удовлетворения информационных потребностей субъектов информационных отношений.

1. Приведите определения информации и информационных ресурсов.

**Информация** — это сведения о фактах, событиях, процессах и явлениях, о состоянии объектов вне которой предметной области, необходимые для оптимизации принимаемых решений в процессе управления этими объектами.

**Информационные ресурсы** — отдельные документы, а также отдельные массивы документов, документы и массивы документов в информационных системах.

1. Перечислите категории субъектов информационных отношений.

К субъектам информационных отношений относят:

* Государство в целом или отдельные его ведомства, органы и организации;
* Общественные или коммерческие организации и предприятия;
* Граждан.

1. Охарактеризуйте три свойства информации: конфиденциальность, целостность и доступность.

* **Доступность** — свойство информации быть доступной и готовой к использованию по запросу авторизованного субъекта, имеющего на это прав;
* **Целостность** — свойство информации быть не видоизменённой, защита от несанкционированного разрушения;
* **Конфиденциальность** — свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов.

1. Сформулируйте цели защиты АС и циркулирующей в ней информации.

Цель обеспечения безопасности АС — защита внешних и внутренних субъектов, которые участвуют в процессах информационного взаимодействия, от нанесения им материального, морального или иного ущерба в результате случайных или преднамеренных нежелательных воздействий на информацию и системы ее обработки и передачи.

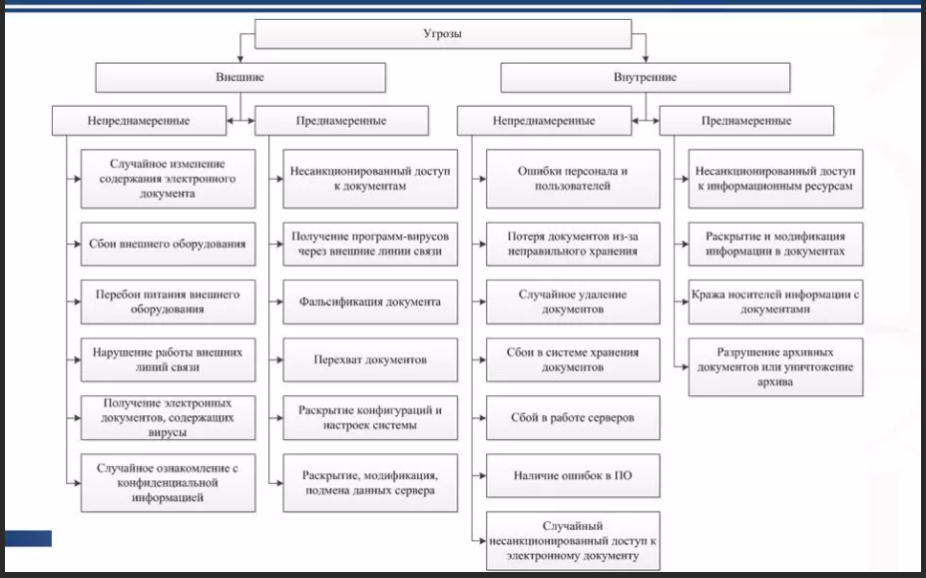
Цель защиты, циркулирующей в АС информации — предотвращение утечки, искажения, утраты, блокирования или незаконного распространения информации.

1. Дайте определение понятий «угроза», «уязвимость» и «атака».

**Уязвимость** - это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

**Угроза** - это потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба чьим-либо интересам.

**Атака** - это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.

17.Какие классификационные схемы угроз ИБ вам известны?

18.Перечислите источники угроз ИБ.

Основными источниками угроз безопасности АС и информации являются:

• стихийные бедствия

• аварии, сбои и отказы оборудования АС;

• ошибки проектирования и разработки компонентов АС

• ошибки эксплуатации.

1. Назовите каналы проникновения в автоматизированную систему иутечки информации.

По способу проникновения в систему различают **прямые и косвенные** каналы.

По типу основного средства реализации угрозы каналы условно разделяют на три группы (в зависимости от объекта воздействия: **программа, оборудование, персонал**).

По способу получения информации потенциальные каналы подразделяют следующим образом:

• **физический;**

**• электромагнитный (перехват излучений);**

**• информационный (программно-математический).**

1. Какие факторы лежат в основе формирования модели нарушителя?

Неформальная модель нарушителя отражает его практические и теоретические возможности, априорные знания, время и место действия и т.п. Для достижения своих целей нарушитель должен приложить некоторые усилия, затратить определенные ресурсы. При построении модели нарушителя обычно формулируются предположения:

* + О категориях лиц, к которым может принадлежать нарушитель;
  + Мотивах действий нарушителя и преследуемых им целях;
  + Квалификации нарушителя и его технической оснащенности;
  + Характере возможных действий нарушителей.

21.Каковы цели разработки моделей угроз и нарушителей?

Правильно построенная модель нарушителя, в которой отражаются его практические и теоретические возможности, время, место действия и другие характеристики — важная составляющая успешного проведения анализа риска и определения требований к составу и характеристикам системы защиты.

1. В чем разница между нарушителем и злоумышленником?

**Нарушитель** — это лицо, предпринявшее попытку выполнения запрещенных операций по ошибке, незнанию или осознанно со злым умыслом или без такового и использующее для этого различные возможности, методы и средства.

**Злоумышленник** – нарушитель, намеренно и нацелено идущий на совершение противоправных действий.

1. Перечислите основные виды мер противодействия угрозам безопасности АС (контрмер).

* законодательные;
* морально-этические;
* организационные;
* физические;
* технические (аппаратные и программные).

1. Охарактеризуйте каждую меру противодействия.

**Законодательные** меры включают в себя указы, постановления, законы, руководящие документы и другие НПА, которые определяют нормы обращения с информацией, права и обязанности участников информационных отношений и устанавливают ответственность за несоблюдение данных норм.

**Морально-этические** меры предполагают соблюдение норм поведения, которые традиционно сложились в обществе или формируются по мере ИТ. Данные нормы необязательны к применению, как требования нормативных актов, однако, их несоблюдение может нередко привести к снижению престижа компании.

**Организационные меры** - меры административного характера, которые устанавливают правила функционирования системы обработки данных и деятельности обслуживающего персонала, а также порядок их взаимодействия для снижения вероятности осуществления угроз безопасности или потерь в случае их реализации. (Охрана территории объекта, соблюдение требований разграничения доступа, формирование дисциплины и ответственности сотрудников и др.).

**Меры физической** защиты на основе механических, электромеханических и электронно-механических устройств позволяют создавать физические препятствия на возможных путях проникновения потенциальных нарушителей к компонентам системы. (Установка средств визуального наблюдения, охранной сигнализации контроля физической целостности компонентов АС, проверка поступающего оборудования, установка средств защиты от перебоев в электроснабжении и помех в линиях связи).

**Технические меры** защиты предполагают использование электронных устройств и программ для осуществления функции идентификации пользователей, разграничения доступа к информации, блокирования системы при НСД и др.

1. Какая мера противодействия является, на ваш взгляд, наиболее важной, а какая — второстепенной?

Придумаем на ходу из 24 вопроса.

1. Перечислите достоинства и недостатки различных мер защиты.

|  |  |  |
| --- | --- | --- |
| **Меры** | **Достоинства** | **Недостатки** |
| Законодательные и морально-этнические | * Определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение. * Универсальны — применимы для всех каналов НСД. * Единственно применимы: * При защите открытой информации от незаконного тиражирования; * При защите от злоупотребления служебным положением   при работе с информацией. | Требуют проведения постоянной разъяснительной работы с пользователями и обслуживающим персоналом АС |
| Организационные | * Играют значительную роль в обеспечении безопасности компьютерных систем. * Единственно применимы, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. * Необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. | * Низкая надежность без соответствующей поддержки физическими, техническими и программными средствами. * Большой объем рутинной деятельности. * Необходимо поддерживать более   надежными физическими и техническими мерами |
| Физические и технические | * Устраняют недостатки организационных мер. * Поставят прочные барьеры на пути злоумышленников. * В максимальной степени исключают возможность неумышленных (по ошибке или халатности) нарушений регламента со стороны персонала и пользователей АС | Сложность осуществления (можно вычислить пароли, электронную цифровую подпись подделать и др.) |

27.Возможно ли создание идеально надежной системы защиты?

Нет

Если допустить возможность создания идеально надежных физических и технических средств защиты, перекрывающих все уязвимые каналы, то всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих средств. Вместе с самими средствами защиты эти люди образуют так называемое «ядро безопасности». В этом случае стойкость системы безопасности будет определяться стойкостью персонала из «ядра безопасности» системы, и повышать ее можно только за счет организационных мероприятий, законодательных и морально-этических мер.

Но даже совершенные законы и оптимальная кадровая политика не могут до конца решить проблему защиты, поскольку, во-первых, сложно найти персонал, в котором можно быть абсолютно уверенными в отношении которого невозможно было бы предпринять действия, вынуждающие его нарушить запреты; а во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

1. Перечислите основные принципы построения систем защиты информации. Какие из них, по вашему мнению, являются

важнейшими? Кратко охарактеризуйте каждый принцип.

* законность;
* системность;
* своевременность;
* преемственность и непрерывное совершенствование:
* персональная ответственность;
* гибкость системы защиты;
* простота применения средств защиты;

**Законность** предполагает проведение защитных мероприятий и разработку системы безопасности информации в организации в соответствии с действующим законодательством в области информации, информационных технологий и защиты информации, других нормативно-правовых актов,

руководящих и нормативно-методических документов по безопасности информации, утвержденных органами государственной власти в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

**Системность** заключается в учете всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, которые имеют существенное значение для решения проблемы обеспечения безопасности информации в организации.

**Своевременность** предполагает применение мер обеспечения безопасности информации упреждающего характера, т. е. параллельно с разработкой и развитием самой защищаемой системы. Это позволяет учитывать требования безопасности при проектировании архитектуры и создавать более защищенные системы.

**Преемственность и совершенствование** — это улучшение организационных и технических решений средств защиты информации на основе анализа функционирования АС и ее системы защиты с учетом последних изменений методов и средств воздействия на компоненты АС, нормативных требований по защите, современного отечественного и зарубежного опыта в этой области.

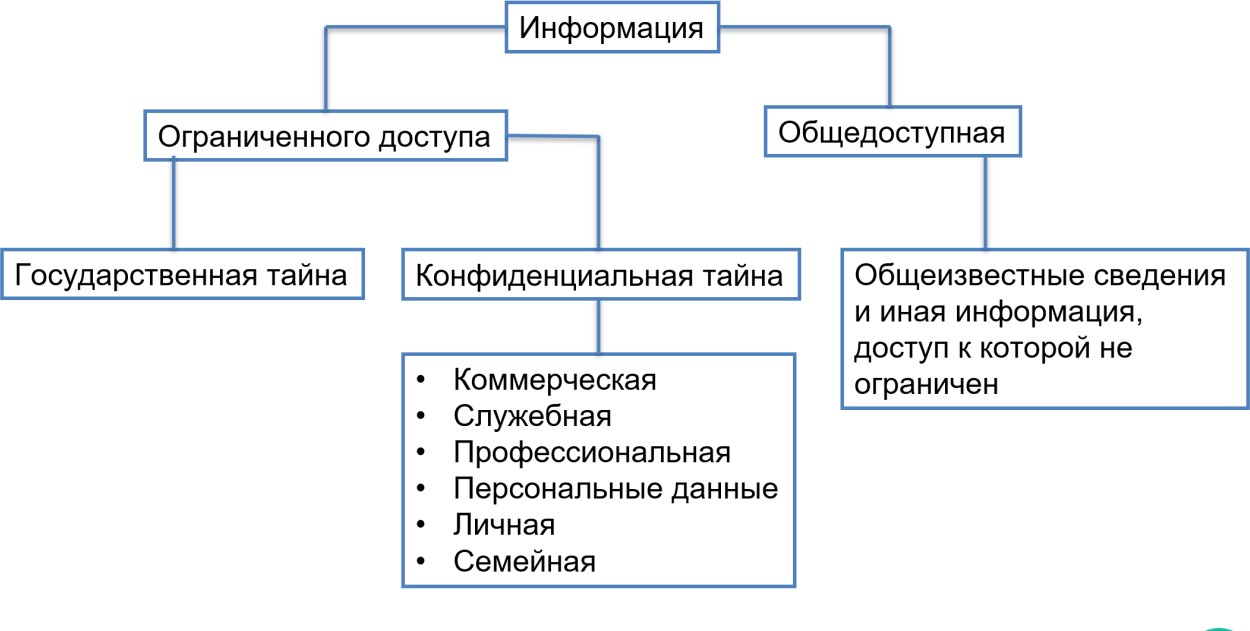
Разделение функций предполагает мандатный доступ к информации, в соответствии с которым ни один сотрудник организации не имеет полномочий, позволяющих ему единолично проводить критичные операции.

**Персональная ответственность** предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий.

**Гибкость** системы защиты предполагает варьирование уровней защищенности, поскольку принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты.

**Простота применения** средств защиты подразумевает, что их использование не должно быть связано со знанием специальных языков или выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей.

1. Приведите классификацию информации по доступности с точки зренияФедерального закона «Об информации, информационных технологияхио защите информации».



1. Дайте определения обладателя информации и оператора информационной системы.

**Обладатель информации** — лицо, которое владеет информацией на законном основании, ограничило доступ к этой информации;

**Оператор** — государственный или муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия(операции), совершаемые с персональными данными.

1. Перечислите права и обязанности обладателя информации.

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

1. Дайте определение понятия «коммерческая тайна» в соответствии с Федеральным законом «О коммерческой тайне».

**Коммерческая тайна** — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах получить коммерческую выгоду;

1. Какая информация не может быть отнесена к коммерческой тайне?

1) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

2) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

3) о состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов;

4) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

5) о задолженности работодателей по выплате заработной платы и социальным выплатам;

6) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

7) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

8) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

9) составляющих информацию о состоянии окружающей среды (экологическую информацию).

34.Каким нормативным актом утвержден Перечень сведений

Конфиденциального характера?

Указ Президента Российской Федерации от 06.03.1997 №188 (с изм. от 23.09.2005 № 1111)

1. В каком кодексе предусмотрена ответственность за нарушение

установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональныхданных)?

Административную ответственность устанавливает Кодекс об административных правонарушениях Российской Федерации (КоАП).

1. В каком кодексе предусмотрена ответственность за «не законные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»?

ст.183 УК РФ.

1. Какие статьи Уголовного кодекса РФ определяют ответственность за преступления в сфере компьютерной информации?

В гл.28 УК РФ «Преступления в сфере компьютерной информации» содержатся три статьи, касающиеся неправомерного доступа к компьютерной информации (ст.272), вредоносных программ для ЭВМ (ст.273) и нарушения правил эксплуатации ЭВМ (ст.274).

1. С какого возраста предусмотрена уголовная ответственность за преступления в сфере компьютерной информации?

16 лет.

1. В какой статье Уголовного кодекса РФ определяется ответственность за создание, использование и распространение вредоносных программ для ЭВМ?

Статьей 273 Уголовного кодекса Российской Федерации устанавливается ответственность за создание, использование и распространение вредоносных компьютерных программ – так называемых «вирусов».

1. Что такое лицензирование?

**Лицензирование** — деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса;

1. Какие виды лицензирования вам известны?

* **Исключительная лицензия**. Этот вид разрешительной документации направлен исключительно на управление имуществом (движимым/недвижимым либо денежными средствами)
* **Простая лицензия**. Это разрешение привязывается не к субъекту, а к территории. Перекрёстная лицензия позволяет предоставлять патентные права.
* **Полная лицензия**. Полное разрешение позволяет оперировать нематериальными благами и правами.
* **Электронная лицензия** – вид разрешительной документации, который выдаётся в электронном виде через интернет и не имеет бумажного дубликата.
* **Патент** (лицензионное соглашение в области патентов) – документ, регулирующий отношения в научно-технической сфере.
* **Открытая лицензия** позволяет любое (как коммерческое, так и некоммерческое) использование материальных и нематериальных благ, которые можно получить от объекта, на который распространяется разрешительная документация.

1. Для кого аттестация АИС по требованиям безопасности информации ФСТЭК России является обязательной?

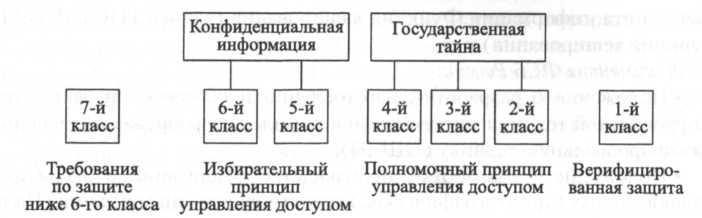
* Объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну;
* Объекты информатизации, предназначенные для управления экологически опасными объектами;
* Информационные системы государственных органов;
* Критические информационные инфраструктуры.

1. Когда проводится аттестация АИС по требованиям безопасности информации ФСТЭК России?

Тогда, когда нужно получать обязательную лицензию ФСТЭК ФСБ. До ввода в эксплуатацию тех, кто содержит что-либо из предыдущего вопроса.

1. Перечислите классы защищенности СВТ в соответствии с руководящими документами ФСТЭК России.

Показатели защищенности от несанкционированного доступа к информации возможные показатели защищенности разделены на семь классов (наиболее защищенный — 1-й класс).

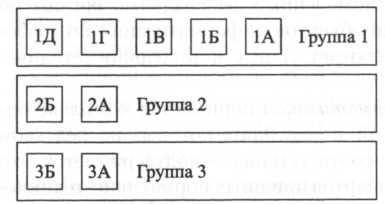


1. Перечислите классы защищенности АС в соответствии с руководящими документами ФСТЭК России.

Руководящий документ ФСТЭК России вводит в рассмотрение девять классов защищенности АС, объединенных в три группы.

Группа1 классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всему объему информации АС. Группа содержит пять классов: 1Д,1Г,1В,1Би1А.

К группе 2 относят АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всему объему информации АС, обрабатываемой (или) хранимой на носителях различного уровня конфиденциальности. Группа объединяет два класса:2Би2А.



Группа 3 классифицирует АС, в которых работает один пользователь, допущенный ко всему объему информации, размещенной на носителях одного уровня конфиденциальности (классы ЗБ и ЗА).

46.Какие подсистемы включает в себя комплекс программно-технических средств защиты информации от НСД в АС?

-управления доступом;  
- регистрации и учета;  
- криптографической;  
- обеспечения целостности;