

SEARCHINFORM

# Шорт-лист задач для DCAP: с чем не справляются другие СЗИ

Дмитрий Софронов

Менеджер по работе с клиентами и  
партнёрами «СёрчИнформ»



# DCAP – 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.

## Архивирование критических документов

Делает теневые 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.

## 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.

## 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.

**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»)



Финансовые данные



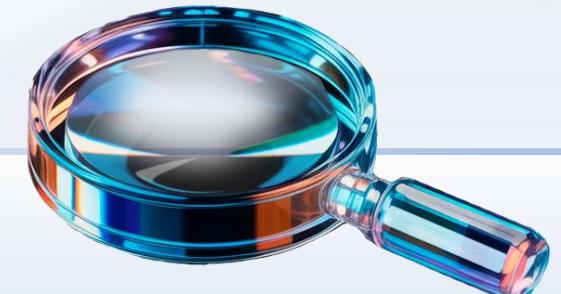
Все о клиентах (договоры,  
клиентские базы, КП)



Коммерческую тайну –  
*задачка со звездочкой\**



Информацию  
из критичных систем



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 menu is visible with tabs like Файл, Главная, Вставка, Конструктор, Макет, Ссылки, Рассылка, Рецензи, Вид, Справка, Конструктор таблиц, Макет, Помощник, and Вход. The "Вставка" tab is selected. In the ribbon, there is a "Метка классификатора" section with icons for different classification levels: Для служебно..., Коммерческого..., Бухгалтерского..., Общедоступного..., Новая метка 10 метки, and Стили. The "Коммерческая тайна" icon is highlighted. A status bar at the bottom indicates "Документу присвоена метка: Коммерческая тайна". The main content area displays a table titled "Коммерческая тайна" with one row labeled "1. Резюме проекта". The table contains various project details, such as "Вид деятельности по ОКВЭД (код и наименование)" and "ИИНН". The entire document is marked with a large watermark reading "Коммерческая тайна".

# 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

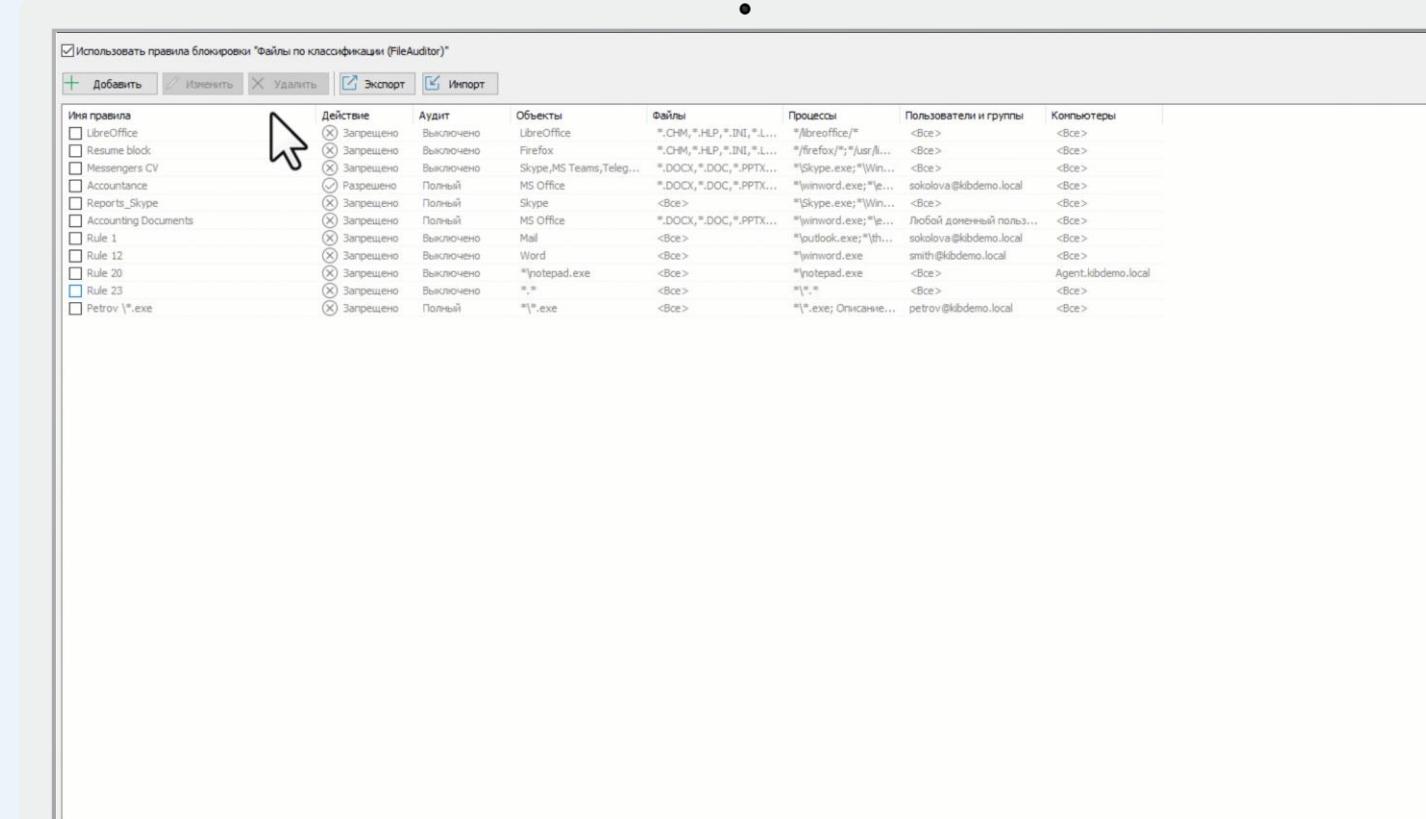
SEARCHINFORM

## 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



The screenshot shows a software interface for managing file classification rules. At the top, there's a toolbar with buttons for 'Добавить' (Add), 'Изменить' (Edit), 'Удалить' (Delete), 'Экспорт' (Export), and 'Импорт' (Import). A checked checkbox says 'Использовать правила блокировки "Файлы по классификации (FileAuditor)"' (Use blocking rules for 'Files by Classification (FileAuditor)'). Below the toolbar is a table with columns: 'Имя правила' (Rule Name), 'Действие' (Action), 'Аудит' (Audit), 'Объекты' (Objects), 'Файлы' (Files), 'Процессы' (Processes), 'Пользователи и группы' (Users and groups), and 'Компьютеры' (Computers). The table lists various rules, such as LibreOffice, Firefox, Skype, MS Office, Mail, Word, Notepad, and a specific rule for 'Petrov \\*.exe'. Most rules have 'Запрещено' (Blocked) in the 'Действие' column, while one has 'Разрешено' (Allowed). Audit status is shown as 'Выключено' (Disabled) or 'Включен' (Enabled). The 'Файлы' column lists file extensions like '.OIM', '.HLP', '.INI', etc. The 'Процессы' column lists processes like 'firefox.exe', 'winword.exe', etc. The 'Пользователи и группы' column lists users like 'sokolova@kibdemo.local' and 'smith@kibdemo.local'. The 'Компьютеры' column lists computer names like 'Agent.kibdemo.local'.

Имя правила	Действие	Аудит	Объекты	Файлы	Процессы	Пользователи и группы	Компьютеры
LibreOffice	Запрещено	Выключено	LibreOffice	*.OIM, *.HLP, *.INI, *...	*libreoffice/*	<Все>	<Все>
Resume block	Запрещено	Выключено	Firefox	*.OIM, *.HLP, *.INI, *...	*firefox/*;/usr/li...	<Все>	<Все>
Messengers CV	Запрещено	Выключено	Skype, MS Teams, Telegram	*.DOCX, *.DOC, *.PPTX, ...	*Skype.exe; *Win...	<Все>	<Все>
Accountance	Разрешено	Полный	MS Office	*.DOCX, *.DOC, *.PPTX, ...	*winword.exe; *le...	sokolova@kibdemo.local	<Все>
Reports_Skype	Запрещено	Полный	Skype	<Все>	*Skype.exe; *Win...	<Все>	<Все>
Accounting Documents	Запрещено	Полный	MS Office	*.DOCX, *.DOC, *.PPTX, ...	*winword.exe; *le...	любой доменный польз...	<Все>
Rule 1	Запрещено	Выключено	Mail	<Все>	*outlook.exe; *th...	sokolova@kibdemo.local	<Все>
Rule 12	Запрещено	Выключено	Word	<Все>	*winword.exe	smith@kibdemo.local	<Все>
Rule 20	Запрещено	Выключено	*notepad.exe	<Все>	*notepad.exe	<Все>	Agent.kibdemo.local
Rule 23	Запрещено	Выключено	*, *	<Все>	**, *	<Все>	<Все>
Petrov \*.exe	Запрещено	Полный	*\*.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

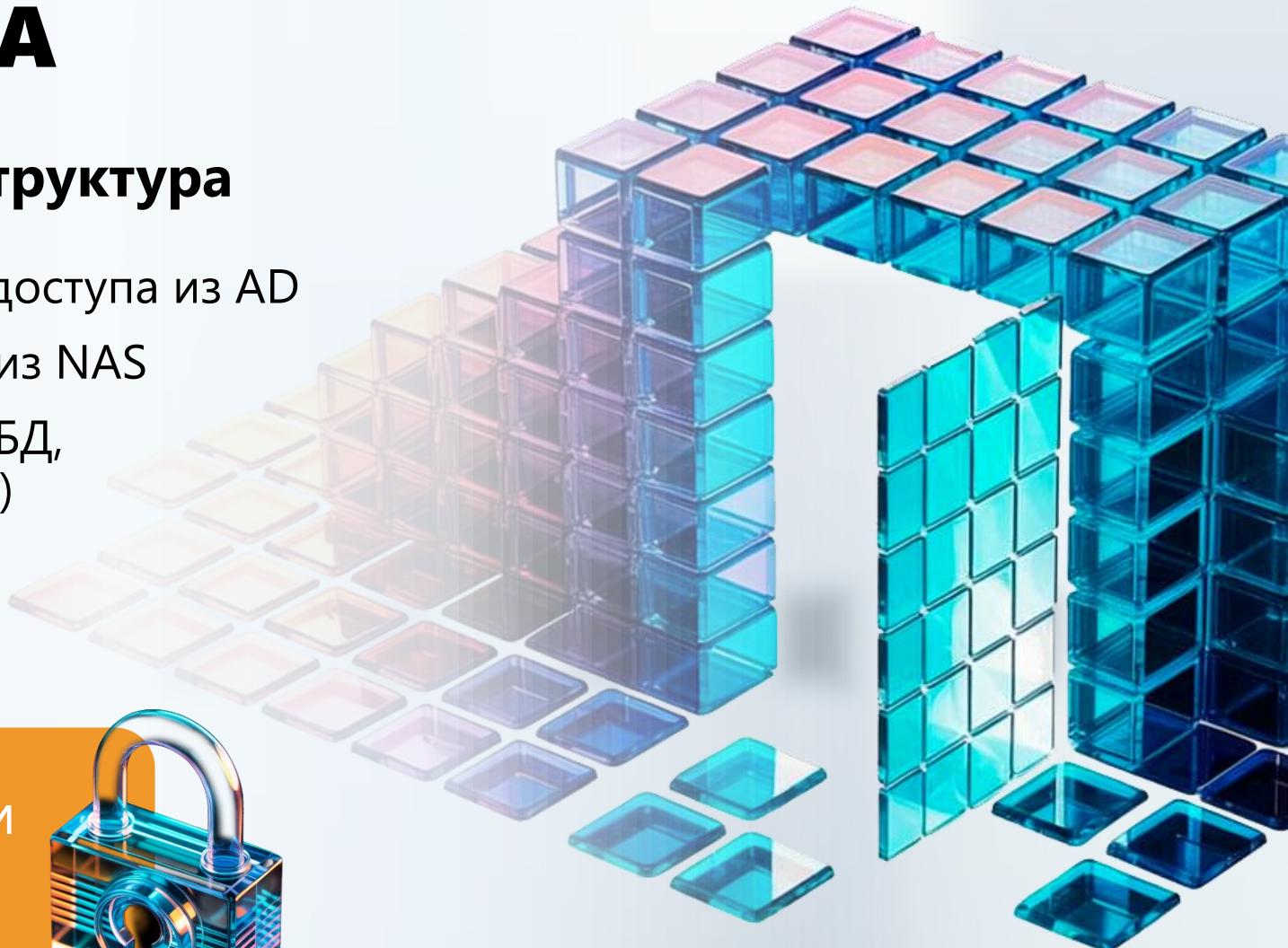
SEARCHINFORM

## 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**.



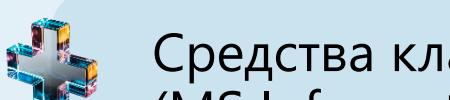
**Средства защиты работают  
с файлами по-разному:**



Антивирусы



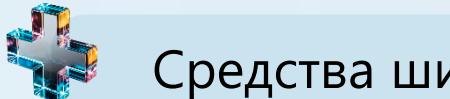
DLP



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 shows the SEARCHINFORM Task Management application interface. The main window displays a search results grid with columns: Тип (Type), Тип файла (File type), Дата/Время (Date/Time), Тема (Subject), От кого (From), Кому (To), Домен (Domain), Компания (Company), Пользователе (User), Размер (Size), Участников (Participants), Сообщений (Messages), and Метки ручной классификации данных (Manual classification data tags). A specific row in the grid is highlighted, showing a file named 'заявка на постав...', which is classified as 'For service use' (red icon).

On the left side, there is a sidebar with two sections: 'Метки ручной классификации данных' (Manual classification data tags) and 'Метки автоматической классификации данных' (Automatic classification data tags). The 'Метки ручной классификации данных' section contains several checked items, including 'Строго конфиденциально' (Confidential), 'Для служебного пользования' (For service use), 'Секретно' (Secret), 'Бухгалтерия' (Accounting), 'Общедоступно' (Public), 'Коммерческая тайна' (Commercial secret), and several new tags like 'Новая метка 8', 'Новая метка 9', and 'Новая метка 10'. The 'Метки автоматической классификации данных' section lists various rules and documents, such as 'Resume', 'StarForce Rule', 'Банковская карта', 'Банковские реквизиты со...', 'ДСП документ', 'Клиентские базы', 'Коммерческое предложение', 'Мобильные телефоны РФ...', 'Скрытые слои в PDF', 'Классификатор изображений', and 'МДС'.

At the bottom right, a detailed view of the document 'заявка на постав...' is shown. The document header includes 'Для служебного пользования' (For service use), 'Кому: ОАО «Интрайд»', 'Директору Климкину С.Р.', 'От ООО «Цветок»', 'г. Тверь, ул. Белая, д. 35, оф.9', 'т. 8 (567) 63-87-69', and the date '01.10.2024 г.'. The body of the document reads 'ЗАЯВКА на поставку сувенирной продукции'.

# УМНЫЙ БЭКАП

SEARCHINFORM

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

## DCAP:

- 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/)