



Результаты аудита рисков в ИТ

Роман
Подкопаев



Итоги 2021

x 15

Пилотных проектов

> 500 Тбайт

Объем данных для обработки

~410 млн

Событий

> 100 млн

Файлов и папок

> 200 тыс.

Учетных записей



Источники проблем

2

МЛН

Ненаследуемые
права

25 тысяч

Неактивные
пользователи

**ФЗ-152,
GDPR...**

Избыточный доступ к
конфиденциальной
информации

14

ТЫСЯЧ

Не обязательные пароли
/ без срока действия

до 50%

Незащищенные
дубликаты

1,8

МЛН

Файлы
с прямыми правами

СЛУЧАИ ИЗ ПРАКТИКИ



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



НАСТРОЙКА ПОЛИТИК БЕЗОПАСНОСТИ



ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ DLP

- ✓ Снижение нагрузки на СЗИ
- ✓ Защита данных внутри инфраструктуры и при пересечении периметра



Makves DCAP

ЧТО НОВОГО?



Новые возможности Makves DCAP



Контроль всех действий
пользователей
и событий



Файловый аудит без штатных
средств
ОС Windows



Песочница



Новый механизм
аномалий



Оперативное
устранение рисков



Защита от внешних угроз –
шифровальщики
и DDoS

Инциденты >

Объекты >

- Сводка
- Анализ
- Риски
- Отчеты
- Аномалии
- Рекомендации
- Оповещения
- Пользователи
- Компьютеры
- Файлы
- Почтовые ящики
- События

Рекомендации

ПОЛЬЗОВАТЕЛИ

Отключите неактивных пользователей ↻ Количество: 144 Важность: ●

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

	Имя	Риск-фактор	Аккаунт	NT-имя
<input type="checkbox"/>	1C_оповещение	76	1C.send	MKVS-DOMAIN-P\1C.send
<input checked="" type="checkbox"/>	1C Программист	76	developer_1C	MKVS-DOMAIN-P\developer_...
<input type="checkbox"/>	Bogdan Prusov	76	bprusov	MV\bprusov
<input type="checkbox"/>	Businesscope	76	businesscope	MKVS-DOMAIN-P\businessco...

Экспорт Переслать по почте Просмотреть учетную запись Инициализировать смену пароля Отключить пользователя

Проинспектируйте пользователей с высоким риском ↻ Количество: 2 Важность: ●

Проверьте обоснованность параметров и поведение пользователей Показать/скрыть список ▾

Проинспектируйте атипичных пользователей ↻ Количество: 2 Важность: ●

Проинспектируйте пользователей с высоким уровнем атипичности Показать/скрыть список ▾

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
www.facebook.com/Makves.ru