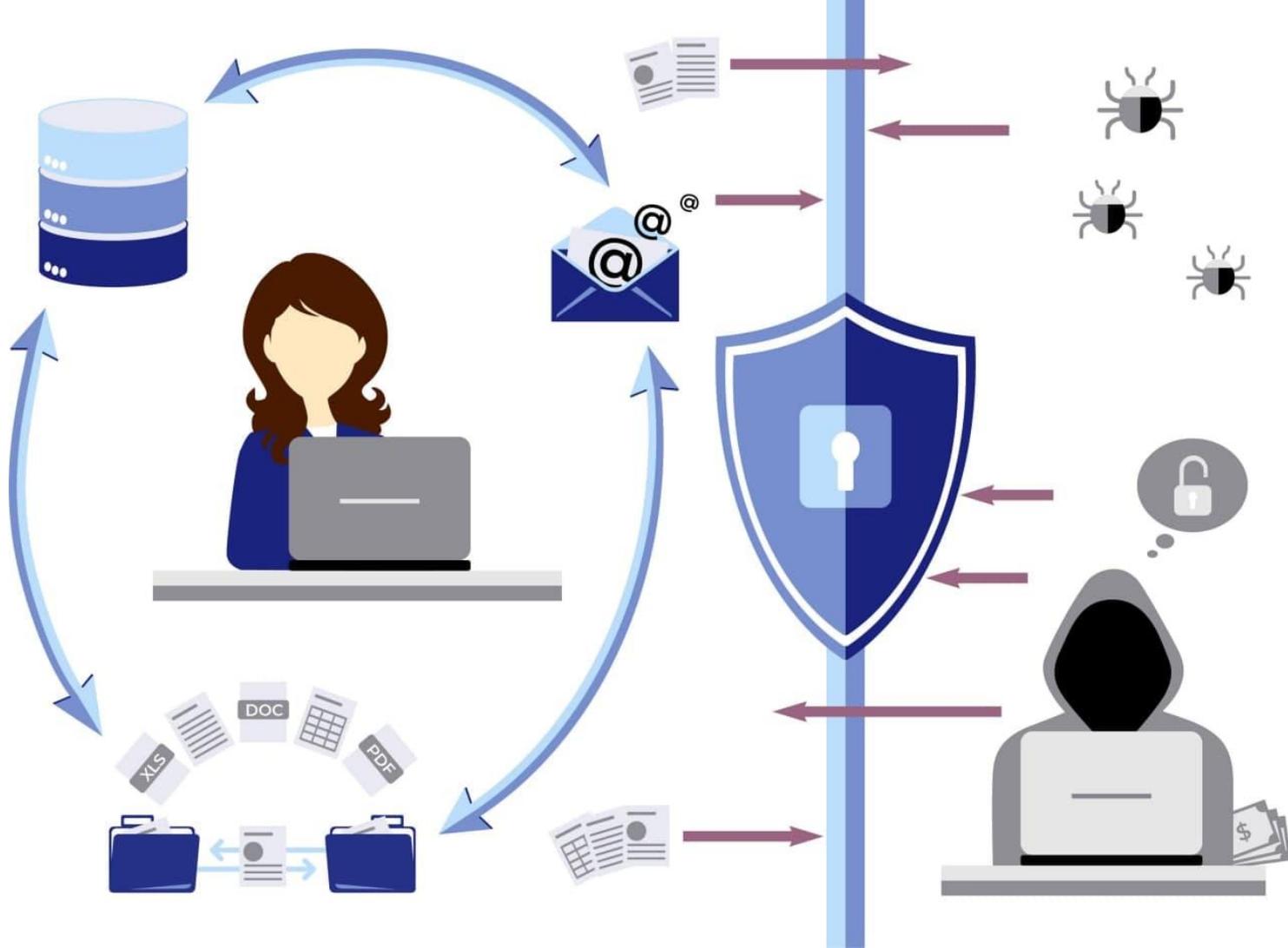




Устранение уязвимостей в IT-инфраструктуре

Роман
Кольцов





Как защитить данные?

1

АУДИТ

файловых хранилищ

2

КАТЕГОРИЗАЦИЯ

(152-ФЗ, GDPR, ком. тайна...)

3

МОНИТОРИНГ

прав доступа и действий
пользователей

4

АКТИВНАЯ РЕАКЦИЯ

оперативное устранение рисков

Как работает DCAP



Поиск данных, требующих защиты, по содержимому и внешним атрибутам.

Анализ и категоризация

2

Определение избыточных (нерегламентированных) прав, нарушения доступа.

Оценка рисков

4

Поиск дубликатов, устаревших данных и учетных записей, версий и активаций ОС.

Актуальность файлов и ПО

6

1

Сбор данных

Аудит Active Directory, рабочих станций, файловых серверов, почтовых серверов.

3

Создание матрицы доступа

Наглядная матрица доступа пользователей к файлам, папкам и почтовым ящикам.

5

Мониторинг

Непрерывный анализ событий системы и действий пользователей.

Типовые проблемы



Ненаследуемые
права



Неактивные
пользователи



Избыточный доступ к
конфиденциальной
информации



Не обязательные
пароли / без срока
действия



Незащищенные
дубликаты



«Временные» доступы
к ресурсам для
подрядчиков и
аудиторов

СЛУЧАИ ИЗ ПРАКТИКИ



КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ В ОТКРЫТОМ ДОСТУПЕ ФЗ-152, GDPR...



ЗАЩИТА ОТ ВНЕШНИХ УГРОЗ



ВОЗМОЖНОСТИ MAKVES DCAP



Уведомления о действиях с файлами и объектами AD

Контроль параметров всех сущностей системы

Фиксация аномалий

АНАЛИЗ СОБЫТИЙ

Анализ рисков и рекомендации

Активная реакция на инцидент



Количество элементов и размеры папок

«Песочница» моделирования изменения прав

Управление доступом к файлам в консоли

УПРАВЛЕНИЕ ПРАВАМИ

Настройка разрешений: просмотр, скачивание

Панель Рекомендаций Makves DСAP

MAKVES admin

Рекомендации

ПОЛЬЗОВАТЕЛИ

Отключите неактивных пользователей Количество: 37 Важность: 🔴

Отключите пользователей, которые уже 2 месяца не осуществляли вход в домен Показать/скрыть список ▾

	Имя	Риск-фактор	Аккаунт	NT-имя
<input type="checkbox"/>	Иванов Иван	26	ivanov	ИВАНОВ
<input checked="" type="checkbox"/>	Петров Петр	78	petrov	ПЕТРОВ
<input type="checkbox"/>	Сидоров Сидор	26	sidorov	СИДОРОВ
<input type="checkbox"/>	Сидоров Алексей Владимирович	78	sidov_avp	СИДОРОВ_ИВАНОВ
<input type="checkbox"/>	Сидоров Алексей	26	sidov_aleksey	СИДОРОВ_ИВАНОВ

📄 Экспорт ✉ Переслать по почте 👁 Просмотреть учетную запись ➔ Отключить пользователя

Проинспектируйте пользователей с высоким риском Количество: 2 Важность: 🔴

Проверьте обоснованность параметров и поведение пользователей Показать/скрыть список ▾

Проинспектируйте атипичных пользователей Количество: 4 Важность: 🔴

Проинспектируйте пользователей с высоким уровнем атипичности Показать/скрыть список ▾

Установите срок действия пароля Количество: 31 Важность: 🟡

Установите срок действия пароля для пользователей, у которых он не установлен Показать/скрыть список ▾

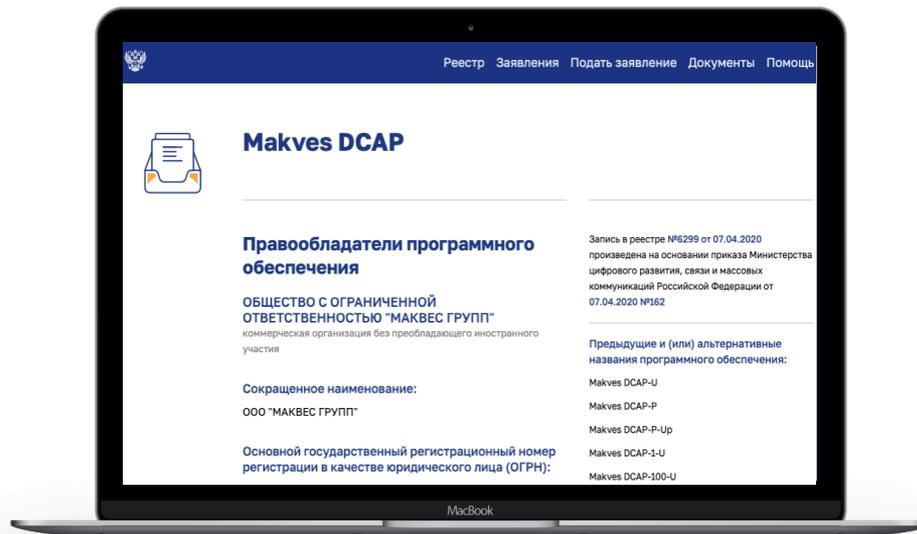
Установите обязательный ввод пароля Количество: 2 Важность: 🟡

Установите обязательный ввод пароля для пользователей, для которых он необязателен Показать/скрыть список ▾

Удалите пустые группы Количество: 88 Важность: 🟢

В РЕЕСТРЕ РОССИЙСКОГО ПО

Приказ Минцифры России
№162 от 07.04.2020



Особенности MAKVES DCAP

Активная реакция на инцидент

Устранение выявленных рисков в интерфейсе системы.

Продвинутый модуль аналитики

Контроль параметров всех сущностей системы позволяет вовремя реагировать на внутренние и внешние угрозы.

Не нарушает контуров безопасности

Выявляет конфиденциальную информацию в документах без создания теневых копий на выделенном ресурсе.



Песочница Makves

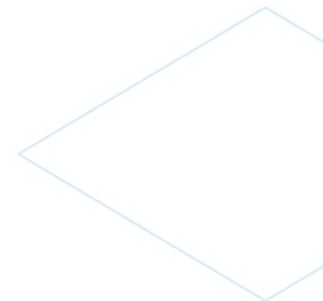
Моделирование последствий изменения прав пользователей.

Бесшовная интеграция

Интегрируется с любыми корпоративными программами и сервисами через REST.API.

Настраиваемые дашборды

Кастомизированная панель сводки с возможностью добавления виджетов по всем объектам анализа.



Как навести порядок в данных?

1

Проверяйте, что хранится в сетевых папках и на ПК

2

Классифицируйте данные (152-ФЗ, ФСТЭК, GDPR, коммерческая тайна...)

3

Изучайте действия пользователей с ценными файлами и права доступа



МЫ НА СВЯЗИ

+7-495-150-54-06

sales@makves.ru

www.makves.ru