ОФИСНЫЙ КОНТРОЛЬ И DLP

safetica

Иван Иванов, *технический консультант*

ESET TECHNOLOGY ALLIANCE

О КОМПАНИИ
SAFETICA TECHNOLOGIES

- Чешская компания, основана в 2009 году, команда 70+
- Клиенты в более чем 95 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

НИКАКИХ СКРЫТЫХ РАСХОДОВ

Сервер

Процессор: четырёхядерный 2,4GHz
Оперативная память: от 2GB
Жесткий диск: от 3GB свободного места (от 100GB с БД)
ОС: MS Windows Server 2008 и выше, 32&64-bit

База данных (MS SQL)

MS SQL 2008 R2 и выше, рекомендуется MS SQL 2012 и выше
MS SQL 2016 Express включена в установочный пакет Safetica

ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

ПРЕДСТАВЛЕНИЕ О ТОМ, ЧТО ПРОИСХОДИТ В КОМПАНИИ

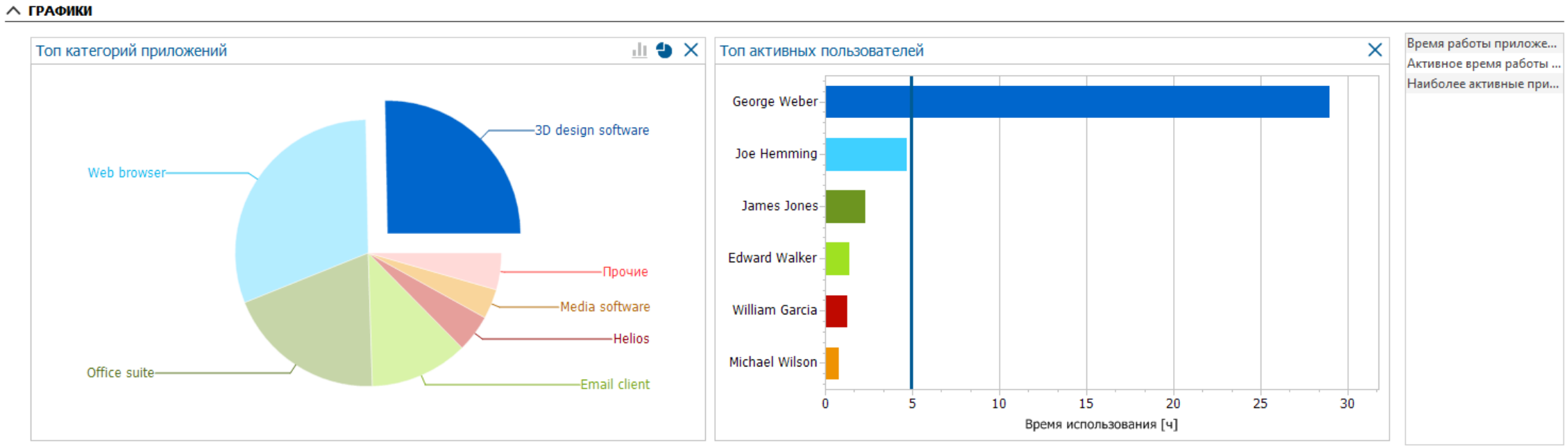
СОБЛЮДЕНИЕ ПОЛИТИК БЕЗОПАСНОСТИ

СРАВНЕНИЕ РАБОТЫ СОТРУДНИКОВ

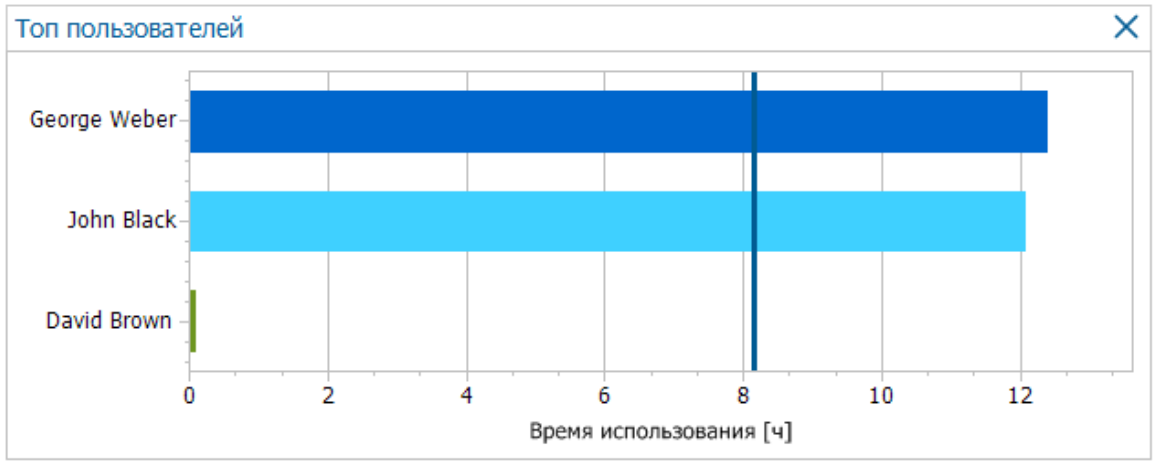
АУДИТ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ КОМПАНИИ

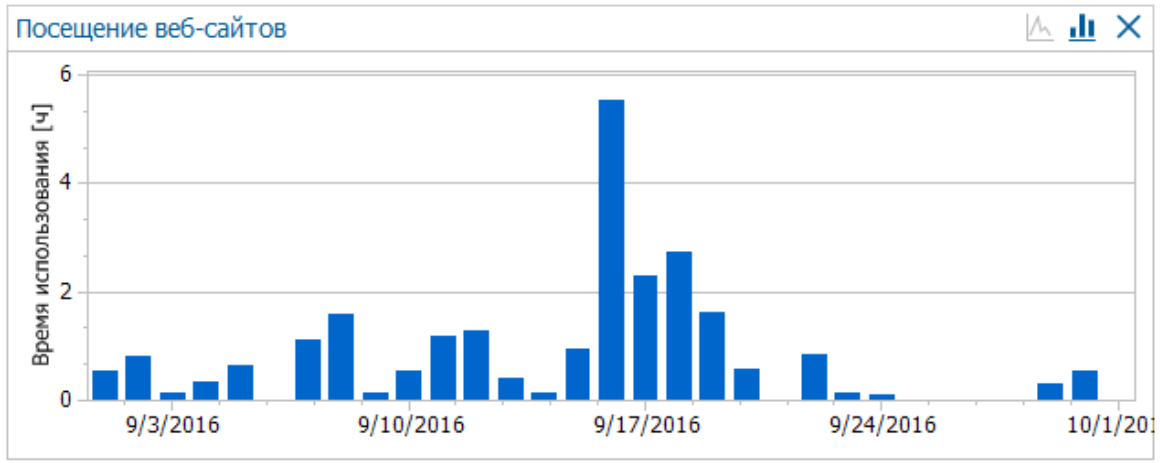
ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ ПО

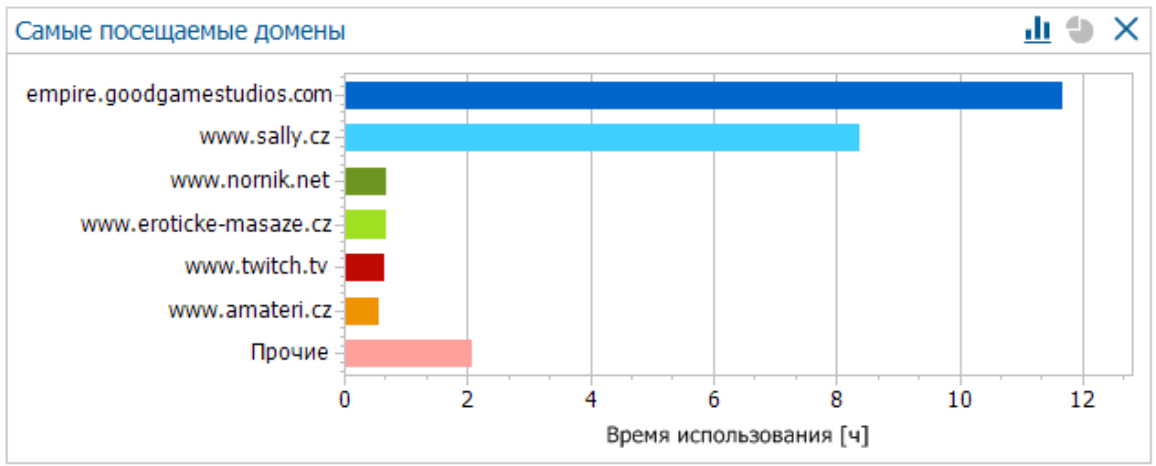
ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

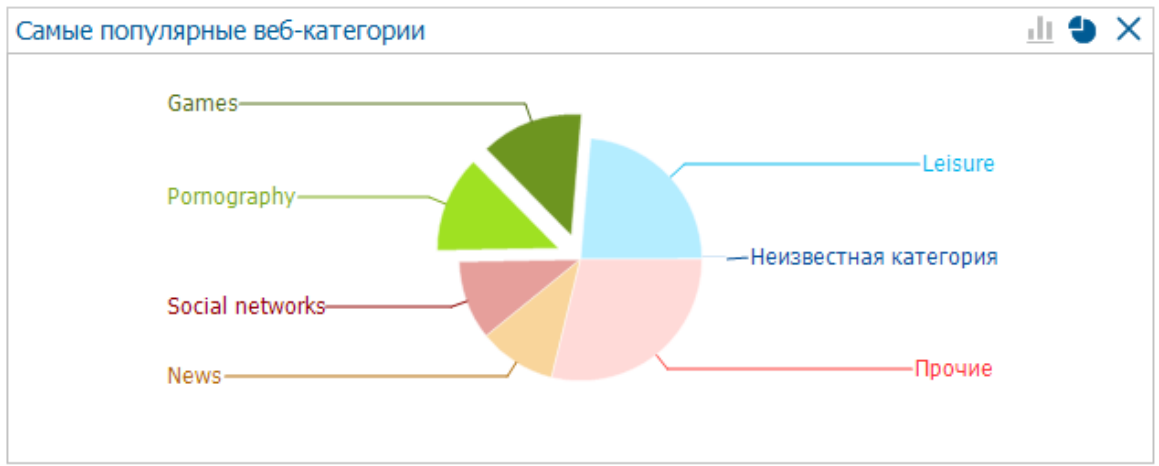


ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

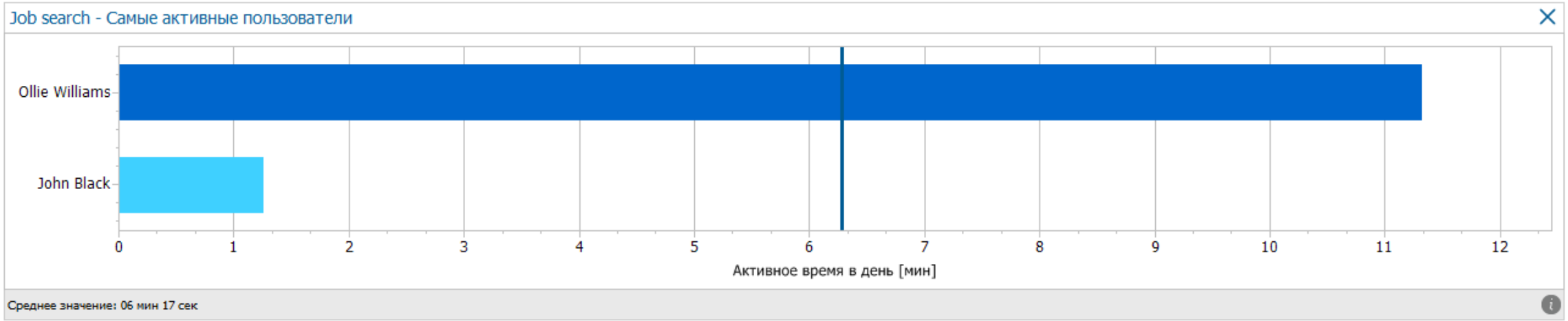


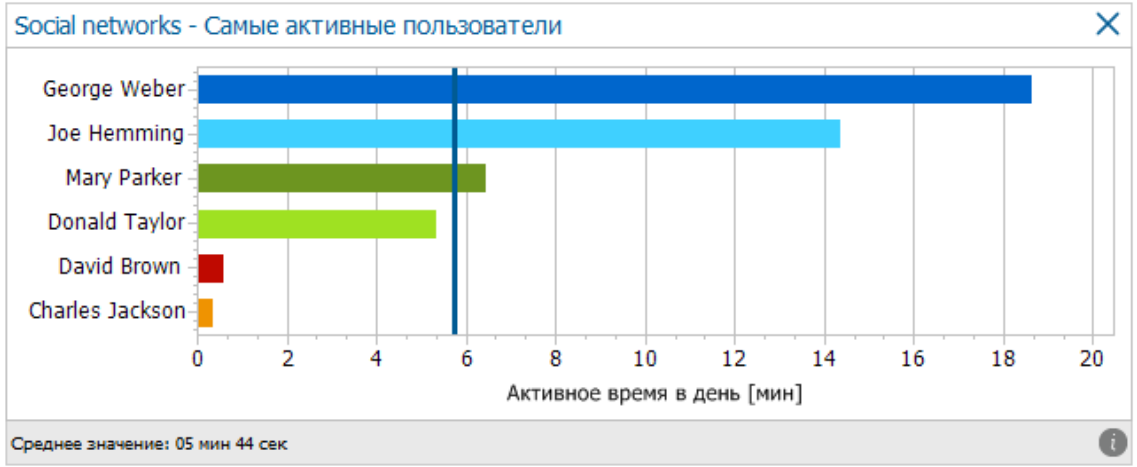


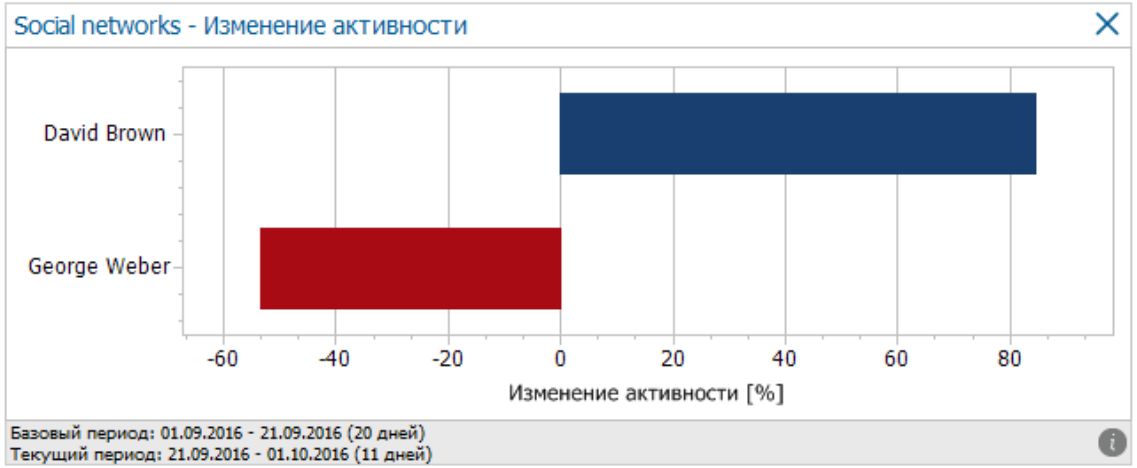




ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)







ОФИСНЫЙ КОНТРОЛЬ (МОДУЛЬ AUDITOR)

- **Дополнительная мотивация сотрудников**

  по итогам оценки эффективности труда

- **Обоснование для расширения штата**

  на основе объективной информации о загруженности

- **Снижение нагрузки на сотрудника/отдел**

  и справедливое распределение обязанностей внутри рабочей группы

- **Ваш вариант**

ОФИСНЫЙ КОНТРОЛЬ
(МОДУЛЬ SUPERVISOR)

› **Web-контроль**

› **Контроль приложений**

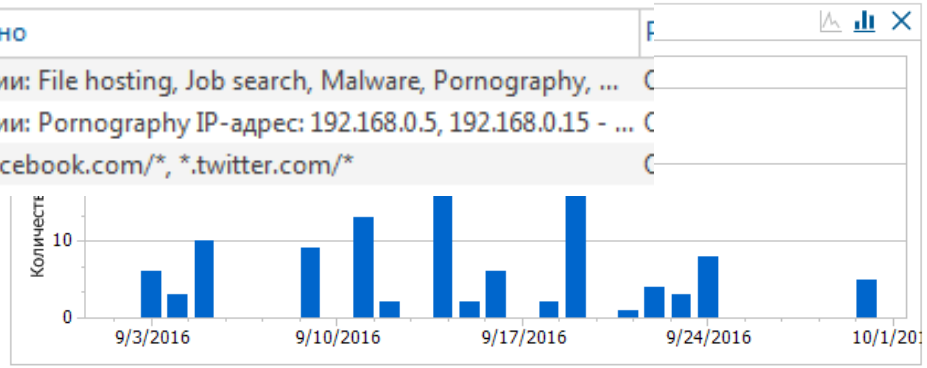
› **Контроль печати**

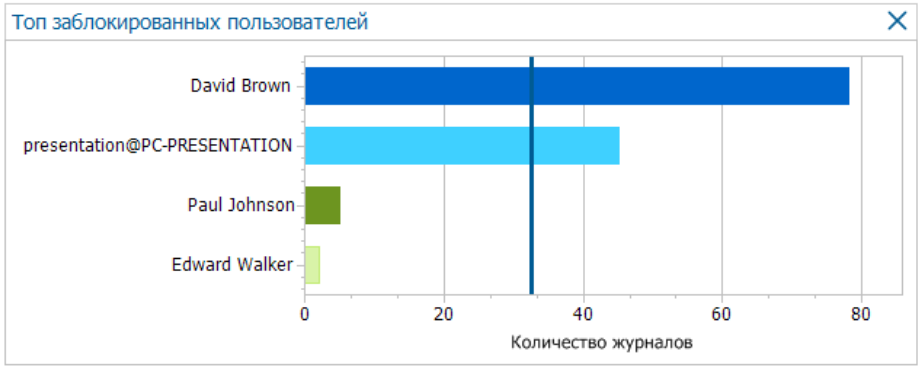
ОФИСНЫЙ КОНТРОЛЬ (WEB-КОНТРОЛЬ)

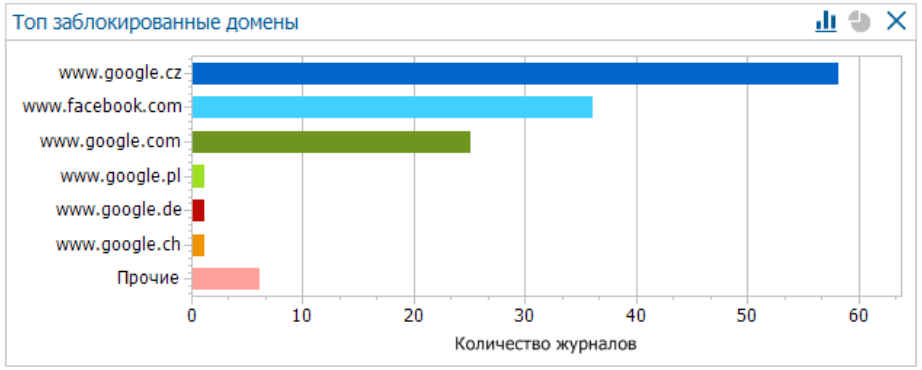
Действие по умолчанию: Разрешено

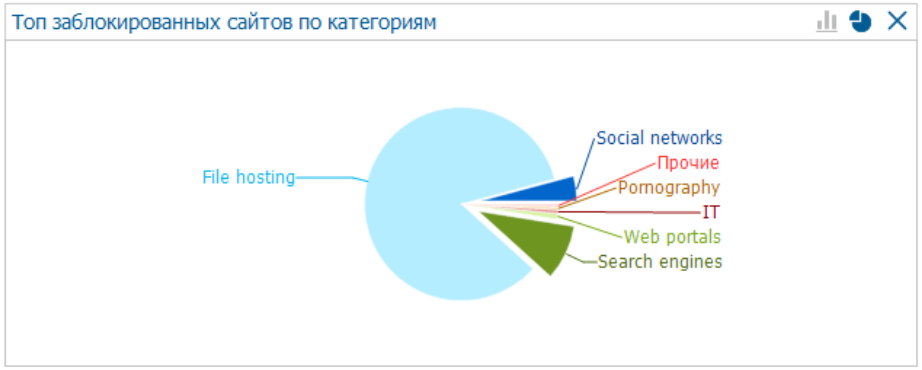
Добавить правило

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

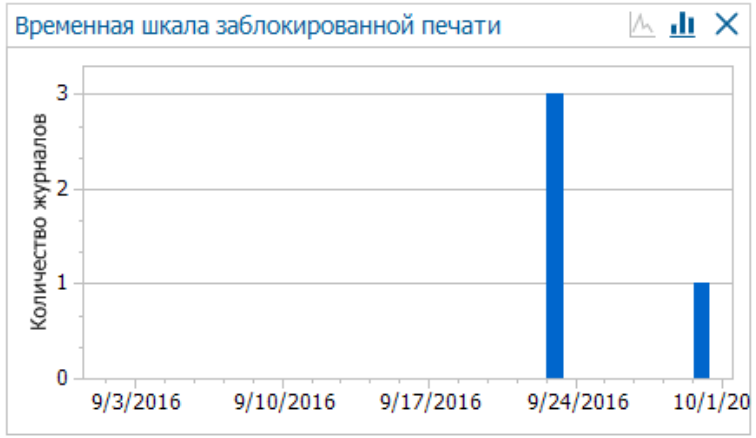


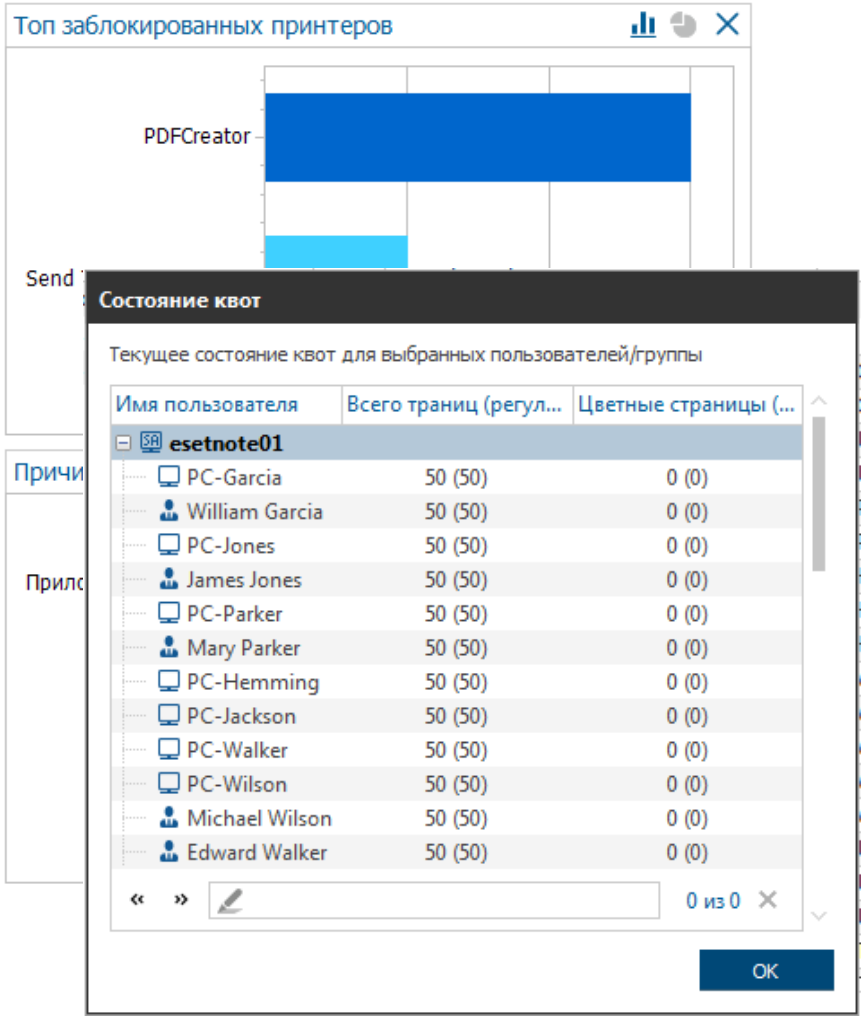


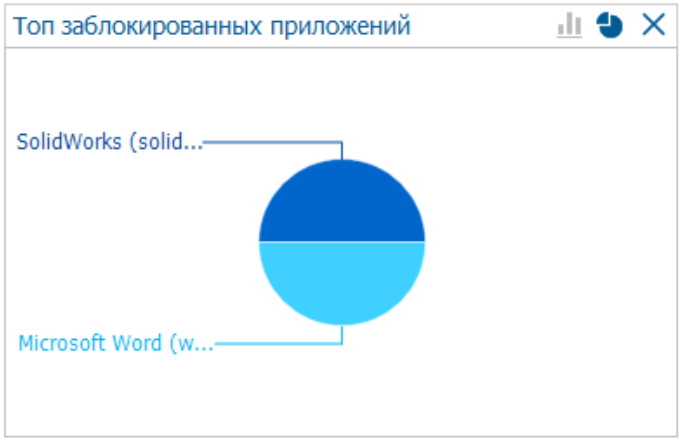


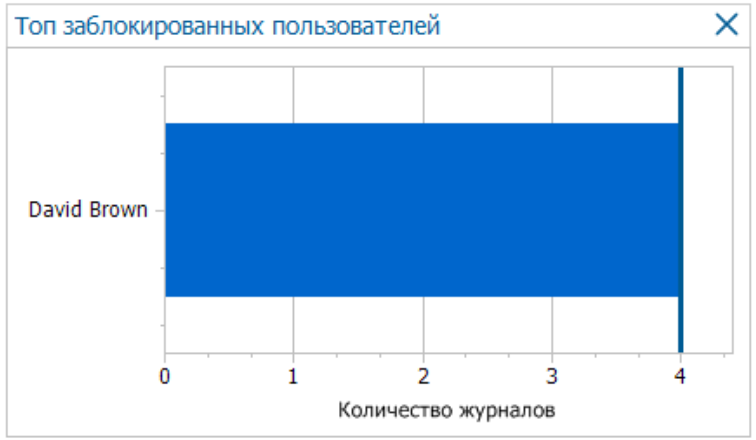


ОФИСНЫЙ КОНТРОЛЬ
(КОНТРОЛЬ ПЕЧАТИ)

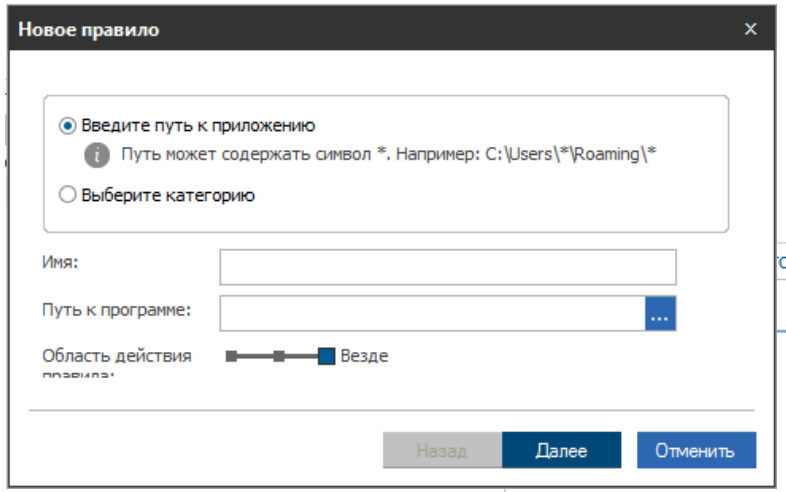


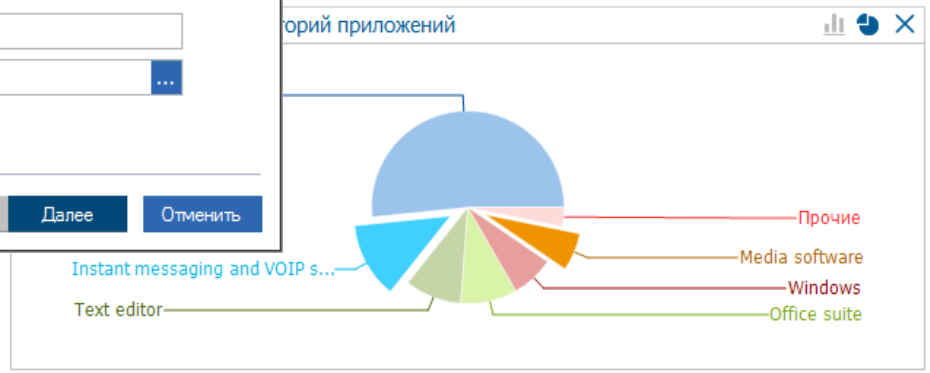


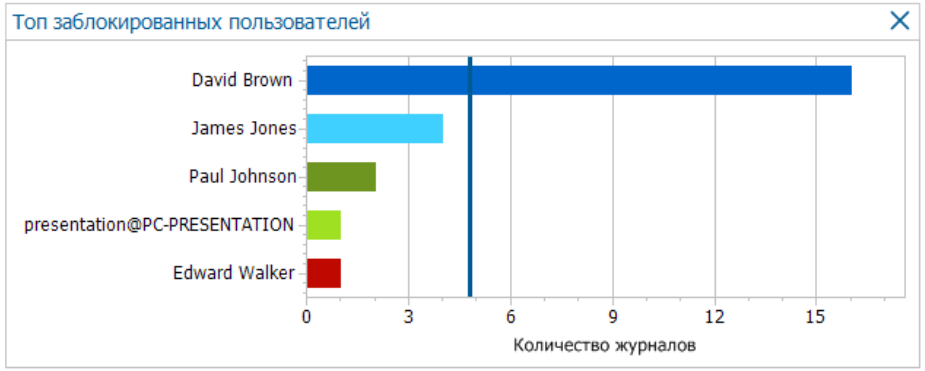


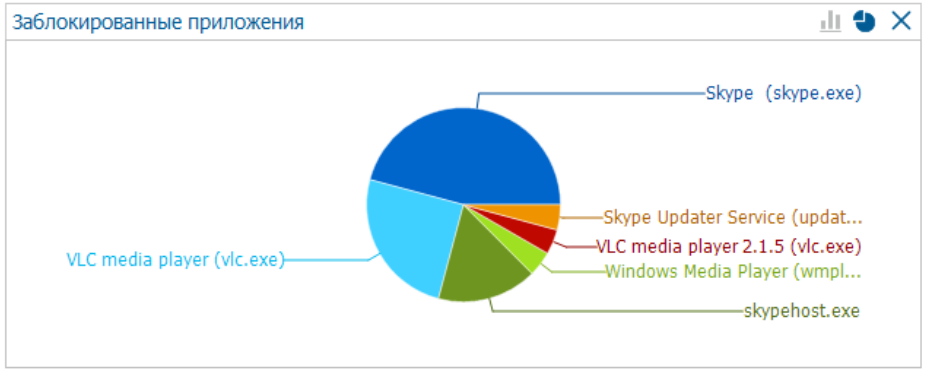


ОФИСНЫЙ КОНТРОЛЬ
(КОНТРОЛЬ ПРИЛОЖЕНИЙ)

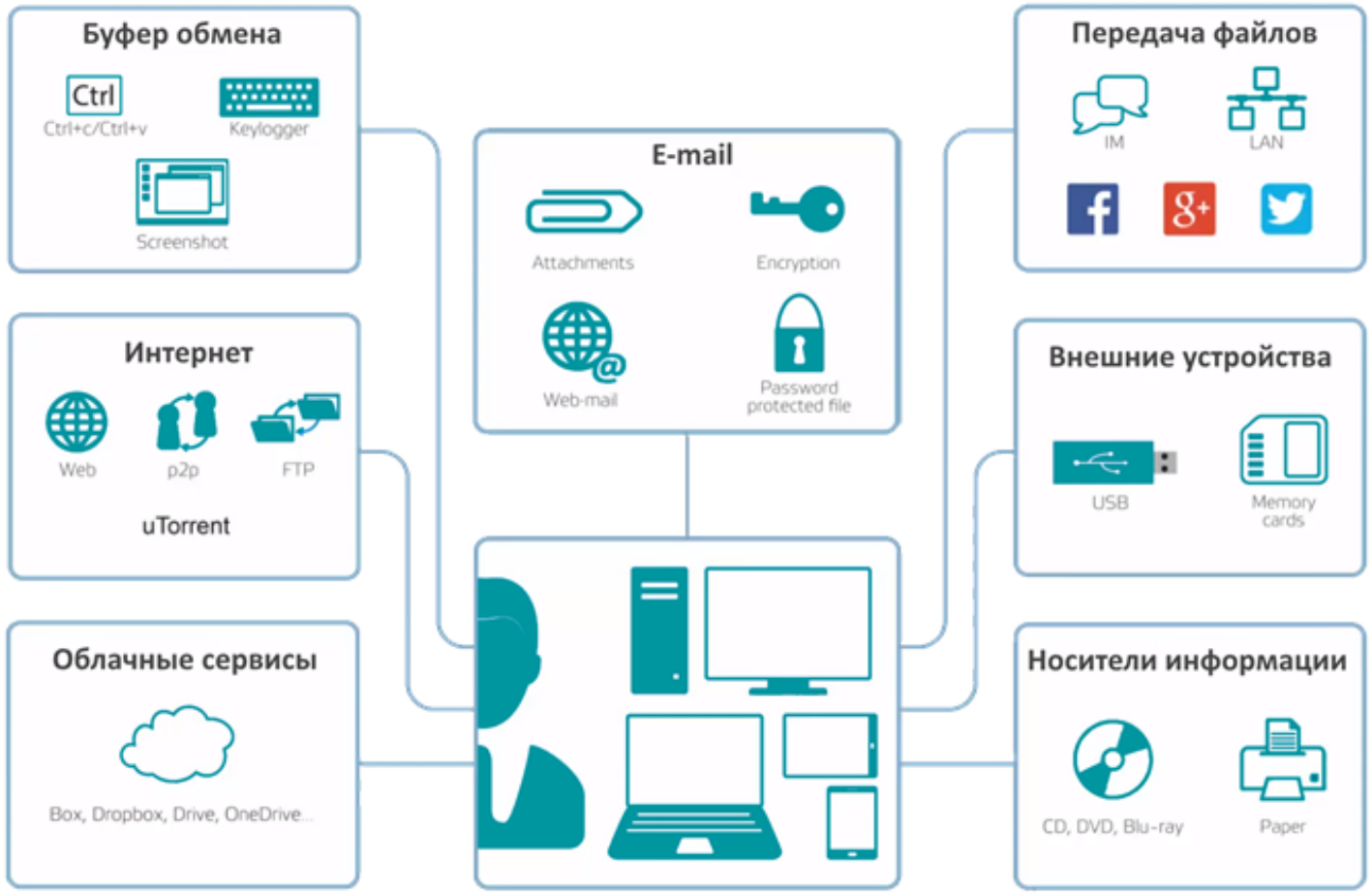








ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕКСТНЫЙ ФИЛЬТР)

› 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

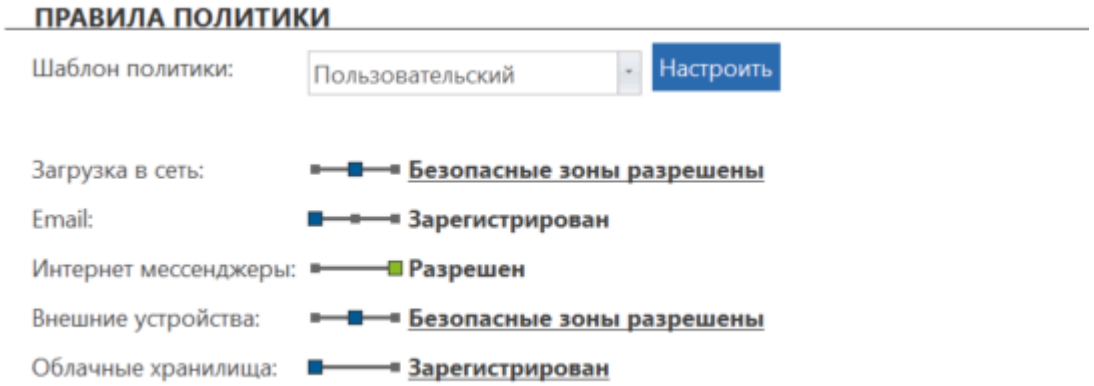
Все файлы, помещенные в определенные папки, будут автоматически получать необходимую метку.

› КОНТЕНТНЫЕ ПРАВИЛА

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

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕНТНЫЙ ФИЛЬТР)

- Электронная почта
- Мессенджеры
- Внешние устройства
- Загрузка файлов в Интернет



ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (КОНТЕНТНЫЙ ФИЛЬТР)

› ПРЕДУСТАНОВЛЕННОЕ СОДЕРЖИМОЕ

Идентификационные номера и номера социального страхования различных стран, номера кредитных карт, номера банковских счетов.

› КЛЮЧЕВЫЕ СЛОВА И РЕГУЛЯРНЫЕ ВЫРАЖЕНИЯ

Любые слова и словосочетания, использование регулярных выражений с применением синтаксиса ECMAScript

› МЕТАДАННЫЕ СТОРОННИХ КЛАССИФИКАТОРОВ

Протестирована поддержка метаданных Microsoft Azure Information Protection, Boldon James, Tukan GREENmod.

ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ
ПРЕДУСТАНОВЛЕННЫЕ ПРАВИЛА

ОСНОВНАЯ ИНФОРМАЦИЯ

Политики DLP настраивают безопасность данных в вашей среде. Политики управляют общим потоком данных, конкретными данными или приложениями и предлагают действия DLP, от автоматической регистрации событий до строгой блокировки. Чтобы ознакомиться с политиками DLP, посетите базу знаний Safetica.

Новая политика безопасности

⚠ Применяется первое соответствующее правило политики.

Политика	Тип	Режим		
Patients + ...	TopSecret	Блокирова...	Изменить	Удалить
Patients + ...	TopSecret	Уведомить	Изменить	Удалить
Patients + ...	TopSecret	Блокирова...	Изменить	Удалить
Patients + ...	TopSecret	Уведомить	Изменить	Удалить
Financial Fil...	Sensitive	Уведомить	Изменить	Удалить
Financial Fil...	Sensitive	Уведомить	Изменить	Удалить
Multimedia...	Multimedia	Зарегистр...	Изменить	Удалить
Multimedia...	Multimedia	Зарегистр...	Изменить	Удалить
Patients + ...	Insurance -...	Блокирова...	Изменить	Удалить
Patients + ...	Insurance -...	Уведомить	Изменить	Удалить
Patients + ...	Insurance -...	Блокирова...	Изменить	Удалить
Patients + ...	Insurance -...	Уведомить	Изменить	Удалить
Design dat...	CAD softw...	Блокирова...	Изменить	Удалить
MS Office ...	Office suite	Блокирова...	Изменить	Удалить
MS Office ...	Office suite	Уведомить	Изменить	Удалить
MS Office ...	Office suite	Уведомить	Изменить	Удалить
Channel co...	Sensitive d...	Уведомить	Изменить	Удалить

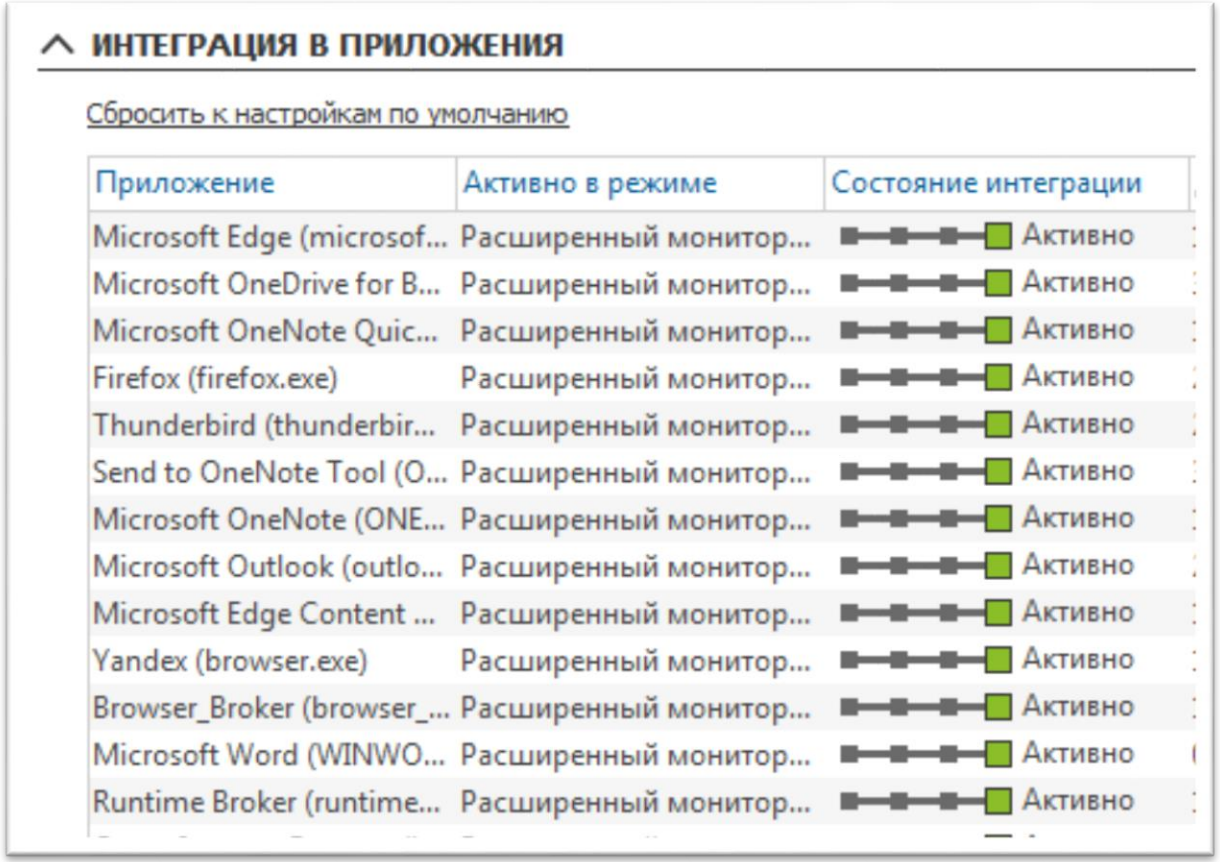
ПОДРОБНОСТИ ПОЛИТИКИ

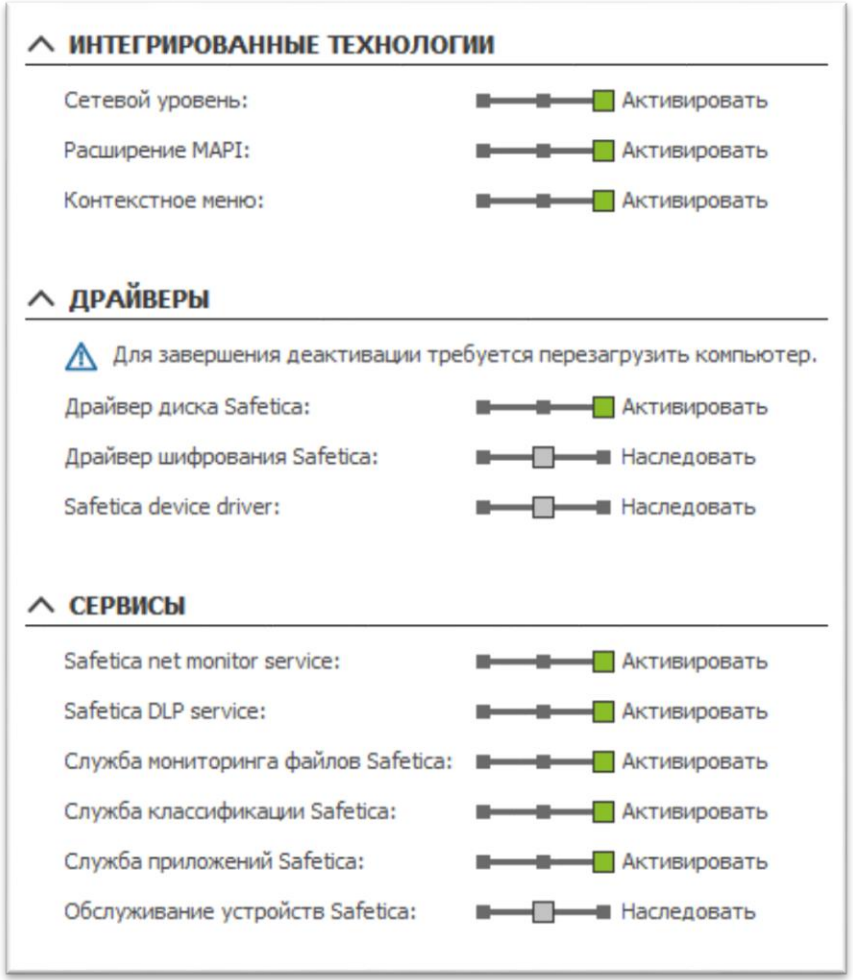
Имя политики:	**Patients + Design Files policy - TopSecret - zone settings - notifying**
Описание политики:	**Please see the manual.**
Тип политики:	**Данные: TopSecret**
Режим политики:	**Зарегистрировать и уведомить**
Политика применяется к:	**Safetica**

ПРАВИЛА ПОЛИТИКИ

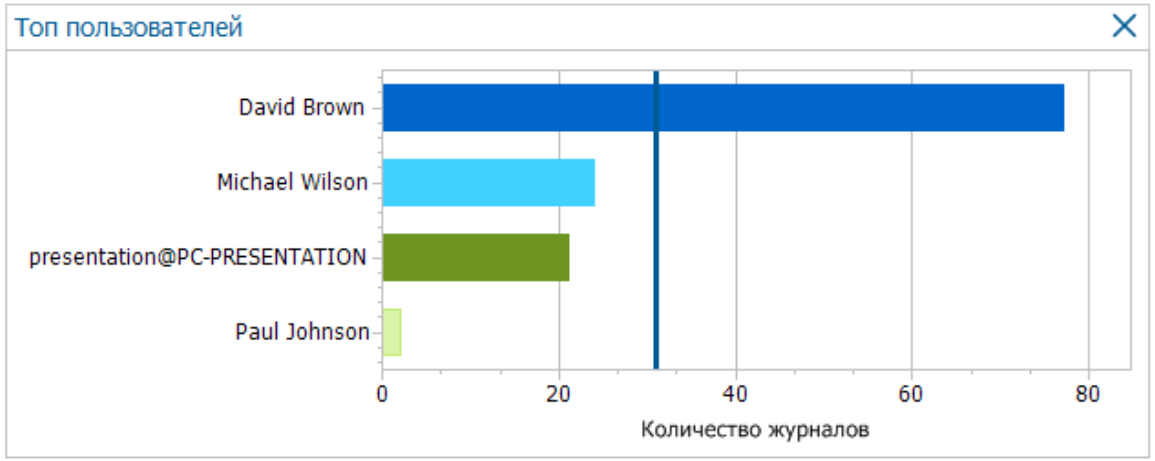
Загрузка в сеть:	**Настройки пользовательской зоны**
Email:	**Настройки пользовательской зоны**
Облачные хранилища:	**Различающиеся настройки**
Буфер обмена (не регистрировать):	**Уведомлен**
Создание скришота (не регистрировать):	**Уведомлен**
Запись на диск:	**Уведомлен**
Сеть (эксперт):	**Настройки пользовательской зоны**
Локальные диски (эксперт):	**Настройки пользовательской зоны**

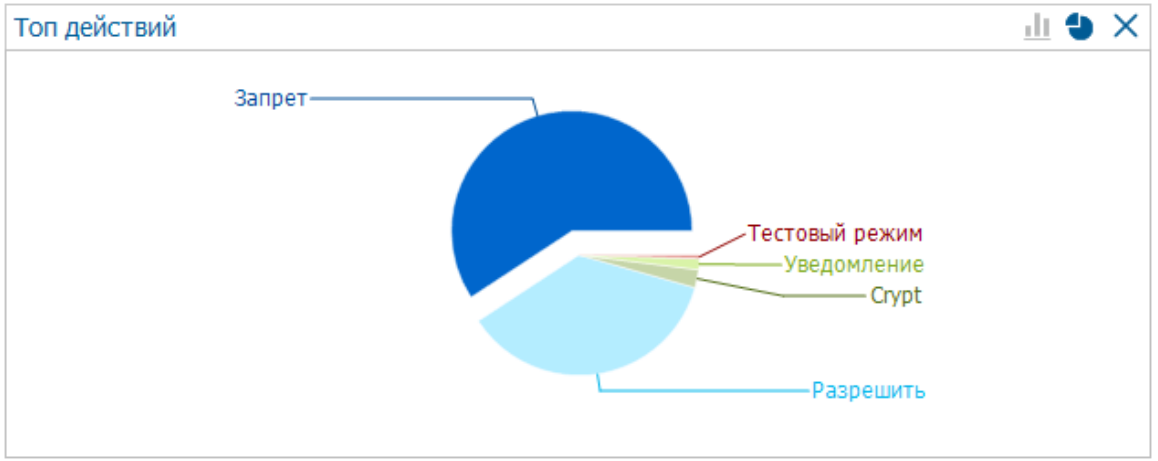
ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)

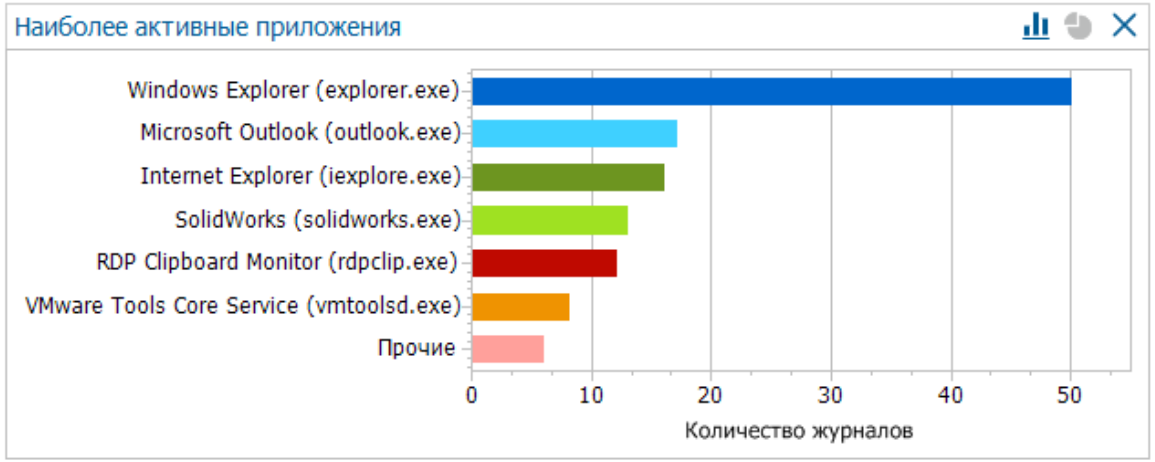


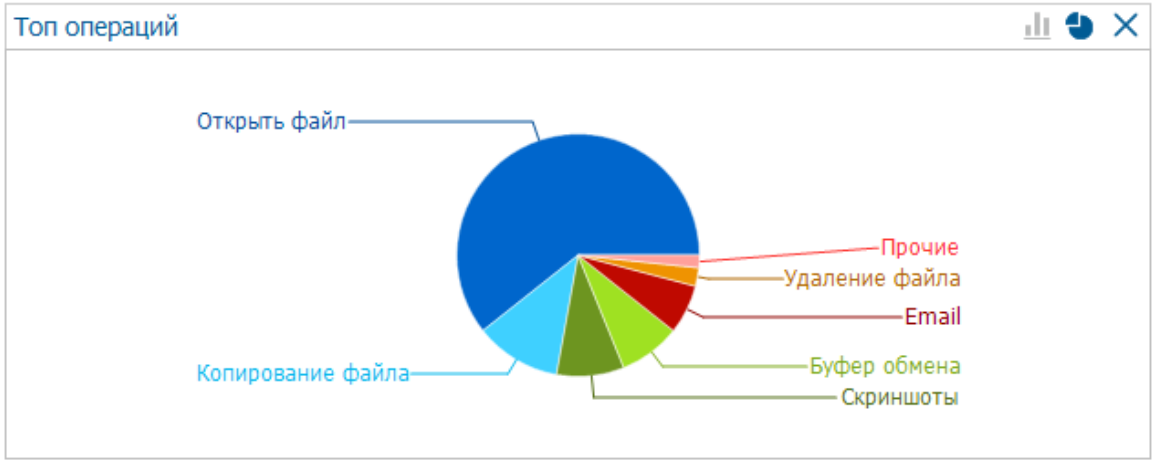


ПРЕДОТВРАЩЕНИЕ УТЕЧКИ ДАННЫХ (МОДУЛЬ DLP)



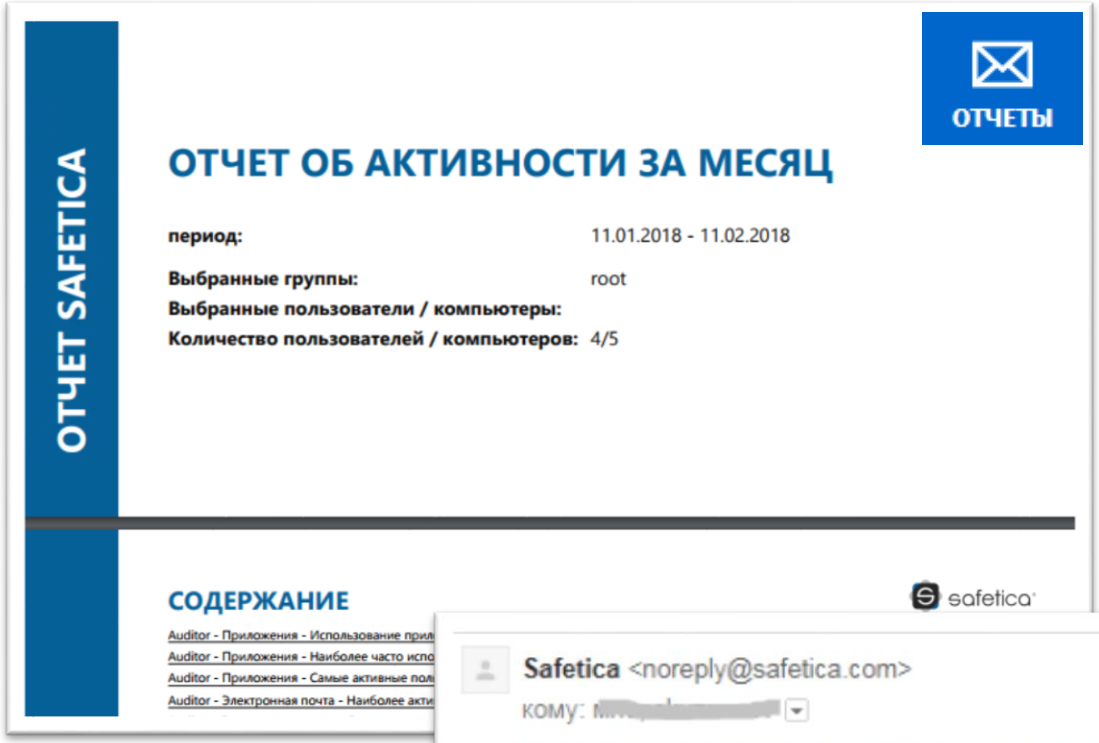


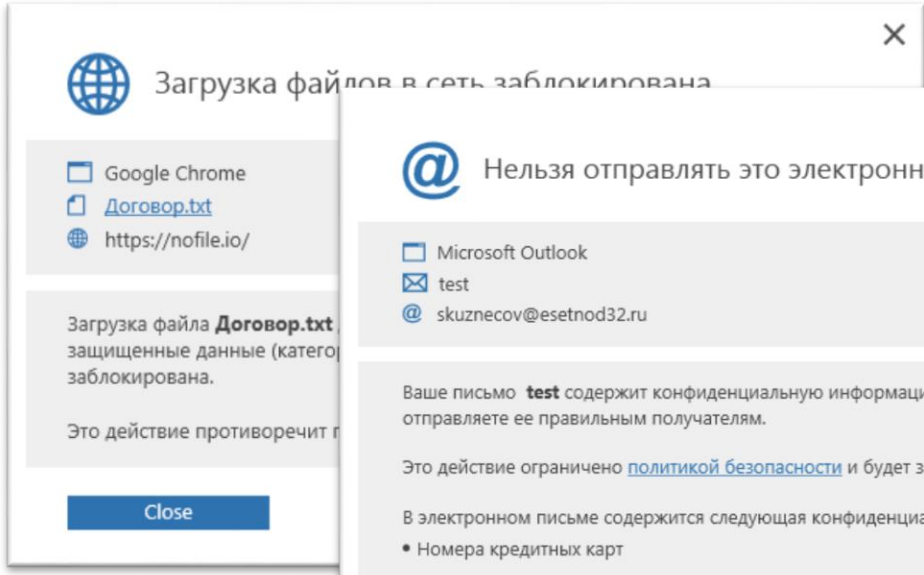


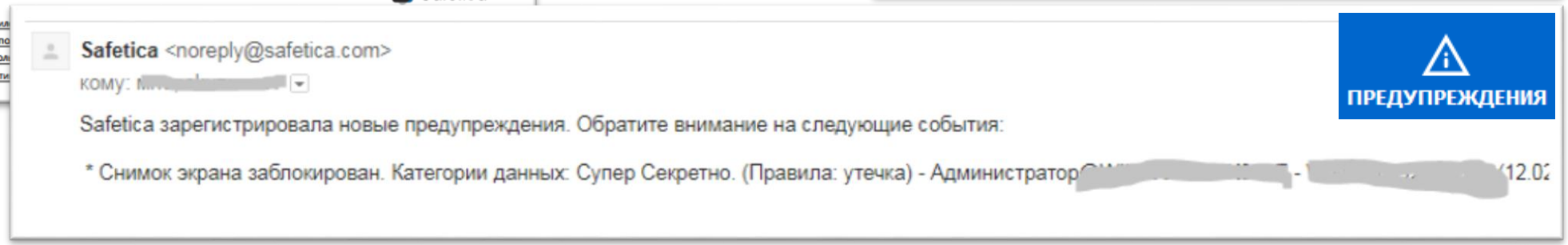


АНАЛИЗ РЕЗУЛЬТАТОВ
WEBSAFETICA

ОТЧЕТНОСТЬ И БЛОКИРОВКА ДЕЯТЕЛЬНОСТИ

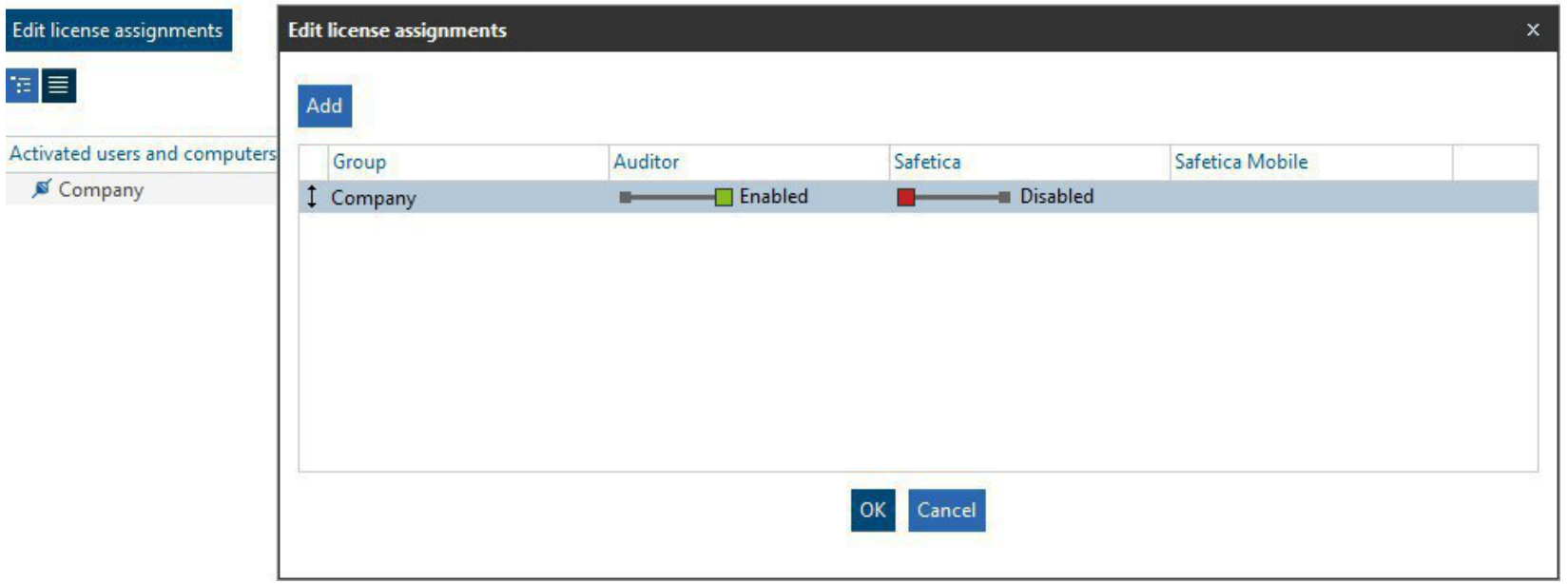




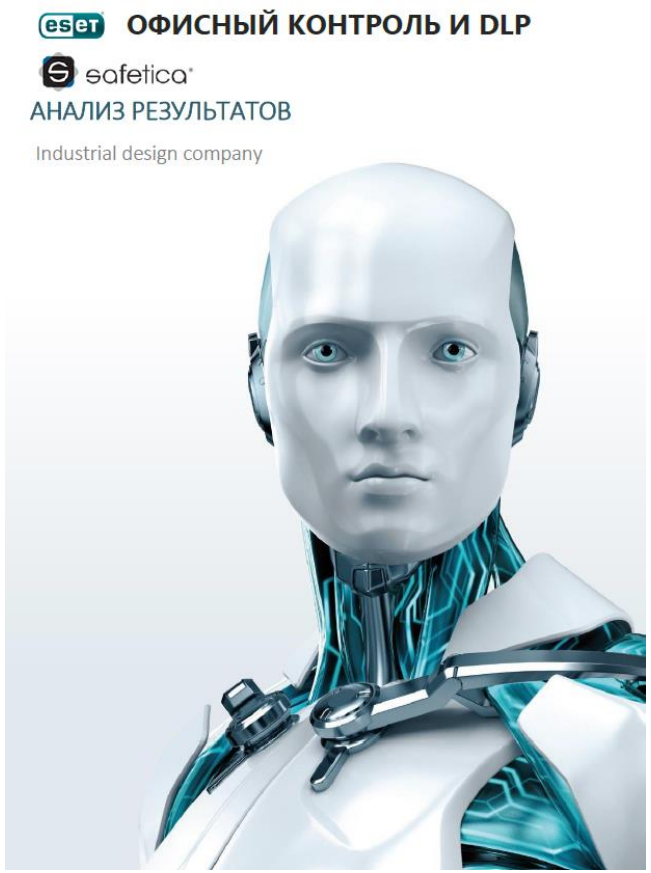


УПРАВЛЕНИЕ ЛИЦЕНЗИЕЙ
РАСПРЕДЕЛЕНИЕ МОДУЛЕЙ

Активируйте необходимые модули



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*

ЛИЦЕНЗИРОВАНИЕ
И ЦЕНЫ

› АУДИТОР

› ОФИСНЫЙ КОНТРОЛЬ

› FULL DLP

Лицензия на один, два или три года
Количество узлов в лицензии: от **10** до **N**

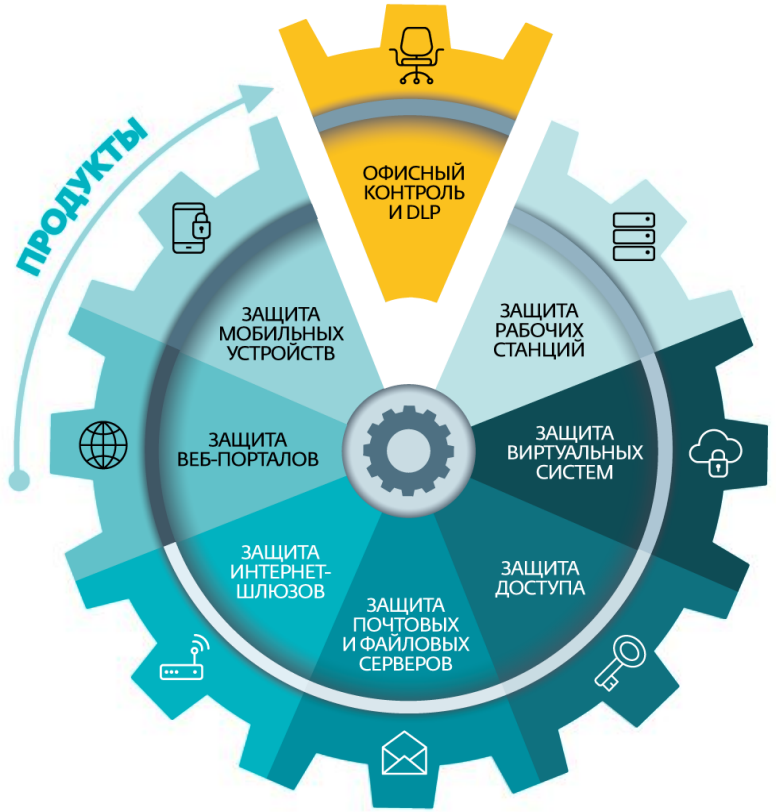
ЛИЦЕНЗИРОВАНИЕ
И ЦЕНЫ

- Продление на 1 год: скидка 40%
- Миграция (с аналогичного продукта конкурента): скидка 20%
- Отраслевая скидка для образования: 50%
- Отраслевая скидка для медицины: 30%

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

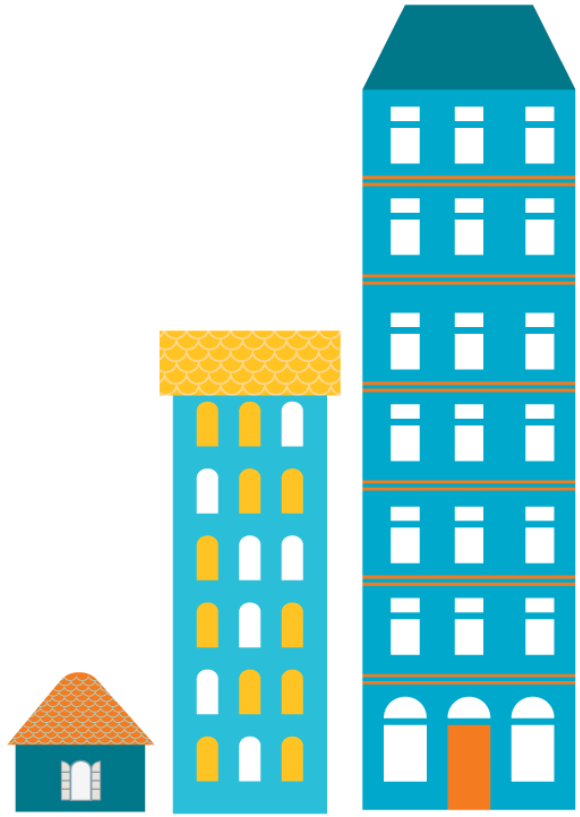
- *Аудит активности пользователей*
- *Ограничение деятельности сотрудников*
- *Предотвращение утечки данных*

✓ ЛЕГКОЕ ВНЕДРЕНИЕ

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

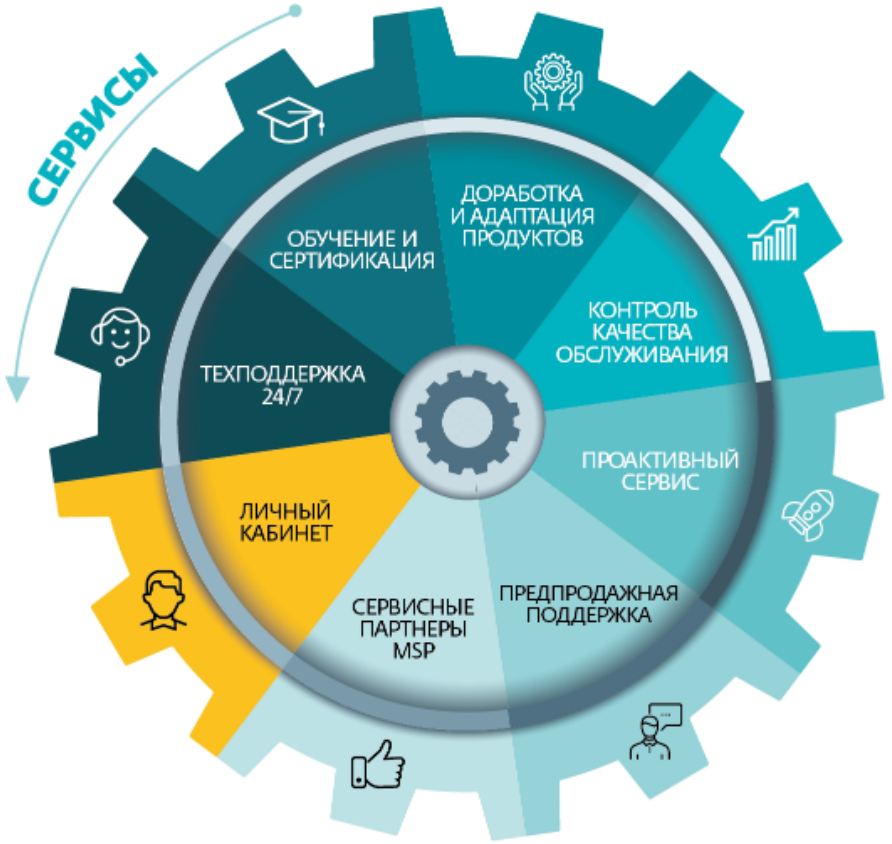
✓ БЕЗ ДОПОЛНИТЕЛЬНЫХ ВЛОЖЕНИЙ

- *Стоимость проекта = стоимость лицензии*



СЕРВИСЫ ESET
ПОМОЖЕМ ВАМ В ЛЮБОЙ СИТУАЦИИ

- ✓ *Предпродажная поддержка*
- ✓ *Доработка и адаптация продуктов*
- ✓ *Техническая поддержка 24/7*
- ✓ *Контроль качества обслуживания*
- ✓ *Обучение и сертификация*



СЕРВИСЫ ESET
ПОДТВЕРЖДЕННОЕ КАЧЕСТВО

ESET – победитель номинаций российского конкурса клиентского сервиса CX Awards:

- ✓ *«Лучшее вовлечение персонала»*
- ✓ *«Лучшие клиентоориентированные организации»*

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Спасибо! Вопросы?