**Методы и средства защиты компьютерной информации.**

**38 вопрос**

**Основные задачи защиты информации**

**Защита информации** – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

Из этого положения можно вывести два важных следствия:

1. Трактовка проблем, связанных с информационной безопасностью, для разных категорий субъектов может существенно различаться. Для иллюстрации достаточно сопоставить режимные государственные организации и учебные институты. В первом случае "пусть лучше все сломается, чем враг узнает хоть один секретный бит", во втором – "да нет у нас никаких секретов, лишь бы все работало".
2. Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации, это принципиально более широкое понятие. Субъект информационных отношений может пострадать (понести убытки и/или получить моральный ущерб) не только от несанкционированного доступа, но и от поломки системы, вызвавшей перерыв в работе. Более того, для многих открытых организаций (например, учебных) собственно защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте.

**39 вопрос**

**Идентификация и аутентификация. Идентификация и ее основные методы** **Биометрическая идентификация**

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация – это первая линия обороны, "проходная" информационного пространства организации.

**Идентификация** позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова " аутентификация " иногда используют словосочетание "проверка подлинности".

(Заметим в скобках, что происхождение русскоязычного термина " аутентификация " не совсем понятно. Английское "authentication" скорее можно прочитать как "аутентикация"; трудно сказать, откуда в середине взялось еще "фи" – может, из идентификации? Тем не менее, термин устоялся, он закреплен в Руководящих документах Гостехкомиссии России, использован в многочисленных публикациях, поэтому исправить его уже невозможно.)

**Аутентификация** бывает **односторонней** (обычно клиент доказывает свою подлинность серверу) и **двусторонней** (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.

Надежная идентификация затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации / аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть – это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация / аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

**Биометрия** представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи.

К биометрии следует относиться весьма осторожно. Необходимо учитывать, что она подвержена тем же угрозам, что и другие методы аутентификации. Во-первых, биометрический шаблон сравнивается не с результатом первоначальной обработки характеристик пользователя, а с тем, что пришло к месту сравнения. А, как известно, за время пути... много чего может произойти. Во-вторых, биометрические методы не более надежны, чем база данных шаблонов. В-третьих, следует учитывать разницу между применением биометрии на контролируемой территории, под бдительным оком охраны, и в "полевых" условиях, когда, например к устройству сканирования роговицы могут поднести муляж и т.п. В-четвертых, биометрические данные человека меняются, так что база шаблонов нуждается в сопровождении, что создает определенные проблемы и для пользователей, и для администраторов.

**40 вопрос**

**Организационные меры обеспечения информационной безопасности. Служба безопасности предприятия**

Служба информационной безопасности (СИБ) является одним из основных компонентов организационного обеспечения информационной безопасности объекта.

**Служба информационной безопасности является органом управления системы защиты информации.**Именно от качества построения службы информационной безопасности, профессиональной подготовленности ее сотрудников, наличия в их арсенале современных средств управления безопасностью во многом зависит эффективность мер по защите информации.

**Основная цель функционирования СИБ:** используя организационные меры и программно-аппаратные средства, избежать или свести к минимуму возможность нарушения политики безопасности, либо, в крайнем случае, вовремя заметить и устранить последствия   нарушения.

**Главное требование к службе информационной безопасности: высокая профессиональная подготовленность.**

Организационно группы службы информационной безопасности должны быть обособлены от всех отделов или групп, занимающихся управлением самой системой, программированием и другими относящимися к системе задачами во избежание возможного столкновения интересов.

Для эффективной работы Службы информационной безопасности необходима соответствующая административная поддержка, заключающаяся в отражении основных положений принятой политики безопасности в соответствующих Инструкциях и Распоряжениях. В них в первую очередь должны быть определены:

* должностные обязанности групп пользователей;
* правила доступа (разграничения доступа) к информации;
* мероприятия по обеспечению контроля и функционирования системы защиты информации;
* меры реагирования на нарушение режима безопасности;
* планирование и организация восстановительных работ.

Для обеспечения успешной работы *службы информационной безопасности* необходимо **определить права и обязанности Службы**, а также **правила ее взаимодействия с другими подразделениями** по вопросам защиты информации на объекте.

**41 вопрос**

**Теоретические и концептуальные основы защиты информации**

Основу правового обеспечения информационной безопасности России помимо нормативно-правовых актов составляют концептуальные документы. Они принимаются на уровне Президента РФ, Правительства РФ и других органов государственной власти. В частности, такими документами являются Доктрина информационной безопасности РФ и Стратегия национальной безопасности РФ до 2020 года.

**Концепция (от лат. conceptio)** - генеральный замысел, определяющий стратегию действий. Концепция защиты информации - это система взглядов на сущность, цели, принципы и организацию защиты информации.

Концепция защиты информации предполагает:

1. Определение понятия, сущности и целей защиты информации.
2. Какую информацию необходимо защищать, каковы критерии отнесения ее к защищаемой.
3. Дифференциацию защищаемой информации: а) по степеням конфиденциальности, б) по собственникам и владельцам.
4. Определение состава и классификации носителей защищаемой информации.
5. Определение источников, видов и способов дестабилизирующего воздействия на информацию, причин, обстоятельств и условий воздействий, каналов, методов и средств несанкционированного доступа к информации.
6. Определение методов и *средств защиты информации*.
7. Кадровое обеспечение защиты информации.

То есть концептуальные документы определяют общие отношение и политику государства в заданной области, а также служат основой для создания нормативно–правовых документов.

Основополагающим концептуальным документом в области информационной безопасности является **Доктрина информационной безопасности,** утвержденная 9 сентября 2000 года. Доктрина информационной безопасности РФ отображает официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ. Доктрина служит основой для:

* формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
* подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
* разработки целевых программ обеспечения информационной безопасности Российской Федерации.

В Доктрине выделены четыре составляющие национальных интересов в области информационных отношений:

* Соблюдение прав и свобод человека в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.;
* Информационное обеспечение внутренней и внешней государственной политики страны;
* Развитие информационных технологий в соответствии со временем;
* Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Дается следующее определение информационной безопасности - состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

**42 вопрос**

**Основные положения ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»**

**Защищаемая  информация** - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями,  устанавливаемыми собственником информации.  
  
    Примечание:  
  
Собственником информации может быть - государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.  
  
2 **Защита  информации**  -   деятельность по предотвращению утечки защищаемой информации,  несанкционированных и непреднамеренных воздействий на защищаемую информацию.  
  
3 **Защита информации от утечки** - деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации [иностранными] разведками.  
  
4 **Защита информации от несанкционированного воздействия**- защита информации от НСВ:  Деятельность по предотвращению воздействия на защищаемую информацию с нарушением  установленных  прав  и/или правил на изменение информации,  приводящего к искажению, уничтожению,  копированию, блокированию доступа к информации, а также к утрате,  уничтожению  или сбою функционирования носителя информации.  
  
5**Защита информации от непреднамеренного воздействия**-  деятельность  по предотвращению воздействия на защищаемую информацию ошибок пользователя информацией,  сбоя технических и  программных средств  информационных  систем,  а  также природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей,  приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.  
  
6 **Защита информации от разглашения**- деятельность по предотвращению  несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.  
  
7**Защита информации от несанкционированного доступа** - защита информации от НСД: Деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением  установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.  
  
    Примечание:  
  
Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.  
  
8**Защита информации от [иностранной] разведки**- деятельность по предотвращению получения защищаемой  информации  [иностранной] разведкой.  
  
9**Защита  информации от [иностранной] технической разведки**- деятельность по предотвращению  получения  защищаемой  информации [иностранной] разведкой с помощью технических средств.  
  
10 **Защита  информации  от агентурной разведки** - деятельность по предотвращению получения защищаемой информации агентурной разведкой.  
  
11 **Цель защиты информации** - желаемый результат защиты информации.

Примечание:  
  
Целью защиты информации  может  быть  предотвращение  ущерба собственнику,  владельцу,  пользователю информации в результате возможной утечки информации и/или несанкционированного и  непреднамеренного воздействия на информацию.  
  
12 **Эффективность  защиты  информации**  - степень соответствия результатов защиты информации поставленной цели.  
  
13 **Показатель эффективности защиты информации** - мера или характеристика для оценки эффективности защиты информации.  
  
14 **Нормы  эффективности защиты информации** - значения показателей эффективности защиты информации, установленные нормативными документами.

**43 вопрос**

**Угрозы информации. Классификация угроз**

**Угроза** - это потенциальная возможность определенным образом нарушить информационную безопасность.

**Угрозы информационной безопасности** – это оборотная сторона использования информационных технологий.

Попытка реализации угрозы называется атакой , а тот, кто предпринимает такую попытку, - злоумышленником . Потенциальные злоумышленники называются источниками угрозы .

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется окном опасности, ассоциированным с данным уязвимым местом. Пока существует окно опасности, возможны успешные атаки на ИС.

Если речь идет об ошибках в ПО, то окно опасности "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Для большинства уязвимых мест окно опасности существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

должно стать известно о средствах использования пробела в защите;

должны быть выпущены соответствующие заплаты;

заплаты должны быть установлены в защищаемой ИС.

Мы уже указывали, что новые уязвимые места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат - как можно более оперативно.

Отметим, что некоторые угрозы нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, угроза отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Рассмотрим наиболее распространенные угрозы, которым подвержены современные информационные системы. Иметь представление о возможных угрозах, а также об уязвимых местах, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий (вспомним все ту же "Проблему 2000"), поэтому незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно уязвимых направлений.

Подчеркнем, что само понятие " угроза " в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать - вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Мы попытаемся взглянуть на предмет с точки зрения типичной (на наш взгляд) организации. Впрочем, многие угрозы (например, пожар) опасны для всех.

Угрозы можно **классифицировать** по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;

по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);

- по расположению источника угроз (внутри/вне рассматриваемой ИС).

В качестве основного критерия мы будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.

**44 вопрос**

**Криптографические меры обеспечения информационной безопасности**

Сама криптография не является высшей ступенью классификации смежных с ней дисциплин. Наоборот, криптография совместно с криптоанализом (целью которого является противостояние методам криптографии) составляют комплексную науку – криптологию.

Необходимо отметить, что в русскоязычных текстах по данному предмету встречаются различные употребления основных терминов, таких как "криптография", "тайнопись" и некоторых других. Более того, и по классификации криптоалгоритмов можно встретить различные мнения. В связи с этим автор не претендует на то, что его вариант использования подобных терминов является единственно верным.

В отношении криптоалгоритмов существует несколько схем классификации, каждая из которых основана на группе характерных признаков. Таким образом, один и тот же алгоритм "проходит" сразу по нескольким схемам, оказываясь в каждой из них в какой-либо из подгрупп.

Основной схемой классификации всех криптоалгоритмов является следующая:

1. Тайнопись.  
   Отправитель и получатель производят над сообщением преобразования, известные только им двоим. Сторонним лицам неизвестен сам алгоритм шифрования. Некоторые специалисты считают, что тайнопись не является криптографией вообще, и автор находит это совершенно справедливым.
2. Криптография с ключом.  
   Алгоритм воздействия на передаваемые данные известен всем сторонним лицам, но он зависит от некоторого параметра – "ключа", которым обладают только отправитель и получатель.
   1. Симметричные криптоалгоритмы.  
      Для зашифровки и расшифровки сообщения используется один и тот же блок информации (ключ).
   2. **Асимметричные криптоалгоритмы.**  
      Алгоритм таков, что для зашифровки сообщения используется один ("открытый") ключ, известный всем желающим, а для расшифровки – другой ("закрытый"), существующий только у получателя.

Весь дальнейший материал будет посвящен криптографии с ключом, так как большинство специалистов именно по отношению к этим криптоалгоритмам используют термин криптография, что вполне оправдано. Так, например, любой криптоалгоритм с ключом можно превратить в тайнопись, просто "зашив" в исходном коде программы некоторый фиксированный ключ. Обратное же преобразование практически невозможно.

В зависимости от характера воздействий, производимых над данными, алгоритмы подразделяются на:

1. Перестановочные  
   Блоки информации (байты, биты, более крупные единицы) не изменяются сами по себе, но изменяется их порядок следования, что делает информацию недоступной стороннему наблюдателю.
2. Подстановочные  
   Сами блоки информации изменяются по законам криптоалгоритма. Подавляющее большинство современных алгоритмов принадлежит этой группе.

Заметьте: любые криптографические преобразования не увеличивают объем информации, а лишь изменяют ее представление. Поэтому, если программа шифрования значительно (более, чем на длину заголовка) увеличивает объем выходного файла, то в ее основе лежит неоптимальный, а возможно и вообще некорректный криптоалгоритм. Уменьшение объема закодированного файла возможно только при наличии встроенного алгоритма архивации в криптосистеме и при условии сжимаемости информации (так, например, архивы, музыкальные файлы формата MP3, видеоизображения формата JPEG сжиматься более чем на 2-4% не будут).

В зависимости от размера блока информации криптоалгоритмы делятся на:

1. Потоковые шифры.  
   Единицей кодирования является один бит. Результат кодирования не зависит от прошедшего ранее входного потока. Схема применяется в системах передачи потоков информации, то есть в тех случаях, когда передача информации начинается и заканчивается в произвольные моменты времени и может случайно прерываться. Наиболее распространенными предствателями поточных шифров являются скремблеры.
2. Блочные шифры  
   Единицей кодирования является блок из нескольких байтов (в настоящее время 4-32). Результат кодирования зависит от всех исходных байтов этого блока. Схема применяется при пакетной передаче информации и кодировании файлов.

**45 вопрос**

**Асимметричные алгоритмы шифрования. Использование асимметричных алгоритмов шифрования**

Асимметричная криптография изначально задумана как средство передачи сообщений от одного объекта к другому (а не для конфиденциального хранения информации, которое обеспечивают только симметричные алгоритмы). Поэтому дальнейшее объяснение мы будем вести в терминах "отправитель" – лицо, шифруюшее, а затем отпраляющее информацию по незащищенному каналу и "получатель" – лицо, принимающее и восстанавливающее информацию в ее исходном виде. Основная идея асимметричных криптоалгоритмов состоит в том, что для шифрования сообщения используется один ключ, а при дешифровании – другой.

Кроме того, процедура шифрования выбрана так, что она необратима даже по известному ключу шифрования – это второе необходимое условие асимметричной криптографии.

То есть, зная ключ шифрования и зашифрованный текст, невозможно восстановить исходное сообщение – прочесть его можно только с помощью второго ключа – ключа дешифрования. А раз так, то ключ шифрования для отправки писем какому-либо лицу можно вообще не скрывать – зная его все равно невозможно прочесть зашифрованное сообщение. Поэтому, ключ шифрования называют в асимметричных системах "открытым ключом", а вот ключ дешифрования получателю сообщений необходимо держать в секрете – он называется "закрытым ключом". Напрашивается вопрос : "Почему, зная открытый ключ, нельзя вычислить закрытый ключ ?" – это третье необходимое условие асимметричной криптографии – алгоритмы шифрования и дешифрования создаются так, чтобы зная открытый ключ, невозможно вычислить закрытый ключ.

В целом система переписки при использовании асимметричного шифрования выглядит следующим образом. Для каждого из N абонентов, ведущих переписку, выбрана своя пара ключей : "открытый" Ej и "закрытый" Dj, где j – номер абонента. Все открытые ключи известны всем пользователям сети, каждый закрытый ключ, наоборот, хранится только у того абонента, которому он принадлежит. Если абонент, скажем под номером 7, собирается передать информацию абоненту под номером 9, он шифрует данные ключом шифрования E9 и отправляет ее абоненту 9. Несмотря на то, что все пользователи сети знают ключ E9 и, возможно, имеют доступ к каналу, по которому идет зашифрованное послание, они не могут прочесть исходный текст, так как процедура шифрования необратима по открытому ключу. И только абонент №9, получив послание, производит над ним преобразование с помощью известного только ему ключа D9 и восстанавливает текст послания. Заметьте, что если сообщение нужно отправить в противоположном направлении (от абонента 9 к абоненту 7), то нужно будет использовать уже другую пару ключей (для шифрования ключ E7, а для дешифрования – ключ D7).

**46 вопрос**

**Симметричные алгоритмы шифрования. Использование Симметричных алгоритмов шифрования**

*Алгоритмы симметричного шифрования* различаются способом, которым обрабатывается исходный текст. Возможно шифрование блоками или шифрование потоком.

Симметричные алгоритмы шифрования используют один и тот же ключ для зашифровывания информации и для ее расшифровывания.

Такие алгоритмы именуются *одноключевыми,*или алгоритмами с секретным ключом, и требуют, чтобы отправитель сообщений и их получатель и рапсе условились о том, каким ключом они будут пользоваться. Надежность одноключевого алгоритма определяется выбором ключа, поскольку его значение дает возможность злоумышленнику без помех расшифровывать все перехваченные сообщения. Поэтому выбранный ключ следует хранить в тайне от посторонних.

Шифрование и расшифрование в симметричных криптографических алгоритмах задаются уже знакомыми формулами:

Е к (Р) = С

D к (С) = Р

Симметричные алгоритмы шифрования бывают двух видов. Одни из них обрабатывают открытый текст побитно. Они называются *потоковыми алгоритмами,*или *потоковыми шифрами.*Согласно другим, открытый текст разбивается на блоки, состоящие из нескольких бит. Такие алгоритмы называются *блочными,*или *блочными шифрами.*В современных компьютерных алгоритмах блочного шифрования обычно длина блока составляет 64 бита.

Если зашифрованную информацию необходимо передавать в другое место, то в этом надо передавать и ключ для расшифрования. Слабое место здесь - это канал передачи данных - если он не защищенный или его прослушивают, то ключ для расшифрования может попасть к злоумышленику. Системы на ассиметричных алгоритмах лишены этого недостатка. Поскольку каждый участник такой системы обладает парой ключей: Открытым и Секретным Ключом.

**47 вопрос**

**Использования хэш-функции для обеспечения информационной безопасности**

**Хэш-функция** – это труднообратимое преобразование данных (односторонняя функция), реализуемое, как правило, средствами симметричного шифрования со связыванием блоков. Результат шифрования последнего блока (зависящий от всех предыдущих) и служит результатом хэш-функции**.**

**Хеш-функция** может называться безопасной, если:

- функция является односторонней. Иными словами, функция создает контрольную сумму из информации с невозможностью восстановления информации по контрольной сумме;

- крайне сложно сконструировать два фрагмента информации с получением одинаковой контрольной суммы при выполнении функции.

Второму условию не так-то просто удовлетворить. Рассматриваемые контрольные суммы должны быть меньше по размеру, нежели информация, для обеспечения простоты подписывания, хранения и передачи информации. Если это условие удовлетворяется, то одной и той же контрольной сумме должно соответствовать большое число различных фрагментов информации. Безопасность функций обеспечивается способом связи всех битов в исходных данных со всеми битами контрольной суммы. Таким образом, если один бит информации изменяется, то также изменяется большое количество битов в контрольной сумме.

Безопасные хеш-функции должны обеспечивать создание контрольной суммы длиной, по крайней мере, в 128 бит. Двумя наиболее распространенными безопасными хеш-функциями являются MD5, генерирующая 128-битную контрольную сумму, и SHA, которая производит контрольную сумму длиной 160 бит. Существует множество других хеш-функций, однако большая их часть признана небезопасными. В MD5 были обнаружены уязвимости, которые могут использоваться при проведении вычислительной атаки. Эта атака позволит создать дополнительный фрагмент информации, что приведет к образованию той же контрольной суммы. Функция SHA была разработана правительством США и в настоящее время считается безопасной. В большей части программного обеспечения по информационной безопасности рассмотренные функции MD5 и SHA доступны для использования.

**48 вопрос**

**Межсетевые экраны, их функции и назначения**

**Межсетевой экран -** комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

**Межсетевой экран** располагается между защищаемой (внутренней) сетью и внешней средой (внешними сетями или другими сегментами корпоративной сети). В первом случае говорят о внешнем МЭ, во втором – о внутреннем. В зависимости от точки зрения, внешний межсетевой экран можно считать первой или последней (но никак не единственной) линией обороны. Первой – если смотреть на мир глазами внешнего злоумышленника. Последней – если стремиться к защищенности всех компонентов корпоративной сети и пресечению неправомерных действий внутренних пользователей.

Вообще говоря, и внешний, и внутренний межсетевой экран может стать узким местом, поскольку объем сетевого трафика имеет тенденцию быстрого роста. Один из подходов к решению этой проблемы предполагает разбиение МЭ на несколько аппаратных частей и организацию специализированных серверов-посредников. Основной межсетевой экран может проводить грубую классификацию входящего трафика по видам и передоверять фильтрацию соответствующим посредникам (например, посреднику, анализирующему HTTP-трафик). Исходящий трафик сначала обрабатывается сервером-посредником, который может выполнять и функционально полезные действия, такие как кэширование страниц внешних Web-серверов, что снижает нагрузку на сеть вообще и основной МЭ в частности.

Теоретически межсетевой экран (особенно внутренний) должен быть многопротокольным, однако на практике доминирование семейства протоколов TCP/IP столь велико, что поддержка других протоколов представляется излишеством, вредным для безопасности (чем сложнее сервис, тем он более уязвим).

Межсетевой экран – идеальное место для встраивания средств активного аудита. С одной стороны, и на первом, и на последнем защитном рубеже выявление подозрительной активности по-своему важно. С другой стороны, МЭ способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой. Правда, нужно отдавать себе отчет в том, что соединение двух сервисов безопасности в принципе может создать брешь, способствующую атакам на доступность.

На межсетевой экран целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

При развертывании межсетевых экранов следует соблюдать рассмотренные нами ранее принципы архитектурной безопасности, в первую очередь позаботившись о простоте и управляемости, об эшелонированности обороны, а также о невозможности перехода в небезопасное состояние. Кроме того, следует принимать во внимание не только внешние, но и внутренние угрозы.

Ситуации, когда корпоративная сеть содержит лишь один внешний канал, являются скорее исключением, чем правилом. Напротив, типична ситуация, при которой корпоративная сеть состоит из нескольких территориально разнесенных сегментов, каждый из которых подключен к Internet. В этом случае каждое подключение должно защищаться своим экраном. Точнее говоря, можно считать, что корпоративный внешний межсетевой экран является составным, и требуется решать задачу согласованного администрирования (управления и аудита) всех компонентов.

Собственная защищенность межсетевого экрана обеспечивается теми же средствами, что и защищенность универсальных систем. Имеется в виду физическая защита, идентификация и аутентификация, разграничение доступа, контроль целостности, протоколирование и аудит. При выполнении централизованного администрирования следует также позаботиться о защите информации от пассивного и активного прослушивания сети, то есть обеспечить ее (информации) целостность и конфиденциальность. Крайне важно оперативное наложение заплат, ликвидирующих выявленные уязвимые места МЭ.

Хотелось бы подчеркнуть, что природа экранирования как сервиса безопасности очень глубока. Помимо блокирования потоков данных, нарушающих политику безопасности, межсетевой экран может скрывать информацию о защищаемой сети, тем самым затрудняя действия потенциальных злоумышленников. Мощным методом сокрытия информации является трансляция "внутренних" сетевых адресов, которая попутно решает проблему расширения адресного пространства, выделенного организации.

Отметим также следующие дополнительные возможности межсетевых экранов:

- контроль информационного наполнения (антивирусный контроль "на лету",

- верификация Java-апплетов, выявление ключевых слов в электронных сообщениях и т.п.);

- выполнение функций ПО промежуточного слоя.

**49 вопрос**

**Антивирусные средства, их функции и назначения**

**Антивирусное средство** - специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

В нашей стране наиболее популярны антивирусные пакеты «Антивирус Касперского» и DrWeb. Существуют также другие программы, например «McAfee Virus Scan» и «Norton AntiVirus». Динамика изменения информации в данной предметной области высокая, поэтому дополнительную информацию по защите от вирусов можно найти в Internet, выполнив поиск по ключевым словам «защита от вирусов».

Вот основные **функции** антивирусных средств:

- Обнаружение вирусов. Антивирусная программа обнаруживает диск,файл или документ, зараженный компьютерным вирусом. Принятие решения остается за пользователем. В крайнем случае, можно уничтожить зараженный файл.

- Дезактивация вируса. Многие вирусы автоматически активируются при загрузке операционной системы и далее действуют как резидентные или серверные программы. Антивирусное средство может удалить такую вредоносную программу из памяти. Другой вариант дезактивации состоит во внесении изменений в тело вируса, препятствующих исполнению вредоносного кода, или в перемещении зараженных файлов таким образом, чтобы исключить их случайное или автоматическое использование.

- Лечение. Лечение состоит в полном устранении вируса и восстановлении незараженного файла. Это возможно потому, что вирус скрывает свое присутствие и зараженная программа должна работать точно так же, как и незараженная. Никакие части пораженного вирусом файла не утрачиваются, что и позволяет восстановить его.

**50 вопрос**

**Инженерно-технические меры обеспечения информационной безопасности**

**Инженерно-техническое обеспечение информационной безопасности**реализуется в двух направлениях: физическая защита элементов информационных систем; программная и аппаратно-программная защита данных.

Первое направление реализуется путем физической защиты кабельных систем и систем энергоснабжения, а также защиты данных путем их дублирования. Также сюда относят разного рода механические, электро- и электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам информационных систем и защищаемой информации, а также технические средства визуального наблюдения, связи и [охранной сигнализации](http://kortesinfo.ru/page/29).

Для осуществления программной и аппаратно-программной защиты данных используются разнообразные средства, среди которых можно выделить:

**1. Средства предупреждения угроз безопасности:**

а) системы разграничения доступа;

б) криптографические средства;

в) антивирусные мониторы и фильтры;

г) межсетевые экраны (файрволлы) и шлюзы;

**2. Средства выявления угроз безопасности:**

а) системы аудита и «ревизоры»;

б) антивирусные сканеры;

в) системные и сетевые мониторы;

**3. Средства минимизации ущерба:**

а) системы резервного копирования;

б) средства обеспечения отказоустойчивости.

**51 вопрос**

**Физическая защита источников информации. Способы защиты охраняемых объектов с помощью охранных и охранно-пожарных извещателей**

**Физические средства защиты информации** - это средства, предназначенные для защиты информации. Эти средства не предназначены для непосредственной обработки, хранения, накопления и передачи защищаемой информации, но находящиеся в одном помещении с ними. Делятся на:

* пассивные – физические (инженерные) средства, технические средства обнаружения, ОС, ПС, СКУД, ВН, приборы контроля радиоэфира, линий связи и т.п.;
* активные – источники бесперебойного питания, шумогенераторы, скремблеры, устройства отключения линии связи, программно-аппаратные средства маскировки информации и др.

Подобно тому, как беззащитен от постороннего доступа радиоканал, беззащитна и кабельная система большинства локальных вычислительных сетей. Есть, конечно, принципиальное отличие: кабельную систему можно спрятать за толстыми стенами офиса, а вот радиоканал ничем не закроешь. Однако именно повреждения кабельной системы являются причиной большинства отказов в работе локальных сетей.

В настоящее время наилучшим образом проявили себя структурированные кабельные системы, использующие одинаковые кабели для передачи данных в локальной вычислительной сети, телефонной сети, сетей пожарной и охранной сигнализации, сетей передачи данных системы видеонаблюдения. Название "структурированность" означает, что кабельную систему здания можно разделить на несколько уровней. Например, кабельная система SYSTIMAX SCS включает в себя:

* - аппаратные
* - внешнюю подсистему
* - административные подсистемы
* - магистрали
* - горизонтальную подсистему
* - рабочие места.

Аппаратные служат для размещения коммуникационной аппаратуры, обеспечивающей работу административной подсистемы.

Внешняя подсистема состоит из кабельной системы (медной или оптоволоконной), устройств защиты от высоковольтных скачков напряжения, надежной системы заземления и связывает коммуникационную и обрабатывающую аппаратуру в здании.

Административная подсистема предназначена, как видно из названия, для управления работой всей кабельной системой. Магистраль представляет собой медный или оптоволоконный кабель, связывающий этажи зданий. Горизонтальная подсистема представляет собой разветвление основной магистрали от административной подсистемы к розеткам на рабочем месте. Ну и, наконец, оборудование рабочих мест представляет собой сетевые адаптеры, всевозможные соединительные шнуры.

Наилучший способ защиты кабеля от всевозможных внешних воздействий (далеко не всегда предумышленных) - прокладка кабеля с использованием прочных защищенных коробов. Также при прокладке кабелей для локальной вычислительной сети необходимо учитывать воздействие внешних электромагнитных полей. При прокладке кабельной системы необходимо соблюдать следующие правила:

* - Неэкранированная витая пара должна отстоять минимум на 15-30 см от электрического кабеля, розеток, трансформаторов и т.д.
* - Требования к коаксиальному кабелю менее жесткие: расстояние до электрической линии или электроприборов должно быть не менее 10-15 см.

Также при прокладке кабельной системы необходимо учитывать соответствие всех ее компонентов требованиям международных стандартов. Наибольшее распространение получили следующие стандарты:

* - Спецификации корпорации IBM, которые предусматривают девять различных типов кабелей. Наиболее распространенным среди них является кабель IBM type 1 - экранированная витая пара (STP) для сетей Token Ring.
* - Система категорий Underwriters Labs (UL) представлена этой лабораторией совместно с корпорацией Anixter. Система включает пять уровней кабелей. В настоящее время система UL приведена в соответствие с системой категорий EIA/TIA.
* - Стандарт EIA/TIA 568 был разработан совместными усилиями UL, American National Standarts Institute (ANSI) и Electronic Industry Association/Telecommunications Industry Association, подгруппой TR41.8.1 для кабельных систем на витой паре (UTP).

Как уже говорилось ранее, для обеспечения надежной работы компьютеров и компьютерных сетей и для предотвращения потерь информации при кратковременных неполадках в системах электропитания необходимы специальные меры защиты. Наиболее надежным средством защиты в настоящее время является установка источников бесперебойного питания. Спектр предложения подобных устройств на рынке сейчас чрезвычайно широк. Различные по своим техническим характеристикам, эти устройства могут обеспечить надежную защиту от кратковременных скачков напряжения в сети питания. Стоит отметить, что большинство современных серверов и концентраторов снабжены собственными источниками бесперебойного питания.

Несмотря на все предосторожности, связанные с защитой данных от перепадов напряжения или неполадок в кабельной системе, возможны ситуации, когда эти проблемы все же могут привести к потере информации. Поэтому необходимо провести предварительное дублирование и архивирование информации. Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия.

**52 вопрос**

**Системы виброакустического зашумления. Сетевые помехоподавляющие фильтры. Экранирование**

Формальная постановка задачи экранирования, состоит в следующем. Пусть имеется два множества информационных систем. Экран – это средство разграничения доступа клиентов из одного множества к серверам из другого множества. Экран осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем.

Контроль потоков состоит в их фильтрации, возможно, с выполнением некоторых преобразований.

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией.

Экранирование помогает поддерживать доступность сервисов внутренней области, уменьшая или вообще ликвидируя нагрузку, вызванную внешней активностью. Уменьшается уязвимость внутренних сервисов безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом.

Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима

**53 вопрос**

**Особенности защиты беспроводных и мобильных подключений**

Существует три механизма защиты беспроводной сети: настроить клиент и AP на использование одного (не выбираемого по умолчанию) SSID, разрешить AP связь только с клиентами, MAC-адреса которых известны AP, и настроить клиенты на аутентификацию в AP и шифрование трафика. Большинство AP настраиваются на работу с выбираемым по умолчанию SSID, без ведения списка разрешенных MAC-адресов клиентов и с известным общим ключом для аутентификации и шифрования (или вообще без аутентификации и шифрования). Обычно эти параметры документированы в оперативной справочной системе на Web-узле изготовителя. Благодаря этим параметрам неопытный пользователь может без труда организовать беспроводную сеть и начать работать с ней, но одновременно они упрощают хакерам задачу проникновения в сеть. Положение усугубляется тем, что большинство узлов доступа настроено на широковещательную передачу SSID. Поэтому взломщик может отыскать уязвимые сети по стандартным SSID.

Первый шаг к безопасной беспроводной сети — изменить выбираемый по умолчанию SSID узла доступа. Кроме того, следует изменить данный параметр на клиенте, чтобы обеспечить связь с AP. Удобно назначить SSID, имеющий смысл для администратора и пользователей предприятия, но не явно идентифицирующий данную беспроводную сеть среди других SSID, перехватываемых посторонними лицами.

Следующий шаг — при возможности блокировать широковещательную передачу SSID узлом доступа. В результате взломщику становится сложнее (хотя возможность такая сохраняется) обнаружить присутствие беспроводной сети и SSID. В некоторых AP отменить широковещательную передачу SSID нельзя. В таких случаях следует максимально увеличить интервал широковещательной передачи. Кроме того, некоторые клиенты могут устанавливать связь только при условии широковещательной передачи SSID узлом доступа. Таким образом, возможно, придется провести эксперименты с этим параметром, чтобы выбрать режим, подходящий в конкретной ситуации.

После этого можно разрешить обращение к узлам доступа только от беспроводных клиентов с известными MAC-адресами. Такая мера едва ли уместна в крупной организации, но на малом предприятии с небольшим числом беспроводных клиентов это надежная дополнительная линия обороны. Взломщикам потребуется выяснить MAC-адреса, которым разрешено подключаться к AP предприятия, и заменить MAC-адрес собственного беспроводного адаптера разрешенным (в некоторых моделях адаптеров MAC-адрес можно изменить).

Выбор параметров аутентификации и шифрования может оказаться самой сложной операцией защиты беспроводной сети. Прежде чем назначить параметры, необходимо провести инвентаризацию узлов доступа и беспроводных адаптеров, чтобы установить поддерживаемые ими протоколы безопасности, особенно если беспроводная сеть уже организована с использованием разнообразного оборудования от различных поставщиков. Некоторые устройства, особенно старые AP и беспроводные адаптеры, могут быть несовместимы с WPA, WPA2 или ключами WEP увеличенной длины.

**54 вопрос**

**Структура системы контроля и управления доступом. Принципы построения системы контроля и управления доступом**

**Системы контроля и управления доступом (СКУД)** представляют собой совокупность программно-технических средств и организационных мероприятий, предназначенных для автоматизации пропускного режима сотрудников и посетителей на территорию и в отдельные помещения объекта.

Необходимость внедрения систем контроля и управления доступом на объектах вызвана двумя основными причинами:

* **1.** обеспечение защиты от проникновения на объект лиц, не имеющих соответствующих прав доступа, с целью исключения диверсий, а так же случаев преступного посягательства на жизнь людей, хищения материальных ценностей и информационных ресурсов объекта.
* **2.** создание условий для повышения трудовой дисциплины и эффективного использования рабочего времени.

**Структурно объект, на котором установлена система контроля и управления доступом, состоит из точек и зон доступа.**

* **Точки доступа** – это специально организованные места, в которых производится идентификация карты, ключа или кода пользователя, проверка на право владения им и санкционированный пропуск в зоны доступа (или запрет в случае предъявления неверного идентификатора). К точкам доступа относятся – двери, оснащенные электромеханическими или электромагнитными замками, турникеты, ворота, шлагбаумы, шлюзовые кабины.
* **Зоны доступа** – это замкнутые пространства (в том числе территория объекта), вход в которые может быть осуществлен только через точки доступа. К зонам доступа относятся – помещения, этажи, здания, охраняемая территория объекта.

Выбор типа точек доступа, распределение их по объекту и организация зон доступа производятся индивидуально исходя из структуры предприятия, внутренних требований к пропускному режиму, наличию особо важных зон доступа и других особенностей объекта.

Организация СКУД на объекте

Построение системы контроля и управления доступом на объекте начинается, как правило, с организации проходной и точек для контроля и управления въездом/выездом автомобилей. Далее на входе в каждое здание или сооружение объекта устанавливаются двери с замками, которые управляются контроллерами. Организуются также точки доступа для выхода на каждый этаж с лестничных клеток и лифтовых холлов. Необходимость в точках доступа в каждое помещение определяется внутренними требованиями к доступу на объекте, наличием в этих помещениях материальных ценностей или важной информации. При наличии на объекте особо важных зон (например, хранилища в банках), на входе в них устанавливаются точки доступа типа «шлюз». Необходимо отметить, что система контроля и управления доступом дополняет охранную сигнализацию в дневное время, не позволяя злоумышленникам проникнуть в помещения, когда они не находятся на охране. Основными параметрами для выбора системы контроля и управления доступом являются – количество и тип пропусков (пользователей), количество и тип точек доступа, количество уровней доступа и режим работы системы.

Структура СКУД

Каждая точка доступа, в общем случае, оснащается контроллером, считывателями электронных пропусков, преграждающим устройством (замок, турникет, шлагбаум и т.д.), датчиками положения двери и фиксации факта прохода. Все контроллеры объединяются по линии связи в единую систему, которая подключается к компьютеру. На компьютере устанавливается специализированное программное обеспечение, предназначенное для регистрации пропусков, назначения прав доступа их владельцам, оперативного контроля за обстановкой на объекте, формирования и вывода необходимых отчетов. Может устанавливаться дополнительное прикладное программное обеспечение, например, позволяющее вести учет рабочего времени каждого сотрудника.

Режимы работы

Системы контроля и управления доступом могут работать в автономном или сетевом режимах. Автономный режим работы отличается от сетевого отсутствием компьютера и линии связи между контроллерами.

**55 вопрос**

**Технические каналы утечки информации и их краткая характеристика**

**Утечка** - бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

**Утечка (информации) по техническому каналу** - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации

Технический канал утечки информации (ТКУИ), так же как и канал передачи информации, состоит из источника сигнала, физической среды его распространения и приемной аппаратуры злоумышленника.

**Классификация технических каналов утечки информации**

Основным признаком для классификации технических каналов утечки информации является физическая природа носителя. По этому признаку ТКУИ делятся на:

- оптические;

- радиоэлектронные;

- акустические;

- материально-вещественные.

Носителем информации в оптическом канале является электромагнитное поле (фотоны). Оптический диапазон подразделяется на:

- дальний инфракрасный поддиапазон 100 – 10 мкм (3 – 30 ТГц);

- средний и ближний инфракрасный поддиапазон 10 – 0,76 мкм (30 – 400 ТГц);

- видимый диапазон (сине-зелёно-красный) 0,76 – 0,4 мкм (400 – 750 ТГц).

В радиоэлектронном канале утечки информации в качестве носителей используются электрические, магнитные и электромагнитные поля в радиодиапазоне, а также электрический ток (поток электронов), распространяющийся по металлическим проводам. Диапазон частот радиоэлектронного канала занимает полосу частот от десятков ГГц до звукового. Он подразделяется на:

- низкочастотный 10 – 1 км (30 – 300 кГц);

- среднечастотный 1 км – 100 м (300 кГц – 3МГц);

- высокочастотный 100 – 10 м (3 – 30 МГц);

- ультравысокочастотный 10 – 1м (30 – 300 МГц);

и т.д. до сверхвысокочастотного 3 – 30 ГГц (10 – 1 см).

Носителями информации в акустическом канале являются упругие акустические волны, распространяющиеся в среде. Здесь различают:

- инфразвуковой диапазон 1500 – 75 м (1 – 20 Гц);

- нижний звуковой 150 – 5 м (1– 300 Гц);

- звуковой 5 – 0,2 м (300 – 16000 Гц);

- ультразвуковой от 16000 Гц до 4 МГц.

В материально-вещественном канале утечка информации производится путем несанкционированного распространения за пределы контролируемой зоны вещественных носителей с защищаемой информацией. В качестве вещественных носителей чаще всего выступают черновики документов и использованная копировальная бумага.

Каналы утечки информации можно также классифицировать по информативности на информативные, малоинформативные и неинформативные. Информативность канала оценивается ценностью информации, которая передается по каналу.

По времени проявления каналы делятся на постоянные, периодические и эпизодические. В постоянном канале утечка информации носит достаточно регулярный характер. К эпизодическим каналам относятся каналы, утечка информации в которых имеет случайный разовый характер.

В результате реализации технических каналов утечки информации, возможно возникновение следующих угроз:

- угроза утечки акустической информации;

- угроза утечки видовой информации;

- угроза утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Канал утечки информации, состоящий из передатчика, среды распространения и приемника, является одноканальным. Однако возможны варианты, когда утечка информации происходит более сложным путем - по нескольким последовательным или параллельным каналам. При этом используется свойство информации переписываться с одного носителя на другой. Например, если в кабинете ведется конфиденциальный разговор, то утечка возможна не только по акустическому каналу через стены, двери, окна, но и по оптическому - путем съема информации лазерным лучом со стекла окна или по радиоэлектронному с использованием установленной в кабинете радиозакладки. В двух последних вариантах образуется составной канал, состоящий из последовательно соединенных акустического и оптического (на лазерном луче) или акустического и радиоэлектронного (радиозакладка - среда распространения - радиоприемник) каналов.