Эшелон
комплексная безопасность

Практический опыт защиты персональных данных в кредитно-финансовых организациях

Дмитрий Олегович Левиев,
Директор Департамента Проектов
ЗАО «НПО «Эшелон»

Круглый стол, Infosecurity Russia 2008
Москва, 8 октября, 2008 г.

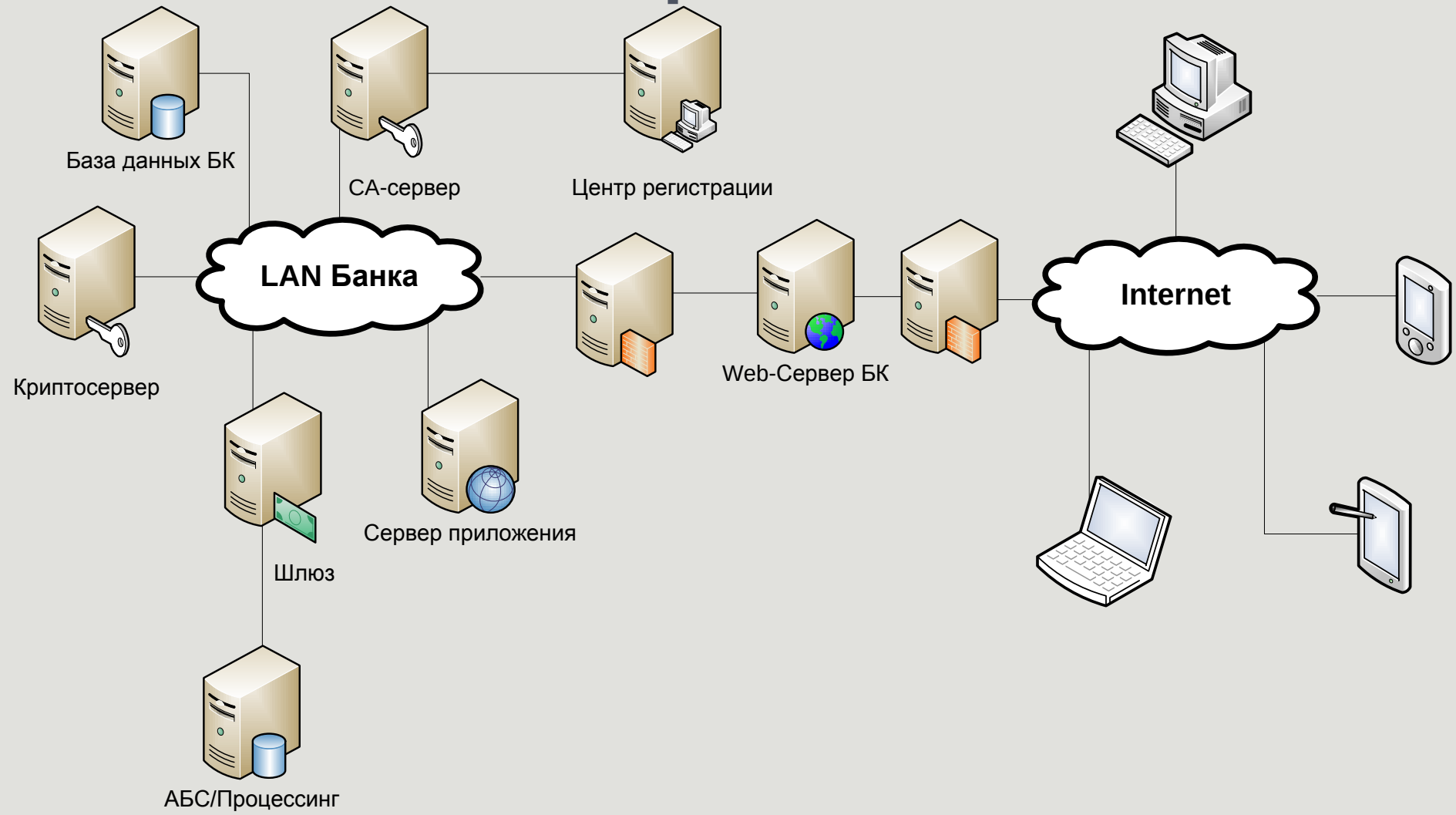
Автоматизированные системы обработки персональных данных

- Автоматизированная система кадрового делопроизводства
- Автоматизированная бухгалтерская система расчета заработной платы
- Система управления и контроля доступа
- Система удаленного контроля и управления счетом (Интернет-Банк-Клиент)

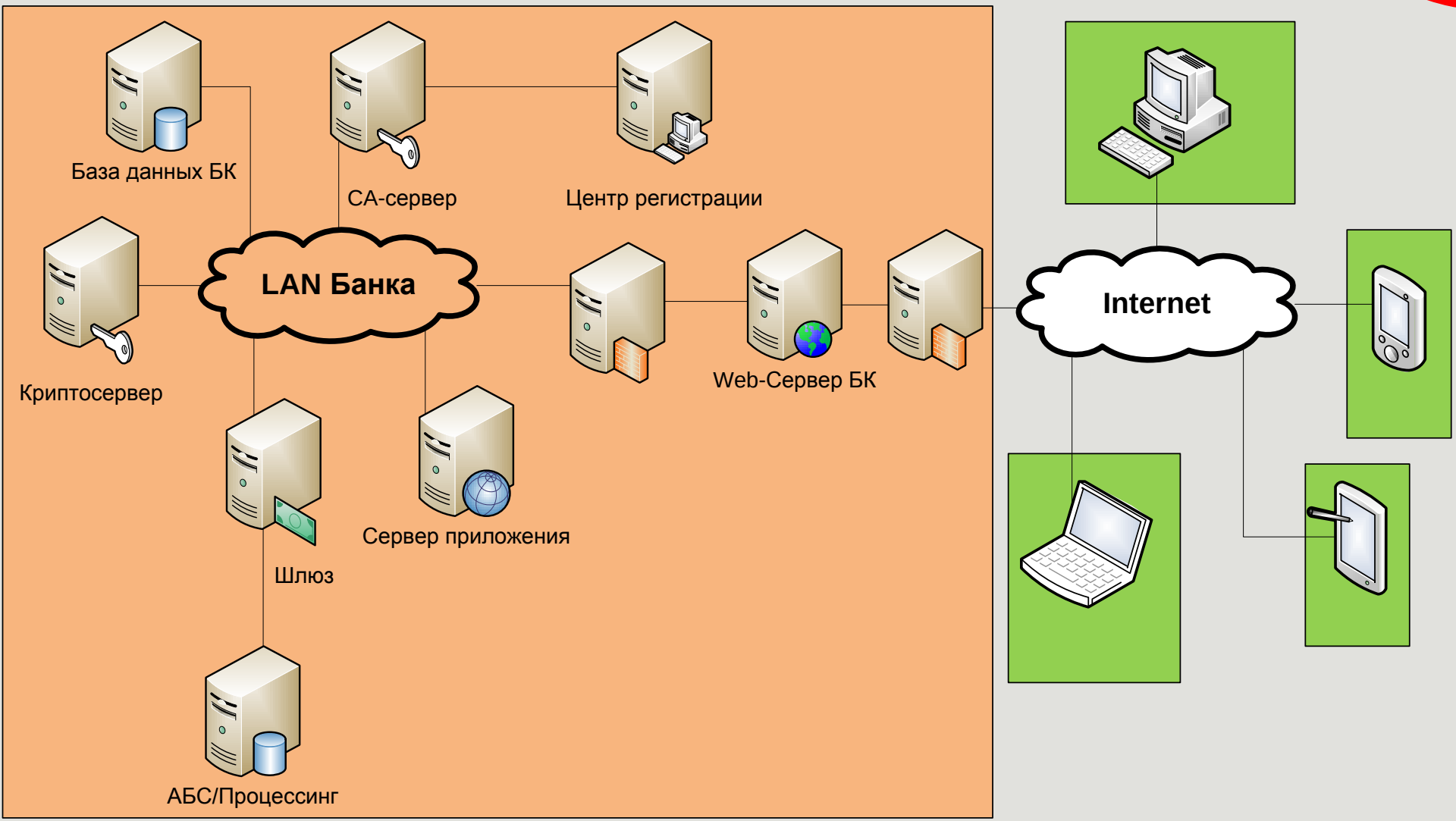
Исходные данные

- Федеральные законы
- Постановления Правительства №№ 781 и 687
- Нормативные документы ФСТЭК и ФСБ по защите персональных данных
- Договоры с Клиентами - все действующие на момент предпроектного обследования
- Договоры с Контрагентами – все действующие на момент предпроектного обследования
- Внутренние нормативные документы Банка по бизнес-процессам и защите информации
- Лицензии ФСБ и ФСТЭК с учетом лицензионных ограничений Банка

Система Интернет-Банк-Клиент



Зоны ответственности



Категория информации в системе

- Анализ договора:
  - .. Клиент дает согласие в целях исполнения Клиентом для целей исполнения Клиентом Договора и осуществления Банком функций по оказанию услуг в соответствии с Договором и распространяется на следующую информацию: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, и любая иная информация, доступная либо известная в любой момент Банку… В анкете присутствует полная информация о родственниках и иждивенцах.
- 1 Категория информации

Тип обработки информации

- Анализ договора
  - … Платежное поручение обрабатывается на основании аналога собственноручной подписи круглосуточно, исключая время проведения профилактических работ….
- Обработка проводится в автоматизированном режиме в понимании Постановления Правительства № 687
- Применимы все положения Постановления Правительства № 781

Количество субъектов ПДн

- Анализ отчетности Банка
  - На… открыто счетов-депозитов физических лиц 125076.
- Объем субъектов персональных данных обрабатываемых в системе более 100 тыс.

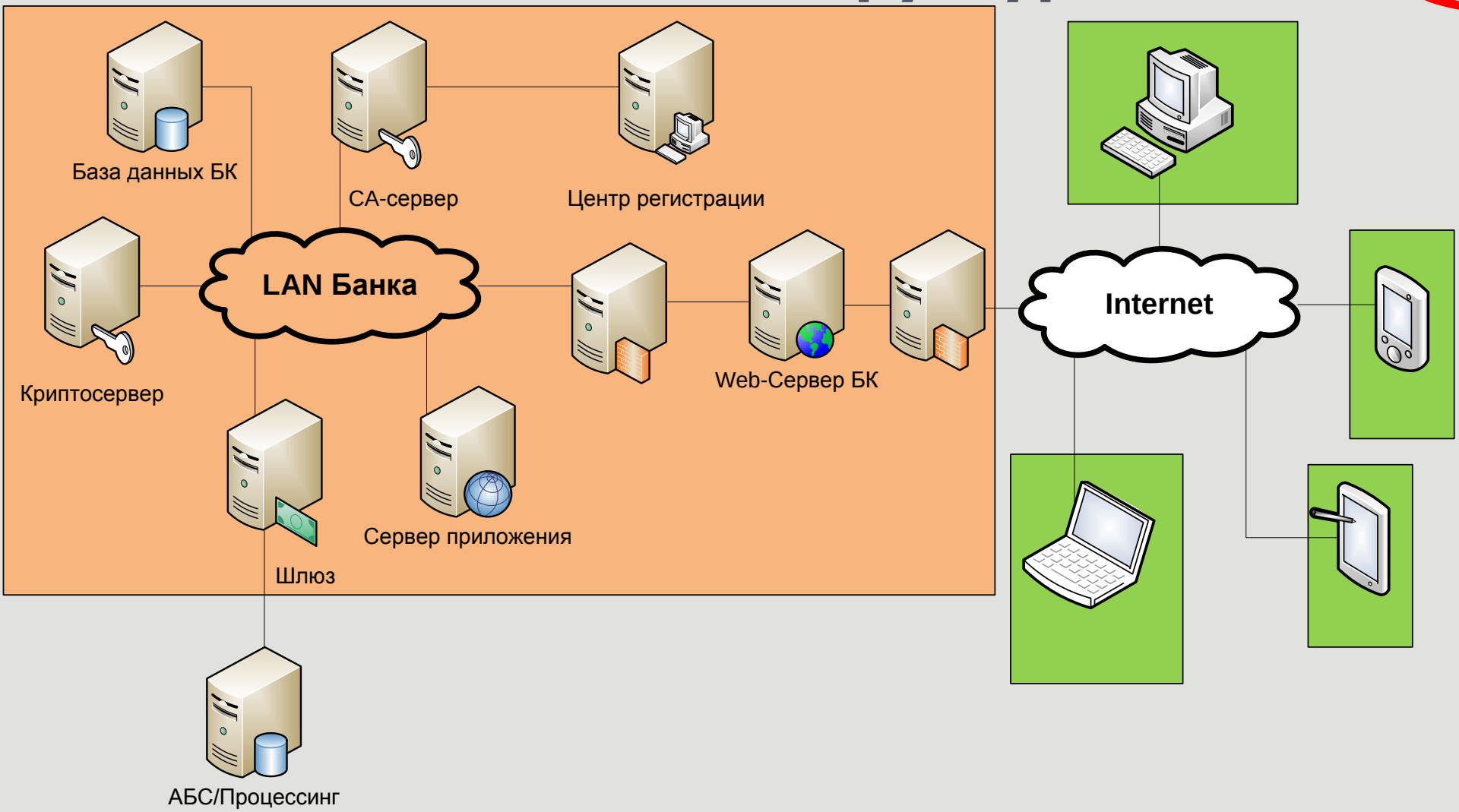
Классификация системы

- Общая предварительная классификация системы:
  - Распределенная Информационная система обработки персональных данных специального типа, находящаяся в пределах границ Российской Федерации, 1 класса (1 категория информации и более 100 тыс. субъектов), функционирующая через сеть общего доступа (Интернет)

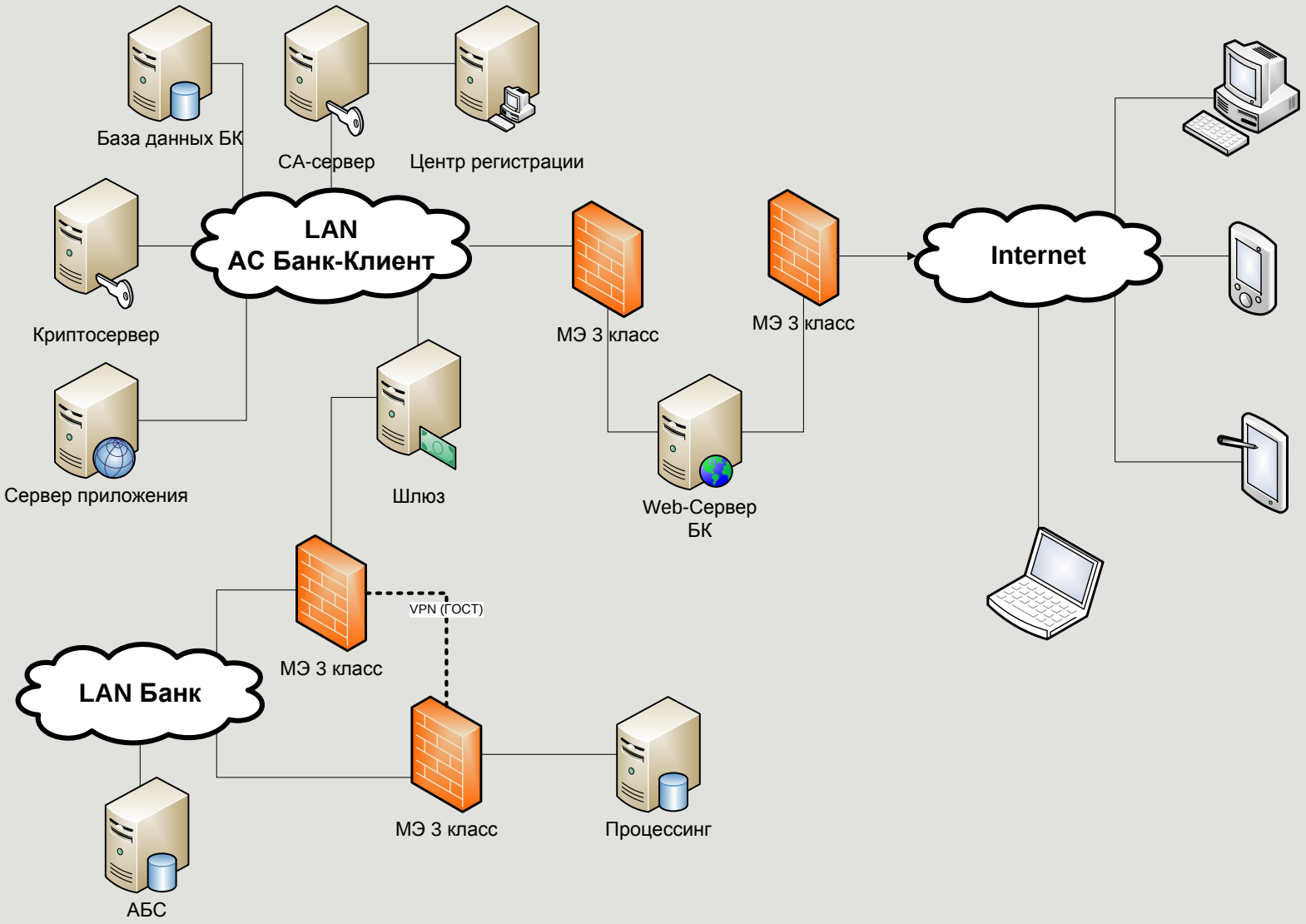
Оптимизация системы по классу информации

- Ограничение класса информации в системе:
  - .. Клиент дает согласие в целях исполнения Клиентом для целей исполнения Клиентом Договора и осуществления Банком функций по оказанию услуг в соответствии с Договором и обработку на следующую информацию: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, имущественное положение, доходы.
- Класс информации – 2 класс

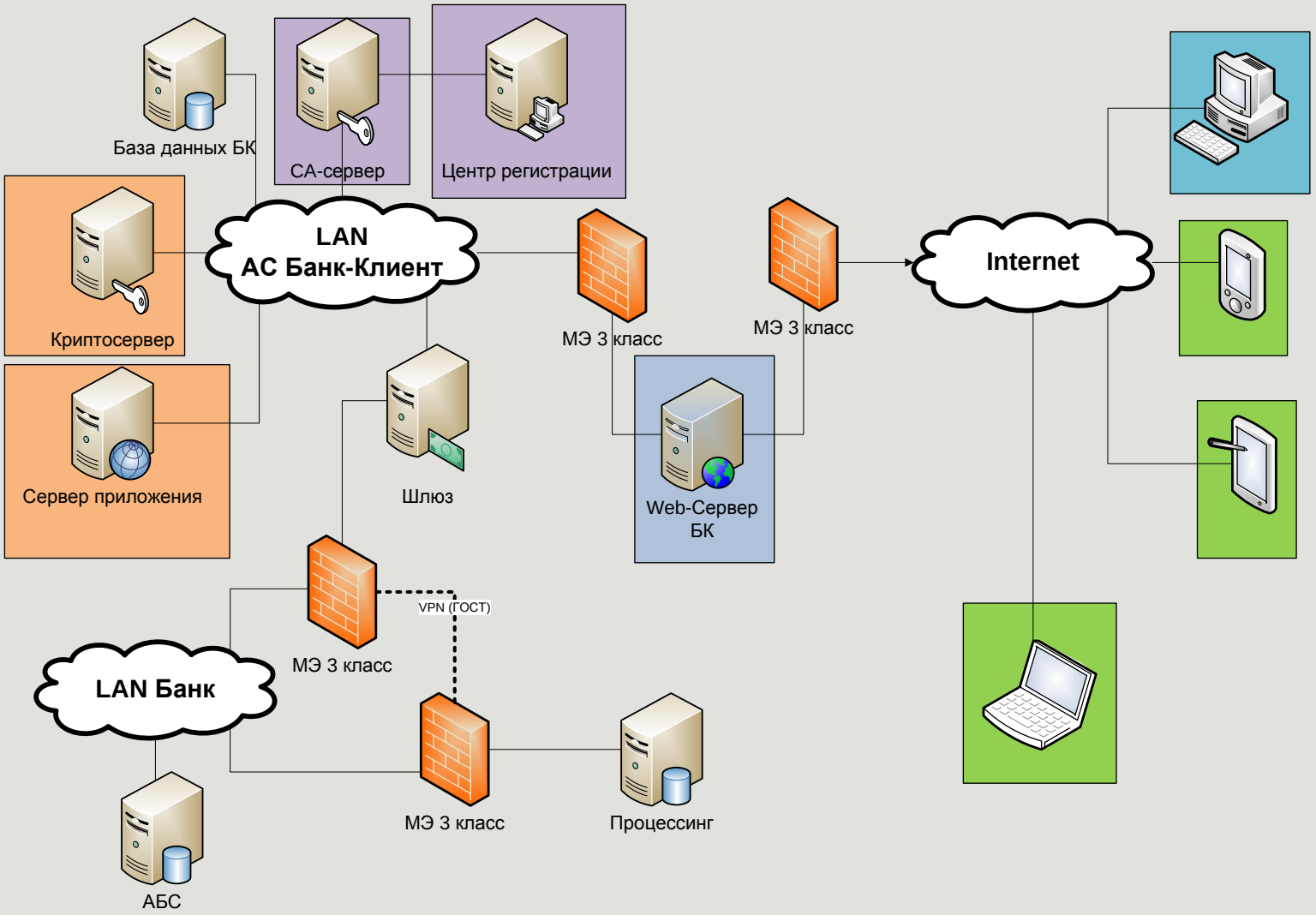
Оптимизация структуры



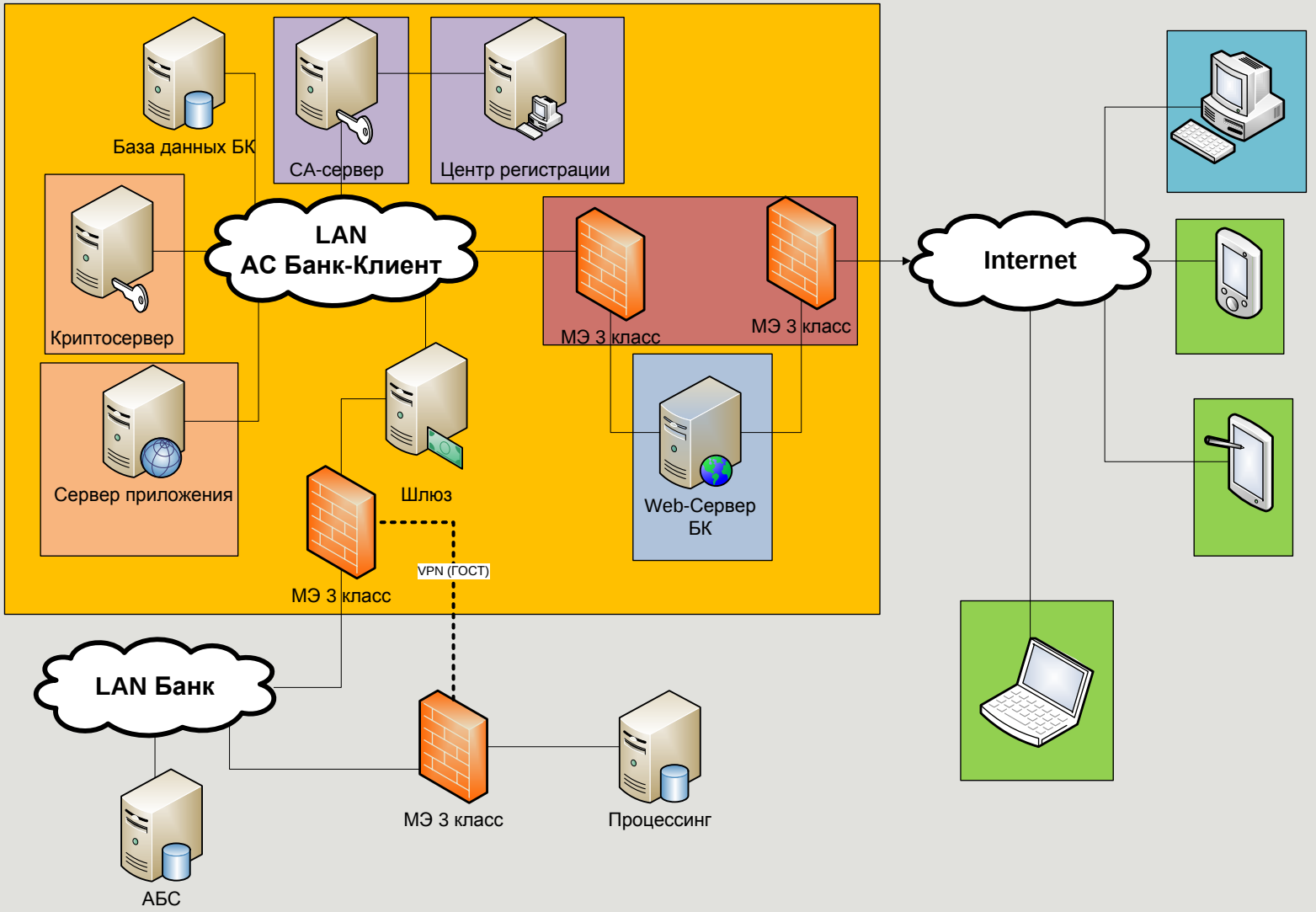
Новая схема комплекса АС



Модель угроз по требованиям ФСБ



Модель угроз ФСТЭК и ФСБ



Спасибо за внимание

Левиев Дмитрий Олегович
Директор Департамента Проектов
ЗАО НПО ЭШЕЛОН

Тел./факс +7 (495) 645-3809
+7 (495) 645-3810
E-mail: d.leviev@npo-echelon.ru
http://www.npo-echelon.ru