



1-й продукт класса DСАР  
в Реестре Минцифры  
Запись № 6299 от 07.04.2020



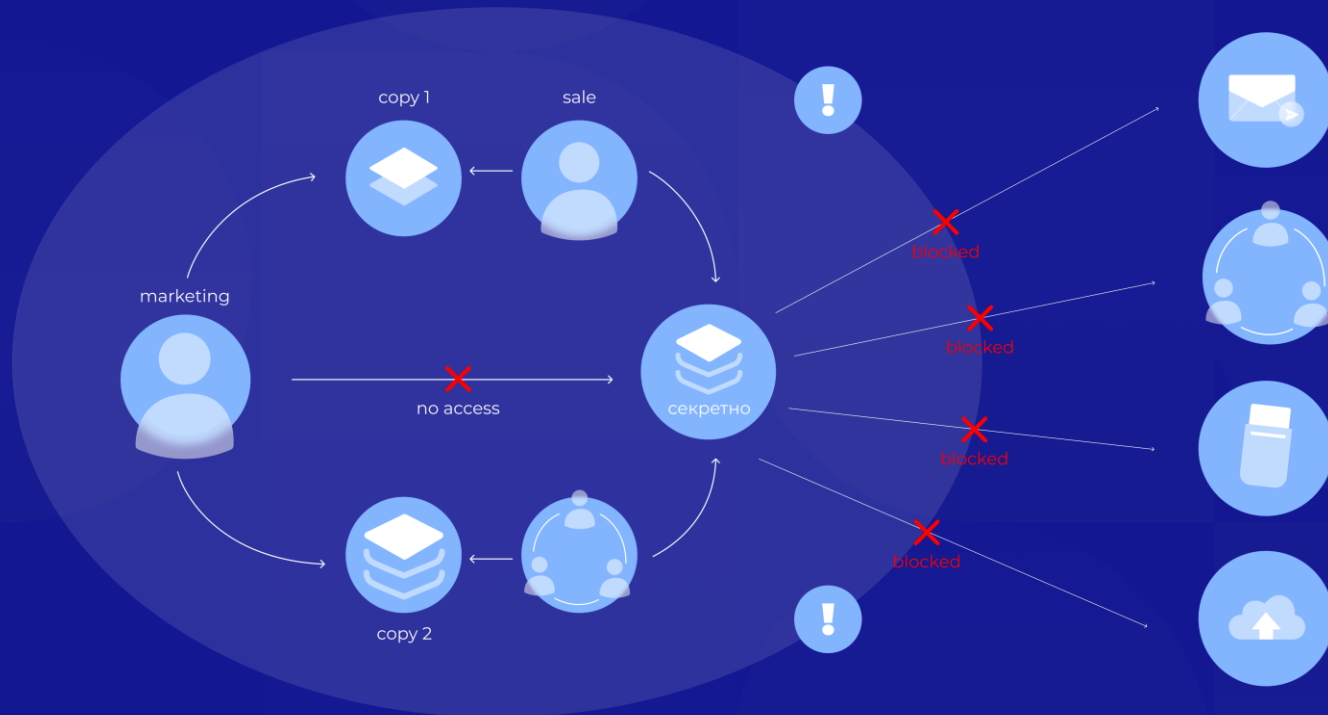
СЕРТИФИКАТ  
ФСТЭК №4744

Роман Подкопаев

# DCAP

От защиты периметра к защите данных

# ТРАДИЦИОННЫЙ ПОДХОД



**Данные становятся  
уязвимыми для  
кибератак и  
неправомерных  
действий**



**Data  
Breach**

# DSAR – НОВЫЙ ПОДХОД К ЗАЩИТЕ ДАННЫХ

## ИТ-инфраструктура и источники данных

Пользователи  
Серверы, СХД  
Рабочие станции  
Почтовые серверы  
Облачные хранилища



Аудит  
Классификация  
Матрица доступа  
Оценка рисков  
Активная реакция  
Мониторинг



## Результаты

Комплаенс  
Автоматизация  
рутины  
Защита информации  
Сокращение  
поверхности  
кибератаки

# Интерфейс. Рекомендации

**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	🟡	ivanov	ИВАНОВ
<input checked="" type="checkbox"/>	Петров Петр	🟡	petrov	ПЕТРОВ
<input type="checkbox"/>	Сидоров Сидор	🟡	sidorov	СИДОРОВ
<input type="checkbox"/>	Сидоров Алексей Владимирович	🟡	sidov_av	СИДОРОВ_АВ
<input type="checkbox"/>	Сидоров Алексей	🟡	sidov_alek	СИДОРОВ_АЛЕКС

📄 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: 🟢

# ВОЗМОЖНОСТИ СОВРЕМЕННЫХ DСАР-СИСТЕМ

---

01 Файловый аудит

02 Поиск  
и категоризация

03 Аудит почты

04 Аудит  
пользователей

05 Анализ событий

06 Исправление  
рисков «на месте»

07 UEBA

08 Кастомные отчеты  
и оповещения

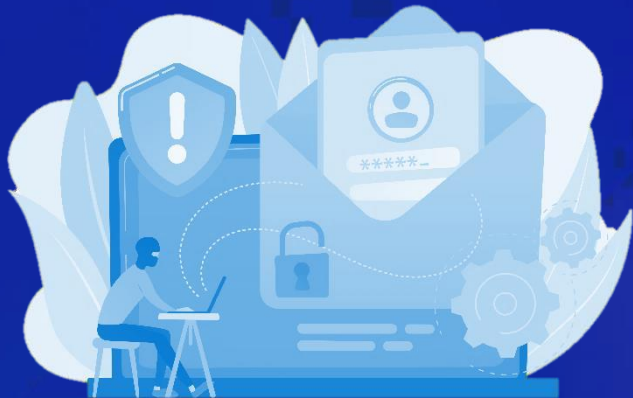
09 Автоматизация

# ДСАР

## ПРАКТИКА ПРИМЕНЕНИЯ



## Техническая атака на учетную запись пользователя



## DCAP

### Аудит

- «ЗАБЫТЫЕ» УЧЕТНЫЕ ЗАПИСИ
- ПРОСРОЧЕННЫЕ ПАРОЛИ
- СЕРВИСНЫЕ УЧЕТНЫЕ ЗАПИСИ
- РЕАЛЬНЫЕ ПРАВА ДОСТУПА



### Мониторинг

- ПОПЫТКИ ПОДКЛЮЧЕНИЯ
- АНОМАЛЬНАЯ АКТИВНОСТЬ:  
СОБЫТИЯ, ФАЙЛЫ, ПОЛЬЗОВАТЕЛИ, ПК





## Конфиденциальная информация в общем доступе



## DCAP

- ГДЕ ХРАНИТСЯ ИНФОРМАЦИЯ И ЕЕ КОПИИ
- В КАКОМ КОЛИЧЕСТВЕ
- КТО ИМЕЕТ К НЕЙ ДОСТУП
- КТО АКТИВНЫЙ ПОЛЬЗОВАТЕЛЬ

**Нарушения  
в 100% случаев**

# Преимущества Makves DCAP

## Архитектура

Гибкое решение для построения отказоустойчивой и территориально-распределенной системы

## Кастомные сводки

Настройка собственных отчетов и контроль самого важного в рамках единого дашборда

## Исправление рисков "на месте"

Управление доступом и активная реакция на инциденты

## Поддержка российских ОС

Широкий спектр систем, включая RedOS, Astra Linux и другие

## Поддержка любых СХД

Выполняет аудит любых СХД вне зависимости от производителя

## Приоритизации рисков

Настройка приоритетов по рискам с учетом особенностей бизнеса компании



## 5 ШАГОВ

к датацентричной  
модели ИБ

01

Контроль  
учетных записей

02

Аудит файловых  
хранилищ

03

Классификация

04

Мониторинг

05

Автоматизация



Узнайте больше о защите данных!

# MAKVES

