Задание:

Компания по продаже автозапчастей работает в Новосибирской области. Компания решила открыть новый филиал в соседнем регионе. Для подключения нового офиса надо создать VPN канал. В VPN канале будут передавать персональные данные клиентов. Количество клиентов в компании более 100 000. Для информационный системы отсутствуют угрозы, связанные с недокументированными возможностями в прикладном и системном программном обеспечении.
Выберите и обоснуйте минимальный класс СКЗИ.
Приведите примеры отечественных криптошлюзов, имеющих сертификат соответствия ФСБ данного класса СКЗИ.

1. Уровень защищенности ИСПДн.

Согласно Федеральному закону № 152-ФЗ «О персональных данных» и приказу ФСТЭК России № 21, определены следующие критерии уровня защищенности информационной системы персональных данных (ИСПДн):

Уровень защищенности УЗ-1. Применяется при наличии хотя бы одной из ситуаций:
- Обработка специальных категорий персональных данных (расовая принадлежность, состояние здоровья, интимная жизнь и др.).
- Обработка биометрических персональных данных.
- Наличие актуальных угроз, связанных с недокументированными возможностями программного обеспечения (НДВ)

Уровень защищенности УЗ-2. Используется, если система не попадает ни под категорию УЗ-1, ни под УЗ-3. Это промежуточный уровень, применяемый чаще всего.

Уровень защищенности УЗ-3. Минимальная защита, которая применяется при соблюдении следующих условий:
- Обрабатываемые данные являются общедоступными персональными данными (ОПДн).
- Обычные персональные данные (ФИО, адрес, контактная информация), если число пользователей не превышает 100 000, и отсутствуют угрозы НДВ.

В нашем случае:
- Тип данных - обычные персональные данные (нет специальных или биометрических данных).
- Объем базы данных - более 100 000 пользователей.
- Отсутствуют угрозы, связанные с недокументированными возможностями (НДВ).

Исходя из данных нашего случая, наша ситуация точно не относится к категории УЗ-1 (так как нет специальных или биометрических данных, а также угроз НДВ) и не удовлетворяет критериям УЗ-3 (число пользователей более 100000). Значит, остаётся уровень защищенности УЗ-2.
Уровень защищенности ИСПДн в нашем случае - **УЗ-2**.

2. Минимальный класс СКЗИ.

Для определения необходимого класса средств криптографической защиты информации (СКЗИ) используем требования приказа ФСБ России № 378. Соответствие классов СКЗИ уровням защищенности:

Уровень защищенности	Необходимый класс СКЗИ
УЗ-1	Не ниже КС2
УЗ-2	Не ниже КС1
УЗ-3	Не ниже КС3

Так как мы определили уровень защищенности нашей системы как УЗ-2, минимальное требование к классу СКЗИ составляет класс КС1.
Минимальный класс СКЗИ в нашем случае - **КС1**.

3. Обоснование выбора класса СКЗИ

Выбор класса СКЗИ основывается на согласовании с установленным уровнем защищенности информационной системы (УЗ-2). Согласно Приказу ФСБ России № 378, минимальная категория СКЗИ должна соответствовать установленному уровню защищенности или превышать его. Поскольку уровень защищенности определён как второй (УЗ-2), минимальным требованием является применение средств криптозащиты класса КС1. Это обеспечивает достаточный уровень надежности для защиты конфиденциальных данных, передаваемых по сетевым каналам связи.

4. Пример СКЗИ

Вот пример устройств, соответствующих классу СКЗИ КС1:

- КриптоПро VPN: Средства защиты, поддерживающие протокол SSL/TLS с использованием российских криптографических алгоритмов и соответствующие классу КС1 (https://www.cryptopro.ru/products/ngate/vpn).
- Континент-АП: Ряд моделей семейства «Континент-АП» имеет сертификацию по классу КС1 (https://www.securitycode.ru/products/skzi-kontinent-ap/).
- Dallas Lock VPN: Шлюзы серии Dallas Lock VPN сертифицированы по классу КС1 и используются для построения защищённых каналов связи (https://dallaslock.ru/).
- ViPNet Coordinator: Многие программные и аппаратные версии сертифицированы по классу КС1. Предназначены для организации виртуальных частных сетей (VPN) с защитой канала передачи данных (https://infotecs.ru/products/vipnet-coordinator-hw-4/).