КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DeviceLock DLP
Proactive Endpoint Security

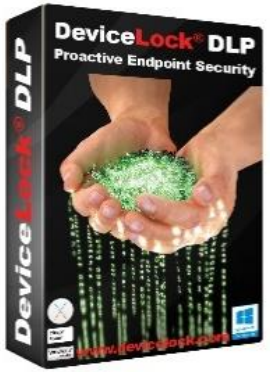
# Как защитить важные данные и не остаться в позиции наблюдателя за утечками?

СЕРГЕЙ ВАХОНИН
Директор по решениям
Смарт Лайн Инк
SV@DEVICELOCK.COM

АО Смарт Лайн Инк
2020

# DeviceLock - 20 лет на мировом рынке информационной безопасности

DeviceLock® DLP




ПЕРВАЯ ВЕРСИЯ
DEVICELOCK -
1996

## Продукт

Программный комплекс **DeviceLock DLP**

Система защиты информации для организаций, которым необходимо простое и доступное решение по предотвращению утечек данных с корпоративных компьютеров под управлением Windows и MacOS, а также виртуализованных рабочих сред и приложений Windows.

## Смарт Лайн Инк / DeviceLock

Отечественная компания с штаб-квартирой и офисом разработки **в Москве** (АО «Смарт Лайн Инк), офисами продаж в США (DeviceLock NA, San Ramon, California), Канаде (DeviceLock Canada, North Vancouver), Великобритании (DeviceLock UK, London), Германии (DeviceLock Europe GmbH, Ratingen), Италии (DeviceLock Italy, Milan), а также партнерской сетью по всему миру.

# Ключевые рынки. Крупнейшие клиенты в России и за рубежом

| Клиент | Количество сотрудников | Объем внедрения (количество агентов) |
|---|---|---|
| **Vodafone,** Индия | >50000 | 28500 |
| **Metro C&C Group,** Германия | >10000 | 10500 |
| **HONG KONG POLICE FORCE,** Гонконг | >30000 | 16000 |
| **Best Buy,** США/Канада | >30000 | 15000 |
| **Промсвязьбанк, РФ** | >10000 | 5000 |

Крупнейшие клиенты DeviceLock DLP – это крупные организации, проходящие аудит на предмет соблюдения безопасности обработки конфиденциальных корпоративных и персональных данных, правительственные учреждения, обрабатывающие секретную информацию, нуждающиеся в защите корпоративных данных, предотвращении утечек данных и контроле их использования и перемещения.

| ## | Государство / регион |
|---|---|
| 1 | Российская Федерация и СНГ |
| 2 | Япония |
| 3 | Германия |
| 4 | США и Канада |
| 5 | Великобритания |
| 6 | Китай и Гонконг |
| 7 | Ближневосточный регион (ОАЭ, Оман, Кувейт) |


Наиболее крупная инсталляция DeviceLock обеспечивает защиту **более 70 тысяч** рабочих мест (США, финансовый сектор).

# DeviceLock – география использования


Число установок программного комплекса DeviceLock DLP только за последние **три года** составило около **4 миллионов компьютеров**, установленных по всему миру в информационных системах **5,5 тысяч организаций** кредитно-финансового, энергетического, оборонного и государственного секторов, а также телекоммуникаций, здравоохранения и образования и других.

# ЧТО ЗАЩИЩАТЬ?

**Защита необходима для информации и сведений, являющиеся критическими для организации.**

- Информация о владельцах бизнеса
- Финансовая и бухгалтерская информация
- Документы стратегического развития (прогнозы, планы выхода на новые рынки, планы по партнерству и т.д.)
- Аналитика – рыночная, маркетинговая
- Интеллектуальная собственность  (разработки и т.д.)
- Техническая информация об ИТ инфраструктуре
- Договора, проекты договоров, приложения
- Информация о клиентах и партнерах
- Информация, полученная от партнеров, в особенности защищенная соглашением о конфиденциальности

*Даже если в компании нет информации с грифом коммерческой или служебной тайны, или же она за пределами организации теряет смысл, всегда есть коммуникации между людьми внутри и снаружи организации – чаты, переписка, другой обмен данными. Если такие коммуникации не контролировать, почти неизбежны случаи мошенничества, сговоры и другие действия, наносящие прямой ущерб компании.*
*Кроме того, в любой организации есть персональные данные (сотрудников, клиентов, пользователей и т.д.), защита которых необходима в соответствии с ФЗ-152, GDPR.*

# DATA LEAK (loss) PREVENTION (protection) = ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

DLP-система - ИТ-решение, обеспечивающее **выявление**, **отслеживание** и **предотвращение неавторизованного использования, хранения и перемещения** данных ограниченного доступа и др., используемых в организации

Обнаружение данных в хранилищах

Отслеживание перемещения данных

Предотвращение утечки по сети и через устройства

**Defining DLP**

Even a decade on, there is still little consensus on what actually compromises a DLP solution. Some people consider encryption or USB port control to be DLP, while others limit the term to complete product suites focused on analyzing and enforcing content usage policies. Securosis defines DLP as:

*Products that, based on central policies, identify, monitor, and protect data at rest, in motion, and in use, through deep content analysis.*

***Контроль** = избирательное **управление доступом** + **регистрация** событий и перемещаемых данных + **инспекция** хранимых данных*

*Full-suite solutions* provide complete coverage across your network, storage repositories, and endpoints, even if you aren't using their full capabilities.

*Источник: 'Understanding and Selecting a Data Loss Prevention Solution', Securosis Whitepaper, 2018, v.3*

# АВТОМАТИЧЕСКАЯ РАБОТА – ОСНОВНОЕ ТРЕБОВАНИЕ К ПОЛНОЦЕННЫМ DLP

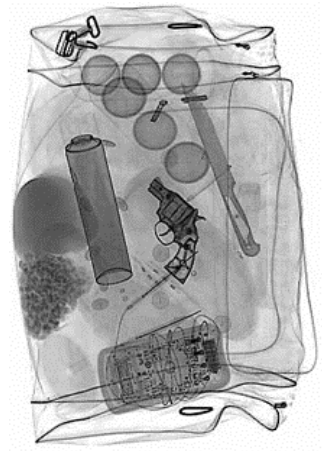
**Автоматическое принятие решений** о возможности передачи/печати/сохранения на основе двух взаимодополняющих методов


## Контекстный контроль

- Пользователь, его права, группы
- Дата и время
- Местонахождение
- Источник / адресат
- Тип файла / данных
- Использование шифрования данных
- Направление передачи данных
- Информация об устройстве / веб-сервисе


## Контентный анализ и фильтрация (проверка содержимого)

- Ключевые слова и сочетания слов, морфологический анализ, транслитерация, промышленные словари
- Встроенные шаблоны данных (номера карт страхования, кредитных карт, др.)
- Цифровые отпечатки (fingerprints)
- Проверка архивов и вложенных архивов, встроенных в файлы-контейнеры
- Возможность проверки как сообщений, так и вложений почты и мессенджеров
- Категории и классификация
- Прочие критерии проверки



# КОГДА ОБНАРУЖИВАТЬ ЗАЩИЩАЕМЫЕ ДАННЫЕ?

## ДО

Анализ **хранимых** данных (discovery)

## ВО ВРЕМЯ ПЕРЕДАЧИ

Анализ **передаваемых** данных **в реальном времени** (передача, сохранение, печать)

## ПОСЛЕ

Анализ **перехваченных** данных в архиве

Проверять содержимое документов и переписки можно и нужно не только после того, как утечка уже произойдет, а утекшие данные будут распространяться бесконтрольно!

***Последствия*** *отсутствия механизма контентной фильтрации в реальном времени для всех каналов в DLP-системе :*

*- в архиве DLP-системы хранятся* ***ВСЕ*** *перехваченные данные, и корпоративные, и* ***личные****.*

- *Блокировка каналов передачи данных целиком там, где можно делать исключения, блокируя только передачу данных ограниченного доступа*

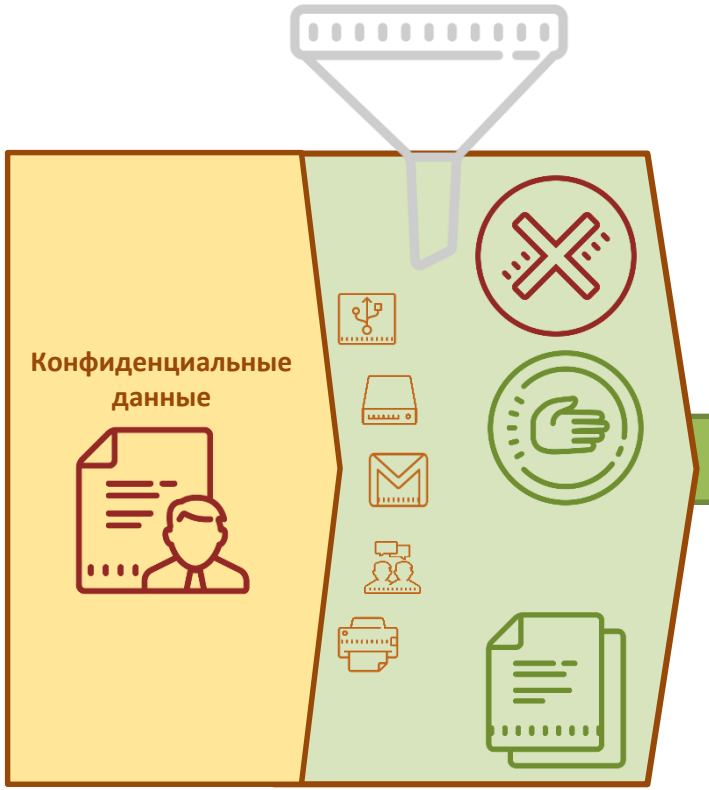
  ***ЛИБО***

- *Ваши возможности защиты информации сводятся к мониторингу каналов передачи данных… без возможности предотвратить утечку*

#если нашли утечку – значит не было утечки!
#проведение расследования

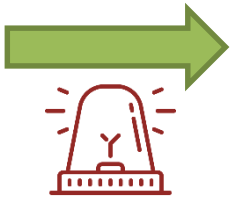
# ПОЛНОЦЕННЫЙ КОНТРОЛЬ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

***Анализ содержимого на каждом этапе – от хранения до архива***




- **Данные передаются после анализа содержимого с запретом передачи только данных ограниченного доступа:**
- **Нет данных ограниченного доступа – передача разрешена**
- **Возможность оперативной реакции по инциденту**

- **Создается копия переданных данных (как при блокировке, так и по факту разрешенной передачи данных)**



**Немедленное выявление инцидента в форме попытки утечки**
**Определение злоумышленника без ущерба для организации**

**Предотвращение утечки и дальнейшего бесконтрольного распространения данных**

**Выявление инцидента *(попытки передачи данных)*, Определение источника**

**Сбор и хранение доказательной базы для расследования попыток хищения данных**

**Детектирование конфиденциальных данных в архиве –**
**Для проведения расследований и создания доказательной базы**

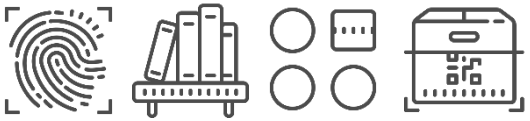
# DeviceLock® DLP

## ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ДАННЫХ

… все устройства и интерфейсы

…каналы сетевых коммуникаций

…с применением технологий контентной фильтрации



**в режиме реального времени, в любых сценариях!**

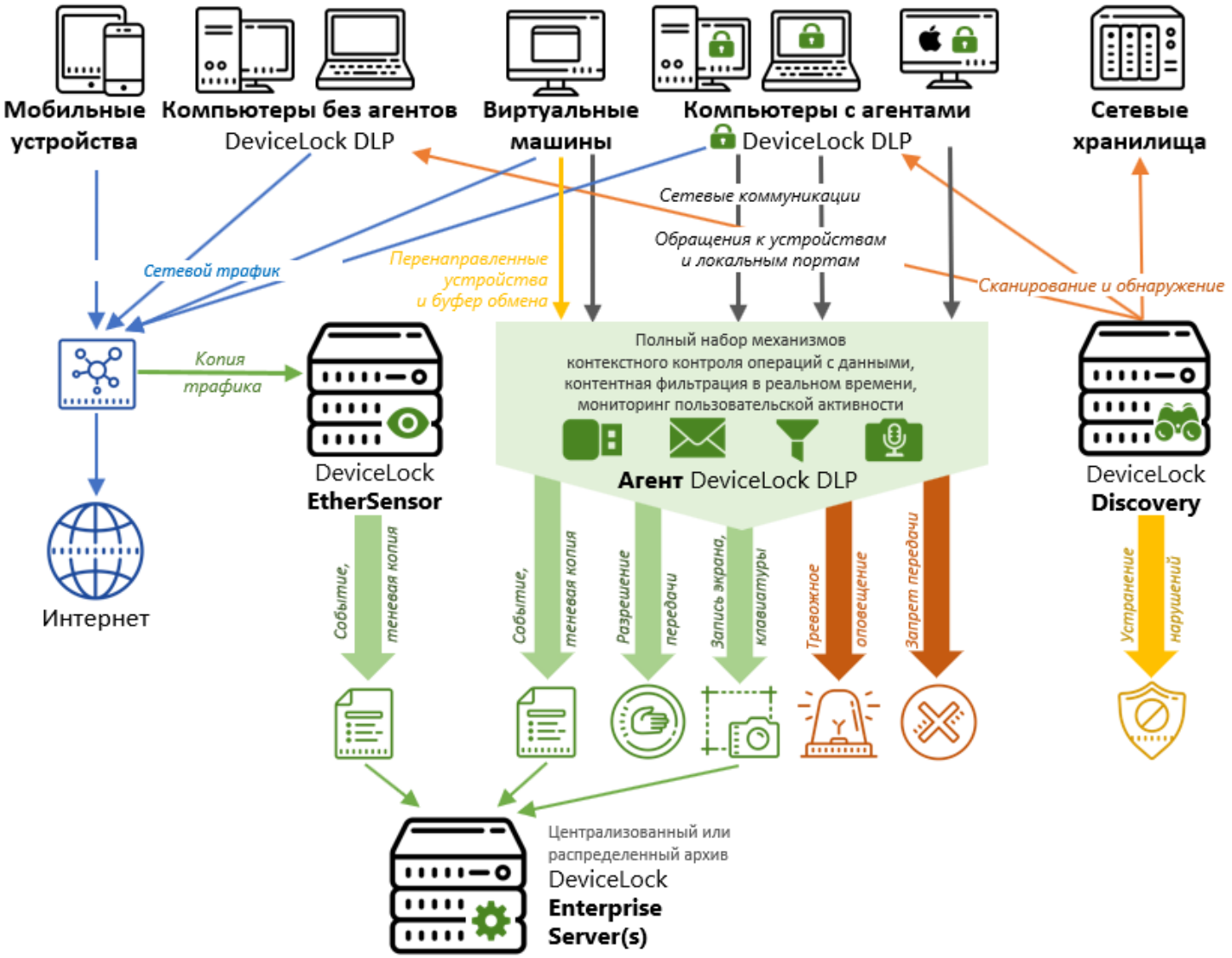
## ДЕТАЛЬНЫЙ МОНИТОРИНГ СОБЫТИЙ

**на уровне агента и на уровне сети**

## СКАНИРОВАНИЕ ХРАНИМЫХ ДАННЫХ

АНАЛИЗ АРХИВА: СЕРВЕР ПОЛНОТЕКСТОВОГО ПОИСКА

# DEVICELOCK DLP В ОДНОЙ КАРТИНКЕ



# КОНТЕНТНЫЙ АНАЛИЗ И ФИЛЬТРАЦИЯ В РЕАЛЬНОМ ВРЕМЕНИ

## Технологии контентной фильтрации

Поиск по ключевым словам и сочетания слов,
Использование шаблонов регулярных выражений.

Морфологический анализ заданных слов на русском, английском и других языках.

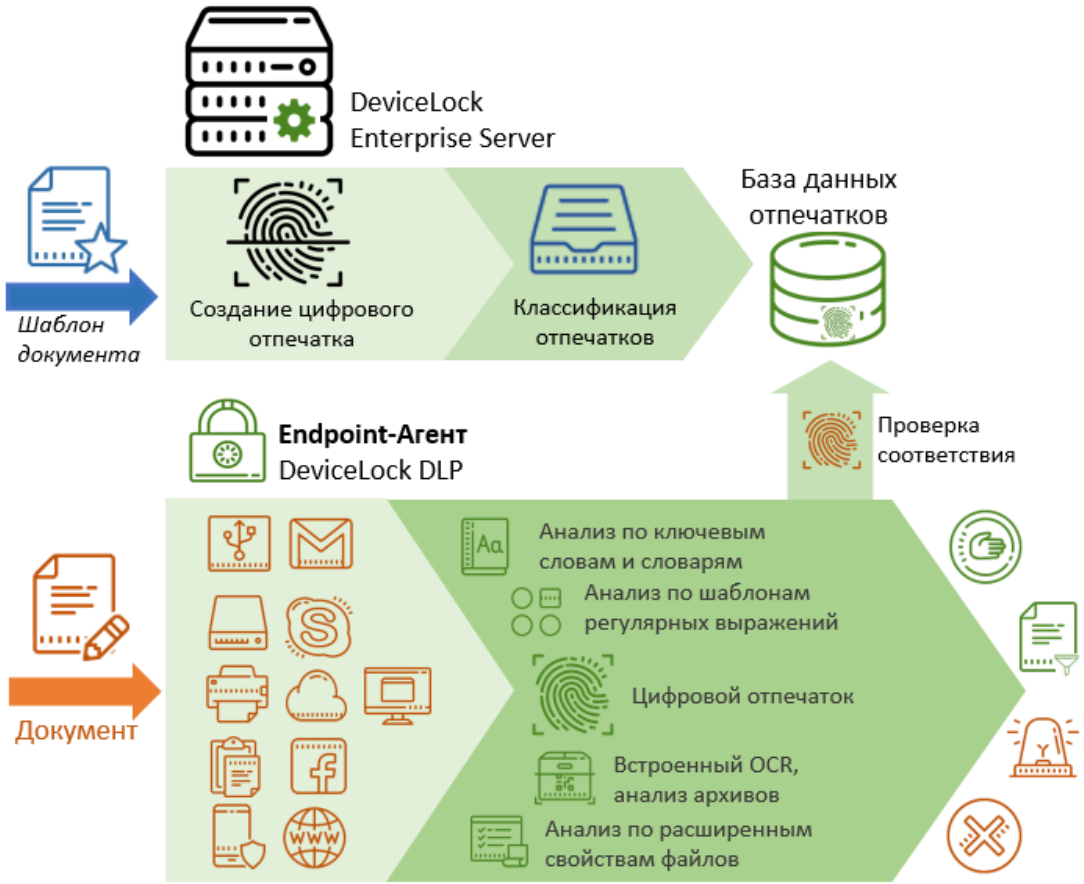
Встроенные промышленные и геоспецифичные терминологические словари.

Бинарно-сигнатурное определение
более 5 300 типов файлов.
Анализ по расширенным свойствам файлов.
Анализ архивов и контейнеров.

**Цифровые отпечатки**
(fingerprinting).

Встроенный модуль
оптического распознавания символов (OCR).

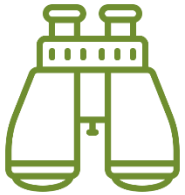
*Все используемые методы контентной фильтрации могут быть объединены в правила любого уровня сложности на базе различных численных и логических условий.*




## КАК ОБНАРУЖИВАТЬ ЗАЩИЩАЕМЫЕ ДАННЫЕ В РЕАЛЬНОМ ВРЕМЕНИ?

# НОВОЕ В DEVICELOCK DLP - В БЛИЖАЙШЕМ БУДУЩЕМ

«**Карточки пользователей**», включая выявление аномалий для пользователя по его типичной активности в прошлом и текущей.
Графики, связи и прочие UEBA-функции.



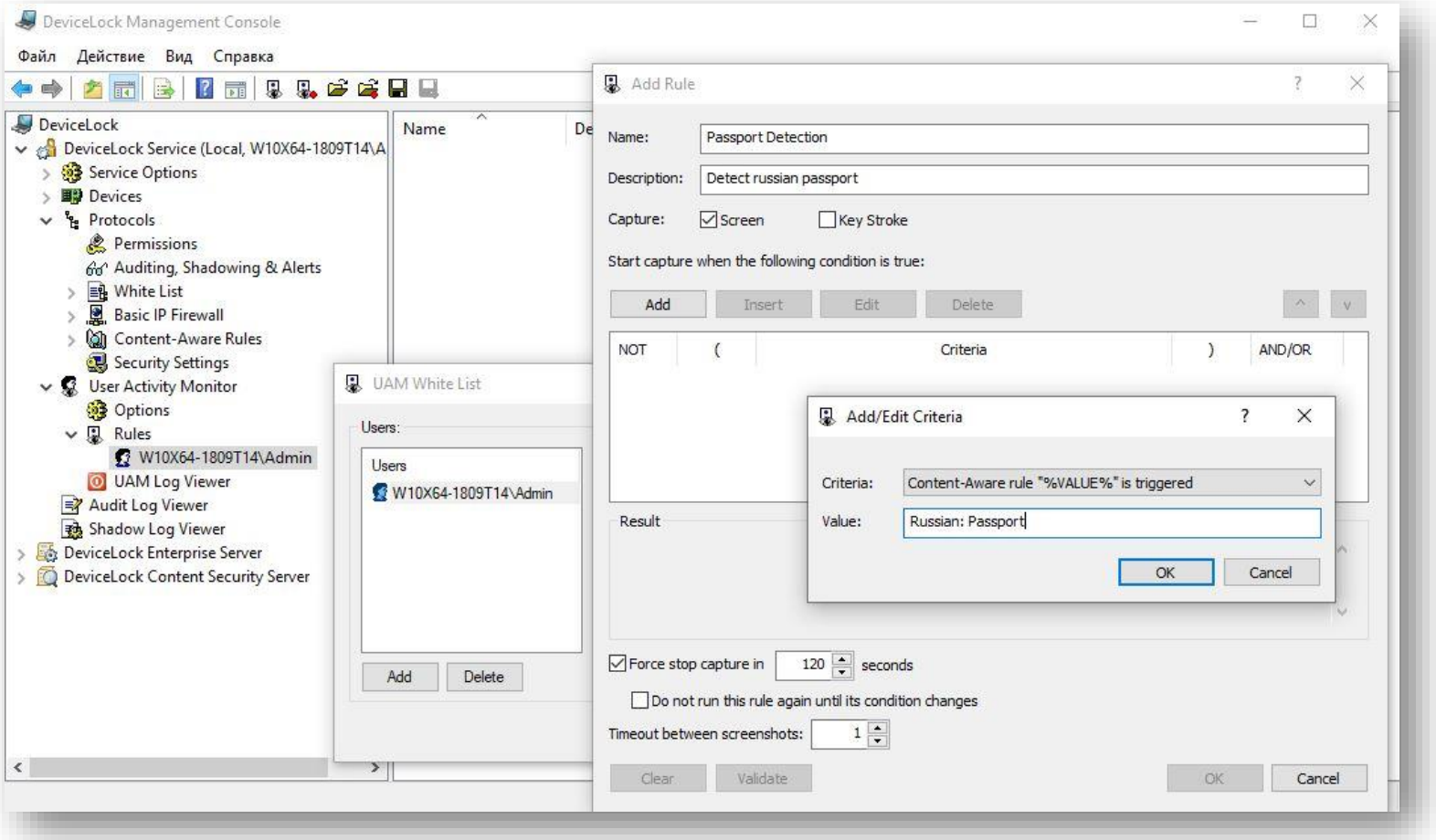
Развитие **DeviceLock Discovery** – сканирование и обнаружение данных на серверах SQL и noSQL, ElasticSearch баз с учетом накопленного нами опыта по нахождению незащищенных баз в Интернете...

Защита данных от фотографирования с экрана –
возможность идентификации пользователя по фотографии экрана.

Модуль **User Activity Monitoring**: снимки и запись экрана, кейлоггер
- **по триггерам**, включая правила анализа содержимого.

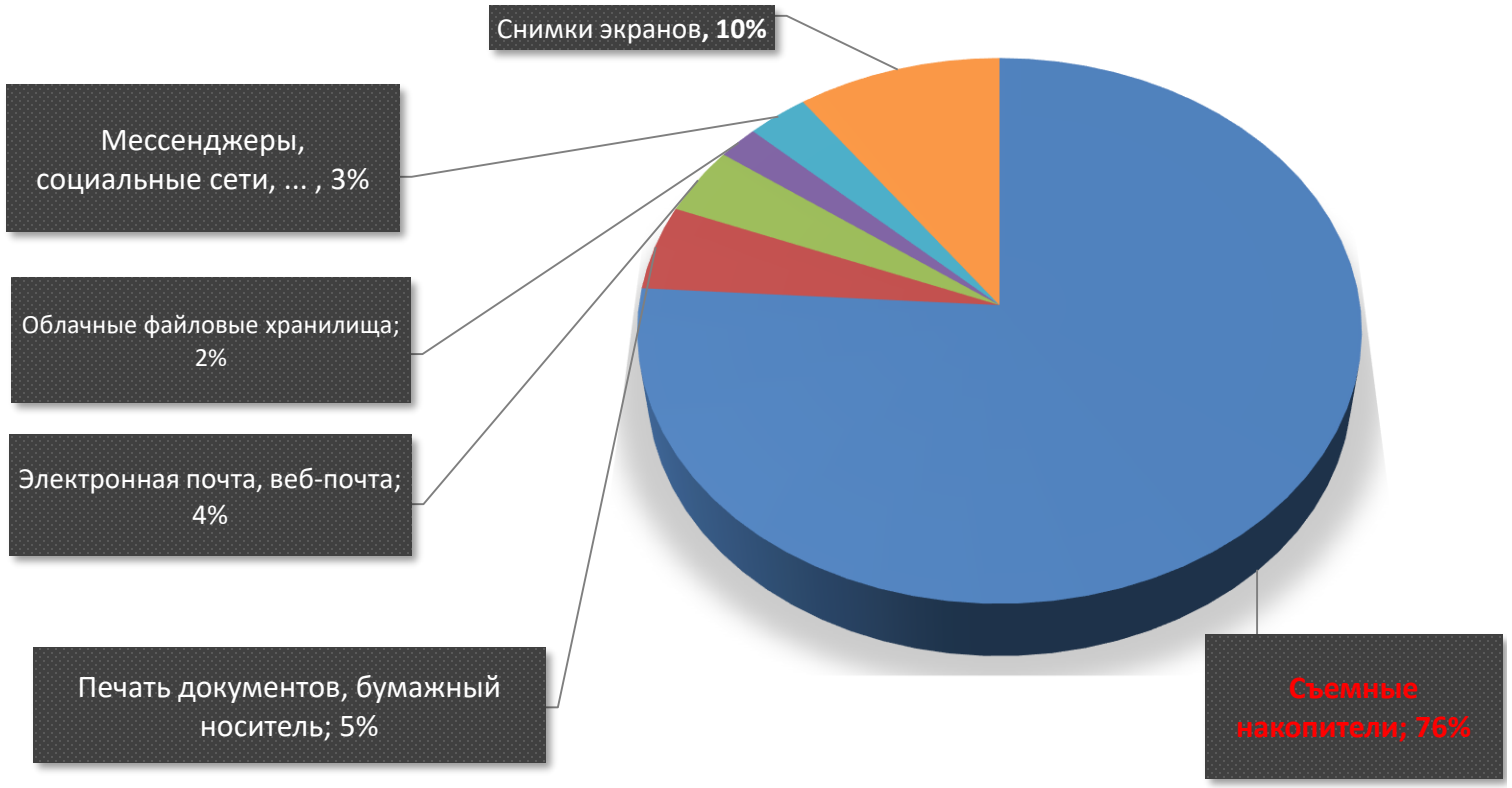
# МОНИТОРИНГ ПОЛЬЗОВАТЕЛЬСКОЙ АКТИВНОСТИ

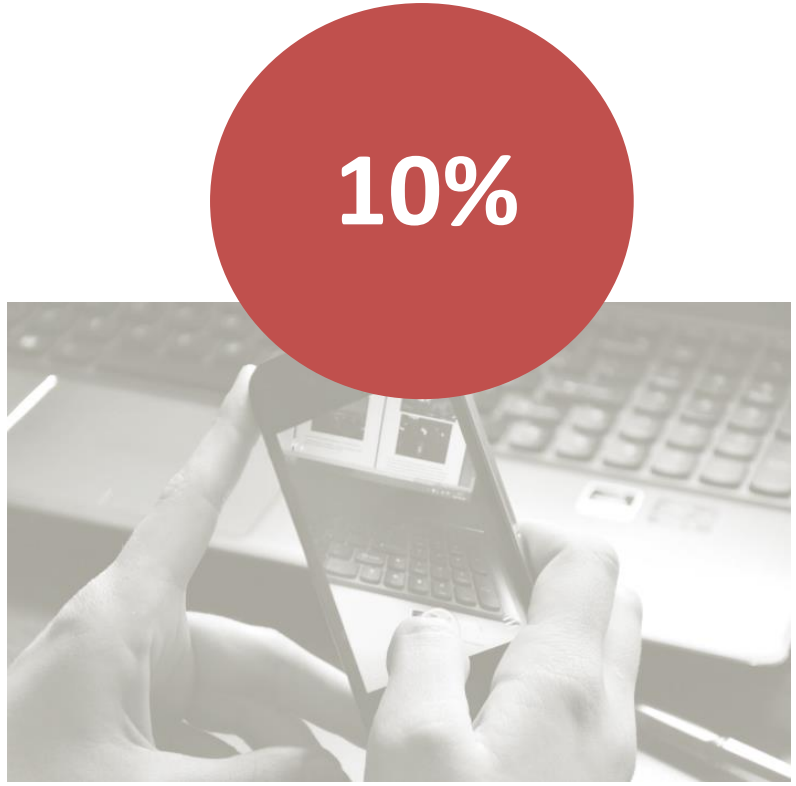
**В ближайшей версии DeviceLock DLP 9 –**
снимки и запись экрана, кейлоггер
- **по триггерам**, включая правила анализа содержимого!



# ВИДЫ УТЕЧКИ ДАННЫХ

**Утечки через фотографирование рабочих экранов** составляют 10% от инсайдерской утечки персональных данных (зарегистрированные инциденты)



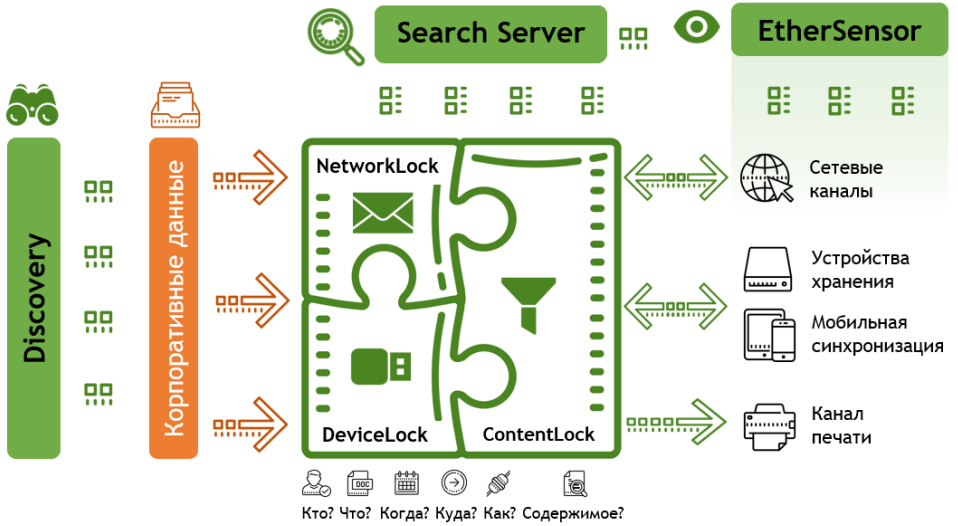




*Источник:* Исследование инсайдерских утечек данных, Смарт Лайн Инк
https://www.devicelock.com/ru/press/issledovanie-insajderskih-utechek-dannyh.html

# ЗАЩИТА ОТ ФОТОГРАФИРОВАНИЯ ЭКРАНОВ – СКОРО!

# СПАСИБО
# ЗА ВНИМАНИЕ!

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ




СЕРГЕЙ ВАХОНИН
SV@DEVICELOCK.COM

www.DeviceLock.com