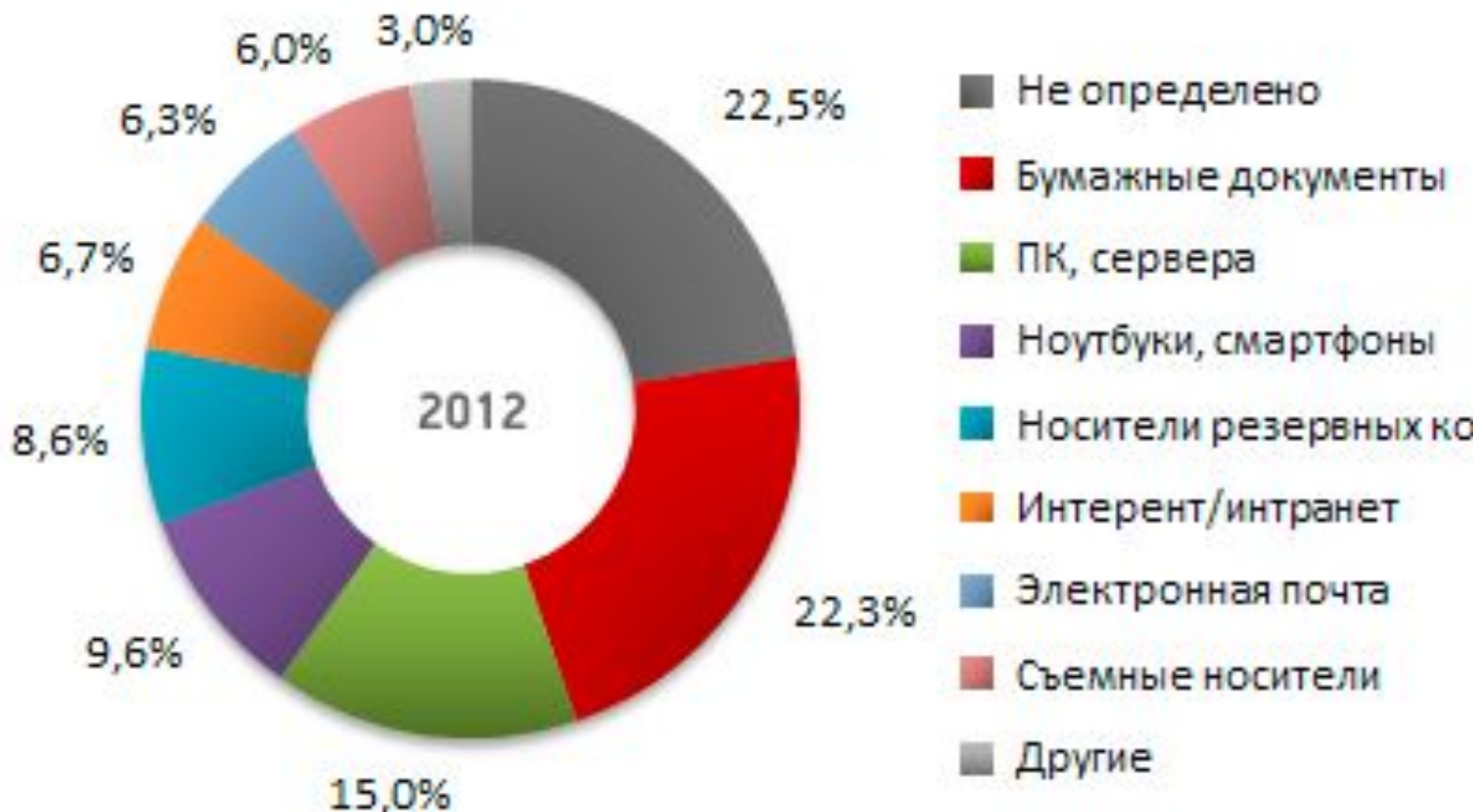
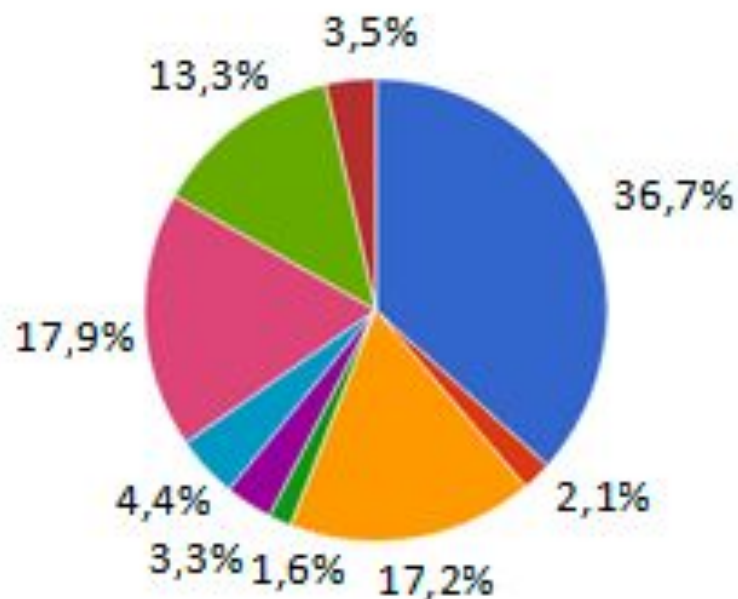


# Протоколирование и аудит

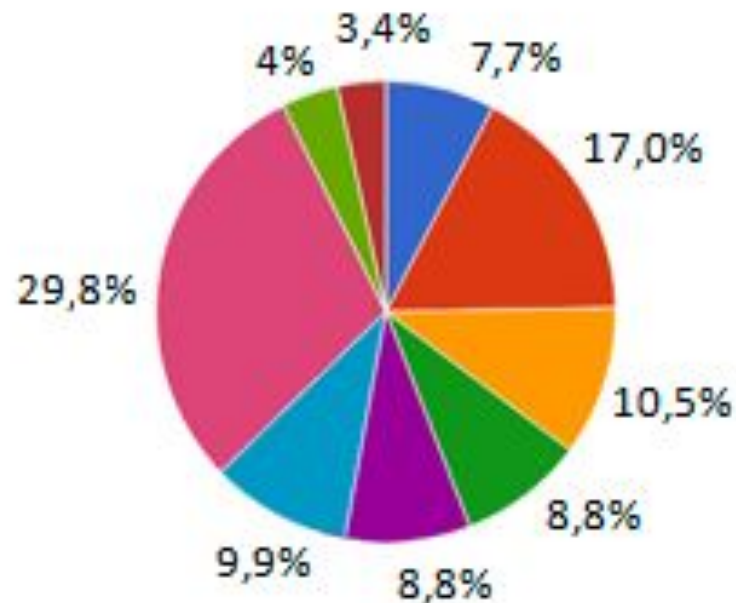
# Каналы утечки информации



## Умышленные



## Случайные



■ Не определено

■ Съемные носители

■ Бумажные документы

■ Ноутбуки, смартфоны

■ Веб, интранет

■ Носители резервных копий

■ ПК, серверы

■ Электронная почта

■ Другие

*Распределение случайных и умышленных утечек по каналам (информация за 2012 год)*

# Сервисы безопасности

- ▶ идентификация и аутентификация;
- ▶ управление доступом;
- ▶ **протоколирование и аудит;**
- ▶ шифрование;
- ▶ контроль целостности;
- ▶ экранирование;
- ▶ анализ защищенности;
- ▶ обеспечение отказоустойчивости;
- ▶ обеспечение безопасного восстановления;
- ▶ туннелирование;
- ▶ управление.

# Протоколирование

- ▶ сбор и накопление информации о событиях, происходящих в информационной системе
- ▶ внешние (вызванные действиями других сервисов)
- ▶ внутренние (вызванные действиями самого сервиса)
- ▶ клиентские (вызванные действиями пользователей и администраторов)

# Аудит

- ▶ анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день)
- ▶ пассивный
- ▶ активный (оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации)

Под **протоколированием** понимается сбор и накопление информации о событиях, происходящих в информационной системе.

У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

**Аудит** — это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день).

Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

- ▶ Реализация протоколирования и аудита преследует следующие **главные цели**:
- ▶ обеспечение подотчетности пользователей и администраторов;
- ▶ обеспечение возможности реконструкции последовательности событий;
- ▶ обнаружение попыток нарушений информационной безопасности;
- ▶ предоставление **информации** для выявления и **анализа** проблем.



- ▶ Реализация протоколирования и аудита решает следующие задачи:
- ▶ обеспечение подотчетности пользователей и администраторов;
- ▶ обеспечение возможности реконструкции последовательности событий;
- ▶ обнаружение попыток нарушений информационной безопасности;
- ▶ предоставление информации для выявления и анализа проблем.

- ▶ **Протоколированию подлежат следующие события:**
- ▶ **ВХОД в систему (успешный или нет);**
- ▶ **ВЫХОД ИЗ СИСТЕМЫ;**
- ▶ **обращение к удаленной системе;**
- ▶ **операции с файлами (открыть, закрыть, переименовать, удалить);**
- ▶ **смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т.п.).**

- ▶ При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:
- ▶ дата и время события;
- ▶ уникальный идентификатор пользователя – инициатора действия;
- ▶ тип события;
- ▶ результат действия (успех или неудача);
- ▶ источник запроса (например, имя терминала);
- ▶ имена затронутых объектов (например, открываемых или удаляемых файлов);
- ▶ описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

- ▶ Характерная особенность **протоколирования и аудита** – зависимость от других средств безопасности. Идентификация и аутентификация служат отправной точкой подотчетности пользователей, логическое управление доступом защищает конфиденциальность и целостность регистрационной информации. Возможно, для защиты привлекаются и криптографические методы.

- ▶ Под **подозрительной активностью** понимается поведение пользователя или компонента информационной системы, являющееся злоумышленным (в соответствии с заранее определенной политикой безопасности) или нетипичным (согласно принятым критериям).
- ▶ **Задача активного аудита** – оперативно выявлять подозрительную **активность** и предоставлять средства для автоматического реагирования на нее.
- ▶ **Активность**, не соответствующую политике безопасности, целесообразно разделить на атаки, направленные на незаконное получение полномочий, и на действия, выполняемые в рамках имеющихся полномочий, но нарушающие политику безопасности.
- ▶ Атаки нарушают любую осмысленную политику безопасности. Иными словами, **активность** атакующего является разрушительной независимо от политики. Следовательно, для описания и выявления атак можно применять универсальные методы, инвариантные относительно политики безопасности, такие как сигнатуры и их обнаружение во входном потоке событий с помощью аппарата экспертных систем.

- ▶ **Сигнатура атаки** – это совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию. Простейший пример сигнатуры – "зафиксированы три последовательные неудачные попытки входа в систему с одного терминала", пример ассоциированной реакции – блокирование терминала до прояснения ситуации.

► Средства **активного аудита** могут располагаться на всех линиях обороны информационной системы. На границе контролируемой зоны они могут обнаруживать подозрительную активность в точках подключения к внешним сетям (не только попытки нелегального проникновения, но и действия по "прощупыванию" сервисов безопасности). В корпоративной сети, в рамках информационных сервисов и сервисов безопасности, **активный аудит** в состоянии обнаружить и пресечь подозрительную активность внешних и внутренних пользователей, выявить проблемы в работе сервисов, вызванные как нарушениями безопасности, так и аппаратно-программными ошибками. Важно отметить, что **активный аудит**, в принципе, способен обеспечить защиту от атак на доступность.

- ▶ В составе средств активного аудита можно выделить следующие функциональные компоненты:
- ▶ компоненты генерации и хранения регистрационной информации.
- ▶ компоненты извлечения регистрационной информации (сенсоры ).
- ▶ компоненты просмотра регистрационной информации;
- ▶ компоненты анализа информации, поступившей от сенсоров.
- ▶ компоненты принятия решений и реагирования;
- ▶ компоненты интерфейса с администратором безопасности.