1. Каковы способы контроля целостности потока сообщений

Для контроля целостности потока сообщений можно, например:

* присвоить сообщению порядковый номер целостности;
* использовать в алгоритмах шифрования сцепление с предыдущим сообщением.

При использовании порядкового номера целостности, который может включать в себя порядковый номер сообщения и имя источника, приемник хранит последний номер принятого сообщения каждого источника. Для контроля целостности приемник проверяет, например, что порядковый номер целостности текущего сообщения от данного источника на единицу больше номера предыдущего сообщения. Если в качестве порядкового номера целостности используется время отправки сообщения, то проверяется, действительно ли время отправки и время приема близки друг к другу с точностью до задержки сообщения в канале связи и разности хода часов источника и приемника.

1. Какие существуют способы контроля целостности сообщений при взаимном доверии сторон

* Имитовставка;
* Шифрование;
* Контроль целостности потока сообщений;

Электронная подпись применяется в информационных системах, в которых отсутствует взаимное доверие сторон.

1. Как контролировать целостность сообщений при высоком уровне помех в каналах связи

Для контроля целостности потока сообщений можно, например:

* присвоить сообщению порядковый номер целостности;
* использовать в алгоритмах шифрования сцепление с предыдущим сообщением.

При использовании порядкового номера целостности, который может включать в себя порядковый номер сообщения и имя источника, приемник хранит последний номер принятого сообщения каждого источника.

1. Как организован обмен документами, заверенными цифровой подписью

Заключается в том, что каждый абонент сети имеет личный секретный ключ, на котором он формирует подпись и известную всем другим абонентам сети проверочную комбинацию, необходимую для проверки подписи. Цифровая подпись вычисляется на основе сообщения и секретного ключа отправителя. Любой получатель, имеющий соответствующую проверочную комбинацию, может аутентифицировать сообщение по подписи.

**5. В чем отличие и сходство обычной и цифровой подписей?**

Сходства:

Подтверждение личности

Передача на расстояние

Сложность подделки

Различие:

-Включение

Обычная подпись включена в документ; это - часть документа. Когда мы пишем чек, подпись находится на чеке; это - не отдельный документ. Но когда мы подписываем документ в цифровой форме, мы передаем подпись как отдельный документ. Передатчик передает два документа: сообщение и подпись. Получатель получает оба документа и проверяет, что подпись принадлежит предполагаемому передатчику. Если это доказано, сообщение сохраняется; иначе оно отклоняется.

-Метод проверки

Второе отличие между двумя типами подписей - метод подтверждения подписи. В случае обычной подписи, когда получатель получает документ, он сравнивает подпись на документе с подписью в архиве. Если они одинаковые, документ подлинный. Получатель должен иметь в архиве копию для сравнения этой подписи. При цифровой подписи - получатель получает сообщение и подпись, но копия подписи не хранится нигде. Получатель должен применить методику проверки комбинации сообщения и подписи, чтобы проверить подлинность.

-Отношения

В случае обычной подписи есть отношения "один ко многим" между подписью и документами. Человек использует ту же самую подпись, чтобы подписать много документов. Для цифровой подписи есть непосредственные отношения между подписью и сообщением. Каждое сообщение имеет свою собственную подпись. Подпись одного сообщения не может использоваться в другом сообщении. Если Боб получает два сообщения, один за другим, от Алисы, он не может использовать подпись первого сообщения, чтобы проверить второе. Каждое сообщение нуждается в новой подписи.

-Резервное копирование

Другая разность между двумя типами подписей - качество, названное резервное копирование. При обычной подписи ее копия на поступившем документе может отличаться от копии, сохраненной в архиве. В цифровой подписи нет такого различия, если нет указателя времени (такого как метка времени) на документе.

**6. Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?**

*Корректность транзакций*

*Аутентификация пользователей*

*Минимизация привилегий*

*Разграничение функциональных обязанностей* – принцип подразумевает организацию работы с данными таким образом, что в каждой из ключевых стадий, составляющих единый критически важный, с точки зрения важности, процесс, необходимо участие нескольких пользователей. Это гарантирует не использование одним пользователем всего процесса целиком.

*Аудит произошедших событий*

*Объективный контроль* – суть данного принципа в том, что контроль целостности данных имеет смысл лишь тогда, когда эти данные отражают реальное положение вещей.

*Управление передачей привилегий* – касается политики безопасности. Если схема назначений привилегий неадекватно отражает орг-структуру предприятия или не позволяет администраторам безопасности гибко манипулировать ею для обеспечения эффективности деятельности, защита становиться обременительной и провоцирует попытки обойти её

*Обеспечение непрерывной работоспособности*

*Простота использования защитных механизмов*

7. В одной из наиболее распространенных трактовок под целостностью данных подразумевается отсутствие ненадлежащих изменений. Смысл понятия «ненадлежащее изменение» раскрывается Д. Кларком и Д. Вилсоном: ни одному пользователю автоматизированной системы, в том числе и авторизованному, не должны быть разрешены такие изменения данных, которые повлекут за собой их разрушение или потерю.

8.Что означает контроль целостности данных на уровне содержания?

Приведите примеры.

Защита от угрозы нарушения целостности информации на уровне содержания в обычной практике рассматривается как защита от дезинформации.

Для успешности борьбы с вероятной дезинформацией следует:

· различать факты и мнения;

· применять дублирующие каналы информации;

· исключать все лишние промежуточные звенья и т.п.

**9. Как обеспечить целостность данных при их хранении?**

Организационно-технологические меры защиты целостности информации на электронных носителях можно разделить на две основные группы:

* организационные меры по поддержке целостности информации;
  + создание резервных копий информации, хранимой на электронных носителях;
  + обеспечение правильных условий хранения и эксплуатации носителей.
* технологические меры контроля целостности битовых последовательностей.
  + контрольный код, контрольные числа которого записываются после соответствующих областей, причем в контролируемую область включаются соответствующие маркеры.
  + методы имитозащиты, основанные на криптографических преобразованиях.

**10. Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?**

*Надежность* — свойство объекта сохранять во времени значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, ремонта, хранения и транспортировки.

Несмотря на явное сходство в определениях надежности для аппаратных средств и программного обеспечения, фактически последнее имеет принципиальные отличия:

* программа в большинстве случаев не может отказать случайно;
* ошибки в программном обеспечении, допущенные при его создании, зависят от технологии разработки, организации работ и квалификации исполнителей;
* ошибки не являются функцией времени;
* причиной отказов является набор входных данных, сложившихся к моменту отказа.

**11. Следует ли различать защиту от случайных угроз и от действий злоумышленника при обеспечении беспрепятственного доступа к информации? Обоснуйте свой ответ.**

*(????Я не нашёл норм ответа в учебнике ????)*

Да, так как действия злоумышленника могут планироваться заранее и в процессе данной планировки злоумышленник способен заранее изучить систему различными способами наблюдения. Также злоумышленник способен воздействовать на систему удаленно, вне контролируемой зоны.

**12. Как защитить программное обеспечение от изучения логики его работы?**

*(????Ну такое ????)*

Важен вопрос обеспечения секретности параметров информационной системы, в которой циркулирует конфиденциальная информация. Методы защиты параметров такой системы аналогичны общим методам, применяемым для защиты конфиденциальности информации.

**14. Как изменяется надежность аппаратуры с течением времени?**

При обеспечении защиты информационной системы от угрозы отказа функционирования обычно считается, что надежность аппаратных компонентов достаточно высока и данной составляющей в общей надежности можно пренебречь. Это связано с тем, что темпы морального старения вычислительной техники значительно опережают темпы ее физического старения и замена вычислительной техники, как правило, происходит до ее выхода из строя.

**15. Каковы способы повышения надежности аппаратуры и линий связи?**

*(?????? Я всё ещё хз, что сюда писать ??????)*

Линии связи:

* Имитовставка. Для обеспечения целостности в текст сообщения часто вводится некоторая дополнительная информация(*имитовставка* (в зарубежных источниках используется термин код аутентификации сообщений — Message Authentication Code (MAC)), которая легко вычисляется, если секретный ключ известен, и является трудновычислимой в противном случае.
* Шифрование. Целостность данных можно обеспечить и с помощью их шифрования симметричным криптографическим алгоритмом при условии, что подлежащий защите текст обладает некоторой избыточностью.
* Контроль целостности потока сообщений. Контроль целостности потока сообщений помогает обнаружить их повтор, задержку, переупорядочение или утрату. Для контроля целостности потока сообщений можно, например:
  + присвоить сообщению порядковый номер целостности;
  + использовать в алгоритмах шифрования сцепление с предыдущим сообщением.
* Электронная подпись. Термин «электронная подпись» (ЭЦП) используется для методов, позволяющих устанавливать подлинность автора сообщения при возникновении спора относительно авторства этого сообщения.

Для аппаратуры:

* Обеспечение контроля работы компонентов оборудования и их взаимосвязи;
* Упрощение схемы технического устройства при проектировании и разработке;
* Выявление скрытых неисправностей, допущенных при проектировании или нарушении технологии изготовления;
* Контроль износа и устаревания оборудования.