

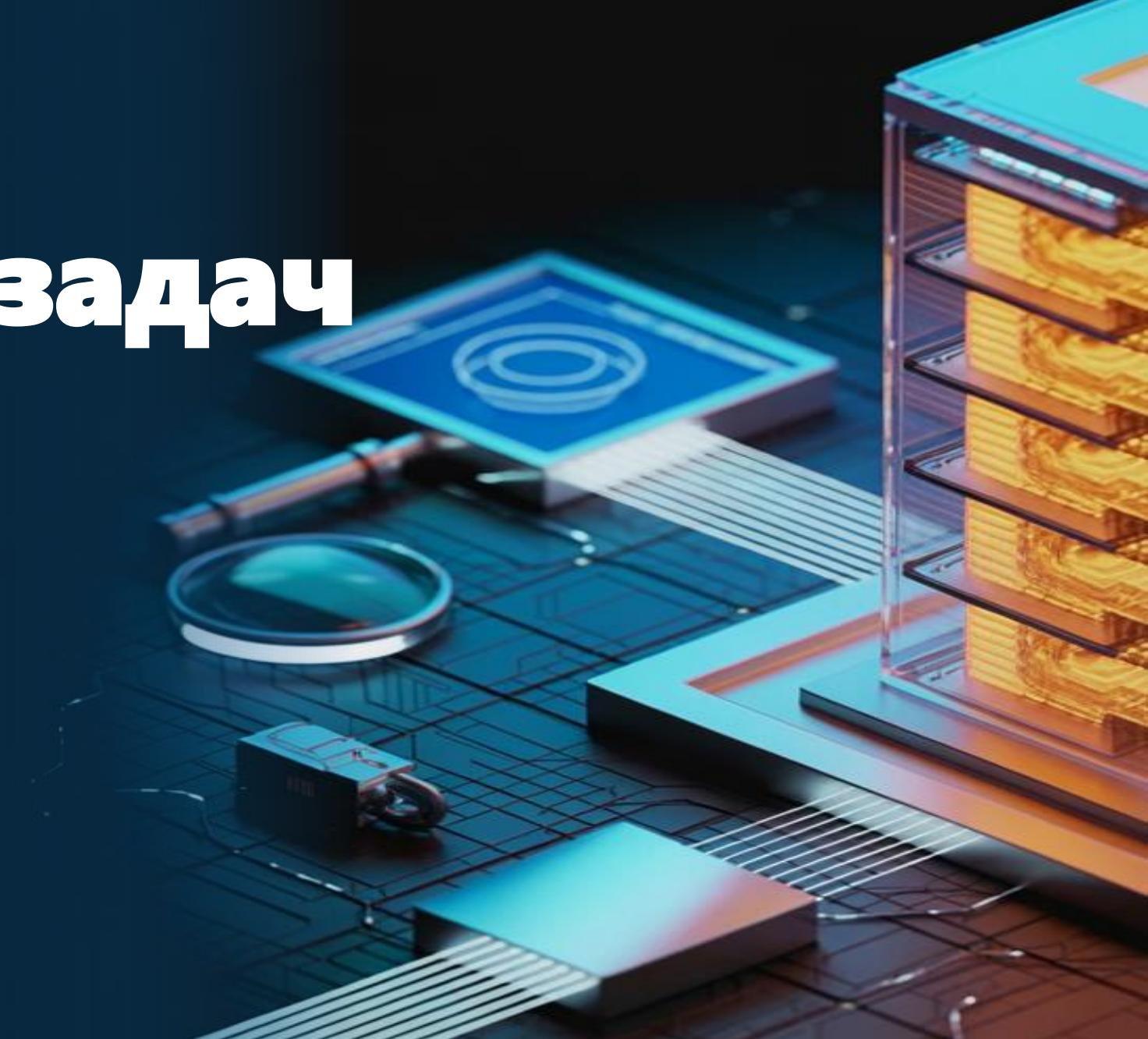
SEARCHINFORM

Шорт-лист задач для DCAP:

с чем не справляются
другие СЗИ

Никита Фарзалиев

менеджер по работе с клиентами
«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.

SEARCHINFORM

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



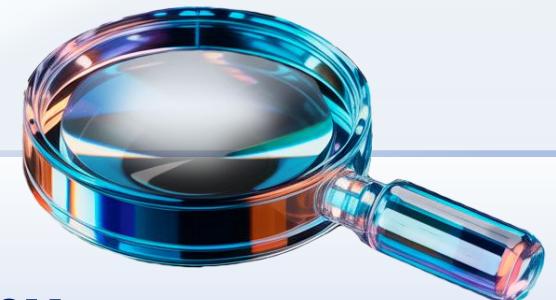
Все о клиентах (договоры,
клиентские базы, КП)



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 at the top. In the "Вставка" tab, there is a "Метка классификатора" section containing several shield icons with different colors and labels: "Коммерческая тайна" (orange), "Бухгалтерия" (red), "Общедоступная" (green), "Новая метка 10 метки" (yellow), and "Все метки" (blue). Below this, a message says "Документу присвоена метка: Коммерческая тайна". A preview window titled "Коммерческая тайна" displays the first page of the document, which is a business plan summary. The page contains several table rows with various project details.

1. Резюме проекта	
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

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

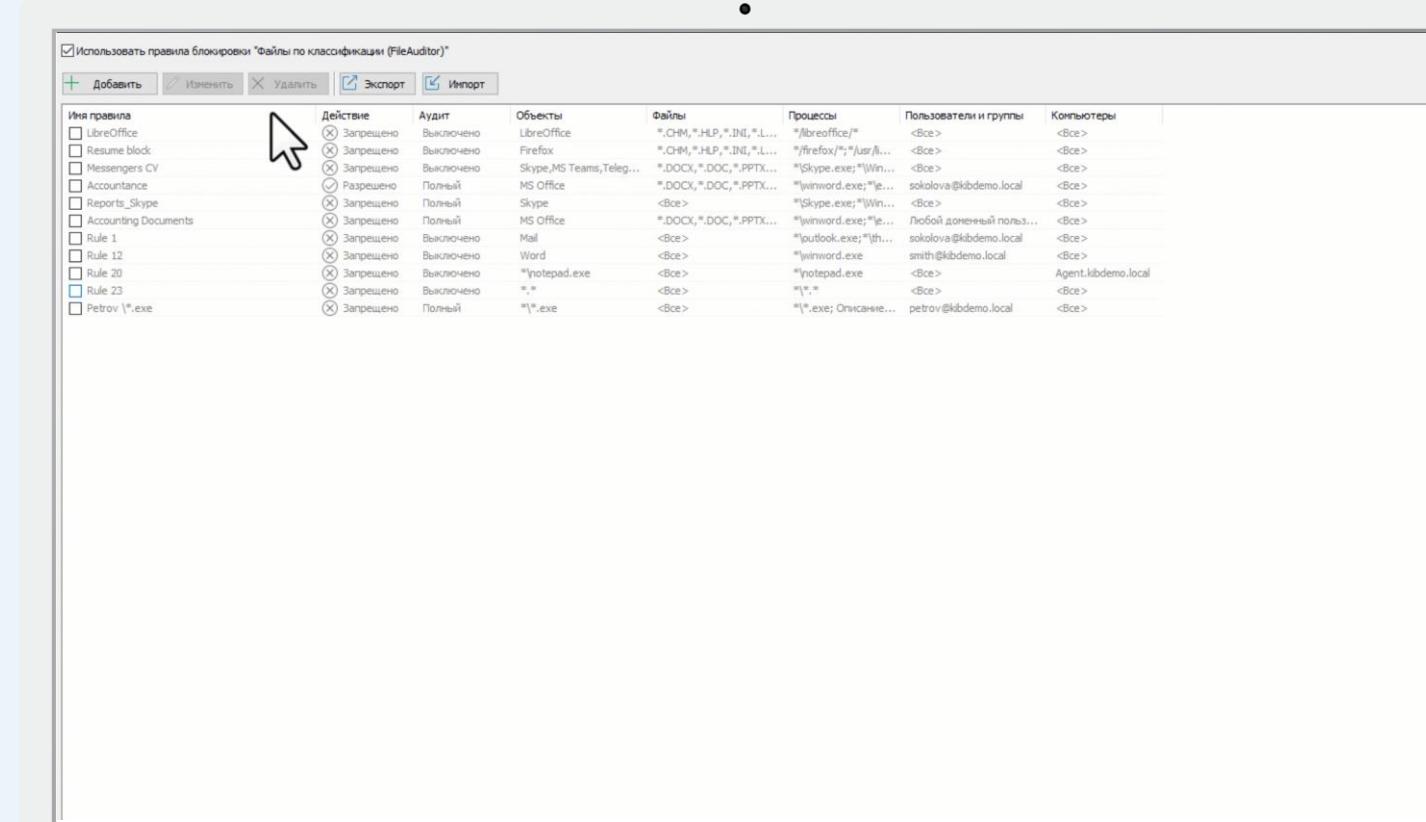
SEARCHINFORM

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 access controls. 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 блокировок "Файлы по классификации (FileAuditor)"' (Use rules for blocking "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, and different file types like .DOCX, .DOC, .PPTX, etc. Each row shows whether the action is 'Запрещено' (Blocked) or 'Разрешено' (Allowed). A cursor is pointing at the 'Action' column header. The data is as follows:

Имя правила	Действие	Аудит	Объекты	Файлы	Процессы	Пользователи и группы	Компьютеры
LibreOffice	Запрещено	Выключено	LibreOffice	*.OIM, *.HLP, *.INI, *.L...	"/libreoffice/*"	<Все>	<Все>
Resume block	Запрещено	Выключено	Firefox	*.OIM, *.HLP, *.INI, *.L...	"/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; "/e...	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; "/e...	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

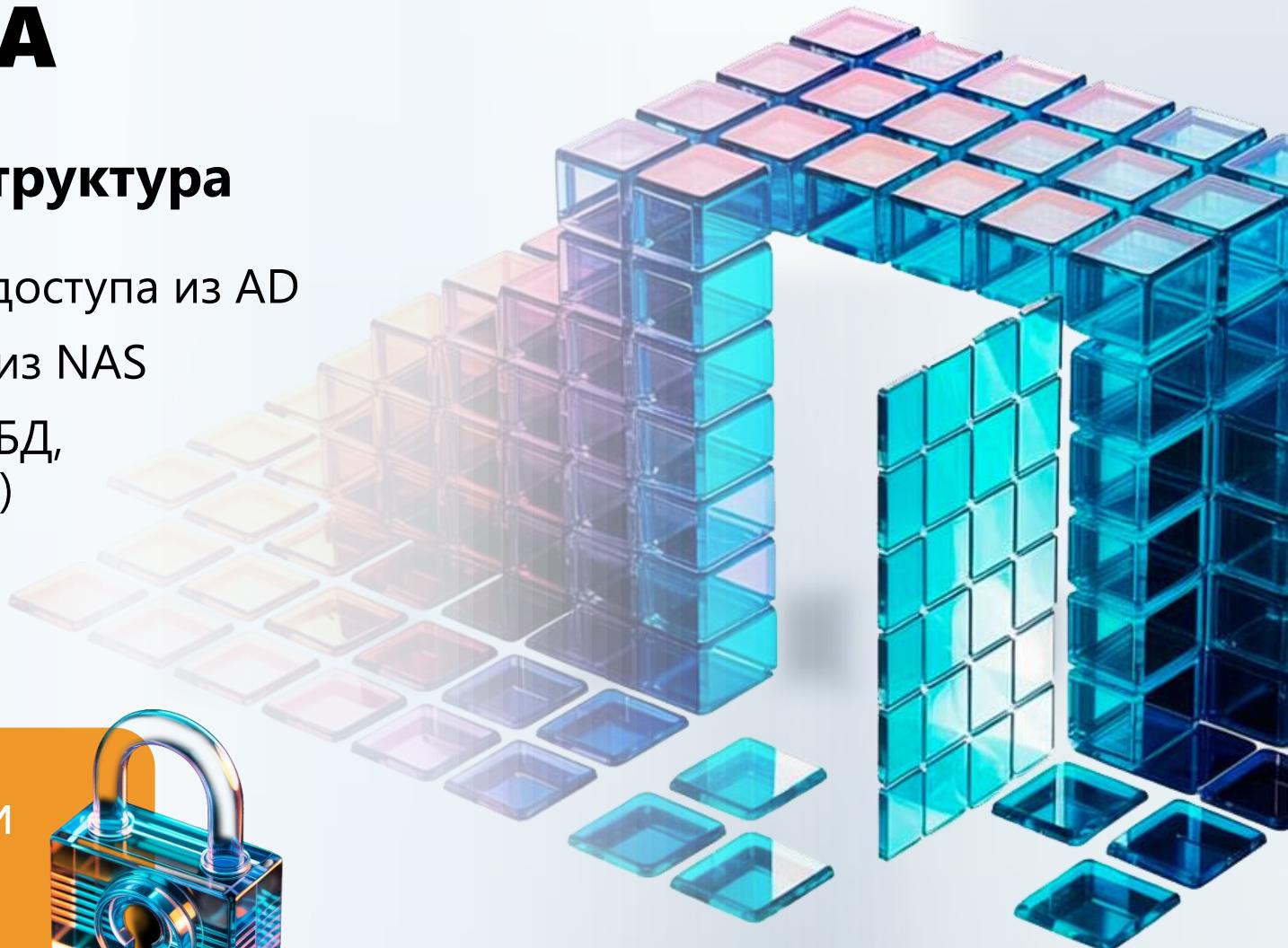
SEARCHINFORM

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.



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 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 sections for 'Метки' (Tags) and 'Метки автоматической классификации данных' (Automatic classification data tags). Under 'Метки' are categories like 'Без метки' (No tag), 'Строго конфиденциально' (Confidential), 'Для служебного пользования' (For service use), 'Секретно' (Secret), 'Для служебного пользования' (For service use), 'Бухгалтерия' (Accounting), 'Общедоступно' (Public), 'Коммерческая тайна' (Commercial secret), 'Новая метка 8' (New tag 8), 'Новая метка 9' (New tag 9), and 'Новая метка 10' (New tag 10). Under 'Метки автоматической классификации данных' are listed: 'Resume', 'StarForce Rule', 'Банковская карта', 'Банковские реквизиты со...', 'ДСП документ', 'Клиентские базы', 'Коммерческое предложение', 'Мобильные телефоны РФ...', 'Скрытые слои в PDF', 'Классификатор изображений', and 'МД5'.

At the bottom right, a detailed view of the document 'заявка на постав...' is shown. It includes fields for 'Кому' (Recipient), 'От' (From), 'Тема' (Subject), and 'Сообщение' (Message). The subject is 'ЗАЯВКА на поставку сувенирной продукции'. Below the message area, it says 'Выделенные строки: 1' and 'Время отбора: 9 сек.'.

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/)