

SEARCHINFORM

Шорт-лист задач для **ДСАР:**

с чем не справятся
другие СЗИ

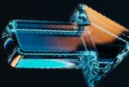
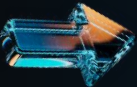
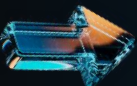
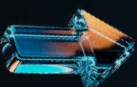
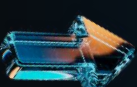
Дмитрий Софронов

Менеджер по работе с клиентами и
партнёрами «СёрчИнформ»



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 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.

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»)



Финансовые данные



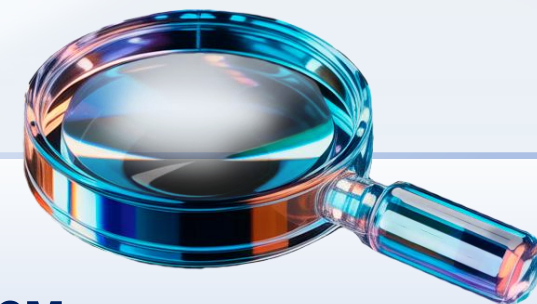
Все о клиентах (договоры, клиентские базы, КП)



Коммерческую тайну –
*задача со звездочкой**



Информацию
из критичных систем



450+

правил уже готовы «из коробки»,
достаточно включить

SEARCHINFORM

КАК ОПРЕДЕЛИТЬ, ГДЕ КОМТАЙНА?

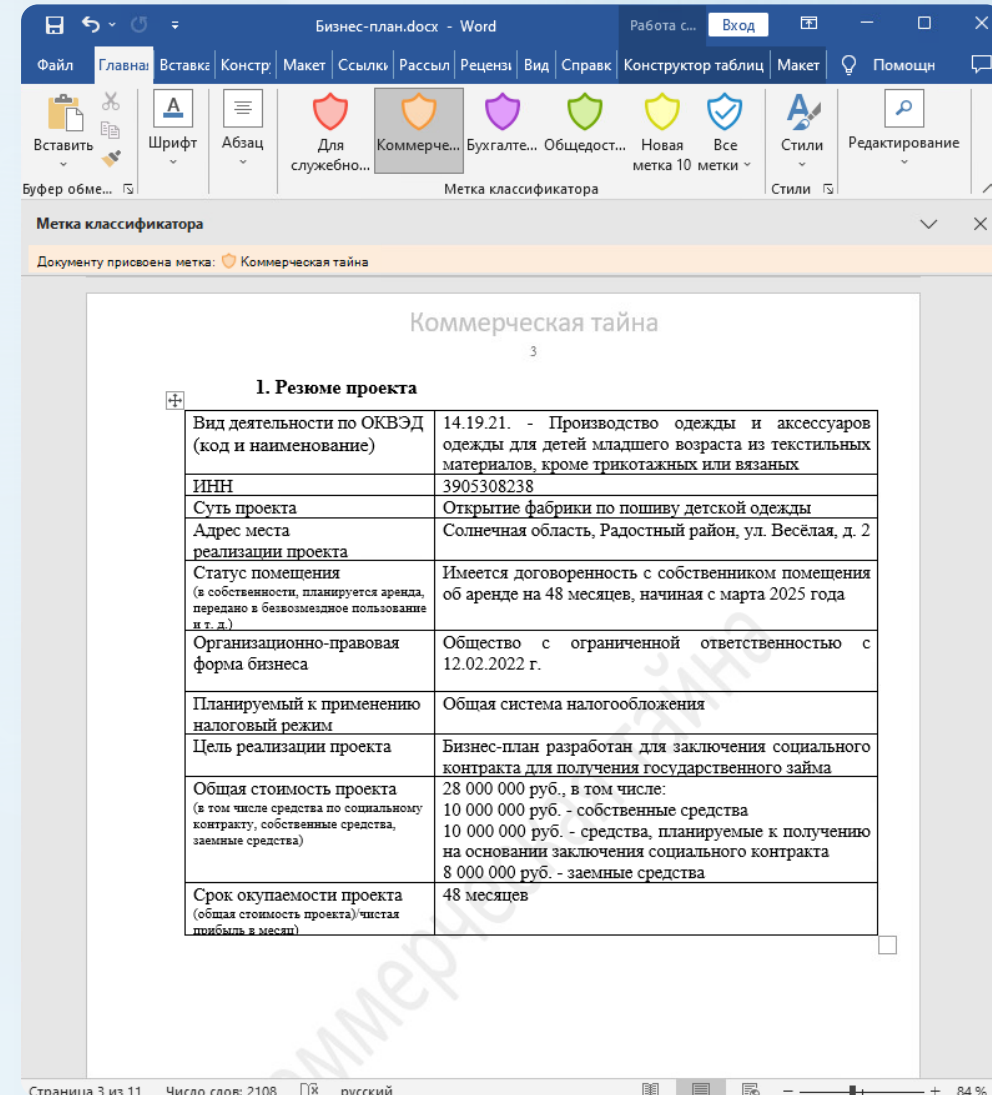
Проблема:

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



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

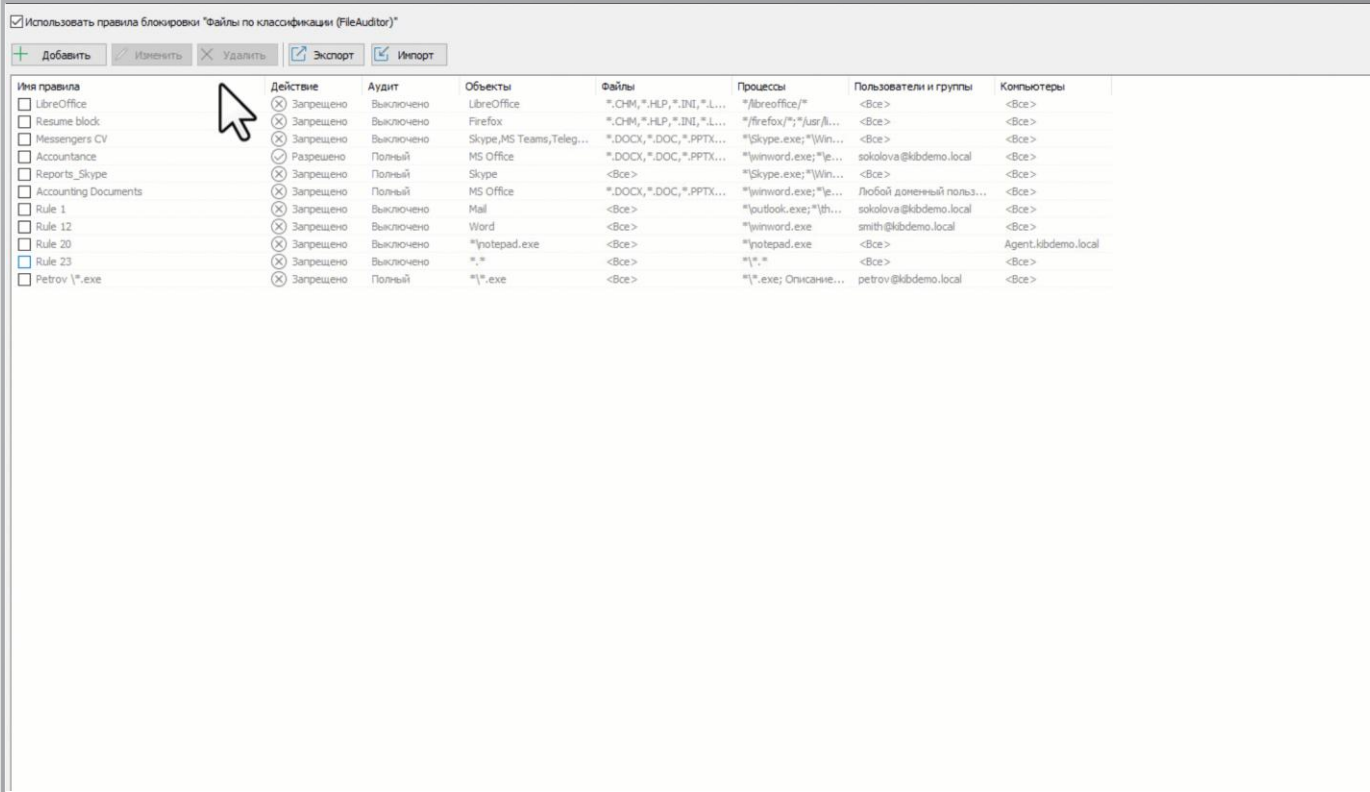
SEARCHINFORM

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



Использовать правила блокировки "Файлы по классификации (FileAuditor)"

Добавить Изменить Удалить Экспорт Импорт

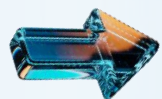
Имя правила	Действие	Аудит	Объекты	Файлы	Процессы	Пользователи и группы	Компьютеры
<input type="checkbox"/> LibreOffice	<input checked="" type="checkbox"/> Запрещено	Включено	LibreOffice	*.ODT, *.HLP, *.DOC, *.L...	*libreoffice/*	<Все>	<Все>
<input type="checkbox"/> Resume block	<input checked="" type="checkbox"/>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

КОНТРОЛЬ «СЛЕПЫХ ЗОН»

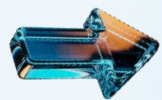
SEARCHINFORM

ДСАР – 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. The top navigation bar includes tabs for 'Поиск' (Search), 'Текущая активность' (Current activity), 'Отчеты' (Reports), 'Карта расположения сотрудников' (Employee location map), 'Карточки пользователей' (User cards), 'Файловый аудитор' (File auditor), 'Профайл центр' (Profile center), 'Карантин' (Quarantine), and 'Task Management'. The main window shows search results for 'Поиск 2', 'Поиск 3', and 'Поиск 4'. A table lists search results with columns for 'Тип' (Type), 'Дата/Время' (Date/Time), 'Тема' (Subject), 'От кого' (From), 'Кому' (To), 'Домен' (Domain), 'Копия' (Copy), 'Пользователь' (User), 'Размер' (Size), 'Участников' (Participants), 'Сообщений' (Messages), and 'Метки ручной классификации данных' (Manual data classification tags). The table shows several entries, with one entry highlighted in blue. Below the table, a document preview is shown, displaying a letterhead for 'ОАО «Интерейд»' (OJSC 'Interейd') and a request for 'ЗАЯВКА на поставку сувенирной продукции' (Application for supply of souvenir products). The interface also includes a sidebar with filters for 'Метки ручной классификации данных' and 'Метки автоматической классификации данных'.

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

Страница: 1/1

Для служебного пользования

Кому: ОАО «Интерейд»
Директору Климикину 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

Родной формат | Только текст | Атрибуты

Показано документов: 19 (19) | 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:

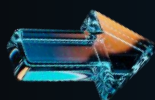
- ➡ **Сохраняет** теневые копии **критичных документов** на основе контента
- ➡ **Защищает** от нежелательных изменений и удалений по вине пользователей
- ➡ **Страхует** на случай атаки шифровальщика
- ➡ **Экономит** ресурс:
 - можно бэкапировать выборочно – классы и конкретные документы
 - хранится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



БОНУС: ОПТИМИЗАЦИЯ ХРАНЕНИЯ

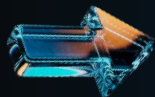
SEARCHINFORM

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



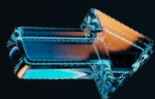
Найти «файловый мусор»:

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/)