



MAKVES

# Как провести аудит и управлять информационными ресурсами организации

Подкопаев  
Роман



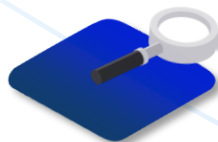
# Основные тренды ИБ 2019



ФЗ 187 (КИИ)



Атаки и проникновение извне



SOC, SIEM, ГосСОПКА



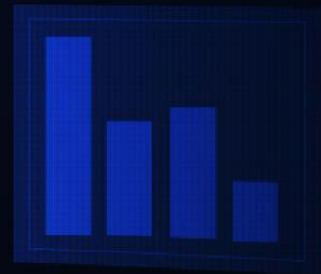
Изменения ФЗ 152  
(ужесточение ответственности), GDPR



Утечки  
от инсайдеров

08 - K11 Docks

# А ЧТО ЕЩЁ???



# АУДИТ И УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РЕСУРСАМИ ПРЕДПРИЯТИЯ

MAKVES



# Решаемые проблемы



Превышение прав пользователей в домене



Категоризация данных



Доступ к чужим почтовым ящикам



Излишний доступ к файлам и папкам



Мониторинг установленного ПО, версий и активации Microsoft



Дублирование файлов

# СЛУЧАИ ИЗ РЕАЛЬНОЙ ПРАКТИКИ



## КОЛЛИЗИЯ ДОСТУПА

У сотрудника  
нет доступа  
к группе или папке,  
но оказывается доступ к  
отдельному файлу



## ЧУЖОЙ ПРОФИЛЬ НА АРМ

---

Сотрудник является  
локальным администратором  
на чужих компьютерах





## ИНВЕНТАРИЗАЦИЯ ПО

---



В структуре выявлены  
запрещенные  
к использованию ОС  
об удалении которых уже  
отчитались исполнители



## ДОСТУП К ЧУЖОЙ ПОЧТЕ

---

У сотрудника был доступ  
к чужим почтовым ящикам



## «МЕРТВЫЕ» ДУШИ

---

Созданы учетные записи  
для новых сотрудников,  
но под ними полгода никто не  
заходил



# КАТЕГОРИЗАЦИЯ ДАННЫХ

---

На соответствие  
стандартам и законам  
ФЗ 152, PCI DSS, GDPR



## ДАЛИ ДОСТУП АУДИТОРАМ

---

Дали временный  
доступ к ресурсам  
и забыли отключить



Основные  
возможности  
"Makves-DCAP"

Поддержка облачных сервисов

Помощь в расследовании  
инцидентов ИБ

Кроссплатформенность

Аудит данных и полная  
информация о правах доступа  
к корпоративным ресурсам

Гибкая система отчётности

Активная система  
уведомлений

Автоматическое сценарии  
отработки инцидентов

Поиск неиспользуемых  
и дублированных файлов

Соответствие стандартам

Поведенческий анализ

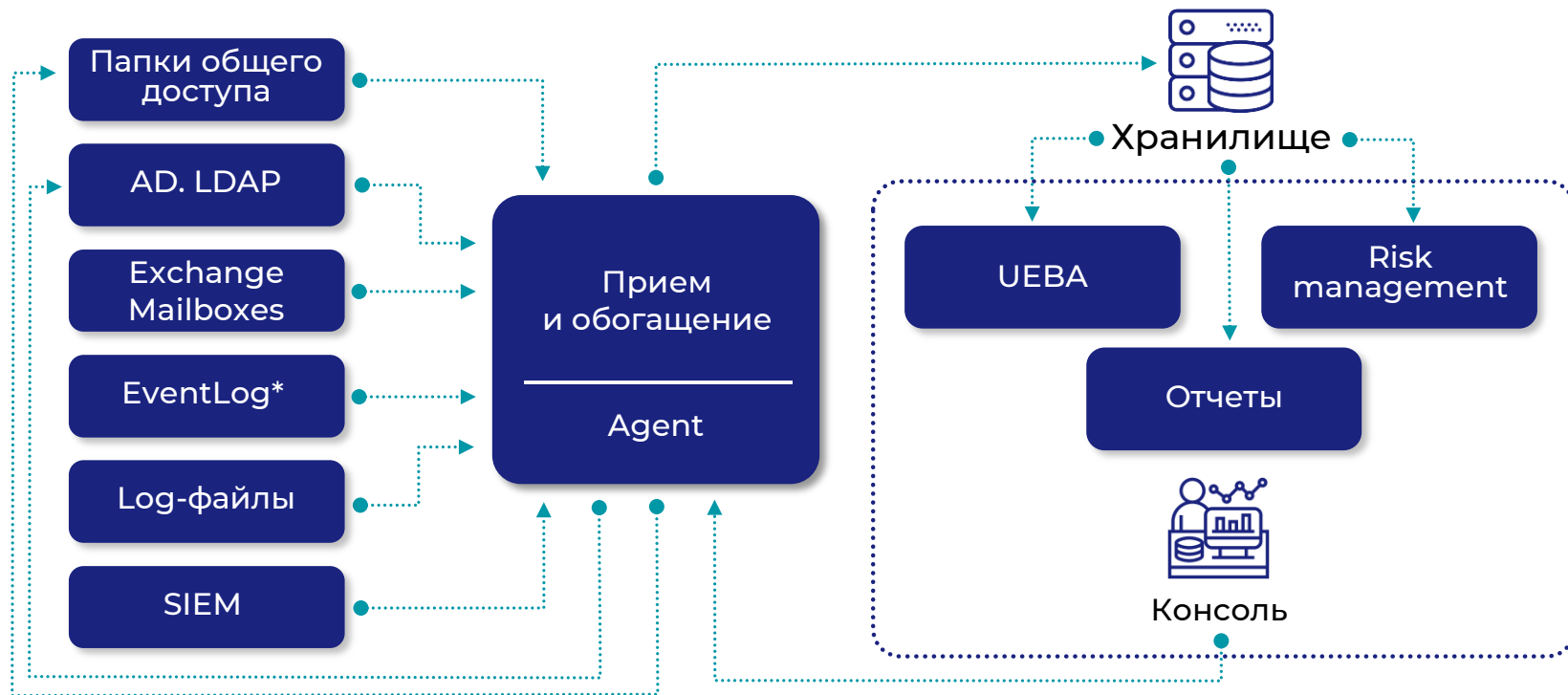
Анализ рисков

Интеллектуальный поиск

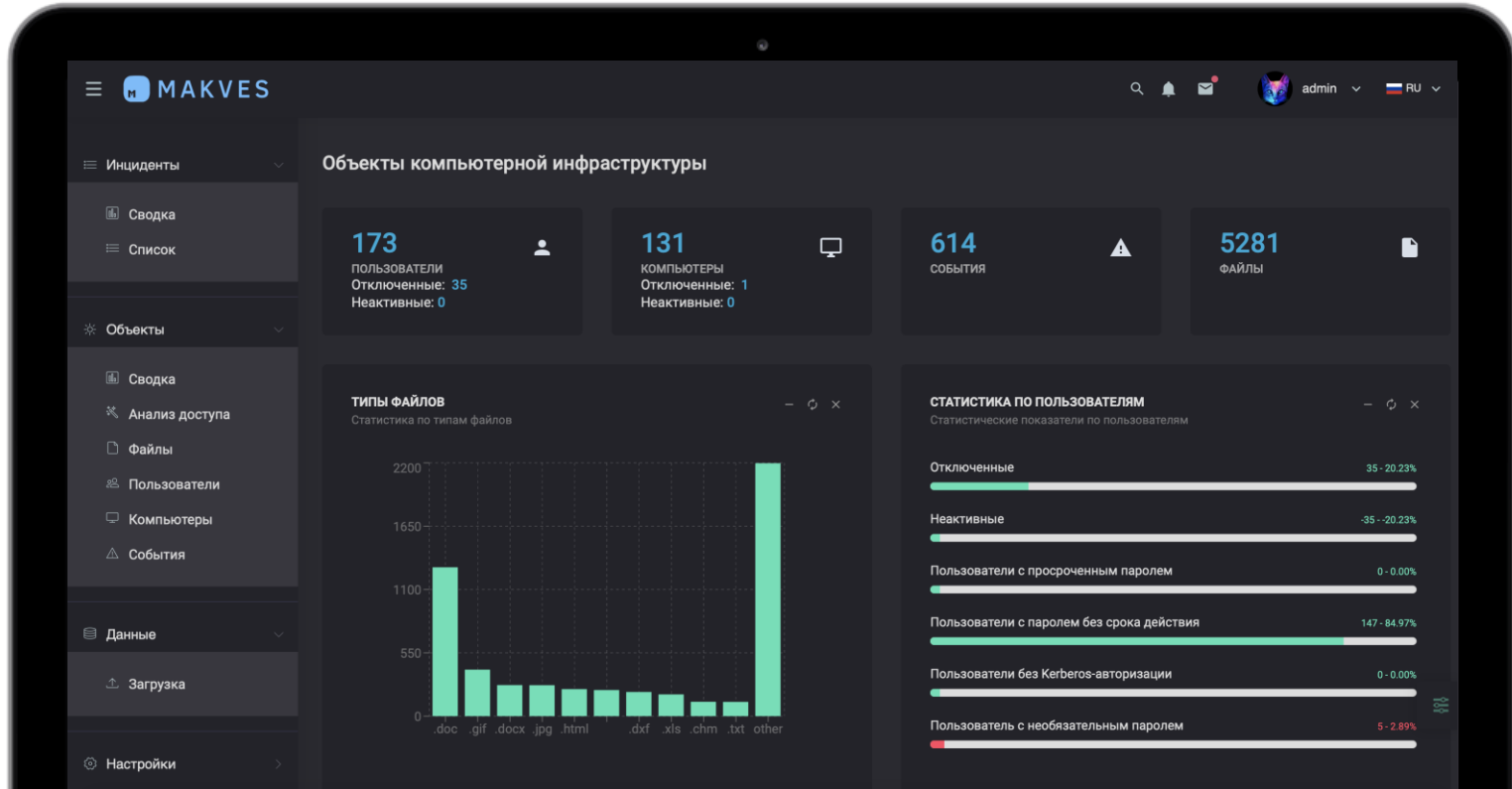
Выявление наиболее востребованных  
и "забытых" пользователями ресурсов

Интеграция с системой реагирования  
на инциденты Makves IRP

# Архитектура системы



# Рабочее место оператора системы





# Оценка рынка 2019 года и перспективы 2020

- До сентября 2019 были только западные решения
- Импортзамещение, появление первых отечественных решений
- Положительные отзывы клиентов и резкое увеличение интереса
- В 2020 ожидаем появление новых отечественных производителей



# Наши планы на 2020



Наращивание функционала до уровня западных конкурентов



Функции поведенческого анализа



Запуск процесса сертификации ПО



Внедрение технологии машинного обучения



BigData

# ЗАПИШИТЕСЬ



# НА БЕСПЛАТНЫЙ АУДИТ

по итогам которого вы получите:

1

Построение  
матрицы доступа

2

Аудит доступов к файлам и  
почтовым ящикам

3

Классификацию данных  
в соответствии со стандартами (152ФЗ,  
GDPR и др.)

# Мы на СВЯЗИ



+7-495-150-54-06



[www.makves.ru](http://www.makves.ru)



[sales@makves.ru](mailto:sales@makves.ru)

