ОПК-3

1. Дайте определение терминам информация и информационные отношения

2. Что такое автоматизированная система обработки информации и управления?

3. Что такое информационная безопасность автоматизированной системы?

4. Перечислите и раскройте базовые свойства защищаемой информации и систем ее обработки.

5. Что такое целостность информации?

6. Что такое доступность информации?

7. Что такое конфиденциальность информации?

8. . Особенности современных автоматизированных систем обработки информации и управления как объекта защиты

9. Дайте определение угрозы безопасности информации.

10.Дайте определение уязвимости объекта/ информационной системы.

11. Виды угроз информационной безопасности

12. Приведите примеры коммерческой тайны предприятия

13.Приведите примеры основных преднамеренных искусственных угроз информационной безопасности.

14.Приведите примеры основных случайных искусственных угроз информационной безопасности.

15. Какие виды нарушителей информационной безопасности Вы знаете?

16.Есть разница между понятиями нарушитель и злоумышленник, если есть – какая?

17. Перечислите и раскройте основные меры противодействия угрозам безопасности (методы защиты информации).

18. Определение канала утечки информации.

19. Какие виды технических каналов утечки Вы знаете?

20. Основные принципы обеспечения безопасности автоматизированных систем обработки информации.

21. Перечислите основные механизмы обеспечения конфиденциальности информации.

22. Перечислите основные механизмы обеспечения доступности информации.

23. Перечислите основные механизмы обеспечения целостности информации.

24. Раскройте понятие идентификация

25. Раскройте понятие аутентификация.

26. Какие виды систем аутентификации Вы знаете?

27. Что такое биометрическая аутентификация? Приведите примеры.

28. Перечислите особенности парольных систем аутентификации.

29. Рекомендации по практической реализации парольных систем аутентификации.

30. Какие методы (модели) разграничения доступа Вы знаете? Кратко опишите их.

31. Какие криптографические методы обеспечения конфиденциальности информации Вы знаете?

32. Какие алгоритмы шифрования Вы знаете?

33. Раскройте понятие симметричных криптосистем.

34. Раскройте понятие асимметричных криптосистем.

35. Опишите основные способы (средства) обеспечения сетевой безопасности.

36. Что такое межсетевой экран?

37. Что такое система обнаружения вторжений/атак?

38. Протоколирование и аудит в системе информационной безопасности.

39. Перечислите основные принципы обеспечения целостности (Кларка-Вилсона).

40. Что такое ЭЦП и для чего они применяются?

41. Что такое хэш-функции и для чего они применяются?

42. Есть ли разница в дублировании и зеркалировании серверов, если есть –какая?

43. Какие механизмы защиты применяются от угроз нарушения доступности?

44. Какие базовые механизмы защиты информации в операционных системах Вам известны?

45. Перечислите основные организационно-распорядительные документы, необходимые для организации комплексной

системы безопасности информации.

46. Что такое СКУД? Примеры.

47. Что такое контролируемая зона?

48. Что такое политика информационной безопасности организации?

49. Какие основные разделы должна содержать политика информационной безопасности организации?

50. Что такое организационные методы защиты информации? Примеры.

ОПК-3

1.Сведения любого характера (производственные, технические, экономические, организационные и др.), в том

числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах

осуществления профессиональной деятельности, которые имеют действительную или потенциальную

коммерческую ценность

в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном

основании, -это… а) информация, составляющая коммерческую тайну;

б) информация, составляющая государственную тайну;

в) персональные данные;

г) информация, составляющая профессиональную тайну;

д) все ответы верны.

УП: z11.03.02\_2023\_Сети связи и системы коммутации.plx стр. 7

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию и на

информацию ограниченного доступа, к которой можно отнести: а) государственная тайна;

б) служебная тайна;

в) конфиденциальная информация;

г) персональные данные;

д) все ответы верны.

3.Распределите следующие информационные ресурсы по видам: 1 -общедоступная информация и 2 -

информация, которую можно отнести к коммерческой тайне:

а) информация о ноу-хау;

б) условия действующих контрактов;

в) документы, дающие право на осуществление предпринимательской деятельности;

г) планы, перспективы, предполагаемые шаги по развитию компании;

д) учредительные документы юридического лица;

е) о численности и оплате труда работников некоммерческих организаций

**1. Информация и информационные отношения**

* **Информация** — это данные, сведения или знания, представленные в любой форме, которые могут быть восприняты, интерпретированы и использованы.
* **Информационные отношения** — это совокупность общественных отношений, возникающих в процессе создания, передачи, обработки, использования и защиты информации.

**2. Автоматизированная система обработки информации и управления (АСОИУ)**  
АСОИУ — это комплекс технических, программных и организационных средств, обеспечивающий сбор, хранение, обработку, передачу и управление информацией с минимальным участием человека.

**3. Информационная безопасность автоматизированной системы (ИБ АС)**  
Информационная безопасность АС — это состояние защищенности информации и ресурсов АС от угроз нарушения их конфиденциальности, целостности и доступности.

**4. Базовые свойства защищаемой информации и систем ее обработки**

* **Конфиденциальность** — доступ к информации только уполномоченным лицам.
* **Целостность** — защита от несанкционированного изменения или уничтожения данных.
* **Доступность** — обеспечение возможности использования информации и ресурсов, когда это необходимо.

**5. Целостность информации**  
Целостность — это свойство информации сохранять свои оригинальные характеристики без искажений, утрат или несанкционированных изменений.

**6. Доступность информации**  
Доступность — это способность системы обеспечивать доступ к информации для уполномоченных пользователей в требуемое время.

**7. Конфиденциальность информации**  
Конфиденциальность — это защита информации от несанкционированного доступа.

**8. Особенности современных АСОИУ как объекта защиты**  
Современные АСОИУ характеризуются распределенной архитектурой, использованием сетевых технологий, интеграцией с облачными системами и высокой зависимостью от программного обеспечения.

**9. Угроза безопасности информации**  
Угроза безопасности информации — это потенциальное событие или действие, способное нанести ущерб информационным ресурсам.

**10. Уязвимость объекта/информационной системы**  
Уязвимость — это слабое место системы, которое может быть использовано для реализации угрозы.

**11. Виды угроз информационной безопасности**

* Естественные: пожары, наводнения.
* Искусственные: преднамеренные (вирусы, атаки), случайные (ошибки персонала).

**12. Примеры коммерческой тайны предприятия**

* Клиентская база.
* Производственные технологии.
* Финансовые отчеты.

**13. Примеры преднамеренных искусственных угроз**

* Хакерские атаки.
* Распространение вредоносного ПО.
* Шпионаж.

**14. Примеры случайных искусственных угроз**

* Ошибки в конфигурации ПО.
* Случайное удаление данных.
* Сбои оборудования.

**15. Виды нарушителей информационной безопасности**

* Внутренние (сотрудники).
* Внешние (хакеры, конкуренты).

**16. Разница между нарушителем и злоумышленником**  
Злоумышленник действует умышленно с целью нанести вред, нарушитель может быть неосознанным.

**17. Основные меры противодействия угрозам**

* Организационные.
* Технические.
* Программные.

**18. Канал утечки информации**  
Канал утечки информации — это способ, через который информация может быть перехвачена, украдена или искажена.

**19. Виды технических каналов утечки**

* Электромагнитные.
* Акустические.
* Вибрационные.

**20. Принципы обеспечения безопасности АС**

* Многоуровневый подход.
* Минимизация уязвимостей.
* Непрерывный мониторинг.

**21. Механизмы обеспечения конфиденциальности**

* Шифрование.
* Разграничение прав доступа.

**22. Механизмы обеспечения доступности**

* Резервирование данных.
* Использование кластеров.

**23. Механизмы обеспечения целостности**

* Контроль целостности данных.
* Использование цифровых подписей.

**24. Идентификация**  
Процесс установления личности пользователя.

**25. Аутентификация**  
Подтверждение личности пользователя.

**26. Виды систем аутентификации**

* Парольные.
* Биометрические.
* Токены.

**27. Биометрическая аутентификация**  
Использование уникальных биологических данных (отпечатки пальцев, распознавание лица).

**28. Особенности парольных систем**  
Легкость реализации, но высокая зависимость от сложности паролей.

**29. Рекомендации по паролям**

* Длина не менее 8 символов.
* Использование букв, цифр, символов.

**30. Методы (модели) разграничения доступа**

1. **Дискреционная модель (DAC)**
   * Пользователь, имеющий доступ к объекту, может передавать этот доступ другим.
   * Основана на правах, задаваемых владельцем объекта.
2. **Мандатная модель (MAC)**
   * Доступ определяется на основе уровня секретности данных и допуска пользователя.
   * Контроль осуществляется системой, а не пользователем.
3. **Ролевая модель (RBAC)**
   * Пользователи получают права доступа в зависимости от роли (должности, функции).
   * Удобна для масштабных организаций.
4. **Модель атрибутивного управления доступом (ABAC)**
   * Решение о доступе принимается на основе множества атрибутов (время, местоположение, свойства пользователя).

**31. Криптографические методы обеспечения конфиденциальности информации**

1. **Шифрование данных** (симметричное и асимметричное).
2. **Цифровая подпись** (гарантия подлинности и целостности).
3. **Хэширование** (создание уникальных идентификаторов данных).
4. **Туннелирование** (например, VPN).
5. **Цифровые сертификаты** (удостоверение личности).

**32. Алгоритмы шифрования**

1. **Симметричные**:
   * AES (Advanced Encryption Standard).
   * DES (Data Encryption Standard).
   * Triple DES.
2. **Асимметричные**:
   * RSA.
   * ECC (Эллиптические кривые).
3. **Потоковые**:
   * RC4.

**33. Симметричные криптосистемы**

* Используют один ключ для шифрования и дешифрования.
* Преимущества: высокая скорость обработки данных.
* Недостатки: сложность безопасного обмена ключами.
* Пример: AES.

**34. Асимметричные криптосистемы**

* Используют два ключа: публичный (для шифрования) и приватный (для дешифрования).
* Преимущества: безопасный обмен ключами.
* Недостатки: медленнее симметричных систем.
* Пример: RSA.

**35. Основные способы (средства) обеспечения сетевой безопасности**

1. **Межсетевые экраны (фаерволы)**.
2. **Системы обнаружения/предотвращения атак (IDS/IPS)**.
3. **VPN (виртуальные частные сети)**.
4. **Антивирусные программы**.
5. **Шифрование данных в сети**.
6. **Контроль доступа (ACL)**.

**36. Межсетевой экран**

Программное или аппаратное средство, контролирующее и фильтрующее сетевой трафик в соответствии с заданными правилами.  
Пример: блокировка нежелательных соединений.

**37. Система обнаружения вторжений (IDS)**

Инструмент для мониторинга сети и обнаружения подозрительных действий или попыток атак.

* **Пример**: Snort.

**38. Протоколирование и аудит в ИБ**

* Протоколирование: запись событий и операций для последующего анализа.
* Аудит: проверка и оценка системы на соответствие политикам безопасности.  
  Пример: анализ логов.

**39. Принципы обеспечения целостности (Кларка-Вилсона)**

1. **Разделение обязанностей** — запрет выполнения всех критичных действий одним человеком.
2. **Контроль доступа** — использование привилегий на основе доверенных транзакций.
3. **Аудит** — протоколирование операций для отслеживания.

**40. Электронная цифровая подпись (ЭЦП)**

ЭЦП — средство проверки подлинности данных и их отправителя, основанное на криптографических методах.  
**Применение**: электронные документы, юридически значимые транзакции.

**41. Хэш-функции**

* Односторонние функции, преобразующие данные в уникальный фиксированный хэш.
* Применение: проверка целостности данных, создание цифровых подписей.  
  **Пример**: MD5, SHA-256.

**42. Разница между дублированием и зеркалированием серверов**

* **Дублирование**: создание копии данных на независимом сервере. Может быть не синхронным.
* **Зеркалирование**: синхронное сохранение данных на нескольких серверах, обеспечивающее мгновенную доступность.

**43. Механизмы защиты от угроз нарушения доступности**

1. **Резервирование ресурсов**.
2. **RAID-массивы**.
3. **Кластеры серверов**.
4. **DDoS-защита**.

**44. Базовые механизмы защиты информации в операционных системах**

1. Разграничение прав доступа.
2. Шифрование файлов.
3. Защита системных журналов.
4. Антивирусная защита.

**45. Организационно-распорядительные документы**

1. Политика информационной безопасности.
2. Инструкции по работе с конфиденциальной информацией.
3. Регламенты работы сотрудников.
4. Акт оценки рисков.

**46. СКУД (Система контроля и управления доступом)**

Программно-аппаратные комплексы для контроля доступа в помещения.  
**Примеры**: карточки доступа, биометрические системы.

**47. Контролируемая зона**

Область, доступ в которую ограничен и находится под контролем (например, серверные помещения).

**48. Политика информационной безопасности организации**

Документ, определяющий подходы, меры и процедуры по защите информации.  
**Цели**: предотвращение утечек, обеспечение конфиденциальности и доступности.

### ****49. Основные разделы политики информационной безопасности организации****

1. **Общее положение**
   * Цель разработки политики.
   * Термины и определения.
   * Область применения.
2. **Описание актуальных угроз**
   * Потенциальные риски для информационной безопасности.
   * Перечень внешних и внутренних угроз.
3. **Цели и задачи информационной безопасности**
   * Обеспечение конфиденциальности, целостности и доступности информации.
   * Снижение вероятности реализации угроз.
4. **Организационная структура управления ИБ**
   * Ответственные лица и их роли.
   * Взаимодействие подразделений.
5. **Регламент защиты информации**
   * Технические и программные меры.
   * Организационные мероприятия.
6. **Правила работы с информацией**
   * Порядок доступа к данным.
   * Ограничения на использование информации.
7. **Меры ответственности**
   * Наказания за нарушение политики.
   * Процедуры расследования инцидентов.
8. **Аудит и контроль ИБ**
   * Порядок проведения проверок.
   * Частота и методология аудита.
9. **Обучение персонала**
   * Программы повышения осведомленности сотрудников.
   * Курсы и тренинги по ИБ.
10. **Порядок пересмотра политики**
    * Частота актуализации документа.
    * Условия изменения политики.

### ****50. Организационные методы защиты информации****

**Определение**: Совокупность мер, направленных на регулирование действий персонала и организацию процессов для минимизации угроз информационной безопасности.

**Примеры организационных методов**:

1. **Разграничение полномочий**
   * Установление доступа к информации только для сотрудников, которым это необходимо для выполнения их обязанностей.
2. **Разработка регламентов и инструкций**
   * Политики паролей.
   * Регламенты работы с конфиденциальными документами.
3. **Обучение сотрудников**
   * Проведение тренингов по вопросам ИБ.
   * Распространение памяток и инструкций.
4. **Контроль и аудит действий персонала**
   * Регулярная проверка соблюдения установленных норм.
   * Мониторинг активности пользователей.
5. **Физическая защита объектов**
   * Организация пропускного режима.
   * Установка систем видеонаблюдения.
6. **Проведение аттестации и сертификации ИС**
   * Проверка соответствия систем требованиям безопасности.
7. **Реагирование на инциденты**
   * Создание процедур для расследования и устранения последствий нарушений.