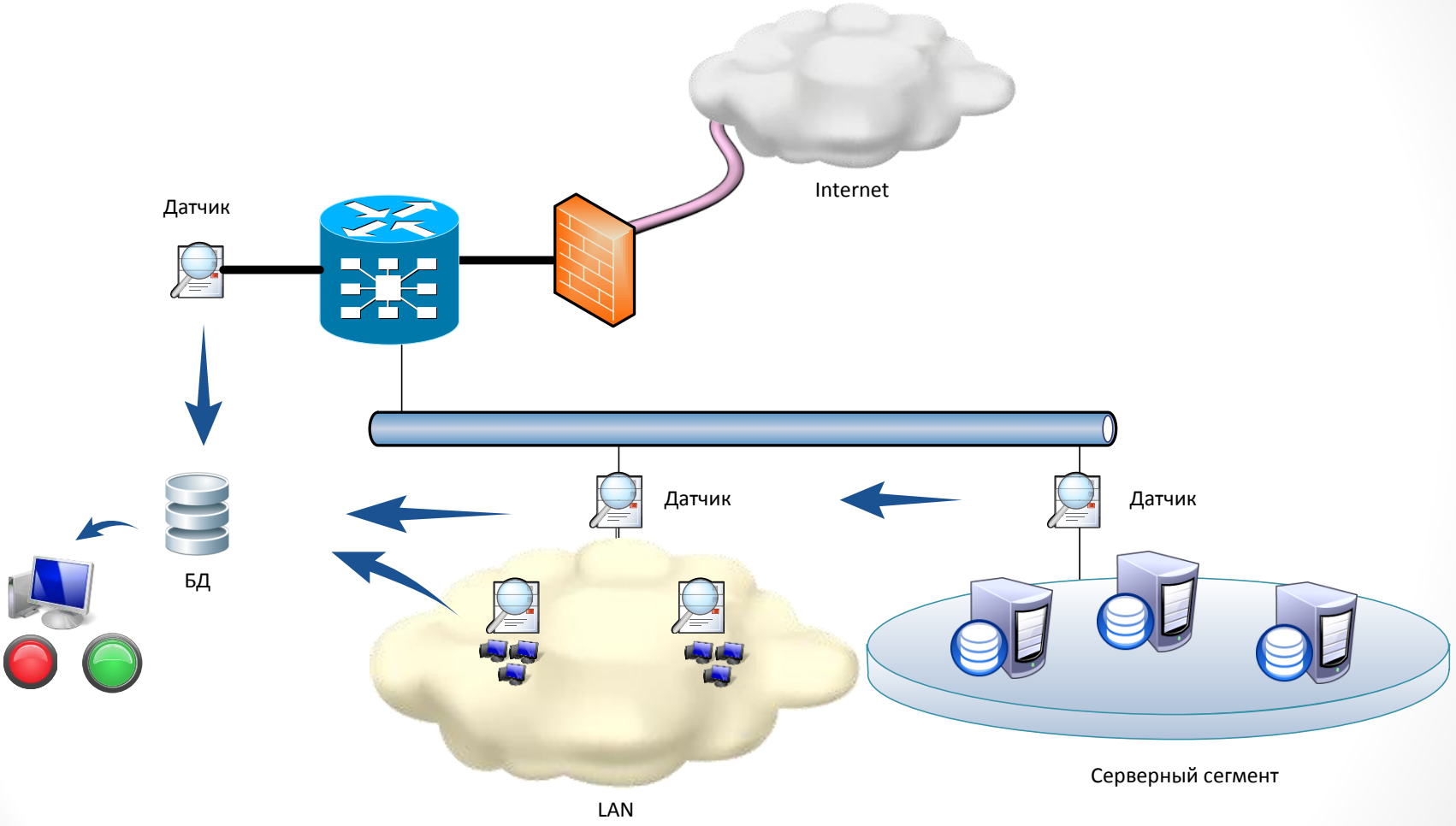
# СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

# Принцип



# СКАНЕРЫ БЕЗОПАСНОСТИ

# Механизмы работы сканеров

- ***Сканирование*** - механизм пассивного анализа, с помощью которого сканер пытается определить наличие уязвимости без фактического подтверждения ее наличия - по косвенным признакам.
- ***Зондирование*** - механизм активного анализа, который позволяет убедиться, присутствует или нет на анализируемом узле уязвимость. Зондирование выполняется путем имитации атаки, использующей проверяемую уязвимость.

# Этапы работы сканера

1. Сбор информации о сети. На данном этапе идентифицируются все активные устройства в сети и определяются запущенные на них сервисы и демоны.
2. Обнаружение потенциальных уязвимостей. Сканер использует свою базу данных для сравнения собранных данных с известными уязвимостями при помощи проверки заголовков или активных зондирующих проверок.
3. Подтверждение выбранных уязвимостей. Сканер использует специальные методы и моделирует (имитирует) определенные атаки для подтверждения факта наличия уязвимостей на выбранных узлах сети.
4. Генерация отчетов. Автоматическое устранение уязвимостей.
5. Автоматическое устранение уязвимостей.

# СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

# Что такое DLP?

**Предотвращение утечек** (англ. *Data Leak Prevention, **DLP***):

- **технологии** предотвращения утечек конфиденциальной информации из информационной системы вовне.
- **технические устройства** (программные или программно-аппаратные) для предотвращения утечек информации.

**Идея:**
**DLP-системы** призваны защищать информацию:

- при непосредственном использовании (***Data in use**/endpoint actions)*
- при передаче *(**Data in motion**/network actions)*
- при хранении *(**Data at rest**/data storage)*

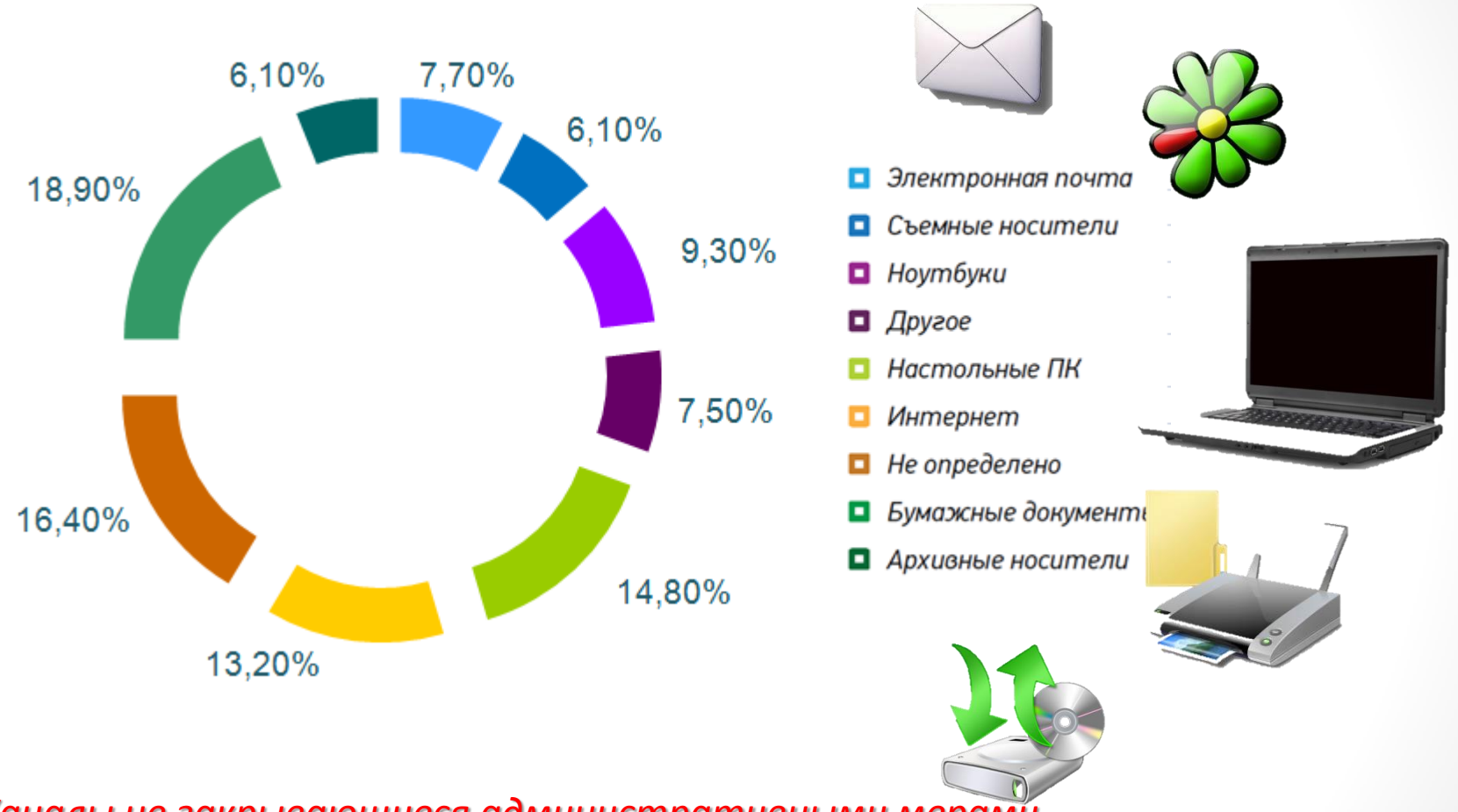
# Внутренние угрозы

- Утечка информации
- Нецелевое использование инфраструктуры
- Использование каналов связи во вред компании
- Нарушение политики информационной безопасности

# Внутренние нарушители

- Сотрудники компаний
- Стажеры, практиканты и т.д.
- Временные сотрудники: переводчики, и т.п.
- Внештатные работники: центры обработки данных, Call-центры
- Транспортные компании, курьеры
- Сотрудники других компаний, имеющие доступ к данным компании: аудиторы, внешние контролеры

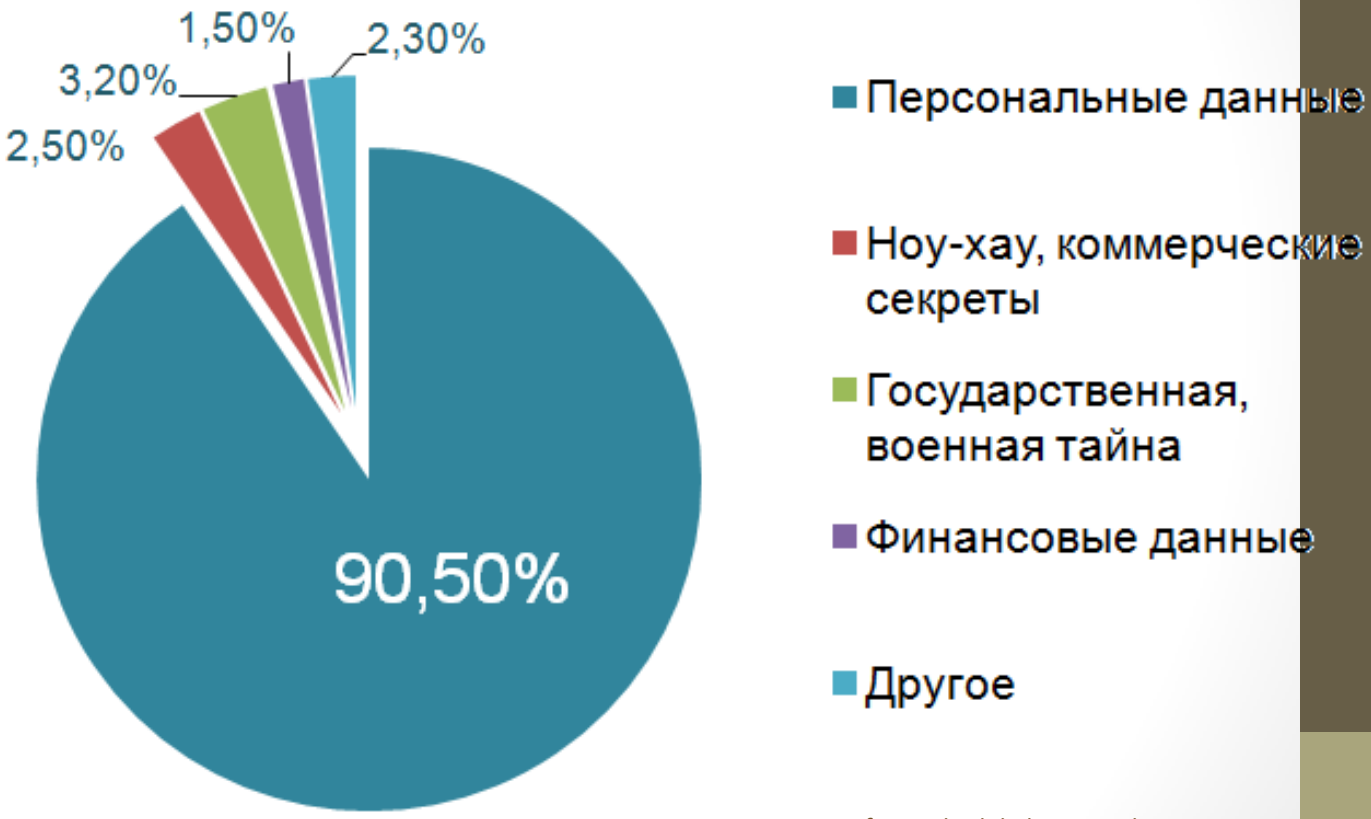
# Каналы утечки информации




*Каналы не закрывающиеся административными мерами или мерами (запрет фото и т.п.)*

# Распределение утечек по типам (2011г.)

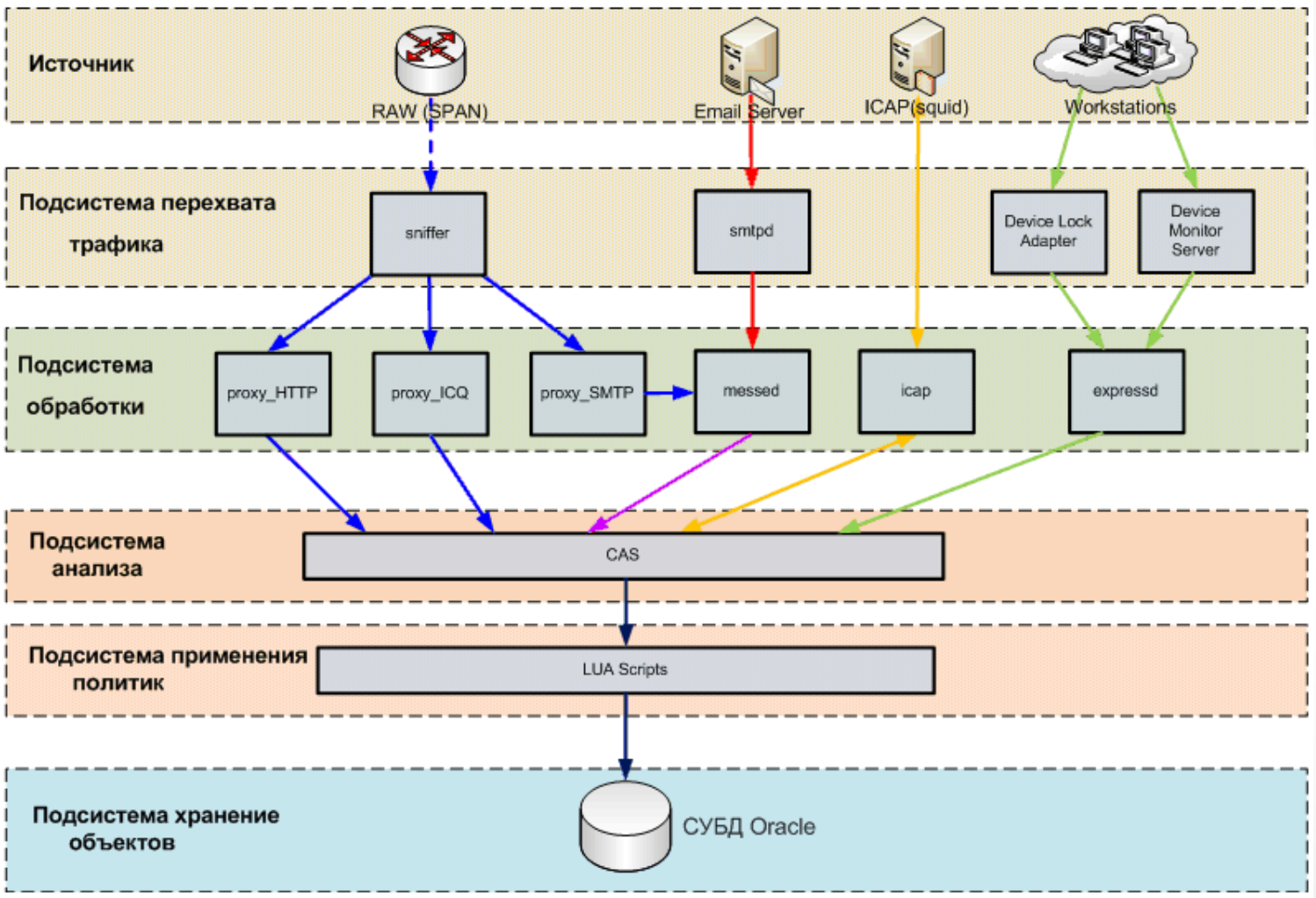
## Тип данных




InfoWatch Global Data Leakage Report

# Схема работы DLP продуктов InfoWatch

# Схема обработки информации



# Схема в режиме SPAN-копии