**Задание 1**

1. B,C

3-ий уровень – это сетевой

Соответственно логическая адресация, а также поиск оптимального маршрута (Например протоколы OSPF, RIP)

1. ARP (Address Resolution Protocol)
2. Коммутаторы и Мосты
3. Описана технология инкапсуляции данных

**Задание 2**

1. B, C, F
2. B, C, D
3. C
4. КЗИ
   1. Средства криптографической защиты по каналу связи – обеспечивает защиту информации при её передаче по различным каналам
   2. Средства криптографической защиты в вычислительных системах – защищают данные хранящиеся или обрабатываемые на компьютерах и серверах
   3. Средства криптографической защиты информации в средствах передачи данных – обеспечивает безопасность в сетях передачи данных
   4. Средства криптографической защиты информации в автоматизированных системах – комплексные решения, которые обеспечивают криптографическую защиту информации во всех компонентах автоматизированных систем

**Задание 3**

1. Аутентификация, основанная на знании
2. Многофакторная аутентификация – это метод подтверждения личности пользователя, при котором используется два или более независимых фактора из разных категорий. (Например на основании знания и на основании обладания)

Значительно повышает уровень защиты, снижает риски взлома при фишинге, перехвата паролей

1. Факторы
   1. Фактор знания (Пароль, ПИН, секретные фразы)
   2. Фактор обладания (Токен, Сертификат)
   3. Биометрический (Отпечатки пальцев, распознование лица)
2. Модели
   1. Дискретная модель (Решение о предоставлении доступа принимает владелец ресурса, пользователи могут сами задавать права доступа другим пользователям к своим ресурсам)
   2. Мандатная модель (Управление доступом основывается на установленной политике безопасности. Пользователь не может изменять права доступа самостоятельно)
   3. Ролевая модель (Доступ предоставляется в зависимости от роли пользователя. Роли как раз напрямую связаны с набором прав доступа)

**Задание 4**

1. ЭП – это криптографический механизм, который позволяет подтвердить авторство и целостности документа. Использует для этого ассиметричное шифрование

Хэш-функция – это односторонняя функция, которая преобразует входные данные в набор символов фиксированной длины

Таким образом это два разных по назначению и реализации механизма.

1. Обе создаются с использованием криптографических программ, могут храниться на физических носителях и выдаются УЦ. Однако отличие в том, что программы для создания квалицированной ЭП проходят обязательную проверку и сертификацию ФСБ
2. В аккредитованном УЦ
3. Алгоритм подписи (Подпись ECDSA X9.62 с SHA-256). Длина ключа (256). Издатель (WE2 - Google Trust Services). Срок действия (23.06.25 – 15.09.25)

**Задание 5**

1. № 187-ФЗ, № 149-ФЗ. Для государственных информационных систем 3-го класса защищённости обязательным является использование средств анализа защищённости
2. № 152-ФЗ, Приказ ФСТЭК России № 58. Классификация персональных данных, уровень угроз и рисков, применяемые технические и организационные меры защиты, уровень подготовки специалистов, соблюдение нормативных актов и стандартов, регулирующих обработку персональных данных.
3. № 187-ФЗ, Приказы ФСТЭК России и Минобороны РФ.

Значимые объекты КИИ — это объекты, которые обеспечивают жизнедеятельность общества и государства и при нарушении их функционирования возникают значительные угрозы национальной безопасности, экономике, общественному порядку и правам граждан.

Незначимые объекты КИИ — объекты, нарушение работы которых не приводит к критическим последствиям для безопасности страны, экономики или общества.

1. № 187-ФЗ, Приказ ФСТЭК России № 58.

Влиянием на безопасность технологического процесса и жизнедеятельность предприятия.

Уровнем возможных экономических потерь и ущерба

Возможными последствиями для окружающей среды и здоровья людей

Соответствием требованиям законодательства и нормативных документов

1. ..
   1. Анализ и оценка угроз безопасности информации
   2. Разработка политики безопасности и требований к СЗИ
   3. Выбор и проектирование средств и методов защиты информации
   4. Разработка документации по СЗИ
   5. Внедрение и настройка средств защиты
   6. Проведение тестирования и оценка эффективности СЗИ
   7. Эксплуатация и сопровождение СЗИ

Перечень разрабатываемой документации:

1. Политика информационной безопасности
2. Положение по обеспечению безопасности информации
3. Требования к безопасности информации
4. План мероприятий по обеспечению безопасности информации
5. Техническая документация на средства защиты информации
6. Акты оценки риска и результатов тестирования
7. Журналы учета и контроля безопасности

**Задание 6**

1. СЗИ НСД (Соболь, Dallas Lock), СКЗИ (КриптоПро CSP, Signal-COM, ViPNet CSP), Межсетевые экраны (Континент, Рубикон), Антивирусная защита (Касперский, Dr.Web), IDS/IPS (Сёрсчер, Контур ИБ), SIEM (MaxPatrol SIEM)
2. Описать **потенциального злоумышленника** - его возможности, ресурсы, мотивацию, уровень доступа, техническую оснащённость и профессиональные навыки. Целью является определить какие угрозы являются реализуемыми, вероятность и способы реализации угроз, разработать адекватные меры защиты, рассчитать стоимость и эффективность защиты
3. BDU:2024-08575
4. А,B,D
5. **Угроза:= злоумышленник(хакер), отсутствие или недостаточная криптографическая защита передаваемой информации, перехват трафика с использованием снифферов или оборудования для анализа сетевых пакетов, данные в процессе передачи по вычислительной сети.**

**Задание 7**

* Между Головным офисом и филиалом (через Интернет)
  + **VPN-шлюзы** - для защиты канала связи от перехвата и модификации данных
  + **Межсетевой экран** - для фильтрации входящего и исходящего трафика
* На границе Головного офиса с Интернетом
  + **Межсетевой экран + IDS/IPS** - для предотвращения атак и фильтрации доступа
  + **Прокси-сервер** - для контроля доступа пользователей к внешним ресурсам и фильтрации контента.
* Между пользовательским и серверным сегментами
  + **Внутренний межсетевой экран** - для разделения зон и ограничения доступа между сегментами.
  + **Сервер авторизации и управления доступом** - реализует централизованное управление учетными записями
* На серверах и АРМ пользователей
  + **Антивирусное ПО** с централизованным управлением
  + Система контроля целостности
  + Средства учета и регистрации событий ИБ
  + Средство разграничения доступа
* Удаленные пользователи
  + **VPN-клиенты с СКЗИ** - защищенное подключение к корпоративной сети
  + Средства защиты рабочих станций
  + Средства аутентификации

**Задание 8**

Дополнительные вопросы:

1. Какие операционные системы используются на **АРМ операторов**, сервере АСУ ТП и контроллере PLC
2. Используются ли **средства резервного копирования** и восстановления данных
3. Каким образом осуществляется **администрирование** серверов и сетевого оборудования
4. Есть ли физический доступ к оборудованию посторонних лиц
5. Поддерживает ли контроллер PLC **средства шифрования или аутентификации**

Перечень **мер защиты информации:**

* Организационные меры
  + Назначение ответственного за ИБ в АСУ ТП
  + **Разграничение прав доступа** к АРМ, серверу и PLC
  + **Ограничение физического доступа** к оборудованию
  + Разработка **локальных нормативных актов** по безопасности
  + Обучение сотрудников по вопросам ИБ
* Технические меры
  + Идентификация и аутентификация пользователей
  + Управление доступом
  + Защита от НСД
  + Межсетевое экранирование
  + Контроль и регистрация событий безопасности
  + Защита данных при передаче по сетям общего пользования
  + Обеспечение целостности ПО и данных

Средства защиты информации производства **АО “ИнфоТеКС**”

ViPNet Coordinator HW/SW - Построение VPN-сети

ViPNet Client - VPN-клиент для АРМ операторов

ViPNet IDS - Система обнаружения вторжений

ViPNet Firewall - Межсетевой экран. Разграничение сетей и фильтрация трафика