Министерство образования Кировской области

«Обеспечение безопасности персональных данных»

Докладчик:

Городилов Сергей Викторович

Руководитель направления ИБ, АСПЕКТ-СЕТИ

gors@aspectspb.ru

46-56-46, 30-13-23

Важные замечания!!!

- Ответственность за реализацию конкретных правовых и организационных мер на своей территории и в рамках своей организации несет её руководитель
- Представленные материалы являются результатом опыта работы докладчика в данной сфере, основанного на доступных на данный момент времени трактовках законодательства,
- Представленные формы, материалы и презентации не являются официальной позицией государства в сфере персональных данных
- Официальную трактовку тех или иных позиций законодательства и нормативных документов в области персональных данных осуществляют: Министерство связи и массовых коммуникаций РФ, Роскомнадзор РФ (только в рамках контроля и надзора), Суды РФ, а также ФСБ, ФСТЭК, Роструд и другие органы власти в рамках своей сферы компетенции.

ПЛАН СЕМИНАРОВ

Организационно-правовая часть

№	Дата проведения	Тема
1.	23.11.2017	Основы информационной безопасности. Персональные данные и другие категории конфиденциальной информации. Законодательство и нормативные документы в области защиты персональных данных
2.	14.12.2017	Правовые меры защиты персональных данных - КАДРЫ
3.	18.01.2018	Правовые меры защиты персональных данных – Образовательная деятельность

Организационно-техническая часть

4.	08.02.2018	Организационные меры защиты персональных данных
5.	27.02.2018	Информационные системы персональных данных (ИСПДн)
7.	05.04.2018	Порядок защиты ИСПДн Модель угроз Средства обеспечения ИБ в различных сценариях
8.	19.04.2018	Реализация мероприятий ИБ, Аттестация, сертификация и лицензирование в области защиты персональных данных. Контроль в области защиты персональных данных

Семинар №6

ПОРЯДОК ЗАЩИТЫ ИСПДН

Общие шаги

1. Собрать информацию
2. Понять угрозы и риски
3. Сформировать мероприятия
4. Внедрить мероприятия
5. Оценить их эффективность
6. Эксплуатировать безопасно
7. Выводить из эксплуатации безопасно

Общие шаги

1. **Собрать информацию**
2. Понять угрозы и риски
3. Сформировать мероприятия
4. Внедрить мероприятия
5. Оценить их эффективность
6. Эксплуатировать безопасно
7. Выводить из эксплуатации безопасно

Какая информация

1. Классификации - семинар 5
2. Инвентаризация всех активов
3. Схематичные представления:
   - Топология сети
   - Технология обработки информации
4. Особенности применяемых ИТ
5. Физическое размещение
6. Пользователи
7. Обслуживающие лица

Инвентаризация всех активов

Цель: знать, что ничто не упущено из вида и актуально.

Активы:

1. Рабочие процессы
2. Информация
3. **Средства обработки информации**
4. **Программное обеспечение**
5. **Информационные системы**
6. Документация

Средства обработки информации, информационные системы, ПО

Рабочие области:

- Компьютеры
- ПО компьютеров
- МФУ/принтеры
- Телефоны
- Периферия
- ИБП
- Кабинеты (оснащение)

Сетевая инфраструктура:

- Кабельная система
- Коммутаторы
- Маршрутизаторы
- Межсетевые экраны
- Модемы
- Телефония/АТС
- Криптошлюзы

Серверные:

- Физические серверы
- СХД
- NAS
- Виртуальные серверы
- ИБП

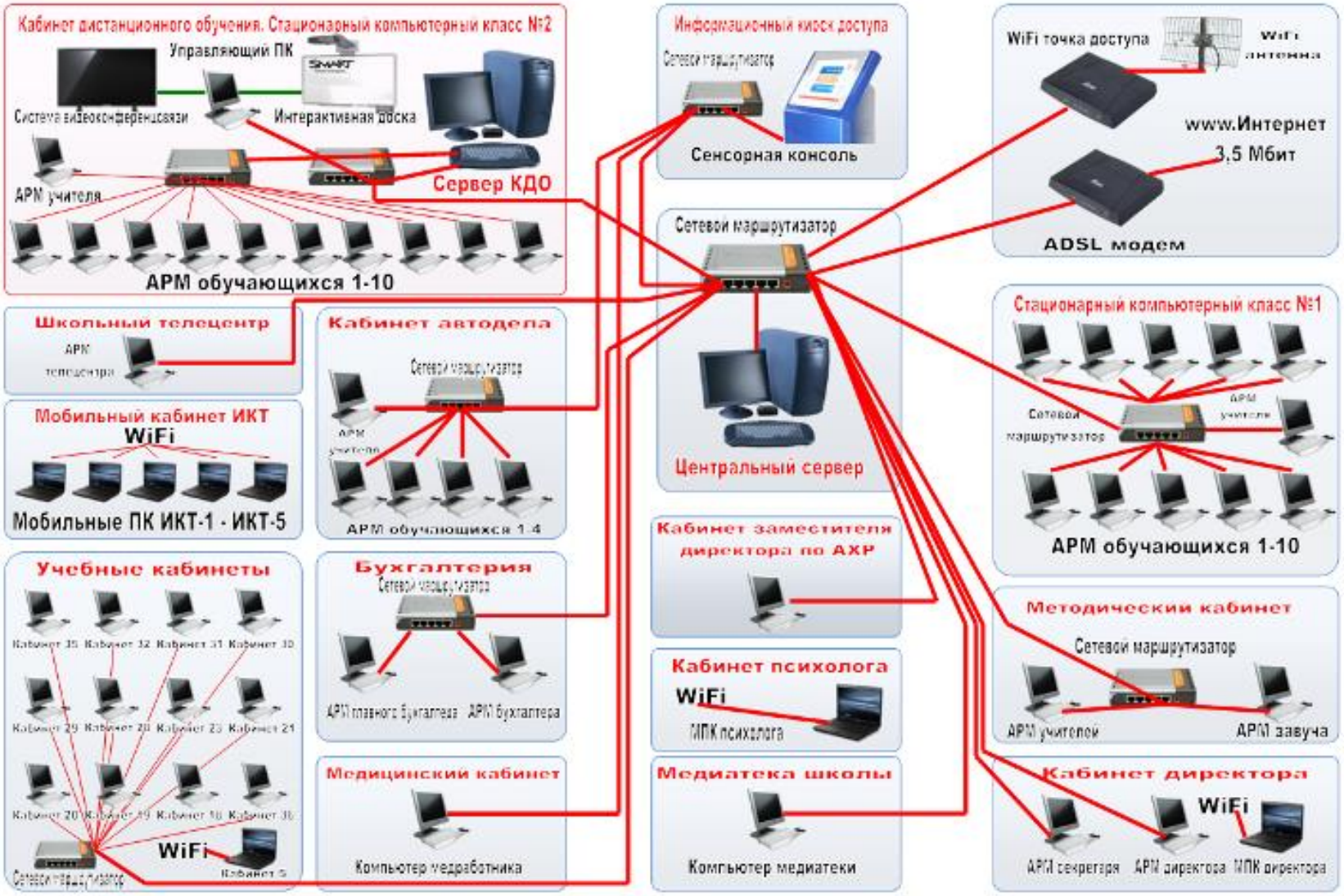
Информационные системы:

- Базовые сервисы
- Универсальные сетевые ресурсы (Общие папки, Принтеры)
- Специализированные ИС (АРМ Директор, 1С, Эл.почта)

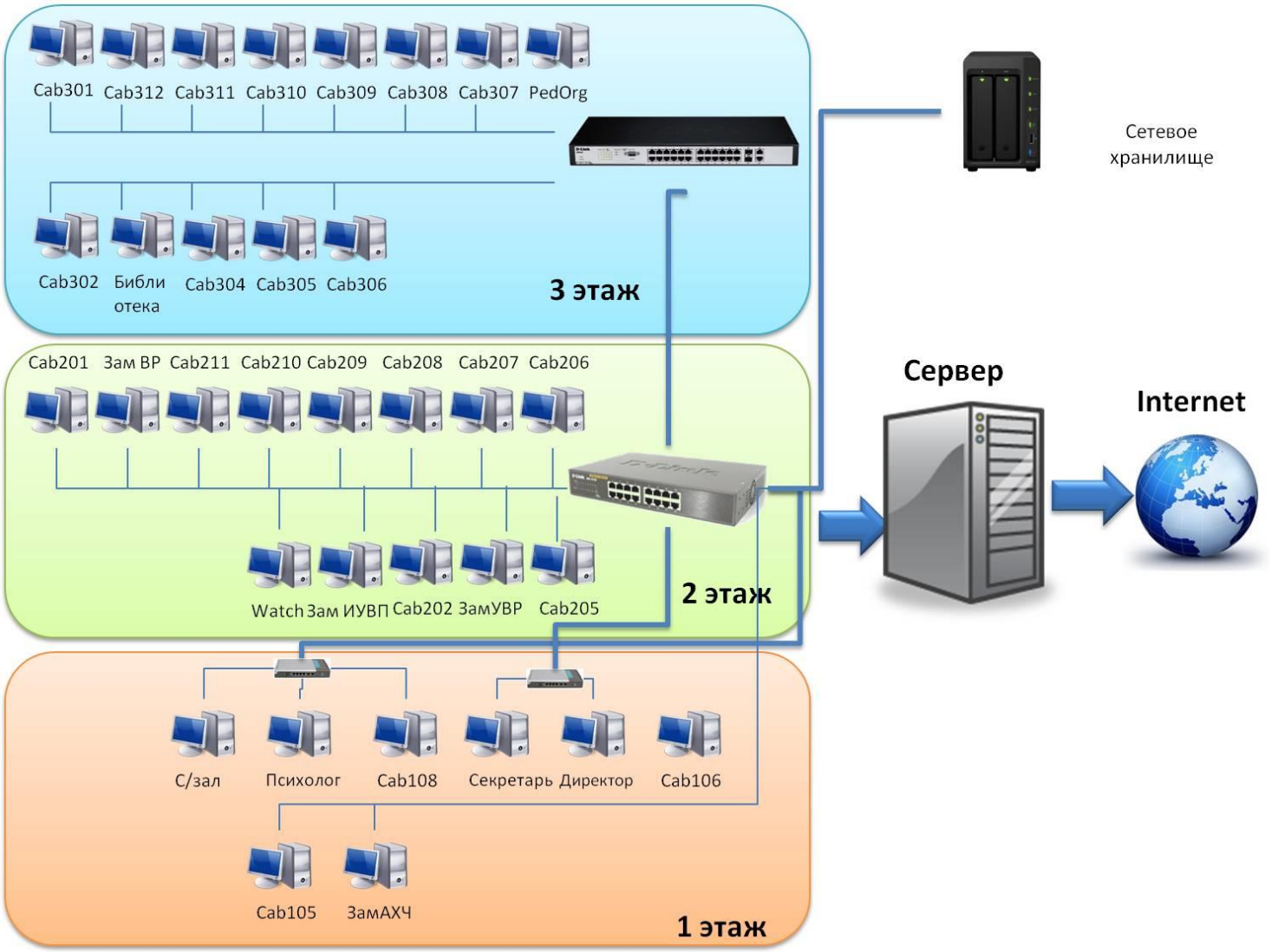
Общие средства ИБ

- Антивирусы
- Средства резервного копирования

Схемы: Топология сети



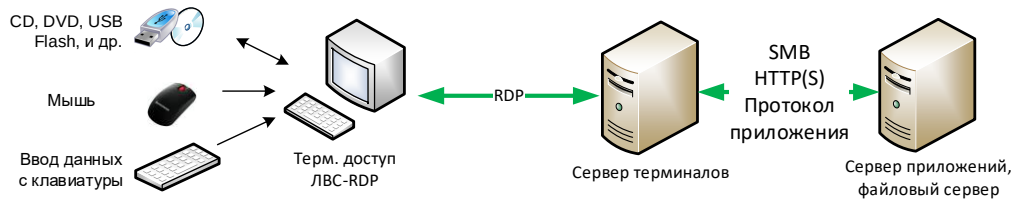
Или такая топология сети



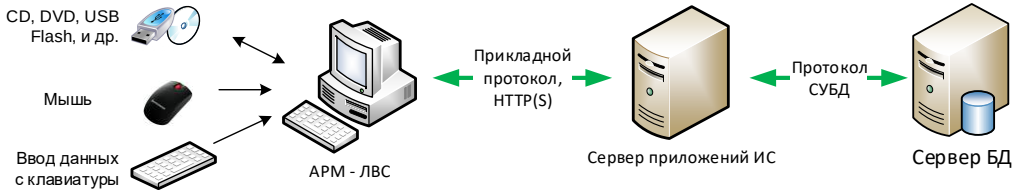
Схемы: Технология обработки информации

Безопасность/сложность

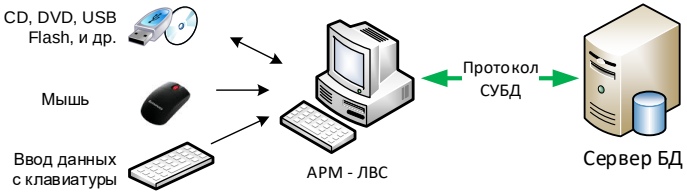
Терминальный доступ



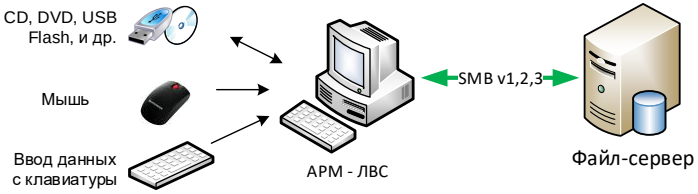
Трехзвенная



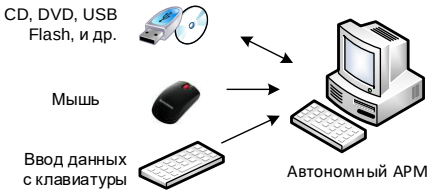
Клиент-сервер



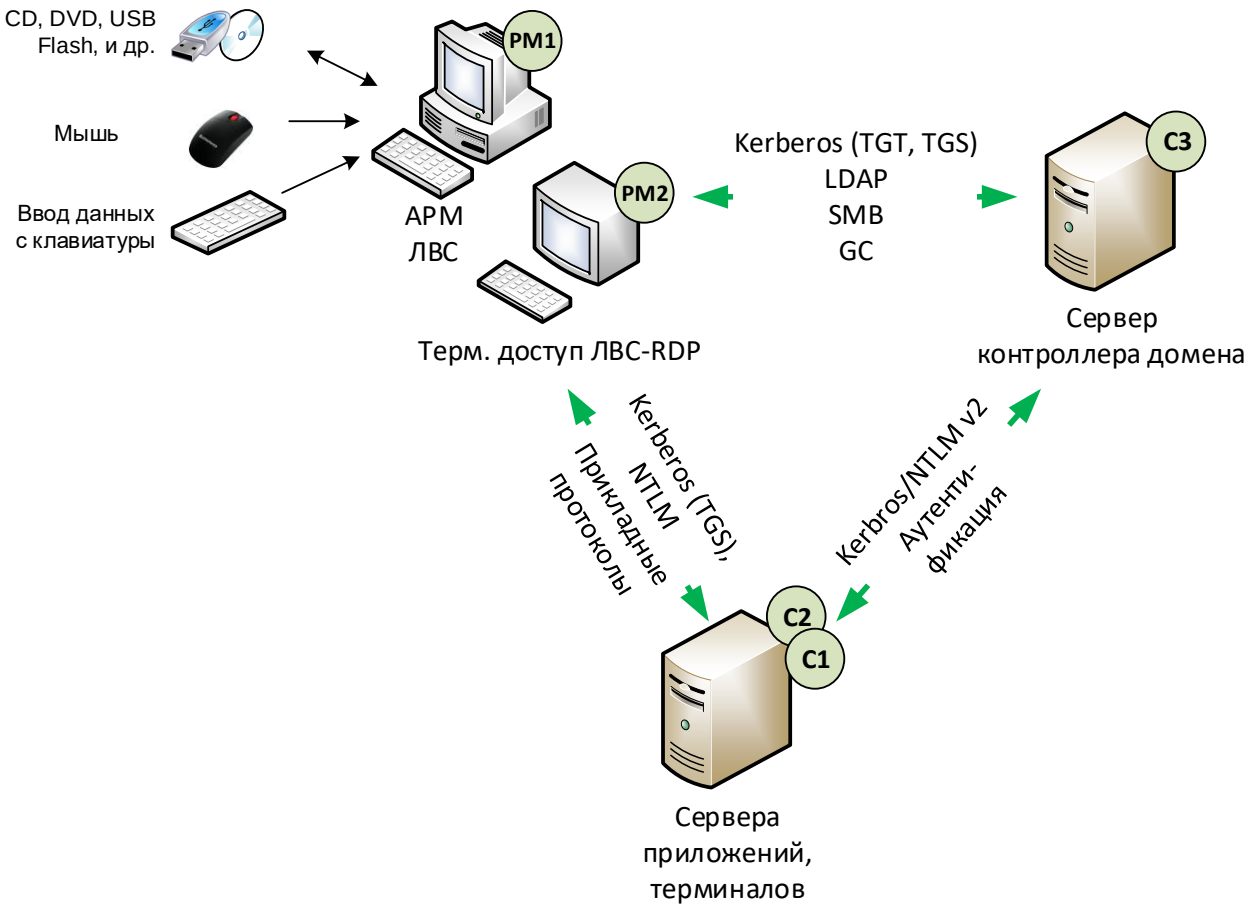
Файл-сервер



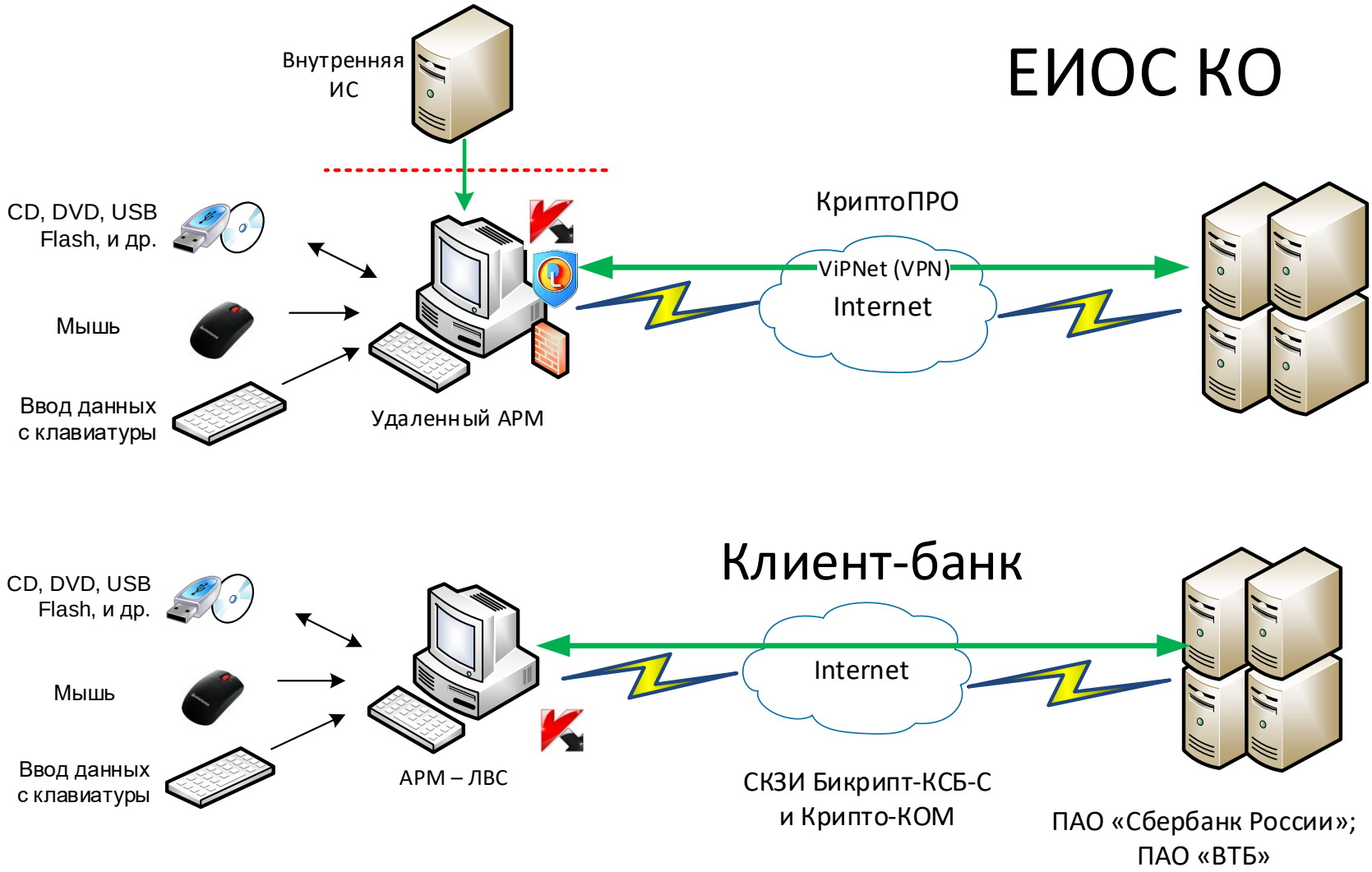
Автономная



Базовые сервисы: Active Directory



Подключения к внешним ИС



Особенности применяемых ИТ

- Мобильные носители информации (МНИ)
- Подключение к сети любого типа
- Виртуализация
- Доступ пользователей в Интернет
- Публикация сервисов в Интернет
- Удаленный доступ через сеть Интернет
- Доступ с мобильных средств
- Беспроводные технологии связи
- Криптография
- Облачные технологии

Пользователи (доступ к данным)

Непривилегированные пользователи:

- Внутренние
- Внешние (при внешнем подключении)

Привилегированные пользователи:

- Системный администратор
- Администратор безопасности
- Программист-разработчик
- Специалисты подрядной организации

Обеспечивающие функционирование (без доступа к данным)

Обслуживающие ИТ:

- поставщики оборудования и ПО
- сервис-центры

Обслуживающие:

- Электроснабжение
- Кондиционирование
- Безопасность
- Помещения

Общие шаги

1. Собрать информацию
2. **Понять угрозы и риски**
3. Сформировать мероприятия
4. Внедрить мероприятия
5. Оценить их эффективность
6. Эксплуатировать безопасно
7. Выводить из эксплуатации безопасно

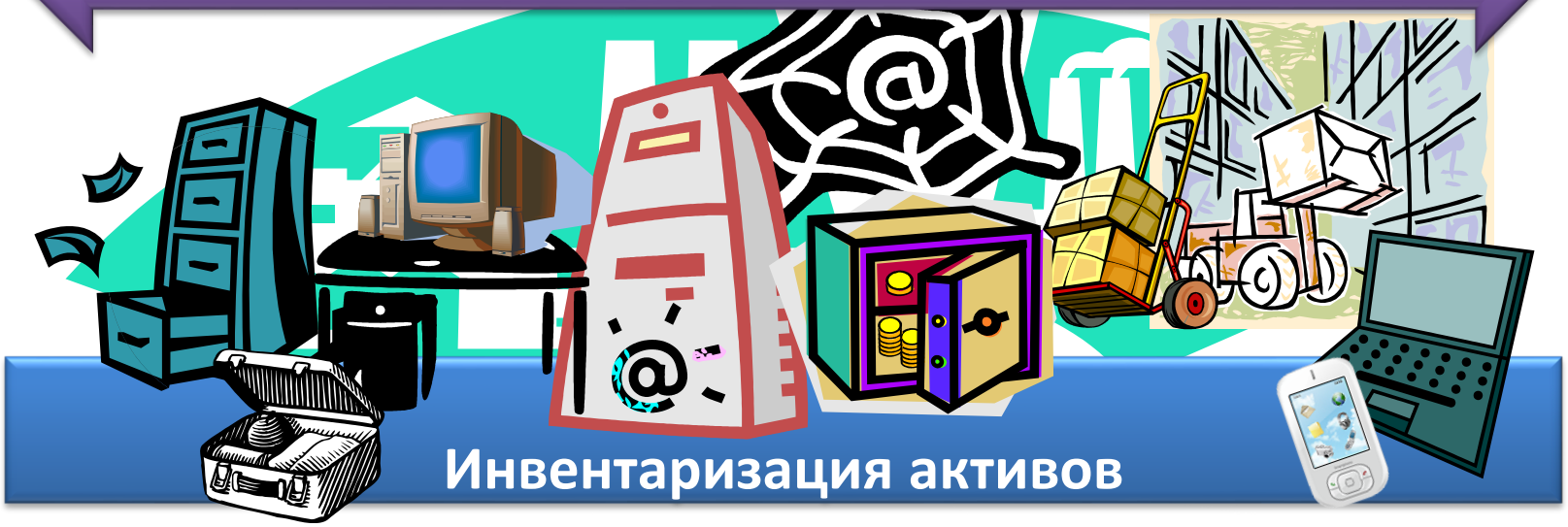
Место управления рисками

Меры по защите активов

Управление рисками

Цель – установить прозрачную взаимосвязь между активами и мерами по их защите.

Классификация активов по степени важности



Инвентаризация активов

Понятия и определения

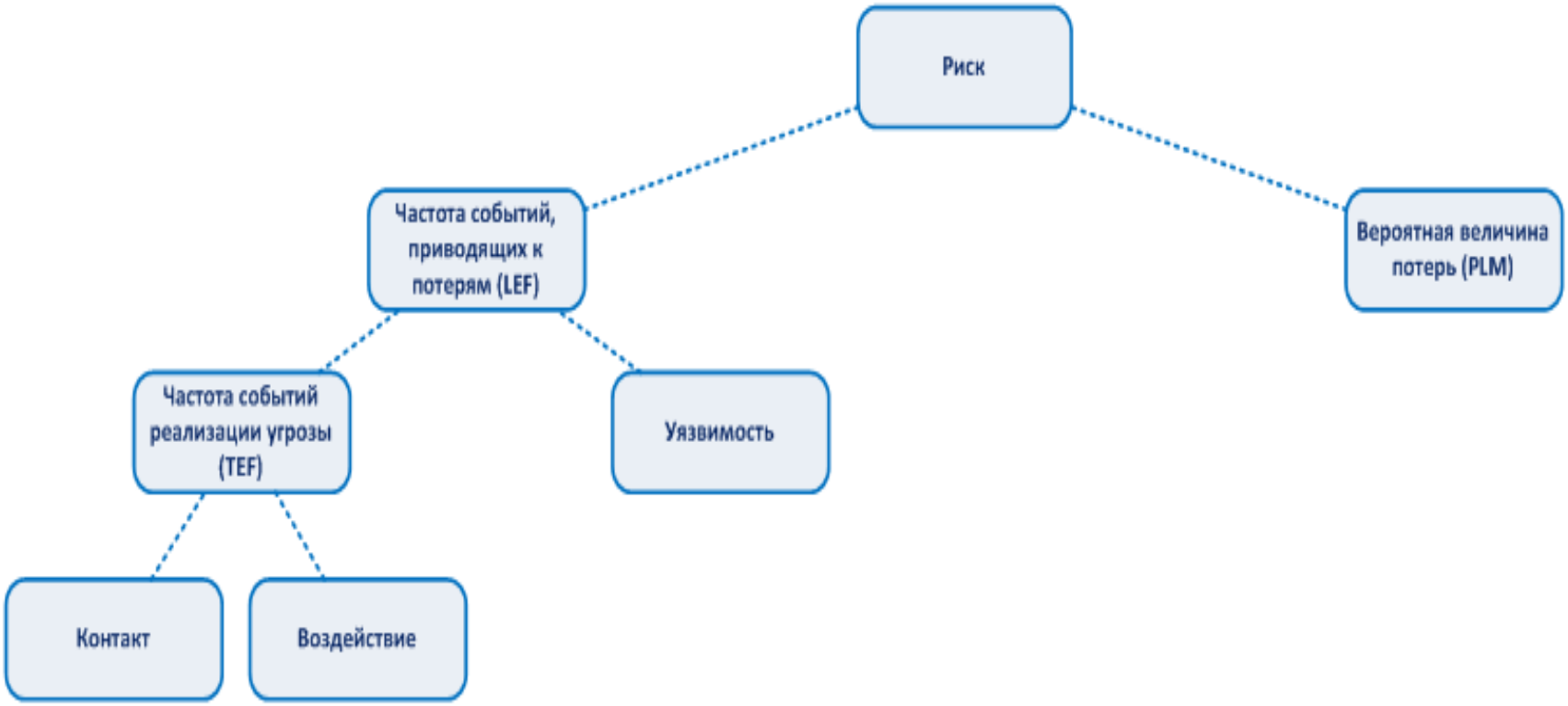
Угроза ИБ – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [ISO 27000]

Уязвимость – слабость актива, эксплуатация которой приведёт к реализации одной или нескольких угроз [ISO 27000]

Источник угрозы - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации [ГОСТ Р 50922-96]

Определение риска

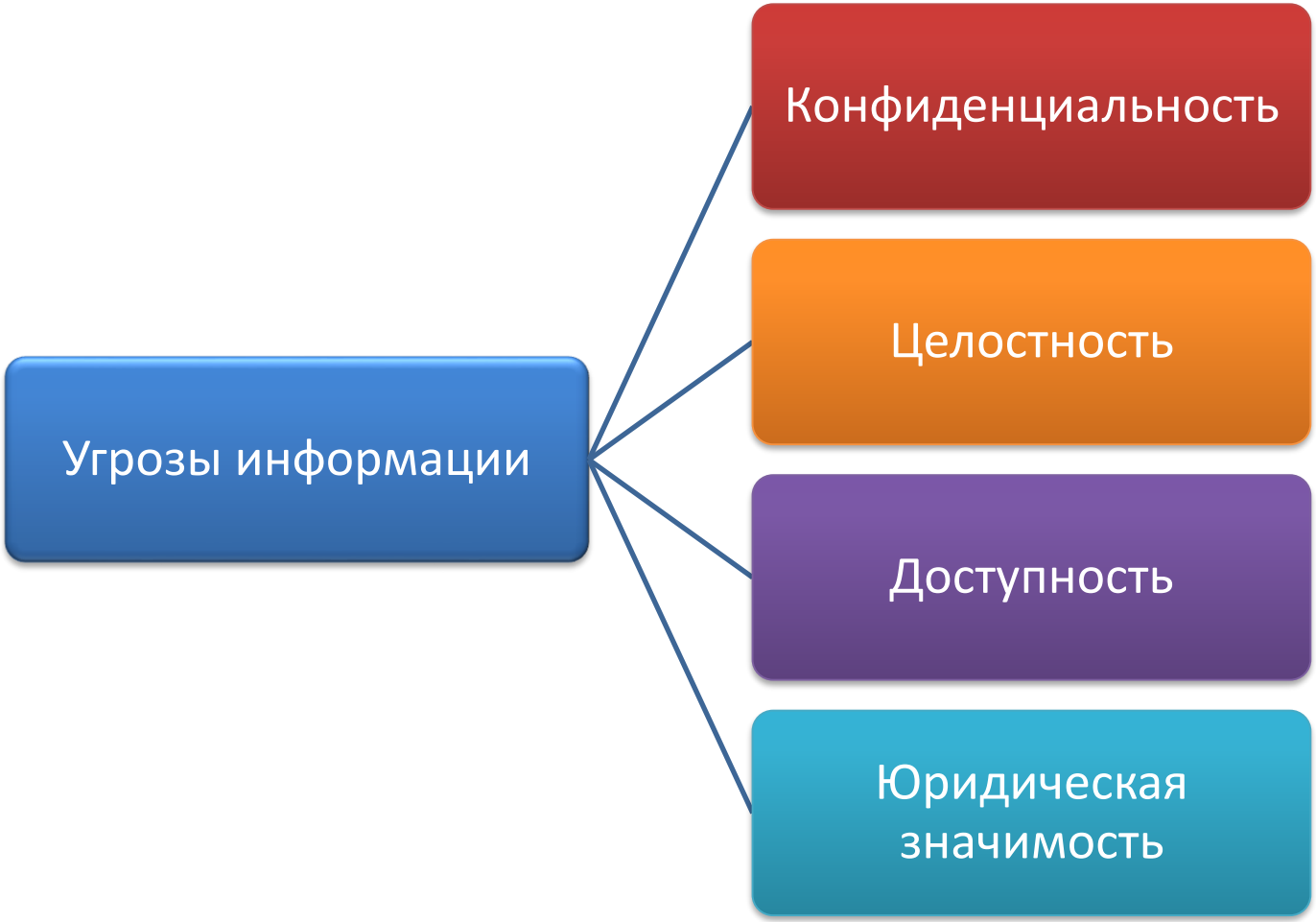
Риск - Сочетание вероятности события и его последствий [ISO 27000]



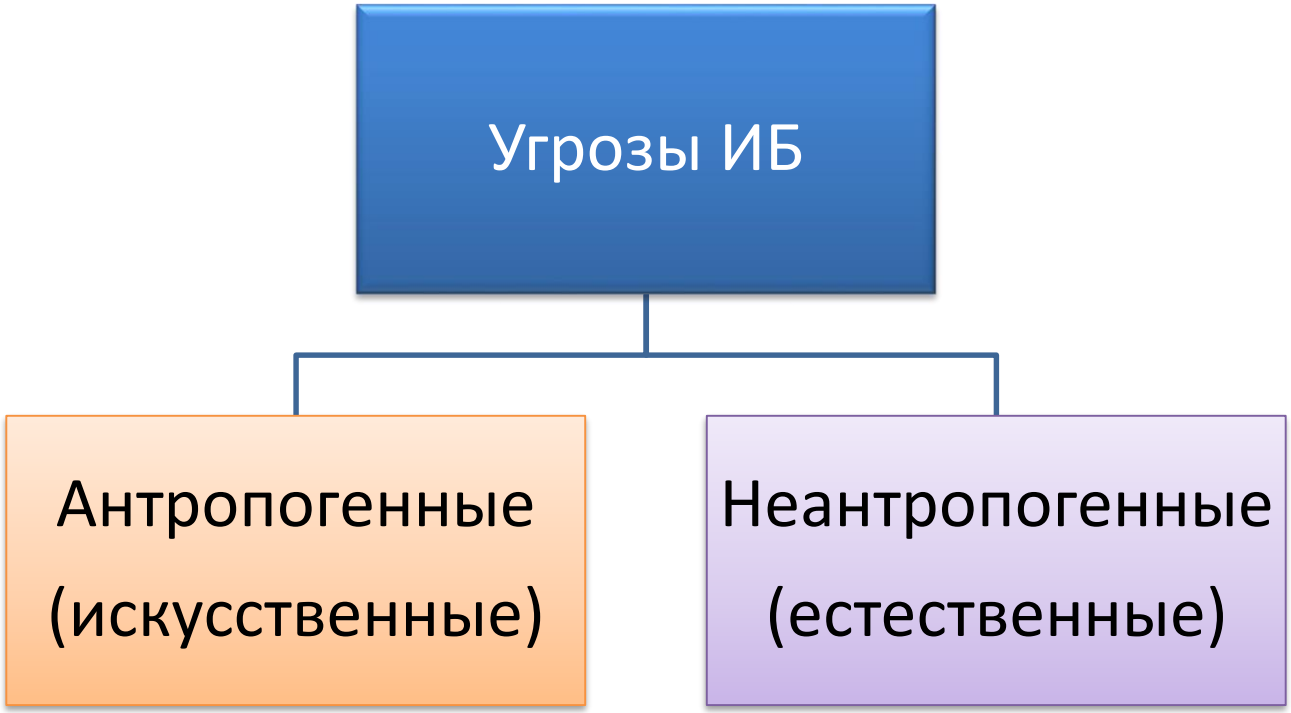
Имеющиеся подходы

- Методические документы ФСТЭК от 2008 года (?)
- Постановление Правительства Кировской области № 421 от 24.08.2017
- Банк данных угроз ФСТЭК (БДУ)
  - наполняется с 2015 года
    - 207 угроз
    - 18317 уязвимостей в ПО и оборудовании
  - не обязателен для ПДн
  - http://bdu.fstec.ru
- Другие методики

Угрозы ИБ в отношении информации



Источники угроз ИБ



Антропогенные угрозы

1) **Атаки** - с применением несанкционированных средств в целях обхода мер безопасности.

2) Угрозы, осуществляемые **санкционированным способом**, то есть легально действующими субъектами доступа, с применением санкционированных средств, правил разграничения доступа и процедур.

Направления атак

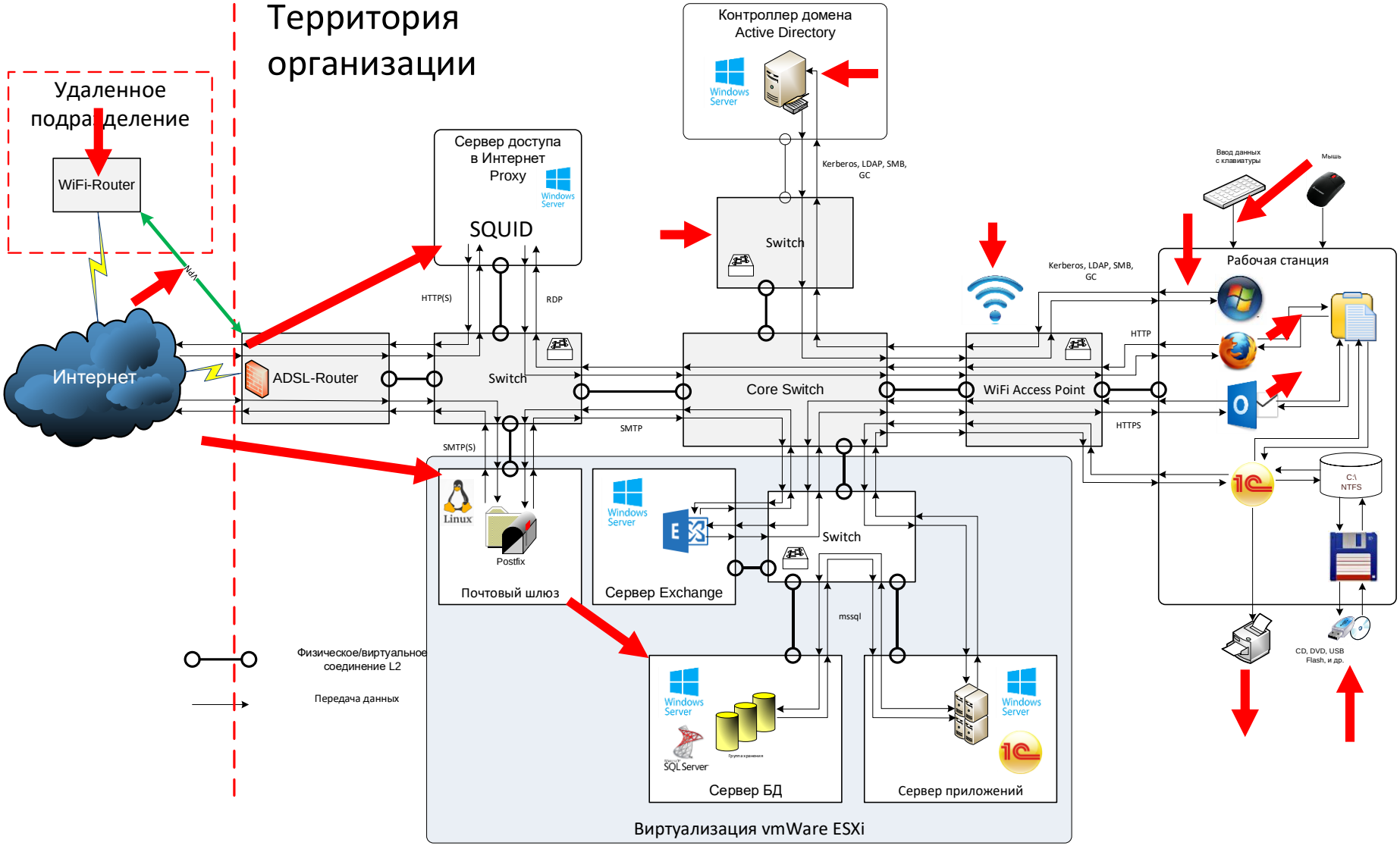
1. Атаки извне территории предприятия, через подключения к сети Интернет.
2. Атаки с территории предприятия.
3. Целенаправленные атаки (специально подготовленные атаки, целью которых является данное предприятие).

APT – Advanced Persistent Threat.

Атаки: этапы

1. Подготовка.
2. Проникновение.
3. Распространение.
4. Воздействие.

Некоторые векторы атаки



Атакуют уязвимые места

Выделяются уязвимости в:

- технологиях (30%*);
- ПО и оборудовании (50%*);
- конфигурации (70%*);
- процессах (15%*);
- персонале (10%*);
- правовых мерах (только для облачных?*).

*% от угроз в банке данных угроз ФСТЭК, содержит 207 угроз и 18317 уязвимостей в ПО и оборудовании

Как снизить вероятность атаки?

- Ограничение доступа:
  - физического
  - к сведениям об используемых ИТ
- Устранение уязвимостей
- Мониторинг и реагирование на инциденты

Внутренние угрозы

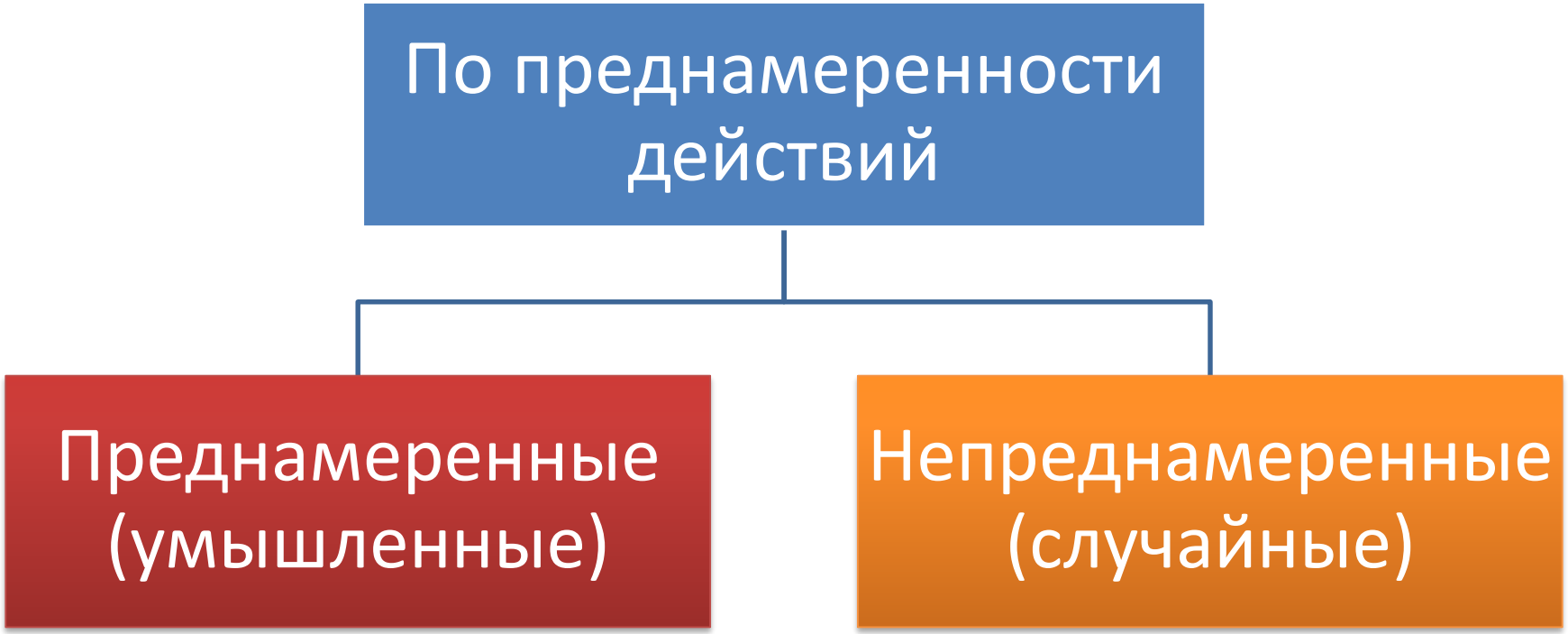
- Источник – внутренний нарушитель:
  - Свои сотрудники
  - Подрядчики
- С использованием имеющихся прав
- Могут действовать по указанию извне:
  - умышленно
  - путем обмана (социальная инженерия)
- 60-70% от всех инцидентов!!!
- Внимание: привилегированные лица

Привилегированные лица

Особое внимание к:

- VIP-сотрудники предприятия;
- сотрудники, ответственные за безопасность;
- сотрудники, имеющие доступ:
  - к особо значимой информации;
  - ко всей информации;
- обслуживающие подразделения;
- системные администраторы;
- администраторы безопасности;
- разработчики ПО и ИС;
- подрядчики, имеющие доступ к ИТ-инфраструктуре.

Преднамеренность



Как снизить вероятность умышленных действий?

- квалифицирование (допуск после испытаний);
- доверие;
- процедуры при работе с персоналом:
  - при приеме
  - при изменении полномочий/переводе;
  - при увольнении;
- правовые, организационные и технические меры по обеспечению соблюдения обязательств и обязанностей;
- мониторинг и реагирование на инциденты.

Случайные действия

Источники:

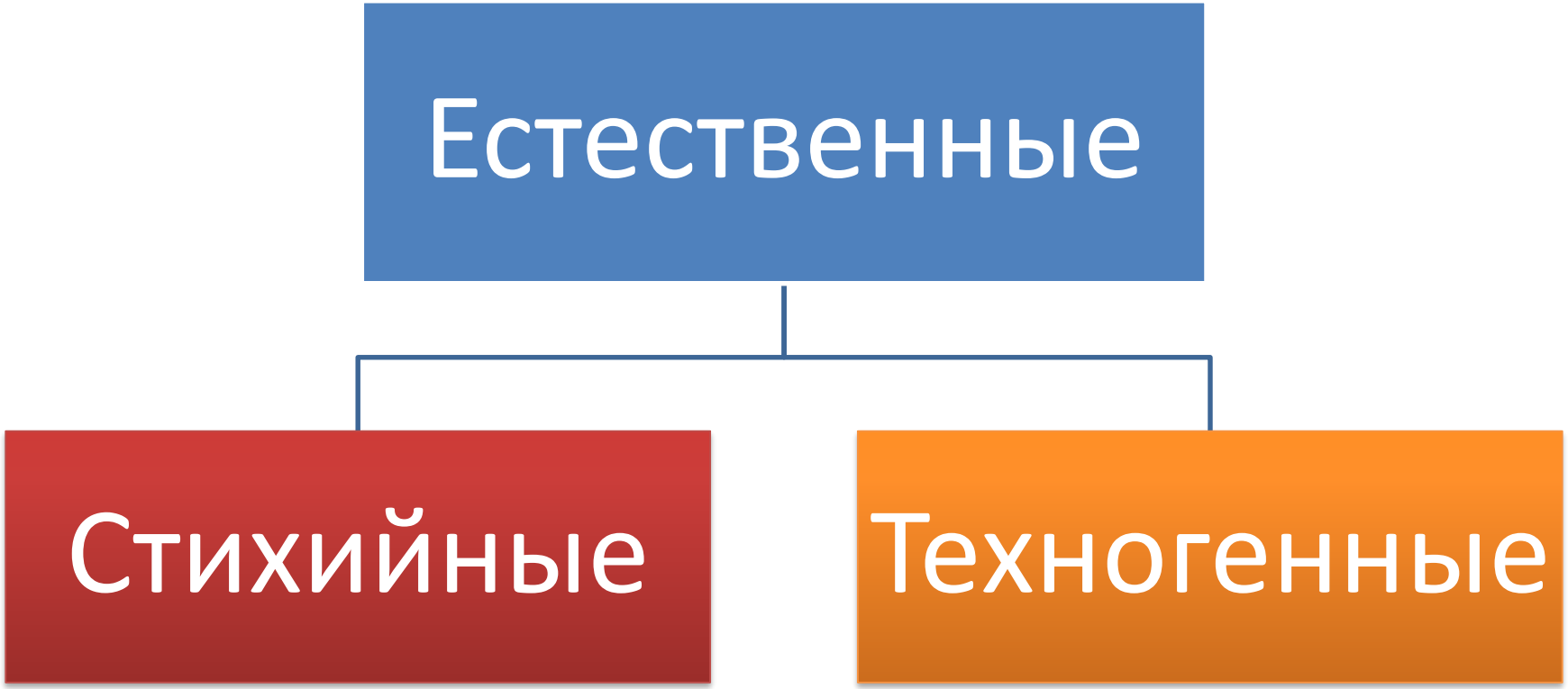
- Халатность, некомпетентность.
- Социальная инженерия!!!!!!!

Дефицит фокуса в нормативке ФСТЭК!?

Снижение вероятности:

- повышение компетентности (осведомленности);
- правовые и организационные меры по обеспечению соблюдения обязательств и обязанностей;
- мониторинг ИС;
- резервирование данных и оборудования;
- 100% соблюдения правил, включая неотвратимость ответственности (путем отработки 100% обнаруженных инцидентов).

Естественные угрозы



Стихийные

- Ураганы
- Наводнения
- Пожары (природного происхождения)
- Землетрясения

Методы защиты:

- строительные решения
- повышение надежности (в т.ч. География)
- пожарная сигнализация

Техногенные

- аварии, катастрофы, пожары
- сбои в электроснабжении
- сбои в климатическом оборудовании
- износ оборудования

Методы защиты:

- строительные решения
- повышение надежности:
  - Резервирование оборудования (горячее, холодное)
  - Резервные копии информации
  - География

Определение актуальных угроз

Варианты:

1. На основе методик ФСТЭК:
   – Методика 2008 года – порядка 50 угроз
   – Банк данных угроз ФСТЭК – 207 угроз
2. Методика ФСБ – только для криптосредств.
3. На основе Постановления правительства Кировской области №421 от 24.08.2017г.

Методика ФСТЭК

1. Выбор актуальных типов нарушителя
2. Определение актуальных угроз

Выбор актуальных типов нарушителя

Внутренние нарушители	
К1	Должностные лица, обеспечивающие нормальное функционирование АС
К2	**Зарегистрированные локальные пользователи АС**
К3	Зарегистрированные удаленные пользователи АС
К4	**Зарегистрированные пользователи с полномочиями Администратора безопасности сегмента (фрагмента) АС**
К5	**Зарегистрированные пользователи с полномочиями Системного администратора АС**
К6	**Зарегистрированные пользователи с полномочиями Администратора безопасности АС**
К7	**Программисты-разработчики (поставщики) прикладного ПО и лица, обеспечивающие его сопровождение на защищаемом объекте**
К8	**Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт технических средств АС**

Выбор актуальных типов нарушителя

Внешние нарушители	
К9	Разведывательные службы государств
К10	**Криминальные структуры (хакеры, группы хакеров)**
К11	Конкуренты (конкурирующие организации)
К12	Недобросовестные партнеры
К13	Внешние субъекты (физические лица)

Методика по ФСТЭК

ПРИМЕР документов.

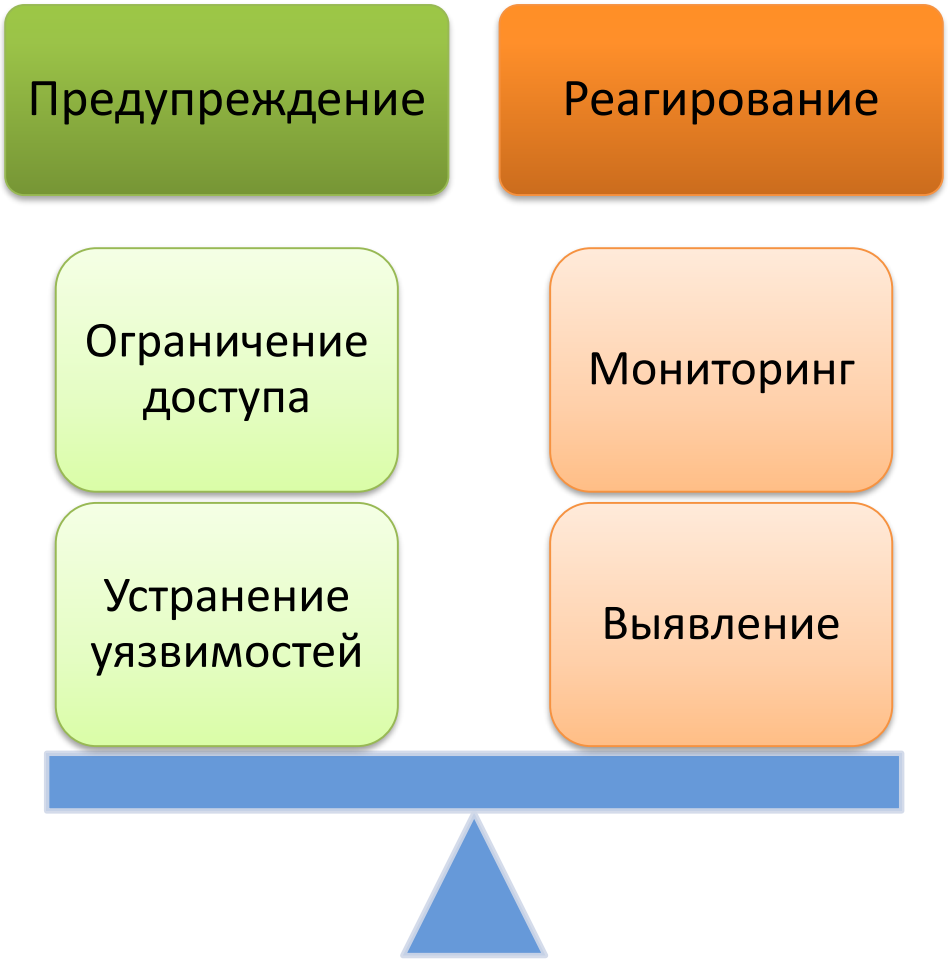
Общие шаги

1. Собрать информацию
2. Понять угрозы и риски
3. **Сформировать мероприятия**
4. Внедрить мероприятия
5. Оценить их эффективность
6. Эксплуатировать безопасно
7. Выводить из эксплуатации безопасно

Вопросы при выборе мер

1. Соответствуют ли меры требованиям?
2. Закрывают ли они угрозы?
3. Понятны ли они нам?

Баланс мероприятий!!!



Мероприятия

На следующем занятии!

Ваши вопросы?

Спасибо за внимание!

Городилов Сергей

Руководитель направления ИБ, АСПЕКТ СПб

gors@aspectspb.ru

www.aspectspb.ru