Вопросы по теме 5

Построение систем защиты от угрозы нарушения целостности …

**1. Каковы способы контроля целостности потока сообщений?**

Способы контроля целостности.

1.**Шифрование** (симметричное, асимметричное)

Шифрование может быть использовано для контроля целостности сообщения при условии структурированности сообщения. Пример: структурированность протокола пакета IPv4 позволяет использовать шифрование для контроля целостности.

2.**Хеш-функция**.

Хэш-функцией называется односторонняя функция, предназначенная для получения хэш-кода (дайджеста, «отпечатков пальцев») файла, сообщения или некоторого блока данных.

3.**Код аутентичности сообщения**

(MAC).

Простым способом преобразовать однонаправленную хэш-функцию в имитовставку (MAC) является шифрование хэш-значения симметричным алгоритмом. Такой MAC может быть преобразован в однонаправленную хэш-функцию с помощью раскрытия ключа.

**2. Какие существуют способы контроля целостности сообщений при взаимном доверии сторон?**

- Использование электронных подписей.

- Договор о неразглашении.

- Разграничение доступа у разных должностей

**3. Как контролировать целостность сообщений при высоком уровне помех в каналах связи?**

Методы контроля целостности данных:

1. Полная копия данных (Создаются полные копии данных и потом сверяются. )
2. Контрольная сумма (Контрольная сумма - значение, рассчитанное по входным данным с помощью определённого алгоритма.)
3. Хеш (Хеш (хэш, криптографический хеш) - значение, рассчитанное по входным данным с помощью криптографического алгоритма.)
4. Имитовставка (Имитовставка -  значение, рассчитанное по входным данным с помощью криптографического алгоритма с использованием секретного элемента (ключа), известного только отправителю и получателю.)
5. ЭЦП (Электронная цифровая подпись - зашифрованное значение вычисленного хеша по входным данным.)

**4. Как организован обмен документами, заверенными цифровой подписью?**

Сверка открытого ключа и заверенного документа.

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

Отличие первое: проверка собственноручной подписи может осуществляться: только путем визуального осмотра (вероятность ошибки высокая), или сравнением с образцом собственноручной подписи (вероятность ошибки средняя), или путем проведения графологической экспертизы (вероятность ошибки низкая).

Отличие второе: собственноручная подпись не несет в себе информации о правомочности лица, подписавшего документ.

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

1. Конфиденциальность: свойство информационных ресурсов, в том числе информации, связанное с тем, что они не станут доступными и не будут раскрыты для неуполномоченных лиц.

2. Целостность: неизменность информации в процессе ее передачи или хранения.

3. Доступность: свойство информационных ресурсов, в том числе информации, определяющее возможность их получения и использования по требованию уполномоченных лиц.

**7. Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?**

В настоящее время всеобщей компьютеризации благополучие и даже жизнь многих людей зависят от обеспечения информационной безопасности множества компьютерных систем обработки информации, а также контроля и управления различными объектами.

При нарушении целостности данных можно будет саботировать и компрометировать определенное лицо, либо получить информацию, которая будет использована против данного лица.

**8. Что означает контроль целостности данных на уровне содержания?**

Означает неизменность содержимого документа.

**Приведите примеры.**

Например при передаче письменного приказа о наложении штрафа на определенное лицо, достаточно изменить реквизиты выплаты штрафа, чтобы получить деньги.

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

- Создание резервных копий

- Ограничение доступа

- Создание средств защиты от сбоев ведущих к потере информации.

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

Надежность системы – характеристика способности программного, аппаратного, аппаратно-программного средства выполнить при определенных условиях требуемые функции в течение определенного периода времени.

С точки зрения надежности принципиальное отличие ПО от аппаратуры состоит в том, что программы не изнашиваются и, следовательно, не выходят из строя из-за поломки. Безотказность ПО определяется его корректностью (правильностью) и, следовательно, целиком зависит от наличия в нем ошибок, внесенных на этапах его создания. В то время как безотказность аппаратуры определяется в основном случайными отказами, зависящими от изменений параметров аппаратуры во время эксплуатации.

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

Да следует.

**Обоснуйте свой ответ.**

Из-за случайной угрозы может быть нарушена целостность информации , даже если предприняты меры по охране информации от действий злоумышленников.

-Например при отключение электропитания могут быть утеряны определенные данные.

-Либо при утере флешки с данными сотрудником.

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

Основными инструментами для исследования программ являются дизассемблеры и отладчики.

Универсальным методом противодействия дизассемблированию программы является шифрование. Рекомендуется использовать шифрование с открытым ключом

Существует два отладочных механизма:

1) контрольные точки останова и

2) трассировка программы.

Идея первого механизма заключается во внесении в программный код специального однобайтового кода (0xСС) - так называемой контрольной точки останова. Заметим, что можно внести в программный код любое количество таких точек. Во время выполнения программы при достижении контрольной точки останова возникает исключительная ситуация - прерывание int 3. В этот момент процессор останавливает работу программы для дальнейших распоряжений пользователя. Для того, чтобы позже продолжить работу программы с точки останова, в стеке запоминаются значения регистра флагов, регистра CS (указатель текущего кодового сегмента) и регистра IP (указатель на следующую выполнимую команду). При этом сбрасывается флаг трассировки.

Для усиления защиты от пошагового выполнения программы авторы успешно используют значение флага трассировки (в совокупности с другими параметрами) для расшифровки критических участков или, что еще сложнее для взлома, в арифметических выражениях.

**13. Предложите меры по обеспечению более надежной работы ЛВС университета.**

**-** Установка новых антивирусов

- Запрет на использование флеш-накопителей студентами

- Обновление оборудования

- Установка бесперебойников

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

В следствие износа компонентов системы надежность оборудования падает.

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

1. резервирование;

2. уменьшение интенсивности отказов системы;

3. сокращение времени непрерывной работы;

4. уменьшение среднего времени восстановления работоспособного

состояния.