1. **Понятия: информационная безопасность. Защита информации. Информационное общество.**

Информационная безопасность — состояние защищенности жизненно-важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз.

Защита информации — комплекс организационных, технических и правовых мер, методов и средств, направленных на обеспечение конфиденциальности, доступности и целостности информации.

Информационная сфера — совокупность информации, информационных процессов, информационных технологий, целью которой является обеспечение, общества информационными ресурсами.

Информационное общество — общество, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, особенно высшей её формы — знаний. Сконцентрировалось в начале 21 века в связи с глобальной информатизацией 99% населения Земли.

1. **Непреднамеренные угрозы информационной безопасности.**

**Искусственные угрозы** — угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить ***непреднамеренные*** (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п., и ***преднамеренные*** (умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников.

Непреднамеренные — (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.

1. **Преднамеренные угрозы информационной безопасности.**

Преднамеренные —(умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников.

1. **Естественные угрозы информационной безопасности.**

**Естественные угрозы** — это угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека. **По природе возникновения:** естественные (объективные) и искусственные (субъективные).

1. **Способы и методы защиты информации.**

Способы защиты информации:

1) Препятствие - создание на пути угрозы преграды, преодоление которой сопряжено с возникновением сложностей для злоумышленника или дестабилизирующего фактора.

2) Управление - оказание управляющих воздействий на элементы защищаемой системы.

3) Маскировка - действия над защищаемой системой или информацией, приводящие к такому их преобразованию, которое делает их недоступными для злоумышленника. (Сюда можно, в частности, отнести криптографические методы защиты ).

4) Регламентация - разработка и реализация комплекса мероприятий, создающих такие условия обработки информации, которые существенно затрудняют реализацию атак злоумышленника или воздействия других дестабилизирующих факторов.

5) Принуждение - метод заключается в создании условий, при которых пользователи и персонал вынуждены соблюдать условия обработки информации под угрозой ответственности (материальной, уголовной, административной)

6) Побуждение - метод заключается в создании условий, при которых пользователи и персонал соблюдают условия обработки информации по морально-этическим и психологическим соображениям.

Частные виды методов защиты информации:

1. Управление доступом – методы защиты информации регулированием использования всех ресурсов ИС и ИТ. Эти методы должны противостоять всем возможным путям несанкционированного доступа к информации.

Управление доступом включает следующие функции зашиты:

• идентификацию пользователей, персонала и ресурсов системы (присвоение каждому объекту персонального идентификатора);

• опознание (установление подлинности) объекта или субъекта по предъявленному им идентификатору;

• проверку полномочий (проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту);

• разрешение и создание условий работы в пределах установленного регламента;

• регистрацию (протоколирование) обращений к защищаемым ресурсам;

• реагирование (сигнализация, отключение, задержка работ, отказ в запросе и т.п.) при попытках несанкционированных действий.

1. Механизмы шифрования – криптографическое закрытие информации. Эти методы защиты все шире применяются как при обработке, так и при хранении информации на магнитных носителях. При передаче информации по каналам связи большой протяженности этот метод является единственно надежным.
2. Противодействие атакам вредоносных программ предполагает комплекс разнообразных мер организационного характера и использование антивирусных программ. Цели принимаемых мер – это уменьшение вероятности инфицирования АИС, выявление фактов заражения системы; уменьшение последствий информационных инфекций, локализация или уничтожение вирусов; восстановление информации в ИС. Овладение этим комплексом мер и средств требует знакомства со специальной литературой.

**6. Классификация средств защиты информации.**

1) Физические средства - механические, электрические, электромеханические, электронные, электронно-механические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.

2) Аппаратные средства - различные электронные и электронно-механические и т.п. устройства, схемно-встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации.

3) Программные средства - специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.

4) Организационные средства - организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации.

5) Законодательные средства - нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности.

6) Психологические (морально-этические средства) - сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

7. **Правовой способ защиты информации.**

Законодательные средства - нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности

**8. Аппаратно-технический способ защиты информации.**

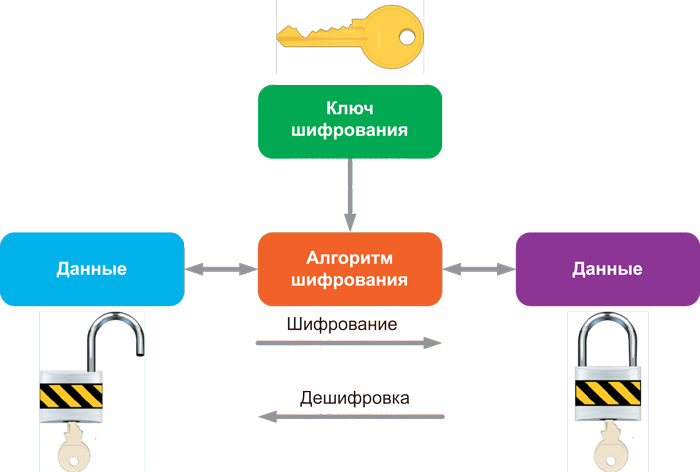
Аппаратные средства - различные электронные и электронно-механические и т.п. устройства, схемно-встраиваемые в аппаратуру системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации. Специальные средства, непосредственно входящие в состав технического обеспечения информационной вычислительной системы и выполняющие функции защиты как самостоятельно, так и в комплекте с другими средствами.

**9. Криптографический способ защиты информации.**

Криптографические средства — методы и средства обеспечения информационной безопасности, использующие криптографические преобразования информации. В узком смысле под криптографическими средствами могут пониматься отдельные устройства, документы и программы, использующиеся для выполнения функций криптосистемы.

Криптографическое преобразование - это преобразование информации, основанное на некотором алгоритме, зависящем от изменяемого параметра (обычно называемого секретным ключом), и обладающее свойством невозможности восстановления исходной информации по преобразованной, без знания действующего ключа, с трудоемкостью меньше заранее заданной.

Основным достоинством криптографических методов является то, что они обеспечивают высокую гарантированную стойкость защиты, которую можно рассчитать и выразить в числовой форме (средним числом операций или временем, необходимым для раскрытия зашифрованной информации или вычисления ключей).



**10.Злоумышленник. Виды угроз.**

Угроза – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам.

Информационные угрозыреализуются в виде:

- нарушения адресности и своевременности информационного обмена;

- противозаконного сбора и использования информации;

- осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;

- хищения информационных ресурсов из банков и баз данных;

- нарушения технологии обработки информации.

Программно-математические угрозыреализуются в виде:

- внедрения в аппаратные и программные изделия компонентов, реализующих функции, не описанные в документации на эти изделия;

- разработки и распространения программ, нарушающих нормальное функционирование информационных систем или их систем защиты

информации.

Физические угрозыреализуются в виде:

- уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации и связи;

- уничтожения, повреждения, разрушения или хищения машинных и других носителей информации;

- хищения программных или аппаратных ключей и средств криптографической защиты информации;

- перехвата информации в технических каналах связи и телекоммуникационных системах;

- внедрения электронных устройств перехвата информации в технические средства связи и телекоммуникационные системы, а также в служебные помещения;

- перехвата, дешифрования и навязывания ложной информации в сетях передачи данных и линиях связи;

- воздействия на парольно-ключевые системы защиты средств обработки и передачи информации.

Организационные угрозыреализуются в виде:

- невыполнения требований законодательства в информационной сфере;

- противоправной закупки несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникации

и связи.

Нарушитель— лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Злоумышленникомбудем называть нарушителя, намеренно идущего на нарушение из корыстных побуждений.

Злоумышленник – основной субъект угроз, источник противоборства с собственником в борьбе за активы и доходы.

**11. Атака. Угроза. Уязвимость. Риск. Ущерб.**

Угроза - совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства

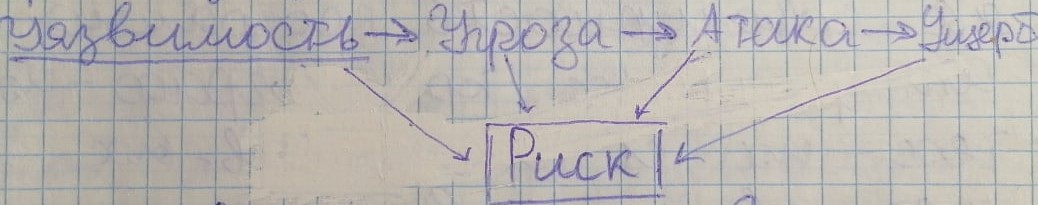
Уязвимость - недостатки или слабые места активов, которые могут быть использованы угрозой.

Ущерб – физическое повреждение или другой вред здоровью людей, имуществу (активам) или окружающей среде. Количественная величина ущерба не всегда поддается оценке. В этих случаях для оценки ущерба может использоваться качественное описание.

Риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба

Атака — попытка реализации угрозы.

Уязвимость Угроза Атака Ущерб



**12. Государственная тайна.**

Ф.З. №54-85 “О государственной тайне” говорит о том, что государственная тайна — Защищаемые государством сведения в области:

* Военной
* Внешнеполитической
* Разведывательной
* Контрразведывательной
* Оперативно-разыскной
* Экономической

деятельности , распространение которых может нанести ущерб безопасности РФ.

Уполномоченные лица:

* Президент РФ (глава СБ)
* Правительство РФ
* Министерство обороны
* Палаты Федерального собрания
* Органы судебной власти

Грифы секретности:

1. Особой важности
2. Совершенно секретно
3. Секретно

**13. Общедоступная информация.**

Согласно ФЗ № 149-ФЗ, информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

К ОИ относится:

* Сведения о ЧС
* Сведения о состоянии окружающей среды
* Сведения о золотом запасе РФ
* Сведения о привилегиях, льготах, компенсациях
* Сведения о состоянии здоровья высших должностных лиц
* Сведения о фактах нарушения прав и свобод человека
* Сведения о фактах нарушения законности органами государственной власти
* Законы РФ
* Информация о деятельности государственных органов (за исключением сведений, составляющих гос. тайну)
* Информация, накапливаемая в фондах библиотек, музеев и архивов.

**14. Конфиденциальная информация.**

Конфиденциальная информация (Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»), которая в свою очередь делится на несколько составляющих, наиболее часто встречающихся в исполнительных органах власти:

* персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу);
* служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с федеральными законами (служебная тайна – сведения, содержащие информацию ограниченного доступа, документы с пометкой «Для служебного пользования»).
* Интеллектуальная собственность — совокупность охраняемых результатов интеллектуальной деятельности и средств индивидуализации.

**15. Компьютерный вирус.**

Компьютерный вирус – вредоносная программа, предназначенная для внедрения в файлы и системные области памяти ПК, иногда распространения по каналам связи. Важное свойство – способность размножаться.

Классификация вирусов

* По начинке вирусы делятся на *деструктивные и недеструктивные*

По среде обитания:

• Сетевые – распространяются по сетям.

• Файловые – инфицируют исполняемые файлы с расширениями .exe, .com.

• Загрузочные – внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record - MBR).

• Файлово-загрузочные – способны заражать и загрузочные секторы и файлы.

По способу заражения:

• Резидентные – оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращения программ к ОС и внедряется в них.

• Нерезидентные – не заражают оперативную память и проявляют свою активность лишь однократно при запуске зараженной программы.

По степени опасности:

• Неопасные – например, на экране появляется сообщение: «Хочу чучу». Если набрать на клавиатуре слово «чуча», то вирус временно «успокаивается».

• Опасные – уничтожают часть файлов на диске.

• Очень опасные – самостоятельно форматируют жесткий диск.

По особенностям алгоритма:

• Вирусы-компаньоны – создают для ехе-файлов новые файлы-спутники, имеющие то же имя, но с расширением com. При запуске такого файла ОС первым обнаружит и выполнит com-файл, т.е. вирус, который затем запустит и ехе-файл.

• Паразитические – изменяют содержимое дисковых секторов или файлов.

• Репликаторы (черви) – распространяются в сети. Они проникают в память компьютера из сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии.

• Невидимки (стелс) – маскируют свое присутствие в ЭВМ, их трудно обнаружить.

• Мутанты (призраки, полиморфные вирусы, полиморфики) – их трудно обнаружить, т.к. их копии практически не содержат полностью совпадающих участков кода. Это достигается тем, что в программы вирусов добавляются пустые команды (мусор), которые не изменяют алгоритм работы вируса, но затрудняют их выявление.

• Макро-вирусы – используют возможности макроязыков, встроенных в системы обработки данных (Word, Excel).

• «Троянские кони» – маскируются под полезную или интересную программу, выполняя во время своего функционирования еще и разрушительную работу (например, стирает FAT) или собирает на компьютере информацию, не подлежащую разглашению. Не обладают свойством самовоспроизводства.

По целостности:

• Монолитные – программа вируса - единый блок, который можно обнаружить после инфицирования.

• Распределённые – программа разделена на части. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать вирус

**16. Законодательная база ИБ**

* N 149-ФЗ. «Об информации, информационных технологиях и о защите информации». Регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий, обеспечении защиты информации.
* 2) N 152-ФЗ «О персональных данных». Рассматривает основные термины и определения в области обеспечения безопасности самих ПД и процессов, связанных с их обработкой.
* N 54-85 ФЗ. «О государственной тайне». Регулирует отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации.
* N 390-ФЗ. «О безопасности». Раскрывает основы обеспечения безопасности личности, общества и государства.

**17. Органы исполнительной власти в сфере информационной безопасности. Их**

**деятельность.**

* **ФСТЭК России** является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по следующим вопросам в области обеспечения информационной безопасности:

1) обеспечению безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере;

2) противодействию иностранным техническим разведкам на территории РФ;

3) обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращению ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории РФ;

4) защите информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств.

Основными задачами в области обеспечения информационной безопасности для ФСТЭК России являются:

1) реализация в пределах своей компетенции государственной политики в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации;

2) осуществление государственной научно-технической политики в области защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

3) организация деятельности государственной системы противодействия техническим разведкам и технической защиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой;

4) осуществление самостоятельного нормативно-правового регулирования вопросов: обеспечения безопасности информации в ключевых системах информационной инфраструктуры; противодействия техническим разведкам; технической защиты информации; размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров РФ, иных программ и проектов на территории РФ, на континентальном шельфе и в исключительной экономической зоне РФ; координации деятельности органов государственной власти по подготовке развернутых перечней сведений, подлежащих засекречиванию, а также методического руководства этой деятельностью;

5) обеспечение в пределах своей компетенции безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

6) прогнозирование развития сил, средств и возможностей технических разведок, выявление угроз безопасности информации;

7) противодействие добыванию информации техническими средствами разведки, техническая защита информации;

8) осуществление координации деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ и организаций по государственному регулированию размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров РФ, иных программ и проектов на территории РФ, на континентальном шельфе и в исключительной экономической зоне РФ;

9) осуществление в пределах своей компетенции контроля деятельности по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, по противодействию техническим разведкам и по технической защите информации в аппаратах федеральных органов государственной власти и органов государственной власти субъектов РФ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов РФ, органах местного самоуправления и организациях;

10) осуществление центральным аппаратом ФСТЭК России организационно-технического обеспечения деятельности Межведомственной комиссии по защите государственной тайны.

* Обеспечение информационной безопасности является одним из основных направлений деятельности органов **Федеральной службы безопасности (ФСБ) России.**

Обеспечение информационной безопасности осуществляется ими в пределах своих полномочий:

• при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;

• при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в РФ и ее учреждениях, находящихся за пределами РФ.

* **Служба внешней разведки РФ** для осуществления своей деятельности может при собственных лицензировании и сертификации приобретать, разрабатывать (за исключением криптографических средств защиты), создавать, эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации от утечки по техническим каналам.
* **Министерство обороны (Минобороны России)** организует деятельность по обеспечению информационной безопасности, защите государственной тайны в Вооруженных силах, а также в установленном порядке в пределах своей компетенции работы по сертификации средств защиты информации.

**18. Совет безопасности РФ.**

Совет Безопасности Российской Федерации является конституционным совещательным органом, осуществляющим содействие главе государства в реализации его полномочий по вопросам обеспечения национальных интересов и безопасности личности, общества и государства, а также поддержания гражданского мира и согласия в стране, охраны суверенитета Российской Федерации, ее независимости и государственной целостности, предотвращения внутренних и внешних угроз.

Задачами Совета Безопасности являются:

а) обеспечение условий для осуществления Президентом Российской Федерации полномочий в области обеспечения национальных интересов и безопасности личности, общества и государства, иных видов безопасности, предусмотренных законодательством Российской Федерации (далее - национальная безопасность);

б) формирование государственной политики в области обеспечения национальной безопасности и контроль за ее реализацией;

в) прогнозирование, выявление, анализ и оценка внутренних и внешних угроз национальной безопасности, оценка военной опасности и военной угрозы, других внутренних и внешних угроз, выработка мер по их нейтрализации;

г) подготовка Президенту Российской Федерации предложений:

о мерах по предупреждению и ликвидации чрезвычайных ситуаций и преодолению их последствий;

о применении специальных экономических мер в целях обеспечения национальной безопасности;

о введении, продлении и об отмене чрезвычайного положения, а также о введении и об отмене военного положения;

о реформировании существующих или об образовании новых государственных органов и организаций, осуществляющих функции в области обеспечения национальной безопасности;

об утверждении и уточнении стратегии национальной безопасности Российской Федерации, иных концептуальных и доктринальных документов в области обеспечения национальной безопасности и обороны;

о мерах по поддержанию гражданского мира и согласия в стране, об охране суверенитета Российской Федерации, ее независимости и государственной целостности;

д) формирование основных направлений государственной внешней и военной политики;

е) координация деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по реализации принятых Президентом Российской Федерации решений в области обеспечения национальных интересов и национальной безопасности, поддержания гражданского мира и согласия в стране, охраны суверенитета Российской Федерации, ее независимости и государственной целостности, предотвращения внутренних и внешних угроз;

ж) оценка эффективности, разработка критериев и показателей деятельности федеральных органов исполнительной власти в области обеспечения национальной безопасности.

Функциями Совета Безопасности являются:

а) рассмотрение вопросов, касающихся обеспечения национальных интересов и национальной безопасности, поддержания гражданского мира и согласия в стране, охраны суверенитета Российской Федерации, ее независимости и государственной целостности, предотвращения внутренних и внешних угроз, пресечения действий, направленных на отчуждение части территории Российской Федерации, призывов к таким действиям, а также касающихся организации обороны, военного строительства, оборонного производства, военно-технического сотрудничества Российской Федерации с иностранными государствами, международного сотрудничества в области обеспечения безопасности;

б) проведение стратегической оценки на основе анализа информации:

о ходе реализации основных направлений государственной политики в области обеспечения национальной безопасности;

о социально-политической и об экономической ситуации в стране;

о соблюдении прав и свобод человека и гражданина в Российской Федерации;

о состоянии правопорядка и законности в стране, об эффективности принимаемых мер по поддержанию гражданского мира и согласия в стране, противодействию терроризму и экстремизму;

о военной опасности и военной угрозе;

о разработке, производстве и внедрении современных видов вооружения, военной и специальной техники, а также техники двойного и гражданского назначения в целях обеспечения национальной безопасности;

о ходе реализации государственной антинаркотической политики;

о состоянии военного и военно-технического сотрудничества Российской Федерации с иностранными государствами, а также международного сотрудничества в области обеспечения безопасности;

о состоянии информационной безопасности Российской Федерации и о развитии информационного общества в Российской Федерации;

о деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации в области обеспечения национальной безопасности;

о координации деятельности федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации по реализации принятых Президентом Российской Федерации решений в области обеспечения национальной безопасности;

в) разработка и уточнение критериев и показателей обеспечения национальной безопасности;

г) осуществление стратегического планирования в области обеспечения национальной безопасности, в том числе:

оценка эффективности работы по реализации документов стратегического планирования;

корректировка документов стратегического планирования и стратегических национальных приоритетов;

координация деятельности по разработке в федеральных округах документов стратегического планирования;

д) участие в реализации основных направлений государственной внешней и военной политики, государственной политики в области оборонного производства, военного и военно-технического сотрудничества Российской Федерации с иностранными государствами;

е) рассмотрение проектов законодательных и иных нормативных правовых актов Российской Федерации по вопросам, входящим в компетенцию Совета Безопасности;

ж) подготовка проектов указов и распоряжений Президента Российской Федерации по вопросам обеспечения национальных интересов и национальной безопасности, поддержания гражданского мира и согласия в стране, охраны суверенитета Российской Федерации, ее независимости и государственной целостности, организации обороны и осуществления контроля деятельности федеральных органов исполнительной власти в области обеспечения национальной безопасности;

з) организация разработки федеральных (государственных) целевых программ в области обеспечения национальной безопасности и осуществление контроля за их реализацией;

и) организация контроля за целевым расходованием бюджетных ассигнований федерального бюджета, направленных на обеспечение национальной обороны и национальной безопасности, а также на осуществление правоохранительной деятельности;

к) рассмотрение ежегодного доклада Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению;

л) рассмотрение ежегодного Сводного доклада о результатах и основных направлениях деятельности Правительства Российской Федерации;

м) рассмотрение ежегодных докладов о результатах и основных направлениях деятельности федеральных органов исполнительной власти, руководство деятельностью которых осуществляет Президент Российской Федерации;

н) организация научных исследований по вопросам, входящим в компетенцию Совета Безопасности.

5. Президент Российской Федерации может возложить на Совет Безопасности иные задачи и функции в соответствии с законодательством Российской Федерации.

6. Совет Безопасности в соответствии с Конституцией Российской Федерации формирует и возглавляет Президент Российской Федерации.

**19. Формы психологического воздействия. Убеждение и внушение.**

Информационно-психологическое воздействие представляет собой целенаправленную психологическую атаку на конкретные сферы психики человека, группы лиц или общественное сознание в целом. Воздействие может осуществляться по средствам информационных раздражителей с использованием всего спектра методов и форм технического, визуального, звукового, медикаментозного, физического, болевого, виртуального подавления воли.

Убеждение — это метод воздействия на сознание людей, обращенный к их собственному критическому восприятию.

Убеждая, необходимо следовать определенным правилам:

 логика убеждения должна быть доступной интеллекту объекта воздействия;

 убеждать надо доказательно, опираясь на факты, известные объекту;

 помимо конкретных фактов и примеров (без них нельзя убедить тех, кому недостает широты кругозора, развитого абстрактного мышления), информация должна содержать и обобщенные положения (идеи, принципы);

 убеждающая информация должна выглядеть максимально правдоподобной;

 сообщаемые факты и общие положения должны быть такими, чтобы вызывать эмоциональную реакцию объекта воздействия.

Внушение — это метод психологического воздействия на сознание личности или группы людей, основанный на некритическом (и часто неосознанном) восприятии информации.

нушению должны быть присущи следующие характеристики:

1. Целенаправленность и плановость. Внушающее воздействие осуществляется на основе конкретных целей и задач, соответствующим планам его организаторов и тем условиям, в которых они проводятся.

2. Конкретность объекта внушения. Внушающее воздействие эффективно в отношении строго определенных групп и слоев населения, при обязательном учете их важнейших социально-психологических, национальных и других особенностей.

3. Некритическое восприятие информации объектом внушения. Внушающее воздействие предполагает очень низкий уровень критичности и сознательности

объекта. В отличие от убеждения, внушение основывается не на логике и разуме человека, а на его способности воспринимать слова другого лица как должное, как инструкцию к действию. Поэтому оно не нуждается ни в системе логических доказательств, ни в активной мыслительной деятельности.

4. Определенность инициируемого поведения. Конечной целью внушения является формирование определенных реакций и поступков людей, соответствующих намерениям его инициаторов.

**20. Сущность и основные отличия информационных войн.**

Информационная война - это любое действие по использованию, разрушению, искажению вражеской информации и ее функций; защите нашей информации против подобных действий; и использованию наших собственных военных информационных функций.

Это определение является основой для следующих утверждений.

•Информационная война - это комплексное совместное применение сил и средств информационной и вооруженной борьбы.

•Информационная война - это коммуникативная технология по воздействию на информацию и информационные системы противника с целью достижения информационного превосходства в интересах национальной стратегии, при одновременной защите собственной информации и своих информационных систем.

•Информационная война - только средство, а не конечная цель, аналогично тому как бомбардировка - средство, а не цель.

•Информационную войну можно использовать как средство для проведения стратегической атаки или противодействия.

Следует отличать информационную войну от компьютерной преступности.

Любое компьютерное преступление представляет собой факт нарушения того или иного закона. Оно может быть случайным, а может быть специально спланированным; может быть обособленным, а может быть составной частью обширного плана атаки. Напротив, ведение информационной войны никогда не бывает случайным или обособленным (и может даже не являться нарушением закона), а подразумевает согласованную деятельность по использованию информации как оружия для ведения боевых действий - будь то на реальном поле брани, либо в экономической, политической или социальной сферах.

информационная операция — действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при защите собственной информации и информационных систем;

информационная война: комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений, а в ходе конфликта полностью парализовало бы функционирование инфраструктуры управления противника.

**21. «Внешние» нарушители информационной безопасности.**

Нарушитель — лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства.

Клиенты, посетители, конкуренты, случайные лица — внешние нарушители.

**22. «Внутренние» нарушители информационной безопасности.**

Пользователи системы, обслуживающий персонал, разработчики АИС, сотрудники службы безопасности, руководители — внутренние нарушители**;**

**23. Модель канала связи.**



**24. Модель комплексной защиты информации и её применение.**

Основную роль в методе формальной разработки системы играет так называемая модель безопасности (модель управления доступом, модель политики безопасности). Целью этой модели является выражение сути требований по безопасности к данной системе. Она определяет потоки информации, разрешенные в системе, и правила управления доступом к информации.

Модель позволяет провести анализ свойств системы, но не накладывает ограничений на реализацию тех или иных механизмов защиты. Так как она является формальной, возможно осуществить доказательство различных свойств безопасности системы.

Хорошая модель безопасности обладает свойствами абстрактности, простоты и адекватности моделируемой системе.

**25. Основные причины и особенности компьютерных преступлений.**

Киберпреступность представляет собой не только техническую и правовую, но и социальную проблему, эффективное решение которой требует, прежде всего, системного подхода к разработке основ обеспечения безопасности жизненно важных интересов гражданина, общества и государства в киберпространстве.

По механизму и способам совершения преступления в сфере компьютерных технологий специфичны, имеют высокий уровень латентности. Наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. Еще одной проблемой, с которой зачастую сталкиваются следователи при расследовании преступлений в сфере компьютерных технологий, является установление факта совершения преступления. Это связано с тем, что зачастую компьютерные преступления совершаются в так называемом «киберпространстве», они не знают границ, очень часто преступления совершаются, не выходя из дома, с помощью своего персонального компьютера. Кроме того, незаконное копирование информации чаще всего остается необнаруженным, введение в компьютер вируса обычно списывается на непреднамеренную ошибку пользователя, который не смог его «отловить» при общении с внешним компьютерным миром. Да и отношение пострадавших к совершенному против них посягательству не всегда адекватно. Вместо того, чтобы сообщить правоохранительными органам о факте незаконного вмешательства в компьютерную систему, пострадавшие не торопятся этого делать, опасаясь подрыва деловой репутации. Обычно, в качестве потерпевшей стороны от компьютерных преступлений выступают локальные сети, серверы, физические лица.

**26. Ценность информации. Чем она определяется.**

Ценность – определяется степенью ее полезности для владельца;

B большинстве случаев со временем ценность информации уменьшается. Зависимость ценности информации от времени приближенно определяется выражением.



где C0 — ценность информации в момент ее возникновения (получения);

t — время от момента возникновения информации до момента определения ее стоимости;

τ — время от момента возникновения информации до момента ее устаревания.

Ценность информации — свойство, определяемое ее пригодностью к практическому использованию в различных областях целенаправленной деятельности. Ценность и полезность информации детерминируются ее качественными и количественными характеристиками.

**27. Модели жизненного цикла программных средств.**

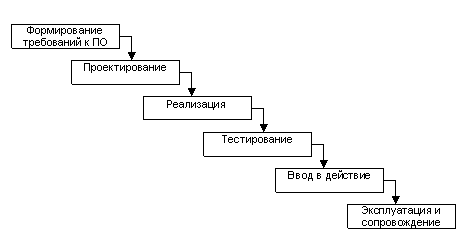
*Модель жизненного цикла:*структура, состоящая из процес­сов, работ и задач, включающих в себя разработку, эксплуата­цию и сопровождение программного продукта, охватывающая жизнь системы от установления требований к ней до прекраще­ния ее использования.

К настоящему времени наибольшее распространение получи­ли следующие основные модели ЖЦ:

•  каскадная модель (70-80-е годы 20 века);

•  спиральная модель (80-90-е годы 20 века).

В изначально существовавших однородных ИС каждое при­ложение представляло собой единое целое. Для разработки тако­го типа приложений применялся каскадный способ. Его основной характеристикой является разбиение всей разработки на эта­пы, причем переход с одного этапа на следующий происходит только после того, как будет полностью завершена работа на текущем.

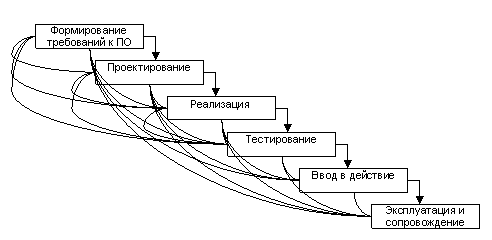


Положительные стороны применения каскадного подхода зак­лючаются в следующем:

•  на каждом этапе формируется законченный набор проектной документации, отвечающий критериям полноты и согласован­ности;

•  выполняемые в логичной последовательности этапы работ по­зволяют планировать сроки завершения всех работ и соответ­ствующие затраты.

Каскадный подход хорошо зарекомендовал себя при постро­ении ИС, для которых в самом начале разработки можно доста­точно точно и полно сформулировать все требования, с тем что­бы предоставить разработчикам свободу реализовать их как мож­но лучше с технической точки зрения. Однако в процессе использования этого подхода обнаружился ряд его недостатков, вызванных прежде всего тем, что реальный процесс создания ПС никогда полнос­тью не укладывался в такую жесткую схему. В процессе создания ПС постоянно возникала потребность в возврате к предыдущим этапам и уточнении или пересмотре ранее принятых решений. В результате реальный процесс создания ПС принимал следую­щий вид:



Основным недостатком каскадного подхода является существен­ное запаздывание с получением результатов. Таким образом, пользователи могут внести свои замечания толь­ко после того, как работа над системой будет полностью заверше­на. В случае неточного изложения требований или их изменения в течение длительного периода создания ПС пользователи получа­ют систему, не удовлетворяющую их потребностям.

Для преодоления перечисленных проблем была предложена спиральная модель ЖЦ, делающая упор на начальные папы ЖЦ: анализ и проектирование. На этих этапах реализуе­мость технических решений проверяется путем создания прото­типов. Каждый виток спирали соответствует созданию фрагмен­та или версии ПС, на нем уточняются цели и характеристики про­екта, определяется его качество и планируются работы следующего витка спирали. Таким образом, углубляются и последовательно конкретизируются детали проекта, и в результате выбирается обоснованный вариант, который доводится до реализации.



Разработка итерациями отражает объективно существующий спиральный цикл создания системы. Неполное завершение работ на каждом этапе позволяет переходить на следующий этап, не дожидаясь полного завершения работы на текущем. Главная же задача — как можно быстрее показать пользователям системы работоспособ­ный продукт, тем самым, активизируя процесс уточнения и до­полнения требований.

Основная проблема спирального цикла — определение мо­мента перехода на следующий этап. Для ее решения необходимо ввести временные ограничения на каждый из этапов жизненного цикла. Переход осуществляется в соответствии с планом, даже если не вся запланированная работа закончена.

**28. Защита информации при работе с Интернетом.**

* Аппаратные средства применяются на всех организационных уровнях. Однако особенно важно правильно организовать хранение информации.

Задача аппаратных средств при этом:

обеспечивать нужную скорость доступа к данным;

гарантировать надлежащую скорость систем проведения расчетов;

обеспечивать целостность данных и гарантию их сохранения при выходе из строя отдельных средств хранения;

организовывать резервное копирование, быстрое восстановление информации при сбоях;

обеспечивать взаимодействие со средствами связи;

реагировать и минимизировать ущерб при аварийных ситуациях (пожар, затопление);

сохранять работоспособность основного оборудования во время отключения основного источника энергии (генераторы, источники бесперебойного питания).

обрабатывать запросы подключенных пользователей.

Аппаратные технологии защиты информации в интернете включают также межсетевые экраны, программно управляемое оборудование, системы идентификации, управления доступом и многое другое.

* Программные

Область программных средств — самая обширная. Выбор конкретного списка пакетов зависит от используемых платформ и операционных систем, принятых механик доступа.

Среднестатистический список защитных мер включает:

систему обнаружения сетевых атак и попыток несанкционированного доступа на узел в составе программно управляемого оборудования;

комплексы шифрования (программные или аппаратные);

средства подтверждения подлинности, электронные ключи и системы для работы с ними;

средства управления доступом, которые могут включать и аппаратные средства.

На практике, правильно выбранный комплекс программных средств может практически исключить прямую атаку на хранилище или отдельный узел системы обработки данных.

Механизм шифрования данных

Меры защиты включают также стандартные шифрованные протоколы передачи информации.

* Смешанные

Смешанные меры защиты разрабатываются для сети хранения и обработки в том случае, когда характер действий с данными отличается для разных групп пользователей.

В перечень используемых средств могут входить программные комплексы на отдельных рабочих местах, системы разделения прав и уровней доступа в пределах одного сектора и общей структуры ответственности.

Популярно применение различных схем взаимодействия исполнителей между собой, а также — методики контроля и мониторинга.

К простейшему случаю смешанных мер защиты можно отнести обязательное использование антивирусов, стандартных шифрованных протоколов передачи, системы идентификации (в том числе — аппаратной) с разноуровневым доступом к работе с информацией.

* Организационные

К организационным мерам защиты информации относится разработка оптимальных схем взаимодействия персонала с информацией и обществом.

Сюда относится:

разработка инструкций, предписаний, четких схем работы с данными для занятого персонала;

предоставление персоналу ограниченного набора сертифицированных, надежных программных средств;

обязательное применение принципов ответственности за разглашение конфиденциальной информации;

разделение зон ответственности каждой трудовой единицы, ранжирование областей доступных данных, формулировка объема доступных действий;

создание средств для предотвращения случайного, умышленного удаления информации;

применение программных средств, полностью исключающих прямой доступ к данным;

формулирование в виде инструкций, правил действия сотрудников, охраны — системы работы с внутренними носителями информации, регламенты выноса документации;

применение средств проверки и подтверждения подлинности (электронные ключи).

В близкой к идеальной схеме работы с персоналом — проводятся постоянные проверки действий каждой трудовой единицы.

При этом работнику предоставляется стандартизированное рабочее место, где установлен регламентированный для его уровня доступа набор программ.

Корпуса компьютеров и другой электронной техники, части которой могут служить носителями важной информации — опечатываются и находятся под постоянным контролем.

На предприятиях, где постоянно ведется работа с важными данными — рекомендуется вводить систему идентификации персонала для доступа в сеть (помещения), основанную на периодически меняющихся и находящихся под строгим учетом электронных пропусков и иных меток.

Для защиты данных в сети интернет при помощи предлагаемых на рынке аппаратных и программных решений — можно построить эффективный и отказоустойчивый комплекс.

**29. Перспективы развития сети Интернет.**

1. Будет расти охват аудитории, Интернет появится в самых отдаленных местах

2. В информационных технологиях начинается эпоха программного обеспечения.

3. Увеличивается скорость передачи данных и пропускная способность.

4. Семантический WEB.

5. Новые объекты передачи.

6. Интернет станет сетью вещей, а не только компьютеров.

7. Роботизация общества.

8. Новый статус человека в Интернете.

9. Изменения рынка труда и сферы образования.

10. Интернет станет более «зеленым».

11. Кибероружие и кибервойны.

12. Выход интернета и сетевых технологий в космос.

**30. Персональные данные**

Персональные данные – любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу.

ПД делятся:

**•**Общие ПД – основные, базовые данные (ФИО, место регистрации и жительства, сведения об образовании, информация о месте работы/учёбы)

•Биометрические ПД – информация, которая есть с рождения(дактилоскопия, анализ ДНК, рост, цвет глаз, вес)

•Специальные ПД (национальная принадлежность и раса, вероисповедание, убеждения философского характера, информация о судимости, состояние здоровья, предпочтения в интимной жизни)

•Обезличенные (общедоступные) ПД – персональные данные, которые можно найти в адресной книге и справочниках.

\*Обработка только для биометрических и специальных ПД не допускается без согласия в письменной форме субъекта ПД!!!!!

N 152-ФЗ «О персональных данных». Рассматривает основные термины и определения в области обеспечения безопасности самих ПД и процессов, связанных с их обработкой.

**31. Структуры и задачи службы информационной безопасности компании.**

рассмотрим основные задачи службы безопасности предприятия:

* обеспечение безопасности производственно-торговой деятельности и защиты информации и сведений, являющихся коммерческой тайной;
* организация работы по правовой, организационной и инженерно-технической защите коммерческой тайны;
* организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;
* предотвращение необоснованного допуска и доступа к сведениям и работам, составляющим коммерческую тайну;
* выявление и локализации возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (аварийных, пожарных и др.) ситуациях;
* обеспечение режима безопасности при проведении всех видов деятельности, включая различные встречи, переговоры, совещания, заседания, связанные с деловым сотрудничеством, как на национальном, так и на международном уровне;
* обеспечение охраны зданий, помещений, оборудования, продукции и технических средств обеспечения производственной деятельности;
* обеспечение личной безопасности руководства и ведущих сотрудников и специалистов;
* оценка маркетинговых ситуаций и неправомерных действий злоумышленников и конкурентов.

Структура службы безопасности зависит от конкретного предприятия и задач, которые ставятся перед ней, а также от уровня развития и структуры производственного потенциала, эффективности его использования и т.д. Поэтому представить универсальную структуру службы безопасности невозможно, однако можно выделить основные структурные подразделения, которые должны присутствовать в большинстве случаев при организации службы безопасности.

Служба безопасности может состоять из следующих структурных подразделений:

* отдел режима и охраны;
* отдел защиты информации;
* инженерно-техническая группа;
* группа безопасности внешней деятельности.

**32. Аудит информационной безопасности.**

Аудит информационной безопасности — системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности автоматизированной системы в соответствии с определёнными критериями и показателями безопасности.

В настоящее время можно выделить следующие основные виды аудита информационной безопасности:

* экспертный аудит безопасности, в процессе которого выявляются недостатки в системе мер защиты информации на основе имеющегося опыта экспертов, участвующих в процедуре обследования;
* оценка соответствия рекомендациям Международного стандарта ISO 17799, а также требованиям руководящих документов ФСТЭК (Гостехкомиссии);
* инструментальный анализ защищённости АС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;
* комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования.

**33. Конфиденциальность. Целостность. Доступность.**

**Доступность**: Свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.



**Целостность**: Свойство информации быть невидоизмененной, а также ее защищенность от разрушения и несанкционированного изменения.

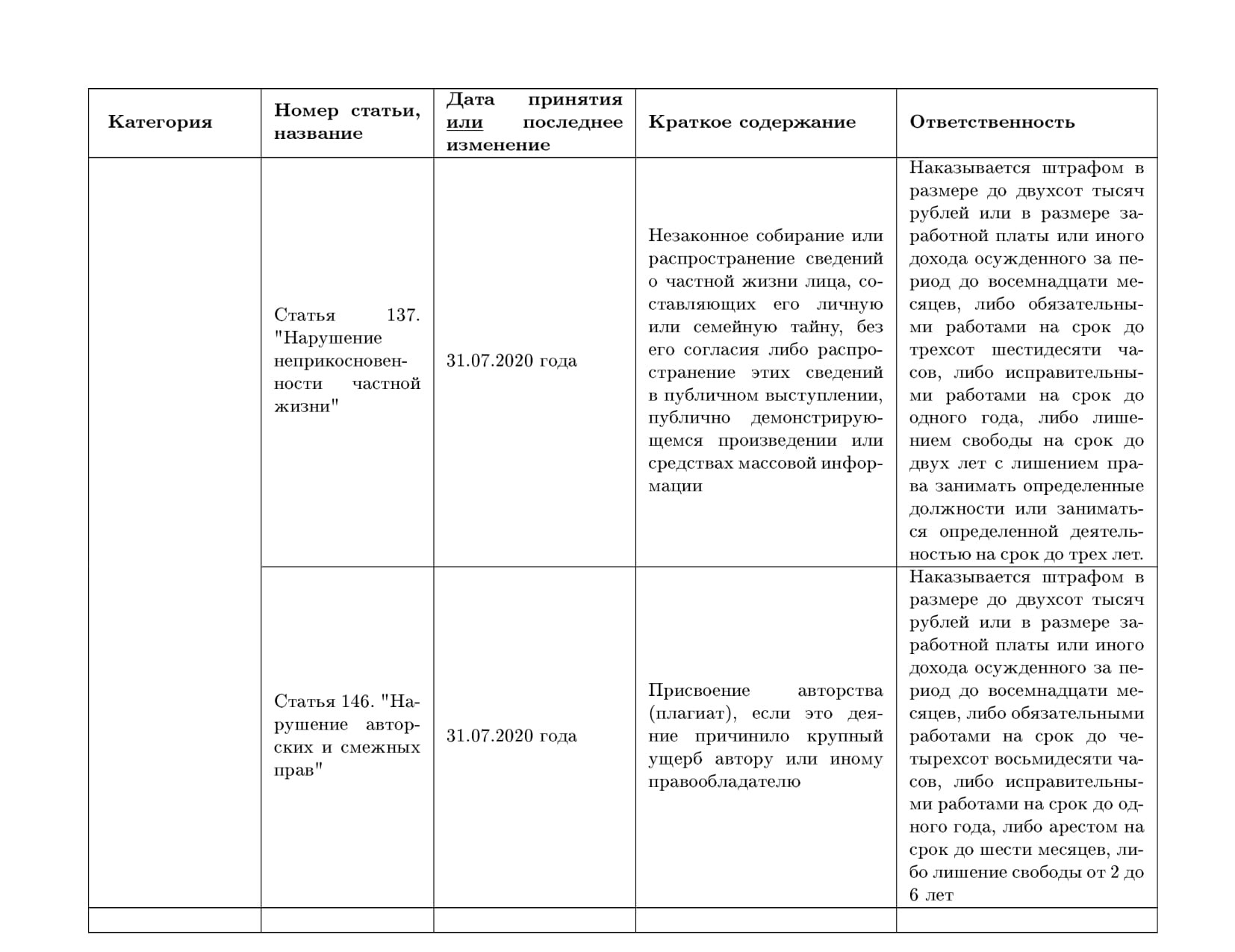
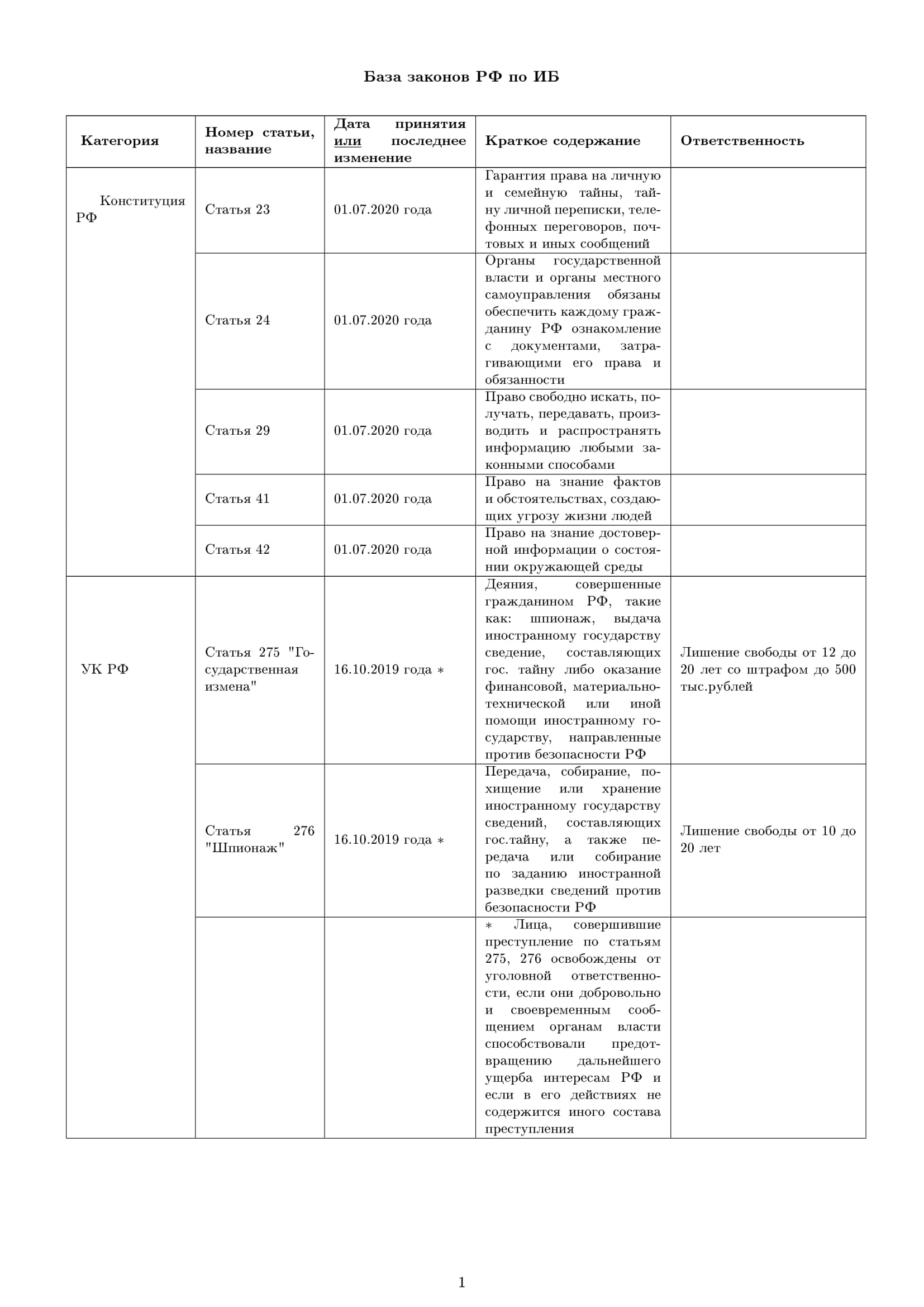
**Конфиденциальность**: Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса

(Примеры тайн: служебная, коммерческая, тайна страхования, медицинская и т.д.)

Персональные данные – любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу.

Интеллектуальная собственность – совокупность охраняемых результатов интеллектуальной деятельности и средств индивидуализации.

**36. Законодательство РФ в области защиты информации (перечень документов и их основные положения)**



**37. Модель злоумышленника. Сценарии действия (пример)**

Модель злоумышленника включает следующие предположения:

1. О категориях лиц, к которым может принадлежать нарушитель: пользователи системы, обслуживающий персонал, разработчики АИС, сотрудники службы безопасности, руководители — внутренние нарушители; клиенты, посетители, конкуренты, случайные лица — внешние нарушители.

2. О мотивах нарушителя — корыстный интерес. В первом случае нарушения вызываются некомпетентностью или небрежностью без наличия злого умысла. Во втором случае нарушитель, преодолевая защиту АИС и получая доступ к системным данным, самоутверждается в собственных глазах или в глазах коллег (такой нарушитель рассматривает свои действия как игру «пользователь — против системы»). Наибольшей опасностью обладает третий тип нарушителя, который целенаправленно преодолевает систему защиты, движимый корыстным интересом.

3. Об уровне знаний злоумышленника: на уровне пользователя АИС, на уровне администратора АИС, на уровне программиста, на уровне специалиста в области информационной безопасности.

4. О возможностях нарушителя (используемых методах и средствах): применяющий только агентурные методы, применяющий только штатные средства доступа к данным (возможно, в несанкционированном режиме), применяющий пассивные средства (возможность перехвата данных), применяющий активные средства (возможность перехвата и модификации данных).

5. **О времени действия:** во время штатного функционирования АИС, во время простоя АИС, в любое время.

6. О месте действия: без доступа на контролируемую территорию организации, с доступом на контролируемую территорию (но без доступа к техническим средствам), с рабочих мест пользователей, с доступом к базам данных АИС, с доступом к подсистеме защиты АИС.