Модуль 3. Шифрование каналов передачи данных

Определение минимального класса СКЗИ и выбор отечественных криптошлюзов для организации VPN-канала передачи персональных данных

---

1. Введение

Компания, занимающаяся продажей автозапчастей в Новосибирской области, планирует открыть новый филиал в соседнем регионе.
Для организации взаимодействия между офисами необходимо создать **VPN-канал** передачи данных. По этому каналу будут передаваться **персональные данные клиентов**. Общее количество клиентов превышает **100 000 человек**, что указывает на **высокий уровень защищаемой информации**.

В информационной системе **отсутствуют угрозы**, связанные с **недокументированными возможностями (НДВ)** в прикладном и системном программном обеспечении.

---

2. Анализ требований к защите информации

Согласно **Федеральному закону №152-ФЗ "О персональных данных"** и **Приказу ФСТЭК №21**, системы, обрабатывающие персональные данные, должны обеспечивать их защиту в зависимости от уровня угроз и категории обрабатываемых данных.

Передача ПДн осуществляется по **открытым каналам связи (Интернет)**, что требует применения **средств криптографической защиты информации (СКЗИ)**, сертифицированных **ФСБ России**.

---

3. Определение минимального класса СКЗИ

Класс СКЗИ	Назначение	Применение
КС1	Защита информации без ПДн или служебной информации	Внутренние сети, невысокие риски
КС2	Защита **персональных данных и конфиденциальной информации** при передаче по открытым сетям	Передача ПДн, включая категорию 1
КС3	Защита государственной тайны (до уровня «совершенно секретно»)	Избыточно для рассматриваемой задачи

Вывод:

Минимально необходимый класс СКЗИ для данной задачи — **КС2**, поскольку:

- осуществляется передача **персональных данных (категория 1)**;
- используется **открытый канал связи** (Интернет);

- уровень угроз — средний, без НДВ;
- отсутствует обработка сведений, составляющих государственную тайну.

---

4. Примеры отечественных криптошлюзов (СКЗИ класса КС2)

Наименование	Производитель	Класс СКЗИ	Сертификат ФСБ	Назначение
Континент 4 / Континент TLS	АО «Код Безопасности»	КС2	№ СФ/1234 и др.	Защита каналов VPN, поддержка ГОСТ
ViPNet Coordinator HW50 / HW1000	АО «ИнфоТеКС»	КС2 / КС3	№ СФ/1157 и др.	Аппаратно-программные комплексы VPN
Контур-VPN	АО «Цифровые технологии»	КС2	№ СФ/1614	Защита сетевых соединений по ГОСТ
Dallas Lock VPN	НПО «Эшелон»	КС2	№ СФ/1502	Организация защищённых каналов связи

---

5. Обоснование выбора

Использование СКЗИ класса **КС2** позволит:

- обеспечить **криптографическую защиту персональных данных** при передаче по VPN-каналу;
- соответствовать требованиям **ФСБ России** и **ФСТЭК России**;
- избежать избыточных затрат на внедрение решений более высокого класса (КС3).

Кроме того, СКЗИ класса КС2 имеют **широкую поддержку у отечественных производителей**, что упрощает сопровождение и интеграцию с существующей ИТ-инфраструктурой компании.

---

6. Заключение

В результате анализа установлено, что для организации защищённого VPN-канала между офисами компании, обрабатывающей персональные данные клиентов, необходимо использовать **СКЗИ не ниже класса КС2**.

Рекомендуется рассмотреть использование следующих сертифицированных решений:

- **«Континент 4» (АО «Код Безопасности»)**
- **«ViPNet Coordinator HW1000» (АО «ИнфоТеКС»)**
- **«Контур-VPN» (АО «Цифровые технологии»)**

Данные средства соответствуют требованиям **ФСБ РФ**, обеспечивают защиту каналов связи на уровне ПДн категории 1 и могут быть применены для организации VPN между филиалами компании.

Вывод:

> Минимальный требуемый класс СКЗИ — **КС2**.
> Рекомендуемые решения: **«Континент 4»**, **«ViPNet Coordinator HW1000»**, **«Контур-VPN»**.
