1 Что понимается под защитой информации в системах и сетях?

Под защитой информации в системах и сетях понимается защита данных, передающихся внутри данной сети от несанкционированного доступа. Применяются меры по

• Ограничению физического доступа к сети.

• Защита от считывания данных

• Защита от вредоносных программ.

• Структурирование и контроль, управление доступом к сети.

• Защита от использования слабых мест. Например защита от Брут атак.

• Получение данных при помощи серии разрешенных действий. (Например зайти на сайт подбором пароля, и скопировать ники пользователей для создания базы данных)

2 Дайте определения ИБ КИС

ИБ КИС – Защищённость информации от намеренных и ненамеренных воздействий пользователем либо иным лицом.

• **Уровни безопасности:**

**• Национальный;**

**• Отраслевой;**

**• Корпоративный;**

**• Персонального.**

**Основные категории ИБ**: доступность (возможность за приемлемое время получить требуемую информационную услугу); целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения); конфиденциальность (защита от несанкционированного ознакомления).

3 Приведите классификацию угроз информации

Основные типы информационной безопасности:

* **Угрозы конфиденциальности** – незаконный, несанкционированный доступ к данным посторонними лицами (Например, кража баз данных).
* **Угрозы целостности данных** – незаконная, несанкционированная модификация, изменение, уничтожение данных. (Например, зайти на учебный сайт, и изменить ответы на тест).
* **Угрозы доступности** – ограничение, блокировка, (наверное, и распространение) доступа к данным. (Изменить чужой пароль на сайте).

4 Какие основные направления и методы реализации угроз Вам известны?

Если не прибегать к использованию интернета, то это

* **Брут атака.** Один из самых простых типов атак, работает на сайтах с плохой защитой при входе. В плане, неограниченное по времени и попыткам повторение входа на сайт, ввода логина и пароля. Как пример, данная уязвимость существует на сайте Md.ksu.edu.kz. Имея базу данных с логинами, а они устроены достаточно просто (их можно найти в авто вводе на пк в университете), в большинстве случаев достаточно знать фио пользователя чтобы составить примерный логин, можно легко, методом подбора подобрать пароль. Зачастую пароль состоит из 4 – 6 чисел, и инициалов.
* **Вирусы и вредоносное ПО** – программы, которые совершают вредоносные действия на компьютере. Например, простенькая программа, сбивающая картинку с рабочего стола, замаскированная под картинку. Вредоносное ПО отправляется в самораспаковывающийся архив, в нём настраивается картинка на фоне архива, и убирается настройка загрузки. После чего архив имеет расширение EXE. После этого, в названии файла выбирается пункт символов с зеркальной раскладкой. Таким образом файл имеющий название Скинь это ЛGPJ.exe станет иметь имя Скинь это Лехе.JPG.

Ещё, существуют вирусы, предоставляющие доступ к пк, и проходящему по нему трафику. Их называют **Троянами**. Они открывают лан порт, и дают доступ внешним устройствам к вашему пк.

* **DDoS атака –** атака на сервер путём превышения максимальной пропускной способности сервера. Допустим, сервер университета может обработать 10 000 запросов в единицу времени. Если большое количество пк будет отправлять большое количество запросов, и их количество превысит максимальное количество, начнут появляться ошибки и лаги, которые создают уязвимости в системе. Сервер может отключиться.
* **Несанкционированный доступ –** получение доступа к файлам используя слабые места, например, получение данных из SQL таблиц , путём добавления символа, если не ошибаюсь, верхнее подчёркивание, что позволяет получить несанкционированный доступ к данным.

**Ещё,** существуют способы отслеживания трафика в открытых сетях, например в кафе. Существуют специальные приложения. В истории был случай, когда крупную компанию взломали, и украли данные, подключившись к системе кондиционеров. То есть – это различные способы получения доступа к данным.

5 Что понимают под информационной системой?

**Информационная система** – система предназначенная для сбора, анализа, передачи, хранения, обработки, поиска и обеспечения безопасности информации. Она предназначена для своевременного обеспечения надлежащих людей надлежащей [информацией](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D1%8F). К ней относятся компьютеры, компьютерные сети, информационное и программное обеспечение, персонал. В зависимости от предметной области информационные системы могут весьма значительно различаться по своим функциям, архитектуре, реализации. Информационные системы ориентированы на конечного пользователя, не обладающего высокой квалификацией в области вычислительной техники. Они должны обладать простым, удобным, легко осваиваемым интерфейсом, который предоставляет конечному пользователю все необходимые для работы функции и в то же время не дает ему возможность выполнять какие-либо лишние действия.

6 Что называют информационными ресурсами?

Информационные ресурсы — в широком смысле — это совокупность данных, организованных для эффективного получения достоверной информации. Информационные ресурсы представляют собой отдельные документы и отдельные массивы документов (используют в библиотеках, архивах, фондах, банках данных, других информационных системах), это накопленная информация об окружающей действительности, зафиксированная на материальных носителях, обеспечивающих передачу информации во времени и пространстве между потребителями для решения конкретных задач.

7 Что составляет основу политики безопасности?

Основу политики безопасности составляет способ управления доступом, определяющий порядок доступа субъектов системы к объектам системы. Название этого способа, как правило, определяет название политики безопасности. В настоящее время лучше всего изучены два вида политики безопасности: избирательная и полномочная (мандатная).

Избирательное управление доступом – метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит.

Мандатное управление доступом – концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности.

8 Проанализируйте механизмы и свойства защиты информации

Выделяют следующие механизмы защиты информации:

· формирование и опознание подписи;

· контроль и разграничение доступа;

· система регистрации и учета информации;

· обеспечение целостности данных;

· обеспечение аутентификации;

· подстановка трафика;

· управление маршрутизацией;

· арбитраж или освидетельствование.

1. Формирование и опознание подписи. Ее механизм основывается на алгоритмах асимметричного шифрования и включает две процедуры: формирование подписи отправителем и ее опознание (верификацию) получателем. Первая процедура обеспечивает шифрование блока данных или его дополнение криптографической контрольной суммой, причем в обоих случаях используется секретный ключ отправителя. Вторая процедура основывается на использовании общедоступного ключа, знание которого достаточно для опознавания отправителя.

2. Контроль и разграничение доступа. Осуществляет проверку полномочий объектов (программ и пользователей) на доступ к ресурсам сети. В основе контроля доступа к данным лежит система разграничения доступа специалистов информационной технологии к защищаемой информации.

3. Система регистрации и учета информации. Отвечает за ведение регистрационного журнала, позволяет проследить за тем, что происходило в прошлом, и соответственно перекрыть каналы утечки информации. В регистрационном журнале фиксируются все осуществленные или неосуществленные попытки доступа к данным или программам. Содержание регистрационного журнала может анализироваться как периодически, так и непрерывно. В регистрационном журнале ведется список всех контролируемых запросов, осуществляемых специалистами, а также учет всех защищаемых носителей информации с помощью их маркировки, с регистрацией их выдачи и приема.

Система регистрации и учета является одним из эффективных методов увеличения безопасности в информационных системах и технологиях.

4. Обеспечение целостности данных. Применяется как к отдельному блоку, так и к потоку данных. Целостность блока является необходимым, но не достаточным условием целостности потока. Целостность блока обеспечивается выполнением взаимосвязанных процедур шифрования и дешифрования отправителем и получателем. Отправитель дополняет передаваемый блок криптографической суммой, а получатель сравнивает ее с криптографическим значением, соответствующим принятому блоку. Несовпадение свидетельствует об искажении информации в блоке. Однако описанный механизм не позволяет вскрыть подмену блока в целом. Поэтому необходим контроль целостности потока данных, который реализуется посредством шифрования с использованием ключей, изменяемых в зависимости от предшествующих блоков.

5. Обеспечение аутентификации. Это механизм установления подлинности, т.е. проверка, является ли объект (субъект) действительно тем, за кого себя выдает. Механизмы аутентификации подразделяются на одностороннюю и взаимную аутентификацию. При использовании односторонней аутентификации один из взаимодействующих объектов проверяет подлинность другого. Во втором случае – проверка является взаимной.

6. Подстановка трафика (подстановка текста). Используются для реализации службы засекречивания потока данных. Они основываются на генерации объектами информационной системы фиктивных блоков, их шифровании и организации передачи по каналам связи. Тем самым нейтрализуется возможность получения информации об информационной технологии и обслуживаемых ее пользователей посредством наблюдения за внешними характеристиками потоков информации, циркулирующих по каналам связи.

7. Управление маршрутизацией. Обеспечивают выбор маршрутов движения информации по коммуникационной сети таким образом, чтобы исключить передачу секретных сведений по скомпрометированным (небезопасным), физически ненадежным каналам.

8. Арбитраж. Обеспечивает подтверждение характеристик данных, передаваемых между объектами информационной системы, третьей стороной (арбитром). Для этого вся информация, отправляемая или получаемая объектами, проходит и через арбитра, что позволяет ему впоследствии подтверждать упомянутые характеристики.

9 Дайте понятие объекта защиты информации

Объект защиты информации – информация или носитель информации, либо же информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации. Также, к объектам защиты информации относят защищаемые информационные системы, защищаемый объект информации, хранилища носителей информации ограниченного доступа. В состав объектов защиты информации включаются: защищаемая информация, носитель защищаемой информации, информационный процесс, защищаемая информационная система, хранилища носителей ИОД, Защищаемый объект информатизации.

10 Что относят к информационным процессам?

Информационные процессы — это любые действия, заключающиеся в получении, создании, сборе, передачи, хранении и обработке информации.

К ним относятся:

* сбор;
* поиск;
* обработка;
* представление;
* хранение;
* передача;
* защита.

11 и 12 повторяют пункты 5 и 6 соответственно.

13 Примеры комплексов программно-аппаратных средств и преимущества использования

На самом деле термин «программно-аппаратные комплексы», не вполне корректен, ведь любые вычислительные системы по определению являются программно-аппаратными комплексами. Правильнее говорить об оптимизированных программно-аппаратных комплексах. Потому что каждый программно-аппаратный комплекс — это результат тщательнейшего проектирования, подбора компонентов, настройки программного обеспечения, комплектации решения функциональностью и, конечно, оптимизации.  
  
Аппаратное обеспечение и программное обеспечение проектируются, тестируются и отлаживаются совместно. И если вы знаете, на каком оборудовании будут работать приложения, то вы можете добиться высочайшей производительности, вероятность «сюрпризов» от несовместимости компонентов при этом становится меньше, а оказание поддержки — проще. Заказчикам не приходится подбирать и оптимизировать компоненты — серверы, диски, процессоры, сетевые компоненты, память и т.п. Устанавливать и настраивать программное обеспечение, тестировать работоспособность каждого сервера, заниматься их последующим обновлением и т.п. тоже не нужно. Существенно упрощается обслуживание ИТ-инфраструктуры.