Вариант 4.

№1.

1. Организационно-технические меры ЗИ
2. Организационные меры ЗИ (Административные меры)
3. Криптографические меры ЗИ
4. Меры технической ЗИ

№2.

УИБ1:

1. Хранить персональные данные в зашифрованном виде (ключи шифрования хранить в отельном месте, например, в отдельной защищённой таблице)
2. Разработать тестирующую систему и регламентировать контроль за программным обеспечением, а также частоту проводимых проверок.
3. Обучение разработчиков в качестве превентивной меры
4. Установка дополнительных уровней доступа

УИБ2:

1. Создание дополнительных серверов и распределение нагрузки между ними
2. Контроль количества обращений с обращающихся к серверу компьютеров и создание политики блокировки-фильтрации запросов
3. Установка ПО по обнаружению атак.
4. Создание регламента по работе обслуживающего персонала в случае обнаружения атаки.