**Вопросы к экзамену по дисциплине «Основы защиты информации»**

**4-й курс направления «программная инженерия»**

**январь 2022**

1. Информация и ее свойства, связанные с обеспечением безопасности. Качество информации. Утечка информации.
2. Конфиденциальность, целостность, доступность информации.
3. Угрозы информационной безопасности. Источники угроз.
4. Цели и средства защиты информации.
5. Классификация методов защиты информации.
6. Стандарты информационной безопасности.
7. Уязвимости ПО. Безопасное программирование.
8. Программная закладка.
9. Скрытый канал.
10. Недокументированные возможности.
11. Сканеры уязвимостей.
12. Обнаружение и предотвращение вторжений.
13. Контроль доступа субъекта.
14. Идентификация. Аутентификация. Авторизация.
15. Разграничение доступа.
16. Криптография. Криптоанализ. Криптология.
17. Симметричное шифрование. Шифр Вижинера. Шифр Цезаря. Пропорциональный шифр. Шифр перестановки.
18. “Вскрытие” симметричных шифров. Усиление симметричных шифров.
19. Сеть Фейстеля. Блочное шифрование.
20. Требования к алгоритму шифрования.
21. DES.
22. ГОСТ-28147-89.
23. Понятие хеш-функции.
24. Требования к криптохеш-функциям.
25. Использование блочных алгоритмов шифрования для формирования хеш-функции.
26. MD5.
27. Семейство алгоритмов SHA.
28. ГОСТ 34.11-2018.
29. Принцип поточного шифрования. Гаммирование.
30. ГСЧ и ГПСЧ.
31. Криптосвойства ГПСЧ.
32. Линейный конгруэнтный ГПСЧ.
33. Метод Фибоначчи с запаздываниями (Lagged Fibonacci Generator).
34. ГПСЧ на основе алгоритма BBS.
35. ГСПЧ на основе сдвиговых регистров с обратной связью.
36. ГСЧ.
37. Симметричное шифрование. Односторонние функции.
38. Алгоритм шифрования Эль-Гамаля.
39. Криптосистема Меркла-Хеллмана.
40. RSA.
41. Алгоритм обмена ключа Диффи-Хеллмана.
42. Информация и ее свойства, связанные с обеспечением безопасности. Качество информации. Утечка информации.

**Информация** - это любое представление данных, которое имеет ценность и может быть использовано для принятия решений, планирования или осуществления действий. Это может быть что угодно, от секретных правительственных планов до личных данных пользователя.

**Свойства информации**, связанные с обеспечением безопасности:

* **Конфиденциальность**: Означает, что информация доступна только авторизованным лицам или системам. Нарушение конфиденциальности приводит к несанкционированному доступу к информации.
* **Целостность**: Означает, что информация является полной, точной и не подвергалась несанкционированной модификации. Нарушение целостности означает, что информация повреждена, искажена или изменена без разрешения.
* **Доступность**: Означает, что авторизованные лица или системы могут получить доступ к информации, когда это необходимо. Нарушение доступности приводит к невозможности использования информации.
* **Подлинность** (Аутентичность): Означает, что информация получена из достоверного источника и не является подделкой. Подтверждение подлинности критически важно для принятия обоснованных решений.
* **Неотказуемость** (Неотрекаемость): Означает, что отправитель информации не может отрицать факт ее отправки, а получатель не может отрицать факт ее получения. Это важно для обеспечения юридической силы транзакций и других операций.

**Качество информации** влияет на ее ценность и на то, насколько эффективно она может быть использована. Вот некоторые ключевые атрибуты качества информации:

* **Точность**: Насколько информация соответствует действительности.
* **Полнота**: Содержит ли информация все необходимые данные.
* **Актуальность**: Насколько информация своевременна и соответствует текущему моменту.
* **Релевантность**: Насколько информация соответствует потребностям пользователя.
* **Понятность**: Насколько легко информация воспринимается и интерпретируется.
* **Согласованность**: Насколько информация согласована с другими источниками информации.

**Утечка информации:**

Утечка информации - это несанкционированное раскрытие конфиденциальной информации лицам или системам, не имеющим права доступа к ней. Утечка может происходить разными путями:

* **Технические каналы**: Взлом компьютерных систем, перехват сетевого трафика, использование вредоносного программного обеспечения (вирусов, троянов), несанкционированный доступ к базам данных.
* **Человеческий фактор:** Небрежность сотрудников (например, отправка конфиденциальной информации по электронной почте без шифрования), социальная инженерия (манипулирование людьми с целью получения информации), подкуп, шпионаж.
* **Физические каналы**: Кража или потеря носителей информации (ноутбуков, USB-накопителей, документов), несанкционированный доступ к физическим объектам (офисам, серверам), прослушивание помещений.
* **Анализ побочных данных:** Получение информации из метаданных, шаблонов использования, анализа сетевого трафика, и других непрямых источников.

1. Конфиденциальность, целостность, доступность информации.

Конфиденциальность, целостность и доступность (ЦЦД) - основа информационной безопасности.

* **Конфиденциальность**: Защита от несанкционированного доступа к информации (кто не должен знать, не должен получить доступ). Обеспечивается шифрованием, контролем доступа, политиками безопасности.
* **Целостность**: Обеспечение точности и полноты информации, защита от несанкционированной модификации (никто не должен изменить информацию без разрешения). Обеспечивается контролем версий, резервным копированием, хешированием.
* **Доступность**: Обеспечение своевременного и надежного доступа к информации авторизованным пользователям (информация должна быть доступна тогда, когда она нужна). Обеспечивается отказоустойчивостью, балансировкой нагрузки, планами аварийного восстановления.

1. Угрозы информационной безопасности. Источники угроз.

**Угроза информационной безопасности:** Потенциальное событие, действие или бездействие, которое может нанести ущерб информации, системам и ресурсам.

**Основные типы угроз:**

* Конфиденциальность: Несанкционированный доступ к информации.
* Целостность: Искажение или уничтожение информации.
* Доступность: Блокирование доступа к информации или ресурсам.

**Основные источники угроз:**

* Злоумышленники: Хакеры, конкуренты, криминальные группы, инсайдеры.
* Пользователи: Ошибки, халатность, некомпетентность.
* Техногенные факторы: Ошибки ПО, аппаратные сбои, перебои в электроснабжении.
* Стихийные факторы: Природные катаклизмы.

**Ключевые примеры угроз:**

* Вирусы и вредоносное ПО.
* Фишинг и социальная инженерия.
* DDoS-атаки.
* Взлом учетных записей.
* Кража оборудования.
* Утечки информации.

1. Цели и средства защиты информации.

Цели:

* Снижение вероятности техногенных угроз,
* Снижение ущерба от стихийных явлений,
* Снижение вероятности угроз, реализуемых по причине халатности или недостаточной квалификации,
* Защита от нарушителей, действующих из любопытства или самоутверждения,
* Защита от нарушителей, действующих злонамеренно.

Средства:

* Аппаратные (межсетевые экраны, IDS/IPS, шифрование)
* Программные (антивирусы, контроль доступа, резервное копирование)
* Организационные (политики, обучение, управление доступом)
* Физические (ограничение доступа, видеонаблюдение)

1. Классификация методов защиты информации.



1. Стандарты информационной безопасности.

* ГОСТ 28147-89 – стандарт шифрования государственной тайны,
* ГОСТ 34.11—2018 – стандарт хэширования,
* ГОСТ 34.10-2018 – стандарт цифровой подписи,
* ГОСТ Р 50739-95 – стандарт защиты от несанкционированного доступа к информации.
* ГОСТ 58142 «Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения»

УК РФ Глава 28. Преступления в сфере компьютерной информации

1. Уязвимости ПО. Безопасное программирование.

* Уязвимость ПО - недостаток программно-технического средства или информационной системы в целом, который может быть использован для реализации угроз безопасности информации.
  + Уязвимость кода,
  + Уязвимость конфигурации,
  + Уязвимость архитектуры,
  + Организационная уязвимость,
  + Многофакторная уязвимость.

**ГОСТ** Р 56939-2016 Разработка **безопасного** программного обеспечения.

Методика разработки программного обеспечения, предотвращающая случайное внедрение уязвимостей и обеспечивающая устойчивость к воздействию вредоносного ПО и несанкционированному доступу.

* Defensive programming(оборонительное программирование)
* Secure coding(безопасное программирование)

1. Программная закладка.

**Закла́дка** (**программная закладка**) — скрытно внедрённая в защищенную систему программа, либо намеренно измененный фрагмент программы, который позволяет злоумышленнику осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты. Закладка может быть внедрена самим разработчиком программного обеспечения.

Часто программные закладки выполняют роль перехватчиков паролей, трафика, а также служат в качестве проводников для компьютерных вирусов.

Программные закладки невозможно обнаружить при помощи стандартных антивирусных средств, их выявление возможно только специальными тестовыми программами.

1. Скрытый канал.

Скрытый канал – это непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности.

С помощью скрытых каналов могут быть реализованы следующие нарушения политики безопасности:

* Угроза внедрения вредоносных программ и данных .
* Угроза подачи нарушителем команд агентом для выполнения его функций .
* Угроза утечки криптографических ключей, паролей (несанкционированный доступ к ним) или отдельных информационных объектов .

Выявление

* ***статистический метод*** - подразумевает сбор статистических данных о пакетах, проходящих через защищаемый участок сети, без внесения в них каких-либо изменений.
* ***сигнатурный метод*** - аналогичен способу, используемому антивирусным ПО для поиска вредоносных программ. При наличии набора известных реализаций скрытых каналов, для каждой из них формируется сигнатура. В потоке данных проводится поиск таких сигнатур.

1. Недокументированные возможности.

Это возможности устройств или ПО, не описанные в официальной документации. Они могут быть:

• Сознательно заложены разработчиками (для тестирования, расширения, совместимости, скрытого контроля).

• Возникнуть случайно как побочные эффекты.

НДВ отличаются от скрытых, но задокументированных возможностей. Их обычно находят через обратную разработку или случайно.

1. Сканеры уязвимостей.

Программы, которые автоматически ищут известные уязвимости в программном обеспечении, сетевых устройствах и веб-приложениях.

Зачем нужны:

* Поиск слабых мест: Обнаружение уязвимостей до того, как ими воспользуются злоумышленники.
* Оценка рисков: Определение приоритетных областей для усиления безопасности.
* Соответствие стандартам: Соблюдение требований безопасности.
* Автоматизация тестирования: Ускорение процесса проверки безопасности.

Web:

* OWASP ZAP
* W9scan
* Wapiti
* Arachni
* Paros
* Tenable.io
* Burp Suite Pro
* Acunetix

1. Обнаружение и предотвращение вторжений.

Комплекс мер и инструментов, направленных на выявление и блокировку несанкционированного доступа или вредоносной активности в компьютерных системах и сетях.

Две основные категории:

* Системы обнаружения вторжений (IDS):
  + Что делают: Мониторят трафик и активность в системе/сети на предмет подозрительного поведения.
  + Как работают: Используют сигнатурный анализ (сопоставление с известными атаками) и аномальный анализ (выявление отклонений от нормального поведения).
  + Действия: Обнаруживают, регистрируют и оповещают об инцидентах, но не блокируют их активно. Это значит, что они информируют о проблеме, но не предпринимают действий для ее устранения.
* Системы предотвращения вторжений (IPS):
  + Что делают: Расширенная версия IDS, которая не только обнаруживает, но и блокирует или смягчает атаки в реальном времени.
  + Как работают: Аналогично IDS, но имеют возможность автоматически реагировать на обнаруженные угрозы.
  + Действия: Блокируют трафик, закрывают порты, сбрасывают соединения, карантинируют файлы, и т.д. Активно предотвращают дальнейшее развитие атаки.

UTM — это универсальный пакет утилит, сочетающий в себе множество мелких модулей защиты. UTM бывают программными или аппаратными и, как правило, включают в себя сразу IDS, IPS, файервол, а зачастую и антивирус, прокси-сервер, почтовые фильтры, VPN и т.д.

1. Контроль доступа субъекта.
2. Идентификация. Аутентификация. Авторизация.
3. Разграничение доступа.
4. Криптография. Криптоанализ. Криптология.
5. Симметричное шифрование. Шифр Вижинера. Шифр Цезаря. Пропорциональный шифр. Шифр перестановки.
6. “Вскрытие” симметричных шифров. Усиление симметричных шифров.
7. Сеть Фейстеля. Блочное шифрование.
8. Требования к алгоритму шифрования.
9. DES.
10. ГОСТ-28147-89.
11. Понятие хеш-функции.
12. Требования к криптохеш-функциям.
13. Использование блочных алгоритмов шифрования для формирования хеш-функции.
14. MD5.
15. Семейство алгоритмов SHA.
16. ГОСТ 34.11-2018.
17. Принцип поточного шифрования. Гаммирование.
18. ГСЧ и ГПСЧ.
19. Криптосвойства ГПСЧ.
20. Линейный конгруэнтный ГПСЧ.
21. Метод Фибоначчи с запаздываниями (Lagged Fibonacci Generator).
22. ГПСЧ на основе алгоритма BBS.
23. ГСПЧ на основе сдвиговых регистров с обратной связью.
24. ГСЧ.
25. Симметричное шифрование. Односторонние функции.
26. Алгоритм шифрования Эль-Гамаля.
27. Криптосистема Меркла-Хеллмана.
28. RSA.
29. Алгоритм обмена ключа Диффи-Хеллмана.