- **Диспетчер учетных записей безопасности (SAM)** — это база данных, которая присутствует на компьютерах под управлением операционных систем Windows, в которых хранятся учетные записи пользователей и дескрипторы безопасности для пользователей на локальном компьютере.
- **SRM** находится в исполняющей системе, это значит, что он работает в режиме ядра. Коротко говоря, этот монитор отвечает за проверку того, может ли один объект получить доступ к другому объекту.
- **Маркер доступа (Access token)** - содержит информацию по безопасности сеанса и идентифицирует пользователя, группу пользователей и пользовательские привилегии.
- **Идентификатор безопасности (Security Identifier (SID))** — структура данных переменной длины, которая идентифицирует учётную запись пользователя, группы, службы, домена или компьютера.
- **Привилегия** — это право учетной записи, например учетной записи пользователя или группы, выполнять различные системные операции на локальном компьютере, такие как завершение работы системы, загрузка драйверов устройств или изменение системного времени.
- **Права доступа** — совокупность правил, регламентирующих порядок и условия доступа субъекта к объектам информационной системы (, её носителям, процессам и другим ресурсам) установленных правовыми документами или собственником, владельцем информации.
- **Объект доступа** – это единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа: файл, документ или иной объект, с которым взаимодействует субъект доступа.
- **Субъект доступа** — это лицо или процесс, действия которого регламентируются правилами разграничения доступа.
- **Олицетворение** — это способность серверного приложения принимать на себя удостоверение клиента. Обычно службы используют олицетворение при проверке доступа к ресурсам.
- **Access Control List (ACL)** — список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).
- **Учётная запись** — хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.
- **Доменное** — имя-символ, помогающее находить адреса интернет-серверов.

Вопросы:

1. **Перечислите типы учетных записей.**

   - Учетная запись администратора
   - Гостевая учетная запись
   - Учетная запись HelpAssistant
   - DefaultAccount

2. **Перечислите способы создания учетных записей.**
   - Через параметры
   - С помощью Win+R (userpassword2)
   - С помощью Win+R (lusrmgr)
   - С помощью командной строки
3. **Что понимается под идентификацией пользователя?**
   Идентификация пользователя – присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным.
4. **Что понимается под аутентификацией пользователей?**
   Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.
5. **Перечислите возможные идентификаторы при реализации механизма идентификации.**
   - Набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи);
   - физиологические параметры человека (отпечатки пальцев, рисунок радужной оболочки глаза, распознавание лица и т. п.) или особенности поведения (особенности работы на клавиатуре и т. п.).
6. **Перечислите возможные идентификаторы при реализации механизма аутентификации.**
   ??? Аналогично 5 вопросу
7. **Какой из механизмов (аутентификация или идентификация) более надежный? Почему?**
   В целом аутентификация по уровню информационной безопасности делится на три категории:
   1. Статическая аутентификация.
   2. Устойчивая аутентификация.
   3. Постоянная аутентификация.

   Постоянная аутентификация обеспечивает идентификацию каждого блока передаваемых данных, что предохраняет их от несанкционированной модификации или вставки. Примером реализации указанной категории аутентификации является использование алгоритмов генерации электронных подписей для каждого бита пересылаемой информации.
8. **Опишите механизм аутентификации пользователя.**
   Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор. В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным условием для защищенных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).
   Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.
9. **Структура маркера доступа.**
   - Идентификатор безопасности для учетной записи пользователя

- Идентификаторы безопасности для групп, членом которых является пользователь
- Идентификатор безопасности входа, идентифицирующий текущий сеанс входа
- Список привилегий , удерживаемых пользователем или группами пользователей.
- Идентификатор безопасности владельца
- Идентификатор безопасности для основной группы
- DaCL по умолчанию, используемый системой при создании защищаемого объекта без указания дескриптора безопасности.
- Источник маркера доступа
- Указывает, является ли маркер основным или олицетворением .
- Необязательный список ограничений идентификаторов БЕЗОПАСНОСТИ
- Текущие уровни олицетворения
- Другая статистика

10. Структура SID.

Формат идентификатора безопасности такой: S-R-IA-SA-SA-RID[1].

Описание каждой части SID:

- S — идентификатор SID. Этот идентификатор служит признаком того, что следующее число является идентификатором безопасности, а не простым большим загадочным числом.
- R — первое число является номером редакции (revision). Все идентификаторы безопасности, сгенерированные операционной системой Windows, используют номер редакции 1.
- IA — источник выдачи (issuing authority). Практически все идентификаторы безопасности в операционной системе Windows указывают NT Authority номер 5. Исключением являются широкоизвестные (well-known) учетные записи групп и пользователей.
- SA — уполномоченный центр (sub-authority). Этот идентификатор определяет специальные группы и функции. Например, число 21 указывает, что идентификатор безопасности был выдан контроллером домена или изолированным компьютером.
- Три длинные последовательности цифр 1507001333-1204550764-1011284298 определяют конкретный домен или компьютер, выдавший идентификатор. Эти числа генерируются случайным образом при инсталляции ОС на компьютер. Таким образом обеспечивается уникальность идентификаторов безопасности.
- RID — относительный идентификатор (Relative Identifier). Это уникальное порядковое число, присвоенное учетной записи (пользователя, компьютера или группы) уполномоченным центром SA (в нашем примере его значение равно 1003).