Постановка задачи 1

Вы стали директором по ИБ небольшого регионального банка. За первый рабочий день вы узнали некоторые данные о его инфраструктуре:

1. Головной офис (далее ГО);
2. Центр обработки данных (далее ЦОД).

Вся сеть разделена на 2 сегмента:

- Серверный. В который вошли серверы СУБД MS SQL, Orac1e, MS Exchange, МБ AD, веб-серверы и т.д;
- Пользовательский. В нем расположены рабочие станции пользователей (300 штук), локальные принтеры.

В компании есть 1 канал в Интернет, пропускная способность канала 100 Мбит/с. Пропускная способность канала между ЦОД и ГО 1 Гбит/с. Здания находятся в разных концах города.

На данный момент Банк не использует никакие меры и средства защиты информации (ни технические, ни организационные), кроме антивирусов. Также, по словам ИТ-службы, базовая безопасность настроена на сетевом оборудовании.

В штате вашего отдела ИБ один глухонемой инженер. Технический уровень сильно ниже среднего.

Задание 1

На второй рабочий день вам сообщают о серьезном инциденте. Департамент продаж обнаружил, что база клиентов вашего банка уже около полугода продается в даркнете. При этом она обновляется раз в 2-3 недели. Судя по всему, база настоящая.

Ваша задача: подготовить план действий на ближайшую неделю для генерального директора (страница А4).

Задание 2

После успешного расследования инцидента генеральный директор понял, что пора серьезно заняться ИБ. Он попросил вас сформировать план развития ИБ в банке на ближайший год. Сформулируйте кратко ваши предложения (страница А4).