АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

ESET NOD 32. НОВЫЕ ГОРИЗОНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Саблин Сергей

Менеджер по работе с корпоративными клиентами

ESET В РОССИИ И МИРЕ:
СВЕЖИЕ НОВОСТИ

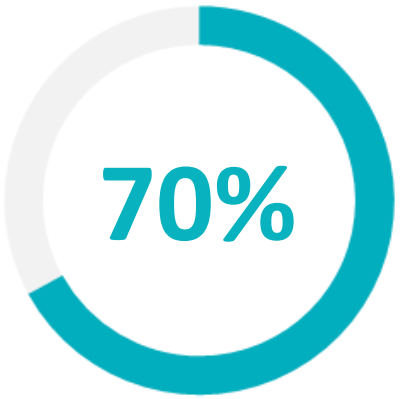
РАЗВИВАЕМ ТЕХНОЛОГИИ БЕЗОПАСНОСТИ УЖЕ 30 ЛЕТ

ПЕРВЫЙ ВЕНДОР, ЗАВОЕВАВШИЙ 100 НАГРАД VIRUS BULLETIN

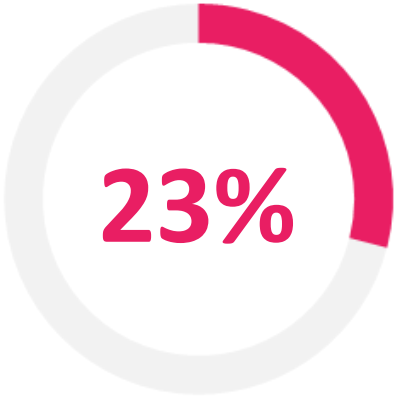
АНТИВИРУСНЫЙ ВЕНДОР №4 В КОРПОРАТИВНОМ СЕГМЕНТЕ В МИРЕ*

**Gartner Market Share: All Software Markets, Worldwide, 2015 report*

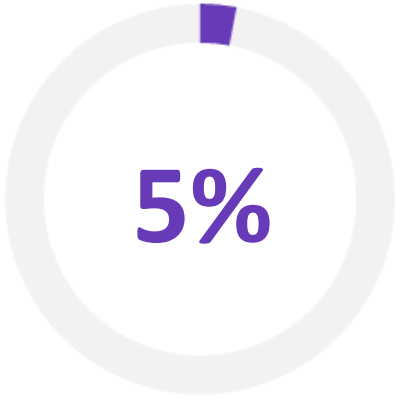
ДЕНЬГИ И ДАННЫЕ
МАГНИТ ДЛЯ КИБЕРПРЕСТУПНИКОВ



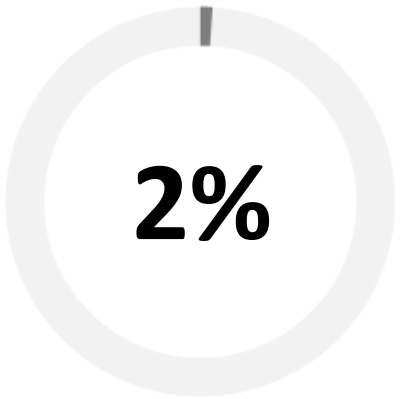
ФИНАНСОВАЯ ВЫГОДА



ПОЛУЧЕНИЕ ДАННЫХ



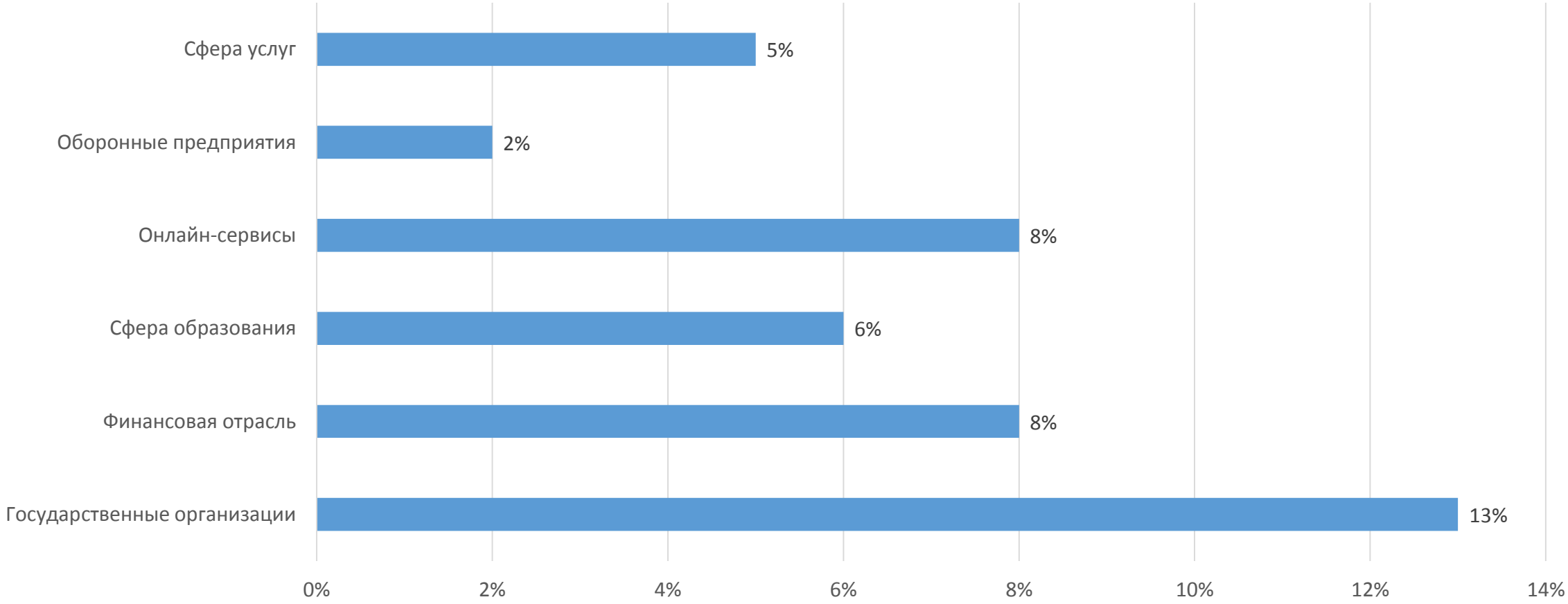
ХАКТИВИЗМ



КИБЕРВОЙНА

**По данным компании Positive Technologies*

КАТЕГОРИИ ЖЕРТВ КИБЕРАТАК



*По данным компании Positive Technologies

2017 ГОД:
ШИФРАТОРЫ ПЕРЕШЛИ В НАСТУПЛЕНИЕ

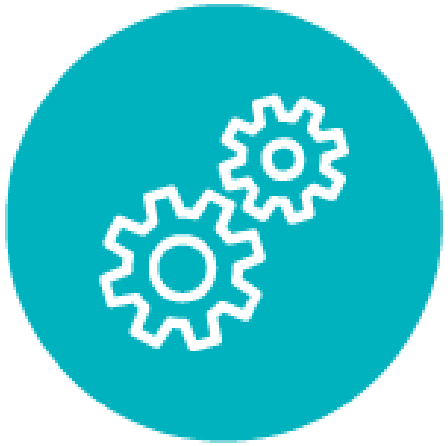
- **WannaCry**
  Уязвимость SMB Windows + эксплойт АНБ EternalBlue + бэкдор Double Pulsar

- **Petya/NotPetya**
  Компрометация сервера обновлений бухгалтерского ПО + EternalBlue + PsExec + WMI

- **Операция RTM**
  Подмена реквизитов исходящих платежей в транспортных файлах 1С

ПОПУЛЯРНЫЕ
ОБЪЕКТЫ АТАК 2017 ГОДА

ВЕБ-РЕСУРСЫ



ИНФРАСТРУКТУРА

БАНКОМАТЫ И POS-ТЕРМИНАЛЫ

**По данным компании Positive Technologies*

УГРОЗЫ 2018 ГОДА
АТАКА НА ЧЕЛОВЕЧЕСКИЕ РЕСУРСЫ

СКРЫТЫЙ МАЙНИНГ

IOT

ШИФРОВАЛЬЩИКИ

СЛАБОЕ ЗВЕНО

Человеческий фактор

*63% инцидентов информационной безопасности в компаниях связано с бывшими и действующими сотрудниками**

** PwC, 2016*

НЕКОМПЕТЕНТНОСТЬ

Нарушение правил информационной безопасности, утечка конфиденциальных данных, ошибки в работе в сети

ЗЛОНАМЕРЕННЫЕ ДЕЙСТВИЯ

Кража информации в пользу конкурентов, уничтожение ПО, переписки или документов, публикация конфиденциальных данных

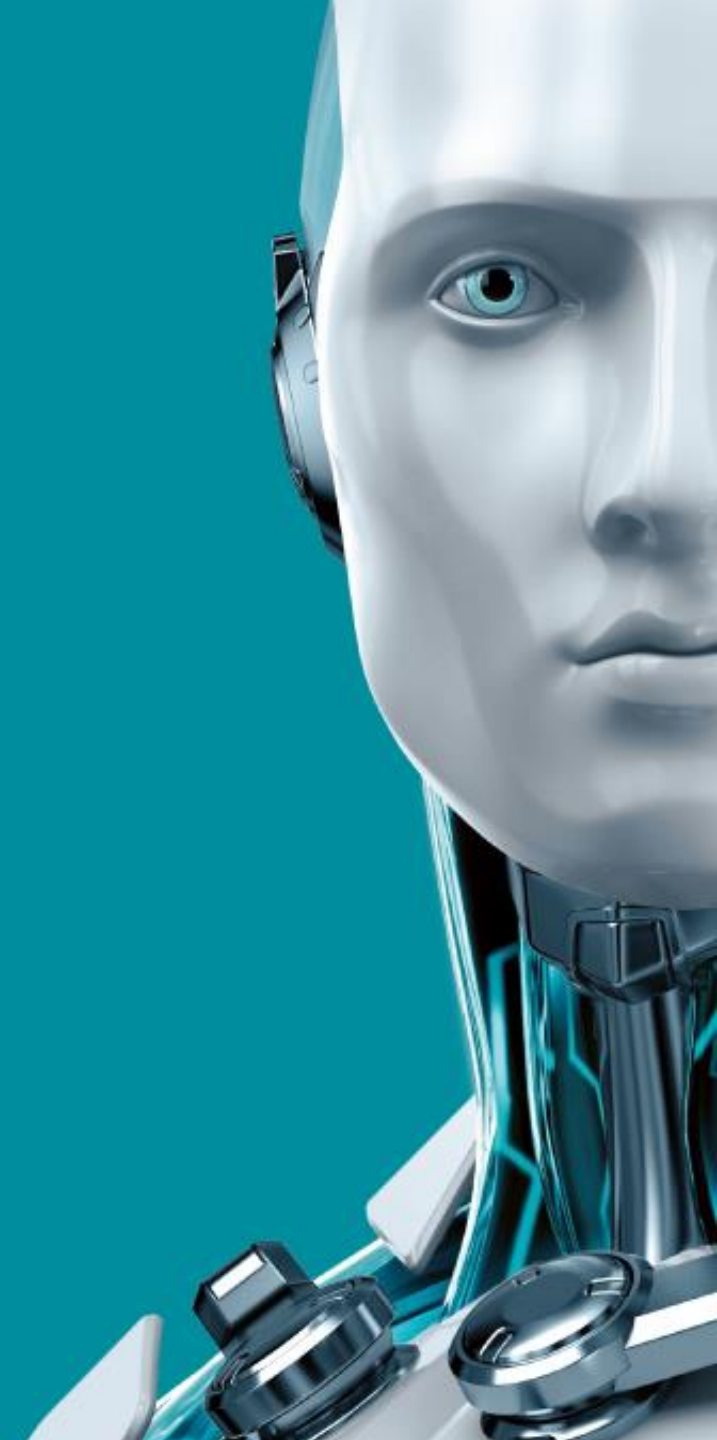
ПРОБЛЕМЫ ЭФФЕКТИВНОСТИ

Непродуктивное использование времени, ПО и компьютеров; падение производительности; поиск новой работы

ОФИСНЫЙ КОНТРОЛЬ И DLP

safetica

ESET TECHNOLOGY ALLIANCE



О КОМПАНИИ
SAFETICA TECHNOLOGIES

- Чешская компания, основана в 2009 году, команда 70+
- Клиенты в более чем 50 странах
- Продукт входит в TOP 5 DLP - в рейтинге журнала SC Magazine
- DLP решение для любого типа бизнеса - по версии Gartner
- Входит в ESET Technology Alliance с 2016 года

УТЕЧКА ДАННЫХ
ПОЧЕМУ ЭТО ПРОИСХОДИТ?

- **Создание собственной компании** на базе уникальных данных
- Продажа информации конкурентам
- **Использование данных** для устройства на новую работу
- Чтобы просто навредить компании или людям в ней
- «Я создавал это, значит **это мои данные**!» (Нет, это не так...)
- Другие причины, которые кажутся сотрудникам логичными

УТЕЧКА ДАННЫХ
КАК ЭТО ПРОИСХОДИТ?

- USB-флешки / телефоны / внешние жесткие диски
- DropBox / и другие облачные хранилища
- Электронная почта
- Различные приложения
- Мессенджеры
- Bluetooth
- …

УТЕЧКА ДАННЫХ
ЭТО РЕАЛЬНОСТЬ!

Человеческий фактор

*63% инцидентов информационной безопасности в компаниях связано с бывшими и действующими сотрудниками**

** PricewaterhouseCoopers, 2016*

- **67% сотрудников распечатывают**
  любые корпоративные документы
- **47% копируют документы**
  или делают скриншоты
- **73% подключают флэшки**
  и другие внешние носители к рабочим ПК
- **47% пересылают рабочие файлы**
  на личную почту
- **44% устанавливают приложения**
  на компьютер в корпоративной сети
- **56% открывают любые сайты**
  без ограничений

ESET Russia, 2017, 750 респондентов

УТЕЧКА ДАННЫХ
КАК ЗАЩИТИТЬСЯ?

ОФИСНЫЙ КОНТРОЛЬ И DLP SAFETICA

ПРИНЦИПИАЛЬНЫЕ РАЗЛИЧИЯ

СЕТЕВЫЕ

АППАРАТНЫЙ ИЛИ ВИРТУАЛЬНЫЙ ШЛЮЗ

АГЕНТНЫЕ

АГЕНТЫ DLP НА КОНЕЧНЫХ ТОЧКАХ

КОНТЕНТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ НА ОСНОВЕ АНАЛИЗА СОДЕРЖИМОГО

КОНТЕКСТНЫЙ ФИЛЬТР

ПРИНЯТИЕ РЕШЕНИЯ ПО ФОРМАЛЬНЫМ ПРИЗНАКАМ

АРХИТЕКТУРА РЕШЕНИЯ
SAFETICA

В четыре шага

- **Анализ – 1 неделя**
- **Установка – 2 недели**
- **Обучение (входит в остальные этапы)**
- **Настройка – 4 недели**

КОМПЛЕКСНОЕ РЕШЕНИЕ
SAFETICA

AUDITOR

РЕГИСТРАЦИЯ АКТИВНОСТИ СОТРУДНИКОВ

SUPERVISOR

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ БИЗНЕС-ПРОЦЕССОВ КОМПАНИИ

DLP

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ КОМПАНИИ

ОФИСНЫЙ КОНТРОЛЬ
(МОДУЛЬ AUDITOR)

ПРЕДСТАВЛЕНИЕ О ТОМ, ЧТО ПРОИСХОДИТ В КОМПАНИИ

СОБЛЮДЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ

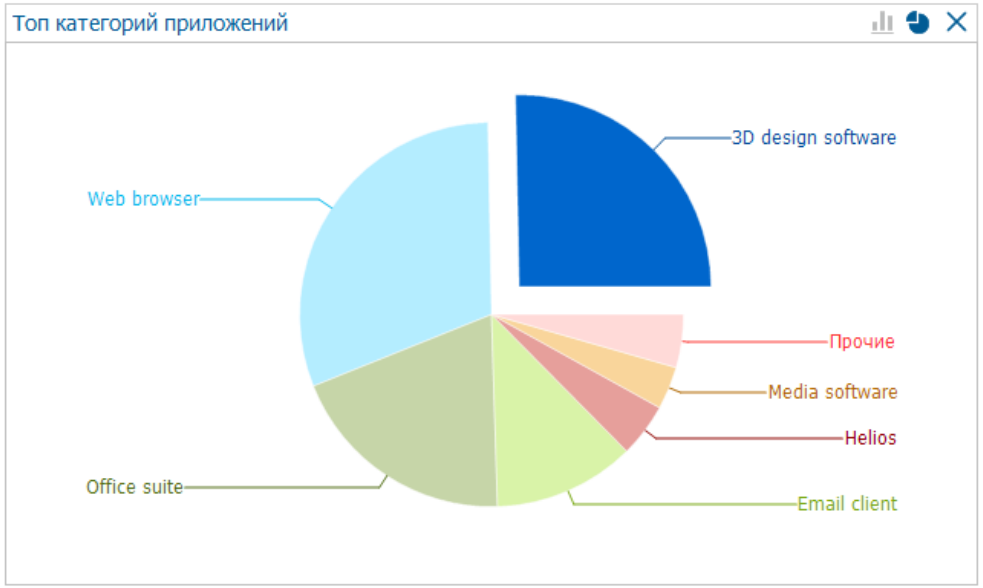
СРАВНЕНИЕ РАБОТЫ СОТРУДНИКОВ

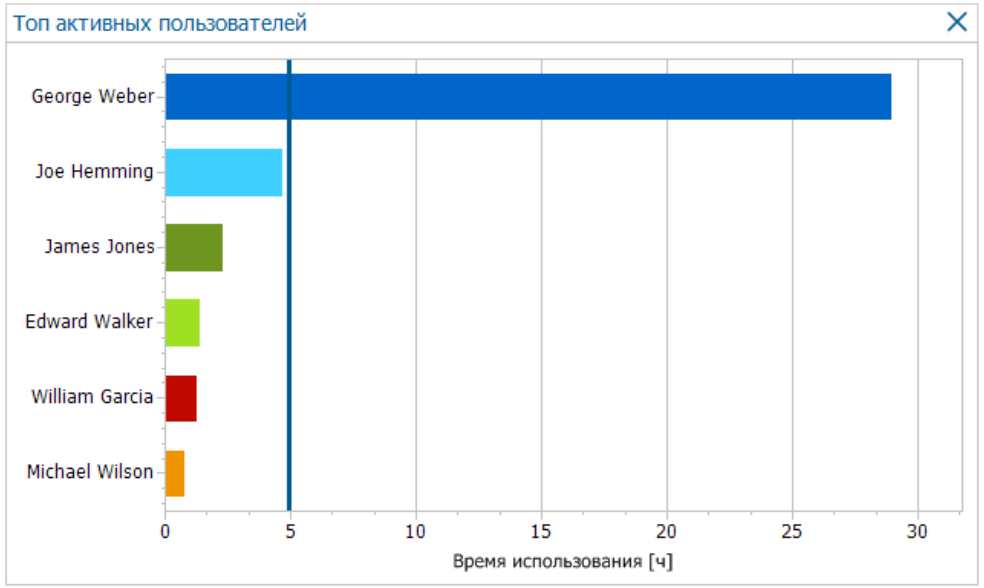
АУДИТ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ КОМПАНИИ

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ПО

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

ГРАФИКИ





Время работы приложе...
Активное время работы ...
Наиболее активные при...

ЗАПИСИ

Перетащите под тот текст столбцы, по которым вы хотите сгруппировать

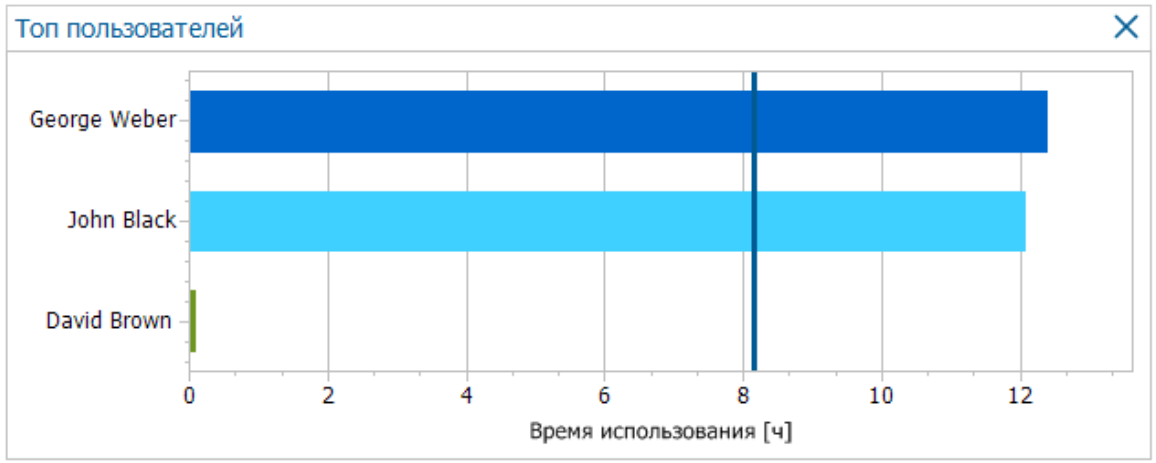
Категория приложен...

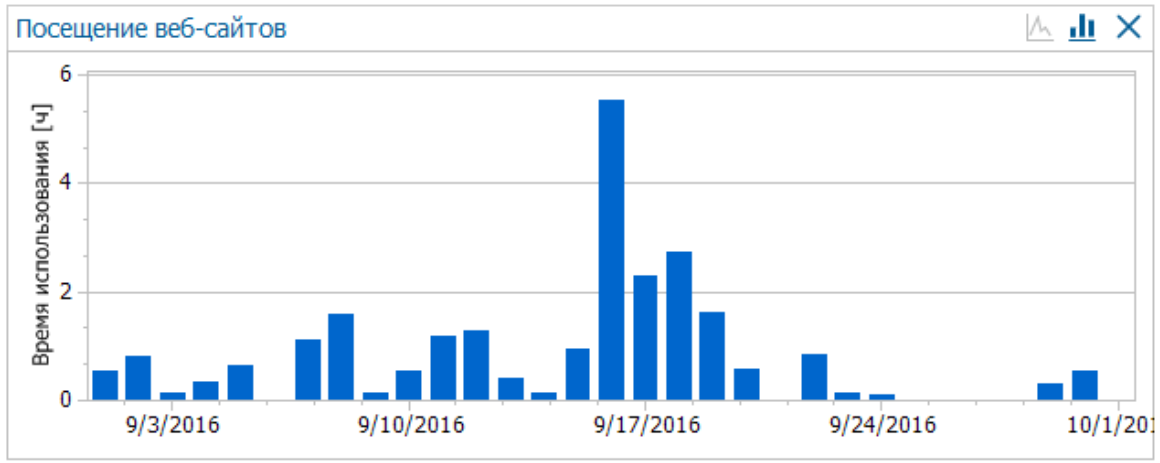
Приложение

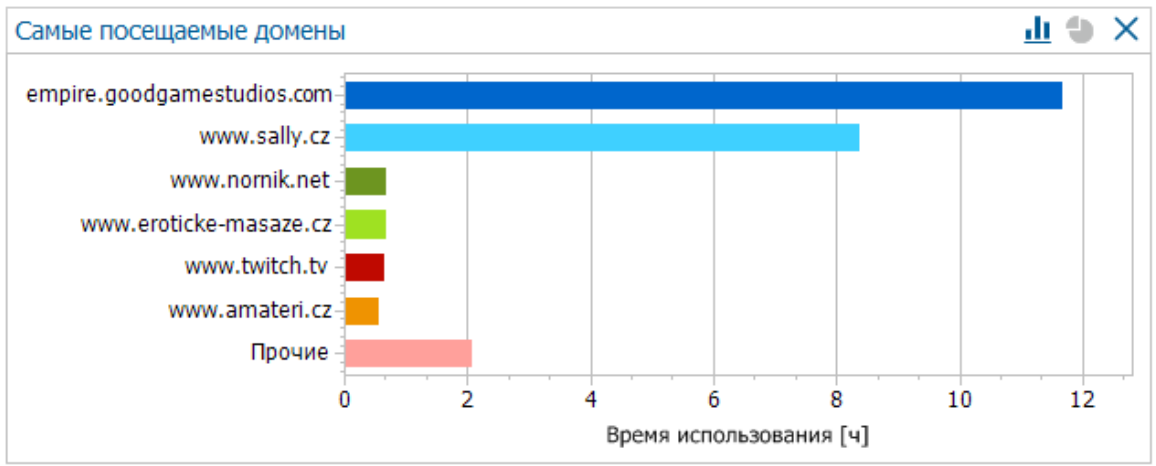
Упорядочить

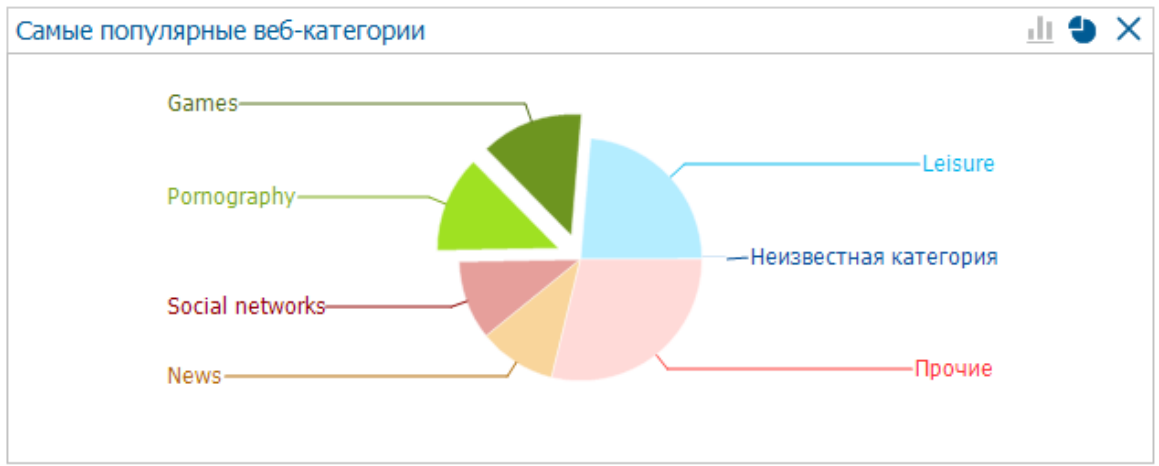
Имя пользователя	ПК	Продолжительность	Путь приложения	Дата и время	С - по
Приложение: AutoCAD 2015					33 h 30 min 36 s активного времени
Приложение: SolidWorks (solidworks.exe)					5 h 36 min 20 s активного времени

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)









ОФИСНЫЙ КОНТРОЛЬ
(МОДУЛЬ SUPERVISOR)

› **Web-контроль**

› **Контроль приложений**

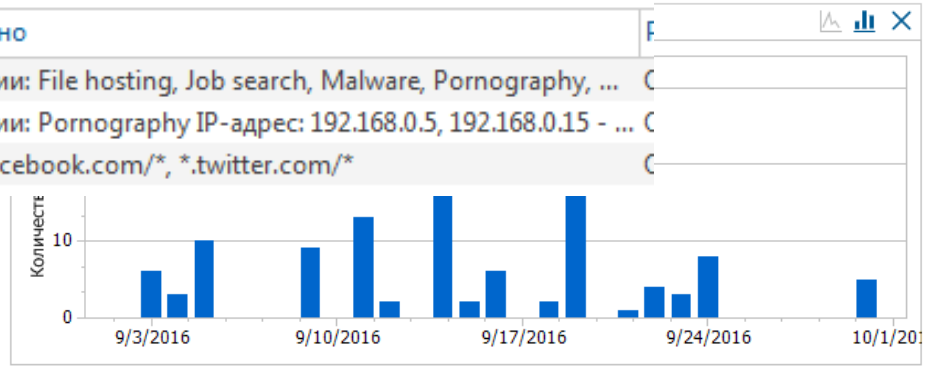
› **Контроль печати**

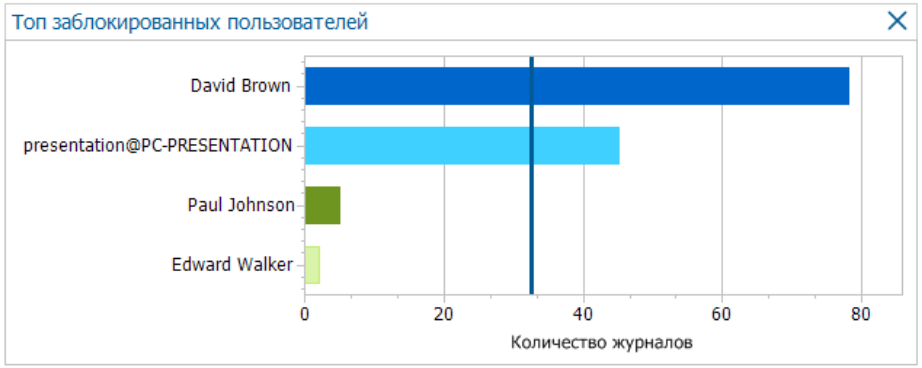
ОФИСНЫЙ КОНТРОЛЬ (WEB-КОНТРОЛЬ)

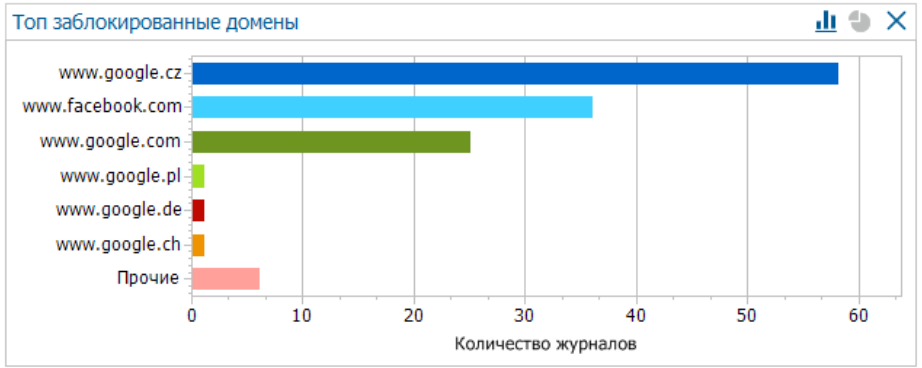
Действие по умолчанию: Разрешено

Добавить правило

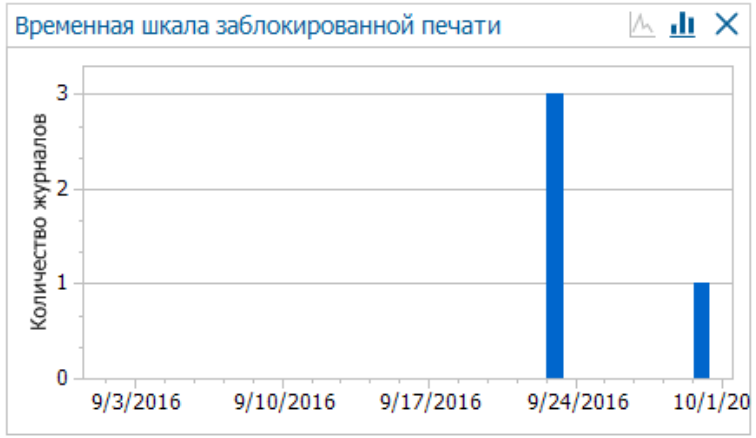
Имя	Подробно	Р
Блокировка по категориям	Категории: File hosting, Job search, Malware, Pornography, ...	С
Блокировка по IP	Категории: Pornography IP-адрес: 192.168.0.5, 192.168.0.15 - ...	С
Блокировка по домену	URL: *.facebook.com/*, *.twitter.com/*	С

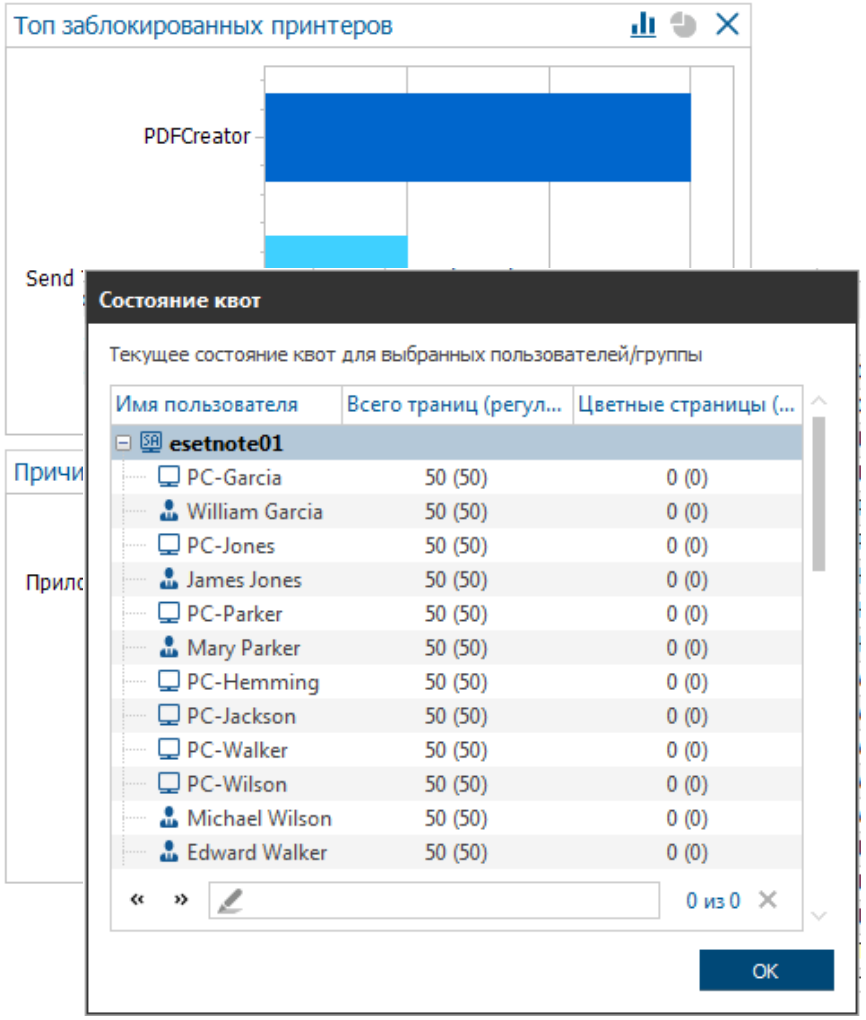


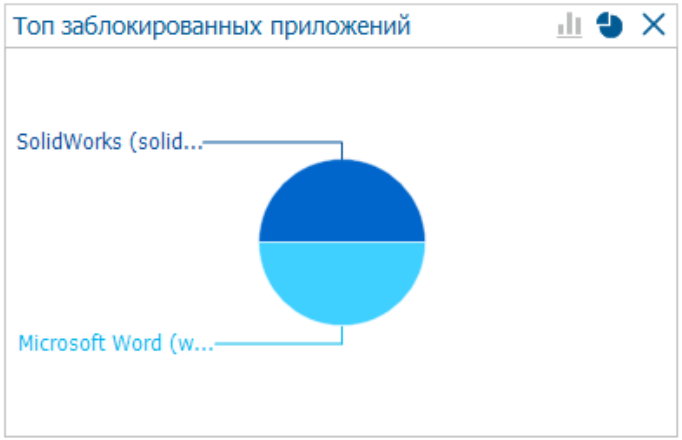


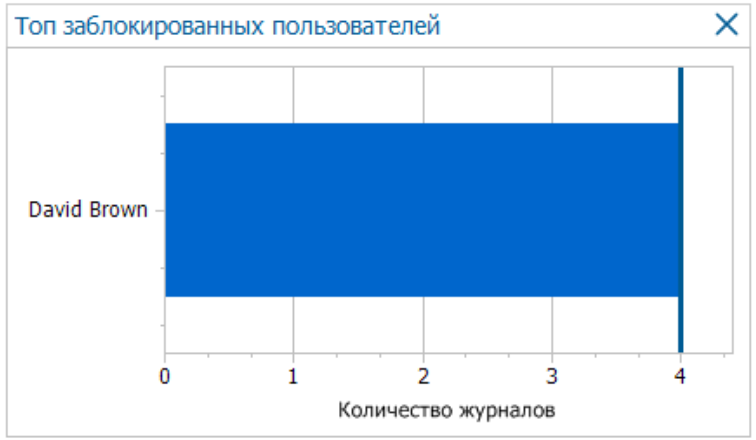


ОФИСНЫЙ КОНТРОЛЬ
(КОНТРОЛЬ ПЕЧАТИ)

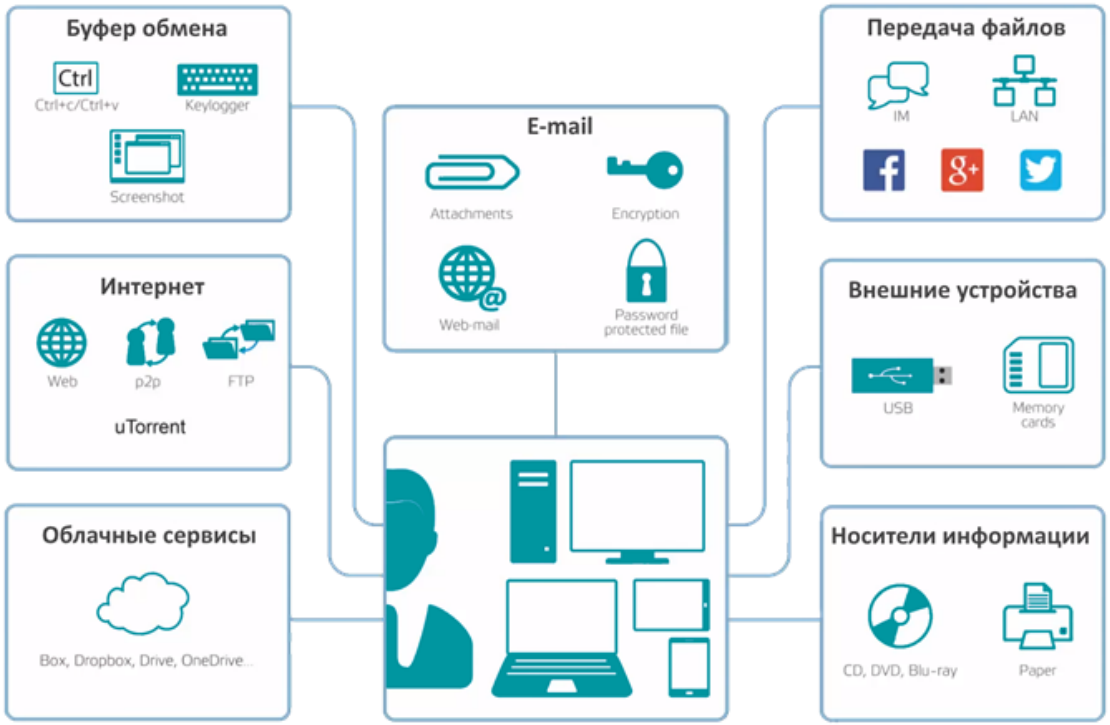


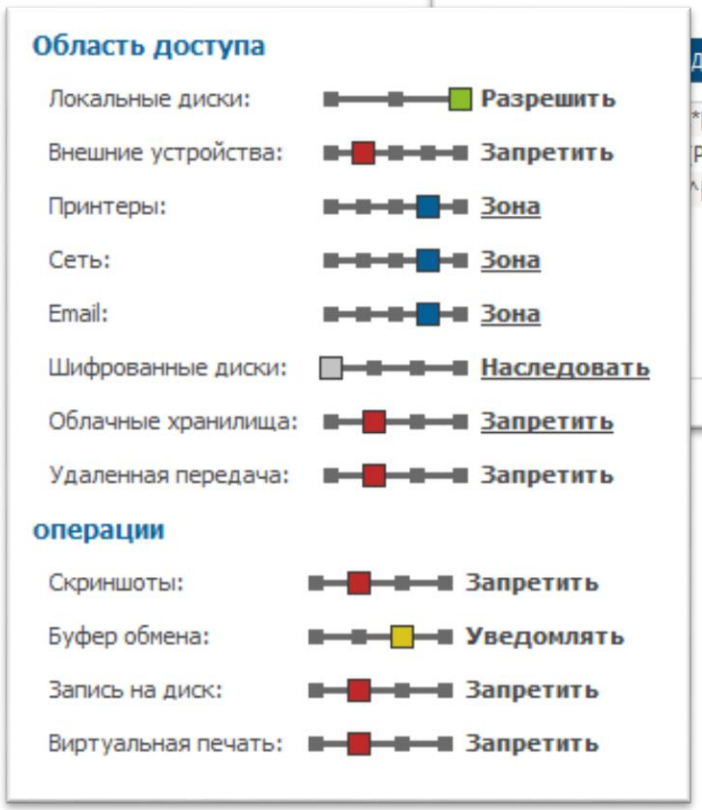


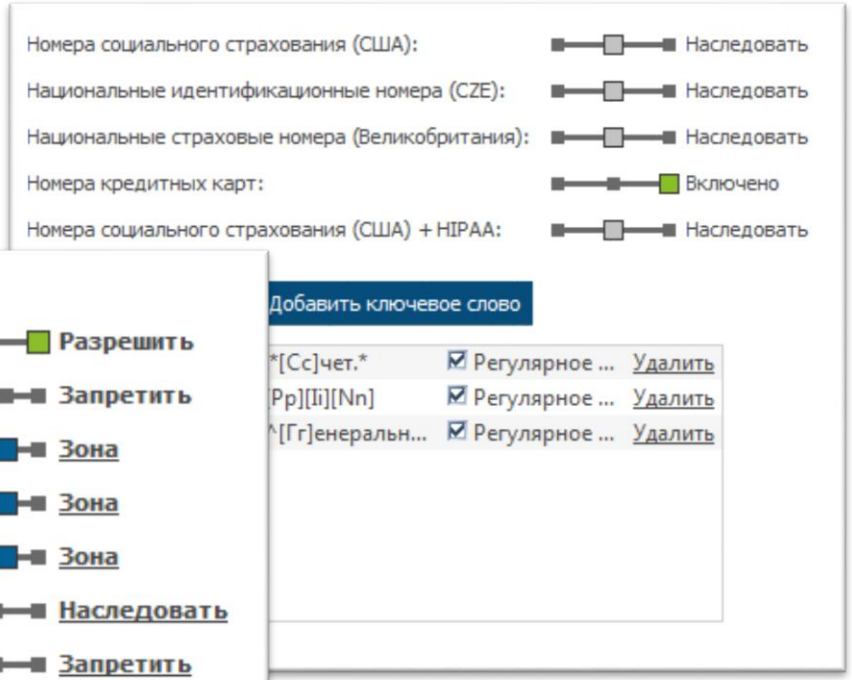




ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)







ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)

› ПРАВИЛА ПРИЛОЖЕНИЙ

Определение приложений и категорий приложений, в которых выходные файлы должны быть помечены выбранной категорией данных

› ВЕБ ПРАВИЛА

Веб-правила могут использоваться для установки меток на файлы, загруженные с определенных доменов или доменов из определенной категории

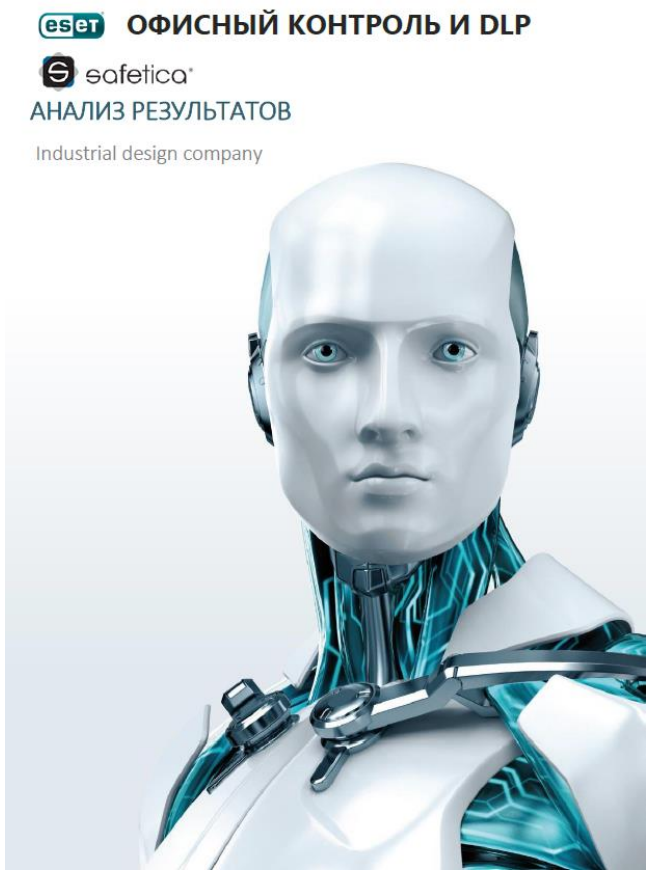
› ПРАВИЛА ПО ПУТИ

Все файлы, помещенные в определенные папки, будут автоматически получать необходимую метку.

› КОНТЕНТНЫЕ ПРАВИЛА

Все файлы, содержащие определенный контент, будут автоматически получать необходимую метку.

РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ



✓ ПРОИЗВОДИТЕЛЬНОСТЬ:

- *Использование приложений*
- *Посещенные сайты*
- *Поиск работы*
- *Общее время непродуктивной деятельности*

✓ РАБОТА С ДАННЫМИ:

- *Утечка данных из компании*
- *Нежелательные действия с данными*

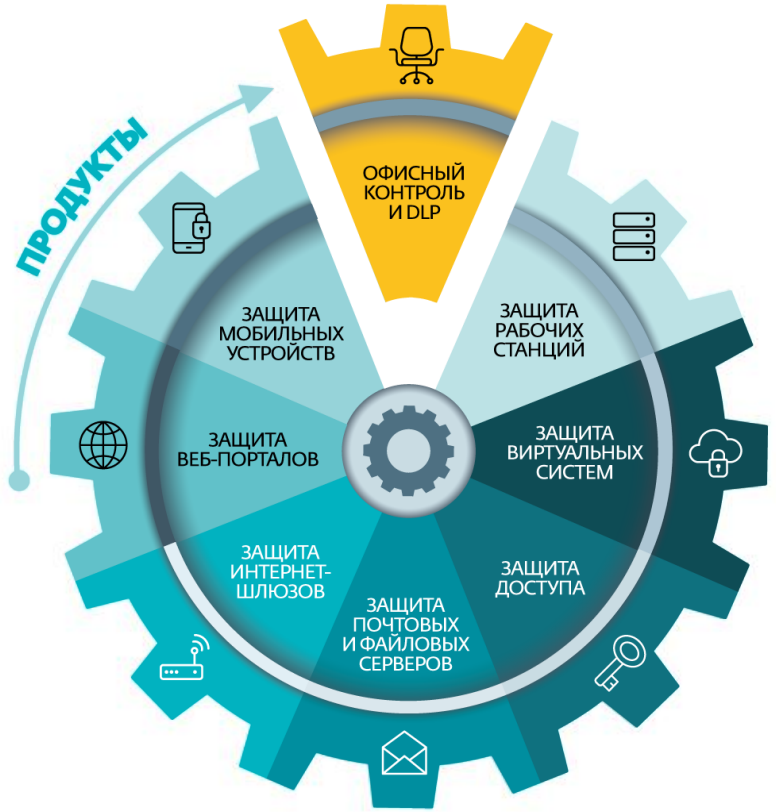
✓ ИСПОЛЬЗОВАНИЕ IT-РЕСУРСОВ:

- *Использование рабочих станций*
- *Печать*
- *Дорогие лицензии*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
КОМПЛЕКСНЫЙ ПОДХОД

У компании есть:

- Антивирус
- Файервол
- Антиспам
- Защита от сетевых атак
- …



Офисный контроль и DLP – это недостающий уровень безопасности!

ДЛЯ ЛЮБОЙ КОМПАНИИ

Офисный контроль и DLP Safetica

Закрывает распространенные проблемы, связанные с человеческим фактором в компании любого размера

✓ КОМПЛЕКСНОЕ РЕШЕНИЕ

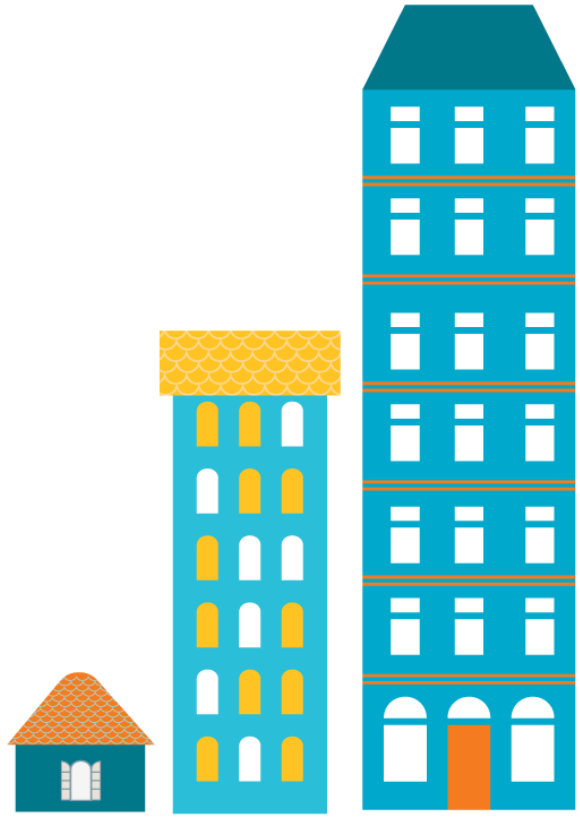
- *Аудит активности пользователей*
- *Ограничение деятельности сотрудников*
- *Предотвращение утечки данных*

✓ ЛЕГКОЕ ВНЕДРЕНИЕ

- *Независимость от структуры и языка документов*
- *Поддержка любых типов файлов*
- *Не требуется составления словарей*

✓ БЕЗ ДОПОЛНИТЕЛЬНЫХ ВЛОЖЕНИЙ

- *Стоимость проекта = стоимость лицензии*



АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Спасибо! Вопросы?