

SEARCHINFORM

# Шорт-лист задач для **ДСАР:**

с чем не справятся  
другие СЗИ

**Александр Янчук**

Заместитель генерального директора  
по СЗФО, УрФО, СФО и ДФО



# DSAR – СИСТЕМЫ ДЛЯ АУДИТА И ЗАЩИТЫ ДАННЫХ В ПОКОЕ. ЧТО ЭТО ЗНАЧИТ?

## В теории (по Gartner):

- Классификация данных.
- Хранение конфиденциальных данных.
- Управление безопасностью данных.
- Мониторинг и аудит данных.
- Защита всех данных от несанкционированного доступа и использования.

# НА ДЕЛЕ: В «СЁРЧИНФОРМ FILEAUDITOR»

## Классификация конфиденциальных данных

Находит в общем документообороте файлы, которые содержат критичную информацию, и присваивает каждому метку определенного типа: персональные данные, коммерческая тайна, номера кредитных карт и т.д.

## Аудит прав доступа

Облегчает контроль за доступом к уязвимой информации – автоматически отслеживает открытые ресурсы, файлы, доступные конкретному пользователю или группе, учетные записи с привилегированными правами.

## Архивирование критичных документов

Делает теньевые копии критичных файлов, найденных на ПК, сервере или в сетевых папках и сохраняет историю их редакций. Архив критичных данных помогает в расследованиях инцидентов и гарантирует восстановление потерянной информации.

## Контроль и блокировки действий пользователей

Производит аудит пользовательских операций в файловой системе. ИБ-служба всегда в курсе актуальной информации о «жизни» файла (создание, редактирование, перемещение, удаление и т.д.). Блокирует нежелательную активность с файлами в любом произвольном приложении.

# ПО СУТИ

SEARCHINFORM

**FileAuditor** отвечает на важные вопросы внутренней информационной безопасности:



Какие документы содержат критичную для бизнеса информацию?



Сколько в компании таких данных и где они находятся?

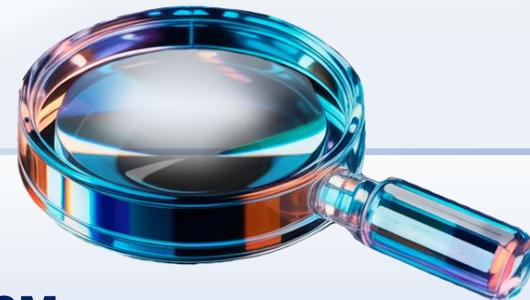


Кто имеет к ним доступ и может их редактировать?

**И позволяет всем этим управлять.**



# ЧТО ИСКАТЬ В ПЕРВУЮ ОЧЕРЕДЬ?



Персональные данные (152-ФЗ для всех, иначе – «оборотка»)



Информацию из критичных систем



Финансовые данные



Все о клиентах (договоры, клиентские базы, КП)



Коммерческую тайну –  
*задача со звездочкой\**

# 450+

правил уже готовы «из коробки»,  
достаточно включить

SEARCHINFORM

# КАК ОПРЕДЕЛИТЬ, ГДЕ КОМТАЙНА?

## Проблема:

Что относится к КТ – решение конкретных людей.

## Решение:

### Ручные метки классификации в FileAuditor

- Автор/рецензент документа ставит метку сам
- Уровень конфиденциальности виден сразу – это выполняет требования к обеспечению режима КТ
- Система автоматически перепроверит, верно ли поставили ручную метку

The screenshot shows a Microsoft Word document titled 'Бизнес-план.docx'. The ribbon is set to 'Главная' (Home). A 'Метка классификатора' (Classification Label) pane is open, showing that the document is classified as 'Коммерческая тайна' (Commercial Secret). The main content of the document is a table with the following data:

Коммерческая тайна	
3	
<b>1. Резюме проекта</b>	
Вид деятельности по ОКВЭД (код и наименование)	14.19.21. - Производство одежды и аксессуаров одежды для детей младшего возраста из текстильных материалов, кроме трикотажных или вязаных
ИНН	3905308238
Суть проекта	Открытие фабрики по пошиву детской одежды
Адрес места реализации проекта	Солнечная область, Радостный район, ул. Весёлая, д. 2
Статус помещения (в собственности, планируется аренда, передано в безвозмездное пользование и т. д.)	Имеется договоренность с собственником помещения об аренде на 48 месяцев, начиная с марта 2025 года
Организационно-правовая форма бизнеса	Общество с ограниченной ответственностью с 12.02.2022 г.
Планируемый к применению налоговый режим	Общая система налогообложения
Цель реализации проекта	Бизнес-план разработан для заключения социального контракта для получения государственного займа
Общая стоимость проекта (в том числе средства по социальному контракту, собственные средства, заемные средства)	28 000 000 руб., в том числе: 10 000 000 руб. - собственные средства 10 000 000 руб. - средства, планируемые к получению на основании заключения социального контракта 8 000 000 руб. - заемные средства
Срок окупаемости проекта (общая стоимость проекта) / чистая прибыль в месяц	48 месяцев

At the bottom of the window, the status bar shows: Страница 3 из 11, Число слов: 2108, русский, 84%.

# КАК ЗАЩИТИТЬ КРИТИЧНОЕ?

SEARCHINFORM

Ни NAS, ни сетевые папки, ни управление через AD не используют контент-зависимые признаки при назначении прав.

Но важны не «все документы PDF», а «все договоры с клиентами»!

## «Классическое» распределение доступа:

- права по пользователям/группам
- зависит от атрибутов
- не учитывает ценность
- **не исключает риски**



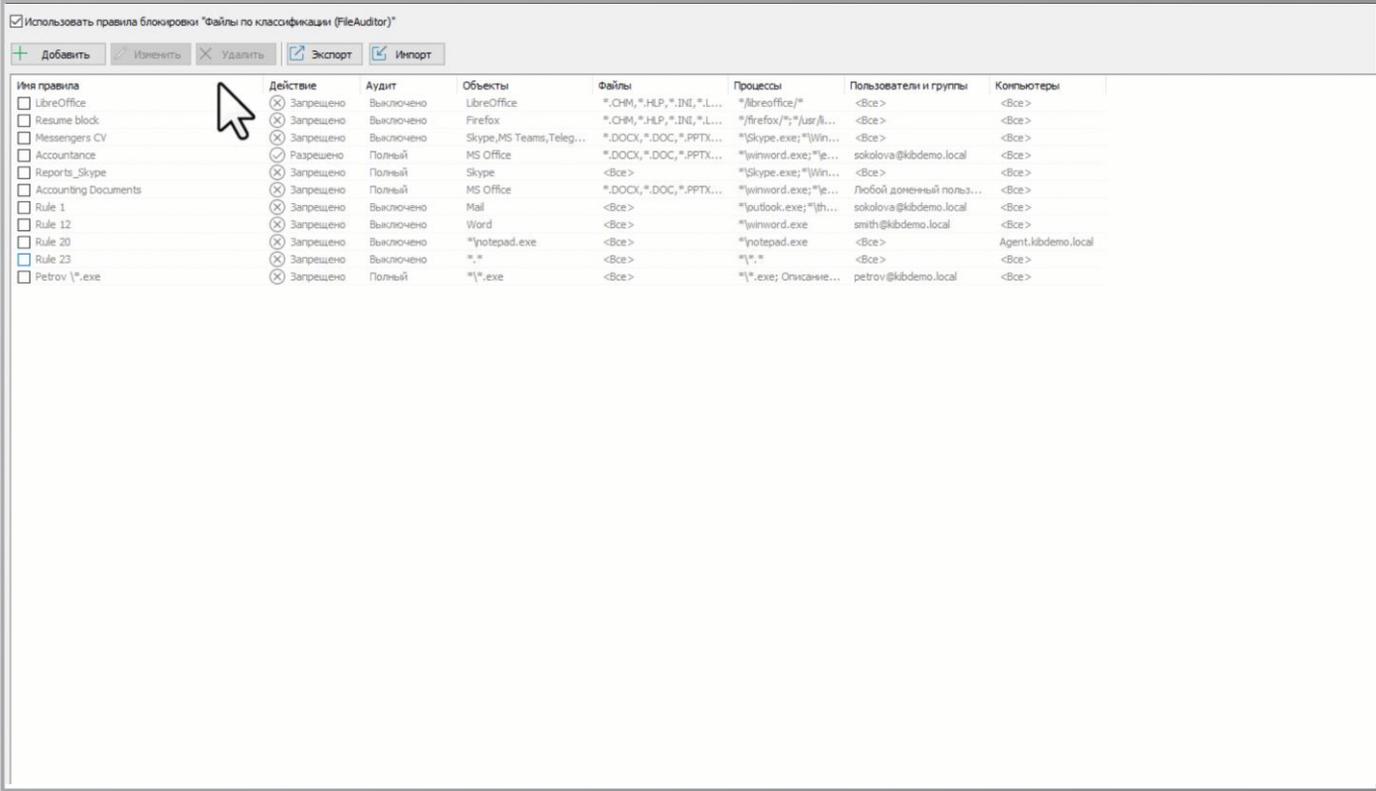
# КАК РАБОТАЕТ КОНТЕНТНОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА

## В FileAuditor:

- Блокировки доступа настраиваются по меткам классификации
- Метка остается на документе, пока в нем есть конфиденциальный контент = блокировка продолжает действовать
- Запрет нежелательных вариантов обработки документа

*Например: нельзя открывать в редакторе, прикреплять в почтовом клиенте/мессенджере и др.*

**Это работает для любого процесса**



Использовать правила блокировки "Файлы по классификации (FileAuditor)"

Добавить Изменить Удалить Экспорт Импорт

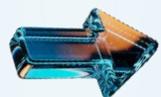
Имя правила	Действие	Аудит	Объекты	Файлы	Процессы	Пользователи и группы	Компьютеры
<input type="checkbox"/> LibreOffice	<input checked="" type="checkbox"/> Запрещено	Выключено	LibreOffice	*.ODM,*.HLP,*.DWG,*.L...	*libreoffice/*	<Все>	<Все>
<input type="checkbox"/> Resume block	<input checked="" type="checkbox"/> Запрещено	Выключено	Firefox	*.ODM,*.HLP,*.DWG,*.L...	*firefox/*;*/usr/li...	<Все>	<Все>
<input type="checkbox"/> Messengers CV	<input checked="" type="checkbox"/> Запрещено	Выключено	Skype,MS Teams,Teleg...	*.DOCX,*.DOC,*.PPTX...	*skype.exe;*Win...	<Все>	<Все>
<input type="checkbox"/> Accountance	<input checked="" type="checkbox"/> Разрешено	Польный	MS Office	*.DOCX,*.DOC,*.PPTX...	*winword.exe;*le...	sokolova@kibdemo.local	<Все>
<input type="checkbox"/> Reports_Skype	<input checked="" type="checkbox"/> Запрещено	Польный	Skype	<Все>	*skype.exe;*Win...	<Все>	<Все>
<input type="checkbox"/> Accounting Documents	<input checked="" type="checkbox"/> Запрещено	Польный	MS Office	*.DOCX,*.DOC,*.PPTX...	*winword.exe;*le...	Любой доменный поль...	<Все>
<input type="checkbox"/> Rule 1	<input checked="" type="checkbox"/> Запрещено	Выключено	Mail	<Все>	*outlook.exe;*th...	sokolova@kibdemo.local	<Все>
<input type="checkbox"/> Rule 12	<input checked="" type="checkbox"/> Запрещено	Выключено	Word	<Все>	*winword.exe	smith@kibdemo.local	<Все>
<input type="checkbox"/> Rule 20	<input checked="" type="checkbox"/> Запрещено	Выключено	*notepad.exe	<Все>	*notepad.exe	<Все>	Agent.kibdemo.local
<input type="checkbox"/> Rule 23	<input checked="" type="checkbox"/> Запрещено	Выключено	*.*	<Все>	*.*	<Все>	<Все>
<input type="checkbox"/> Petrov \*.exe	<input checked="" type="checkbox"/> Запрещено	Польный	*\*.exe	<Все>	*\*.exe; Описание...	petrov@kibdemo.local	<Все>

# КОНТРОЛЬ «СЛЕПЫХ ЗОН»

SEARCHINFORM

**DCAP** – универсальное средство, чтобы защитить файлы в любом канале, который не защищен другими СЗИ.

## Например:



Контроль пользовательского ПО и сервисов



DLP не работает с этим каналом

Вы можете настроить точечную блокировку в FileAuditor:

«в **ЭТОМ** процессе вот **ЭТИ** файлы открыть нельзя».

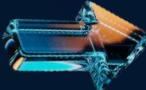
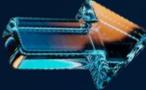
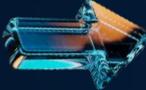


# ЦЕНТРАЛИЗАЦИЯ АУДИТА AD

SEARCHINFORM

Нет единых систем аудита пользовательской активности!

## DCAP:

-  **Локальные операции** через собственный драйвер для разных ОС
-  **Права доступа** для всех СХД, ОС и иных хранилищ
-  **Журналы Контроллеров домена** на случай сетевой работы

Это позволяет применять **ЕДИНЫЕ** правила аудита для разрозненных систем



# СИНХРОНИЗАЦИЯ НАСТРОЕК ДОСТУПА

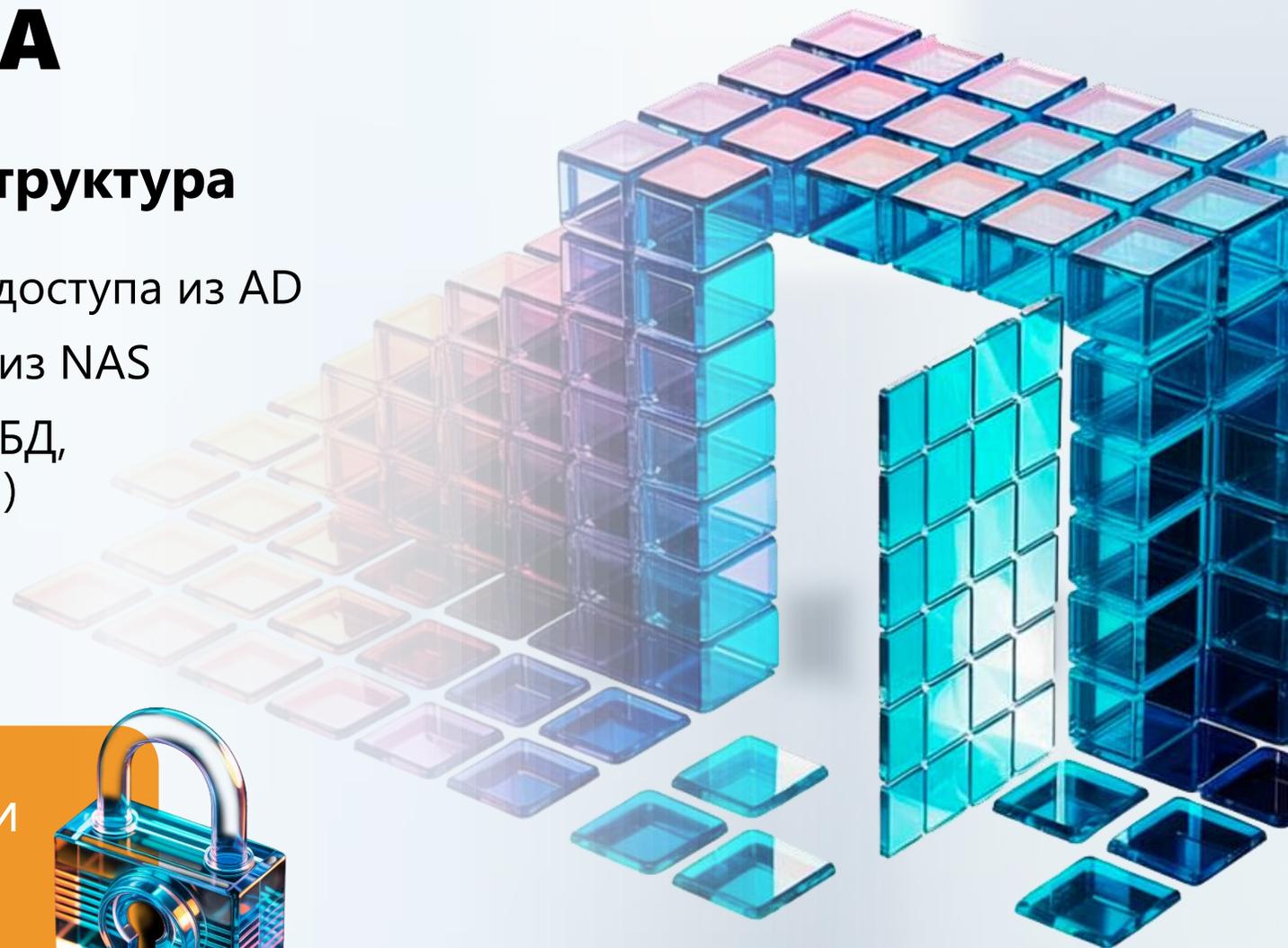
SEARCHINFORM

## Кейс: распределенная инфраструктура

- в локальных хранилищах настройки доступа из AD
- в сетевых папках настройки доступа из NAS
- свои настройки в разных «облаках», БД, критичных системах (например, CRM)

Синхронизировать вручную долго и не всегда возможно.

**DCAP** применяет свои настройки одновременно и одинаково **в любых источниках.**



# ОБЪЕДИНЕНИЕ СЗИ

SEARCHINFORM

Средства защиты работают с файлами по-разному:



Антивирусы



DLP



Средства классификации  
(MS Information Protection и др.)



EveryTag и аналоги



Средства шифрования

**DCAP** «видит» результаты работы разных СЗИ с файлами и позволяет ИБ-специалисту разобраться и **управлять ими в одном окне.**

# БОНУС: «РАЗГРУЗКА» СЗИ

SEARCHINFORM

DCAP снимает нагрузку с других средств защиты информации за счет ускорения контентного анализа.

## Кейс: работа с DLP

- DCAP классифицировал файл по контенту
- DLP не нужно вычитывать файл повторно, чтобы понять, что внутри
- Для сработки политики DLP требуется меньше времени и ресурсов на анализ

The screenshot displays the SEARCHINFORM application interface. At the top, there are navigation tabs: Поиск, Текущая активность, Отчеты, Карта расположения сотрудников, Карточки пользователей, Файловый аудитор, Профайл центр, Карантин, and Task Management. Below the navigation is a search bar with 'Поиск 2', 'Поиск 3', and 'Поиск 4' tabs. The main area shows a table of search results with columns: #, Тип, Тип файла, Дата/Время, Тема, От кого, Кому, Домен, Копы, Пользователь, Размер, Участники, Сообщений, and Метки ручной классификации данных. The table contains several rows of data, with one row highlighted in blue. Below the table is a preview of a document titled 'Заявка на поставку сувенирной продукции'. The document content includes the text 'Для служебного пользования' and contact information for 'ОАО «Интрейд»' and 'ООО «Цветок»'. The interface also shows various filters and settings on the left side, including 'Метки ручной классификации данных' and 'Метки автоматической классификации данных'.

#	Тип	Тип файла	Дата/Время	Тема	От кого	Кому	Домен	Копы	Пользователь	Размер	Участников	Сообщений	Метки ручной классификации данных
			07.08.2025 10:25:40	Отчет_2025.docx...	администрато...	Мах...	kbde...	age...	админис...	190 KB	2		Коммерческая тайна
			07.08.2025 10:25:40	Служебная запис...	администрато...	Мах...	kbde...	age...	админис...	71,9 KB	2		Для служебного пользования
			07.08.2025 10:25:40	База клиентов.xls...	администрато...	Мах...	kbde...	age...	админис...	11,5 KB	2		Общедоступно
			07.08.2025 10:26:12	ДСП.docx->ДСП.d...	администрато...	Мах...	kbde...	age...	админис...	42,8 KB	2		Для служебного пользования
			07.08.2025 10:26:12	Служебная запис...	администрато...	Мах...	kbde...	age...	админис...	71,9 KB	2		Для служебного пользования
			07.08.2025 10:26:12	База клиентов.xls...	администрато...	Мах...	kbde...	age...	админис...	11,5 KB	2		Общедоступно
			07.08.2025 10:26:12	Отчет_2025.docx...	администрато...	Мах...	kbde...	age...	админис...	190 KB	2		Коммерческая тайна
			07.08.2025 10:26:13	заявка на постав...	администрато...	Мах...	kbde...	age...	админис...	199 KB	2		Для служебного пользования
			07.08.2025 10:26:13	Отчет.docx->Отч...	администрато...	Мах...	kbde...	age...	админис...	42,3 KB	2		Для служебного пользования
			08.12.2024 15:35:22	договор с гармон...	Александр Пет...	.cid...	kbde...	age...	Алексан...	26,8 KB	2		Строго конфиденциально
			09.12.2024 10:22:50	договор с гармон...	Александр Пет...	c82f...	kbde...	age...	Алексан...	26,8 KB	2		Строго конфиденциально
			08.12.2024 15:35:22	договор с гармон...	Александр Пет...	.cid...	kbde...	age...	Алексан...	26,8 KB	2		Строго конфиденциально
			09.12.2024 10:22:50	договор с гармон...	Александр Пет...	c82f...	kbde...	age...	Алексан...	26,8 KB	2		Строго конфиденциально

Страница: 1/1

Для служебного пользования

Кому: ОАО «Интрейд»  
Директору Климкину С.Р.  
От ООО «Цветок»  
г. Тверь, ул. Белая, д. 35, оф.9  
т. 8 (567) 63-87-69  
01.10.2024 г.

**ЗАЯВКА**  
на поставку сувенирной продукции

Выделенные строки: 1  
Время отбора: 9 сек.

# УМНЫЙ БЭКАП

SEARCHINFORM

Нет систем бэкапирования, которые работают на основе реальной ценности данных: только по директориям, атрибутам файлов.

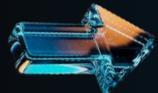
## ДСАР:

- ➔ **Сохраняет** теневые копии **критичных документов** на основе контента
- ➔ **Защищает** от нежелательных изменений и удалений по вине пользователей
- ➔ **Страхует** на случай атаки шифровальщика
- ➔ **Экономит** ресурс:
  - можно бэкапировать выборочно – классы и конкретные документы
  - хранится нужное число редакций
  - работает дедупликация



# БОНУС: ОПТИМИЗАЦИЯ ХРАНЕНИЯ

DCAP анализирует объемы хранения и обращения к данным. С ним можно:

-  **Найти «файловый мусор»:**  
неиспользуемые, неактуальные документы и др.
-  **Найти дубликаты:**  
нежелательные копии, шаблоны, «ползучие бэкапы», повторные скачивания и др.
-  **Составить статистику хранения**  
тяжелых данных (например, медиа),  
которые не нужны в работе

На основе анализа делаете очистку – высвобождаете дорогое место в СХД.

Как мы сами  
«разгребали»  
СХД с FileAuditor



# СПАСИБО ЗА ВНИМАНИЕ!

SEARCHINFORM



<https://t.me/searchinform>



[https://vk.com/  
securityinform](https://vk.com/securityinform)

ПРАКТИКА И АНАЛИТИКА



[https://searchinform.ru/  
practice-and-analytics/](https://searchinform.ru/practice-and-analytics/)