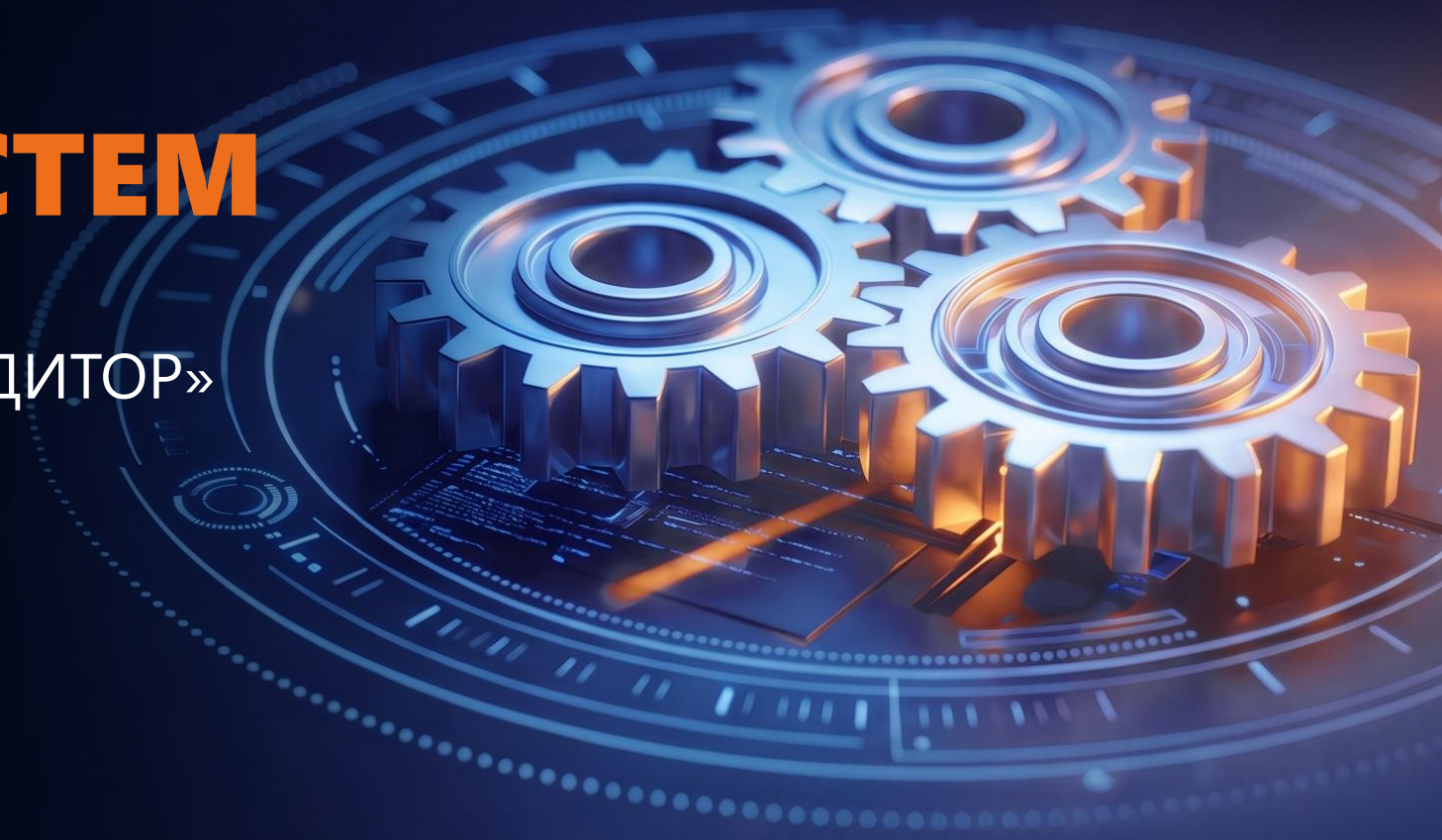
SEARCHINFORM

КОМПЛЕКС СИСТЕМ

«СЁРЧИНФОРМ КИБ» И
«СЁРЧИНФОРМ ФАЙЛОВЫЙ АУДИТОР»
(СЁРЧИНФОРМ FILEAUDITOR)



АКТУАЛЬНОСТЬ ПРОЕКТА

SEARCHINFORM

Приоритет цифровой трансформации организаций –
обеспечение защиты информации на всех стадиях обработки данных, в т.ч. в импортозамещенной и разнородной инфраструктуре



Нормативная база

Защита информации:

- Федеральные законы № 152-ФЗ от 27.07.2006, № 98-ФЗ от 29.07.2004 № 187-ФЗ от 26.07.2017
- Положения Банка России № 757-П, 851-П, 821-П
- ГОСТ Р 57580.1-2017

Импортозамещение:

- Указы Президента РФ № 166, № 250, № 309
- Федеральный закон № 58-ФЗ от 07.04.2025

Проблемы

Сохранение внутренних угроз ИБ:

- 2023 год – 80% финансовых организаций столкнулись с утечками информации *
- 2025 год - 56% финансовых организаций столкнулись с утечками информации*

Защита информации при импортозамещении:

- >60% организаций столкнулись с несовместимостью ПО*
- >30% организаций столкнулись с задачей перестройки ИТ-архитектуры*

* - по данным исследований «СёрчИнформ» о состоянии информационной безопасности в российских организациях в 2023, 2024, 2025 годах

ЗАДАЧИ СИСТЕМ:

SEARCHINFORM

Интегрированные между собой система предотвращения утечек «СёрчИнформ КИБ» и средство аудита и защиты файловых ресурсов «СёрчИнформ Файловый аудитор» – комплексное решение для защиты от внутренних ИБ-угроз.



1. Аудит файловых ресурсов, выявление чувствительной информации (банковской, коммерческой тайны, ПДн)
2. Разграничение доступа пользователей к защищаемой информации, контроль операций с защищаемой информацией
3. Контроль информационных потоков и каналов коммуникации
4. Маркировка электронных документов, содержащих банковскую, коммерческую, иные виды тайны
5. Оповещение о нарушениях политик безопасности, блокировка нежелательных действий
6. Автоматизация расследования инцидентов и составления отчетности, предупреждение будущих утечек

Задача комплекса – найти защищаемые данные, обеспечить полный контроль операций с ними, выявить и предотвратить инциденты ИБ на ранних этапах.

АРХИТЕКТУРА РЕШЕНИЙ

SEARCHINFORM

УПРАВЛЕНИЕ И НАСТРОЙКА

- Административные и аналитические компоненты систем работают на сервере.

  Windows Server, Ubuntu, **Astra Linux**

- Базы данных настроек и перехваченной информации хранятся в защищенных СУБД.

  MS SQL, **PostgreSQL, PostgresPro, PostgreDB, Tantor** и др.

- ИБ-специалист работает с КИБ и FileAuditor через единую консоль.

  Возможен веб-доступ с любого устройства
  Подключение к консоли защищено

Решения включены в реестр российского ПО и сертифицированы ФСТЭК по 4 уровню доверия.

КОНТРОЛЬ И ЗАЩИТА

- Агенты контролируют активность пользователей за ПК:

  Alt Linux
  Astra Linux
  RedOS
  CentOS
  Ubuntu
  СберОС

  Универсальный установщик автоматически собирает агент под версию ядра ОС.

  \+ Windows, MacOS

- КИБ интегрируется с сервисами, СЗИ и прикладным ПО:

  среда, TrueConf, 1С, VK WorkSpace, Колибри, Яндекс 360, МойОфис, облако, Контур.Диадок, IVA

  \+ более 100 сервисов и 10 средств ручной интеграции

КАК КИБ СОБИРАЕТ ДАННЫЕ?

SEARCHINFORM



Модуль контроля почты (MailController)

Контролирует всю электронную почту, включая черновики и входящую через веб-браузер, когда фактически не происходит перемещения информации по протоколам (Gmail, Mail.ru, Яндекс.Почта и т.д.).



Модуль контроля мессенджеров (IMController)

Контролирует чаты, изображения, файлы, видео- и голосовые сообщения, звонки в десктопных и веб-версиях социальных сетей (Вконтакте, Одноклассники и т.д.), мессенджеров и ВКС-платформ (Max, Telegram, Zoom, Express и т.д.).

КАК КИБ СОБИРАЕТ ДАННЫЕ?

SEARCHINFORM



Модуль контроля протокола передачи данных (FTPController)

Контролирует документы, переданные и полученные по протоколу передачи данных (FTP) через обычное или зашифрованное соединение (SSL).



Модуль контроля веб-трафика (HTTPController)

Контролирует запросы и сообщения, передаваемые на любые сайты, в том числе из боковой панели. Может ограничивать доступ к нежелательным ресурсам или отправку данных на них.



Модуль контроля облачных ресурсов (CloudController)

Контролирует передачу информации в облачные хранилища (Яндекс.Диск, Google Drive, Dropbox и т.д.).

КАК КИБ СОБИРАЕТ ДАННЫЕ?

SEARCHINFORM



Модуль контроля монитора (MonitorController)

- Снимает скриншоты и видео экранов рабочих ПК по расписанию или событию (запуск программы/процесса, ввод ключевых слов).
- Фиксирует происходящее в поле обзора веб-камеры ПК.
- Транслирует видео с рабочих столов и веб-камер в реальном времени.
- Распознаёт сотрудников по лицам и попытки сфотографировать экран.



Модуль контроля микрофона (MicrophoneController)

Записывает переговоры сотрудников через любой обнаруженный микрофон (в гарнитуре, ноутбуке и т.д.) на рабочем ПК. Распознает речь и позволяет искать по содержимому переговоров сотрудников, как по тексту. Доступен контроль в реальном времени.

КАК КИБ СОБИРАЕТ ДАННЫЕ?

SEARCHINFORM



Модуль контроля печати (PrintController)

Контролирует содержимое документов, отправленных на печать на локальные, сетевые и виртуальные принтеры. Может снимать теневые копии или блокировать печать в зависимости от контента, типа файла или количества страниц.



Модуль контроля съемных устройств (DeviceController)

Отслеживает подключения внешних устройств к компьютеру, контролирует данные, которые сотрудники записывают на носители. Дает возможность запретить запись, если это нарушает политики безопасности.

КАК КИБ СОБИРАЕТ ДАННЫЕ?

SEARCHINFORM



Модуль контроля клавиатуры (Keylogger)

Фиксирует нажатия клавиш (ввод паролей, ввод команд через комбинации «горячих клавиш» и т.д.), а также информацию, скопированную в буфер обмена.



Модуль контроля приложений (ProgramController)

Собирает данные о приложениях и вкладках браузера, с которыми сотрудник работал в течение дня, и времени, проведенном в них. Показывает, кто в коллективе работает, а кто создает видимость работы.

КАК КИБ АНАЛИЗИРУЕТ ДАННЫЕ?

SEARCHINFORM

Аналитическая подсистема КИБ проверяет данные, собранные всеми компонентами.

Чтобы обнаружить предпосылки инцидентов или произошедшие нарушения, «СёрчИнформ КИБ» использует **8 видов поиска** и их комбинации.



+ ИИ

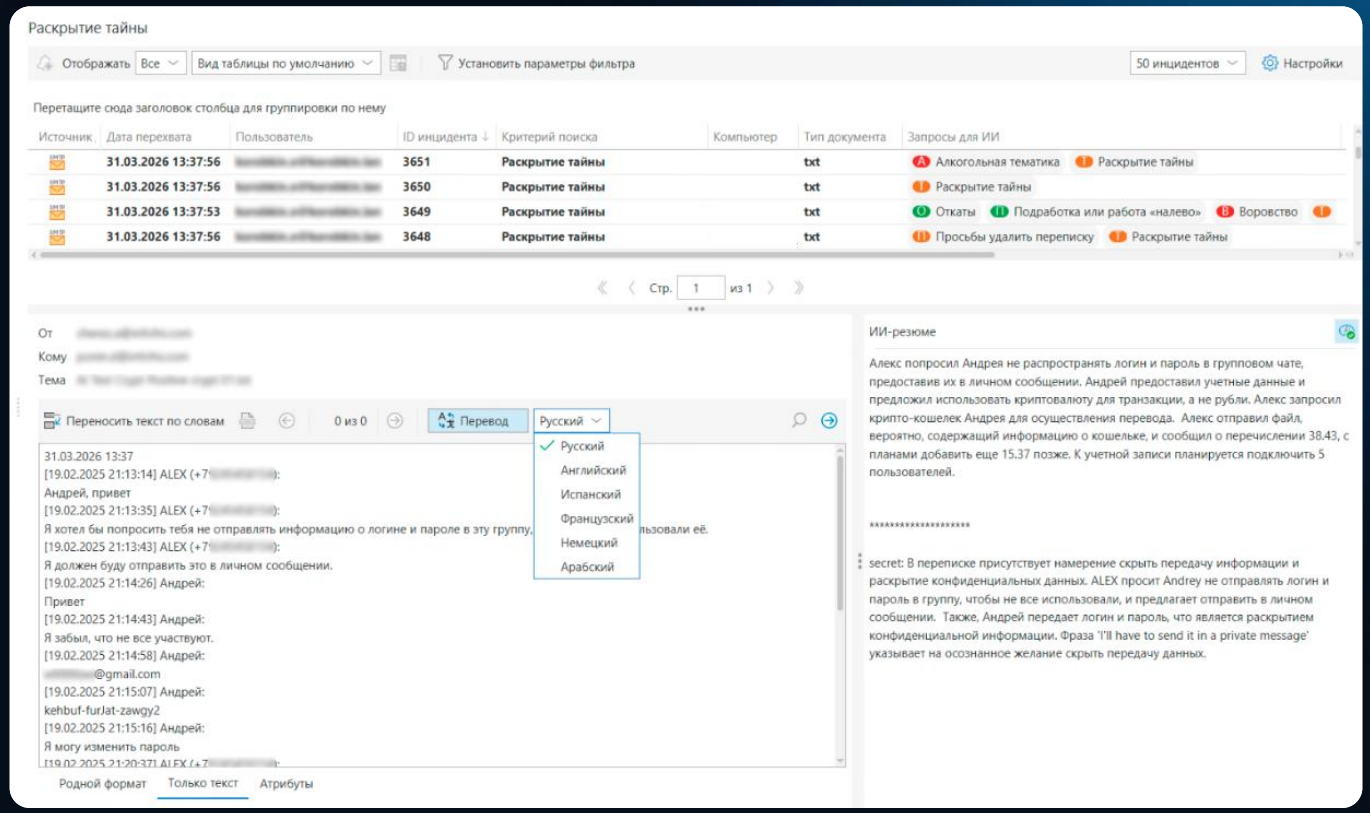
Запросы можно совмещать для создания более сложных алгоритмов поиска и формировать их в политики безопасности.

ИИ-АССИСТЕНТ В «СЁРЧИНФОРМ КИБ»

ИИ-Ассистент – это встраиваемый модуль на базе большой языковой модели (LLM), который обнаруживает угрозы, «невидимые» для стандартных поисковых алгоритмов. Модуль устанавливается локально, что обеспечивает безопасность данных при их обработке.

Задачи модуля:

- **Выявить скрытые инциденты ИБ** по контексту ситуации, благодаря готовым ИИ-политикам.
- **Резюмировать содержание** объемных переписок, переводить коммуникацию с любых языков и указать на признаки угрозы.
- **Автоматизировать анализ контекста коммуникации,** чтобы «увидеть» больше, чем поиск по словарям.
- **Сократить нагрузку на ИБ-специалистов и затраты времени** на анализ данных.



SEARCHINFORM

БЛОКИРОВКИ В «СЁРЧИНФОРМ КИБ»

SEARCHINFORM

- **Блокировка вывода данных** за пределы ИС с помощью облаков, почты, мессенджеров
- **Блокировка доступа к съемным устройствам** на уровне интерфейса (сетевой адаптер, устройства хранения).
- **Блокировка записи данных на съемные устройства** (по контенту и контексту).
- **Блокировка доступа к модемам и сетевым адаптерам.**
- **Блокировка доступа к дисководам**.
- **Блокировка запуска исполняемых файлов.**
- **Блокировка посещения запрещенных сайтов** (категорий сайтов).

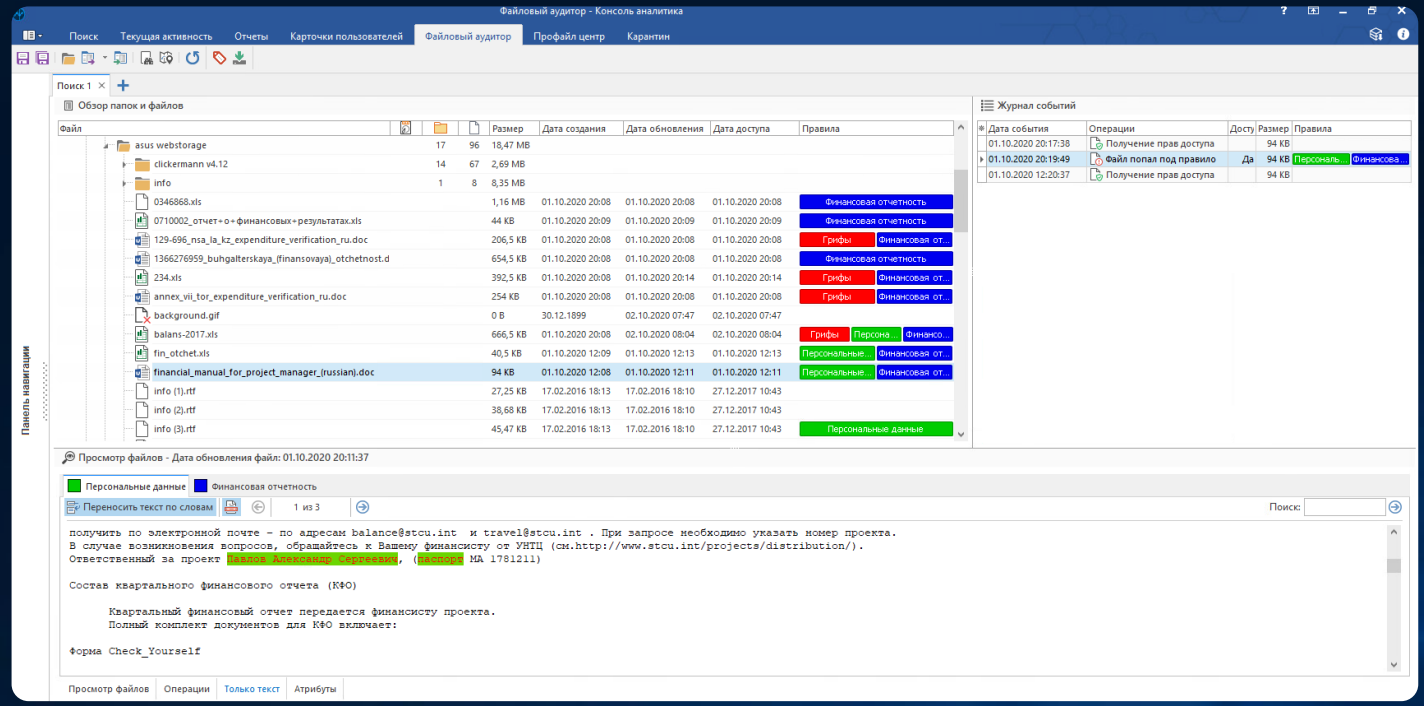


КИБ позволяет блокировать передачу данных по гибким условиям, а также ограничивать опасные действия сотрудников.

«СЁРЧИНФОРМ ФАЙЛОВЫЙ АУДИТОР»

SEARCHINFORM

- **Находит данные, которые подлежат защите**
  Сканирует все хранилища и анализирует содержимое файлов.
- **Классифицирует информацию**
  Присваивает файлам метки на основе их содержимого: ПДн, договоры, финансовая информация и пр.
- **Позволяет маркировать** электронные документы с защищаемыми данными (коммерческой тайной, ДСП).
- **Разграничивает доступ к данным**
  Запрещает работу с файлами пользователям без допуска к ним.
- **Ведет «умный» архив и теневое копирование**
  файлов для исключения порчи или утраты данных.



«СёрчИнформ Файловый аудитор» (СёрчИнформ FileAuditor) – система аудита и защиты файловых ресурсов (DCAP), управляет доступом к чувствительным данным и снижает риск утечки.

ФАЙЛОВЫЙ АУДИТОР:
ОПРЕДЕЛЕНИЕ КЛАССА ИНФОРМАЦИИ

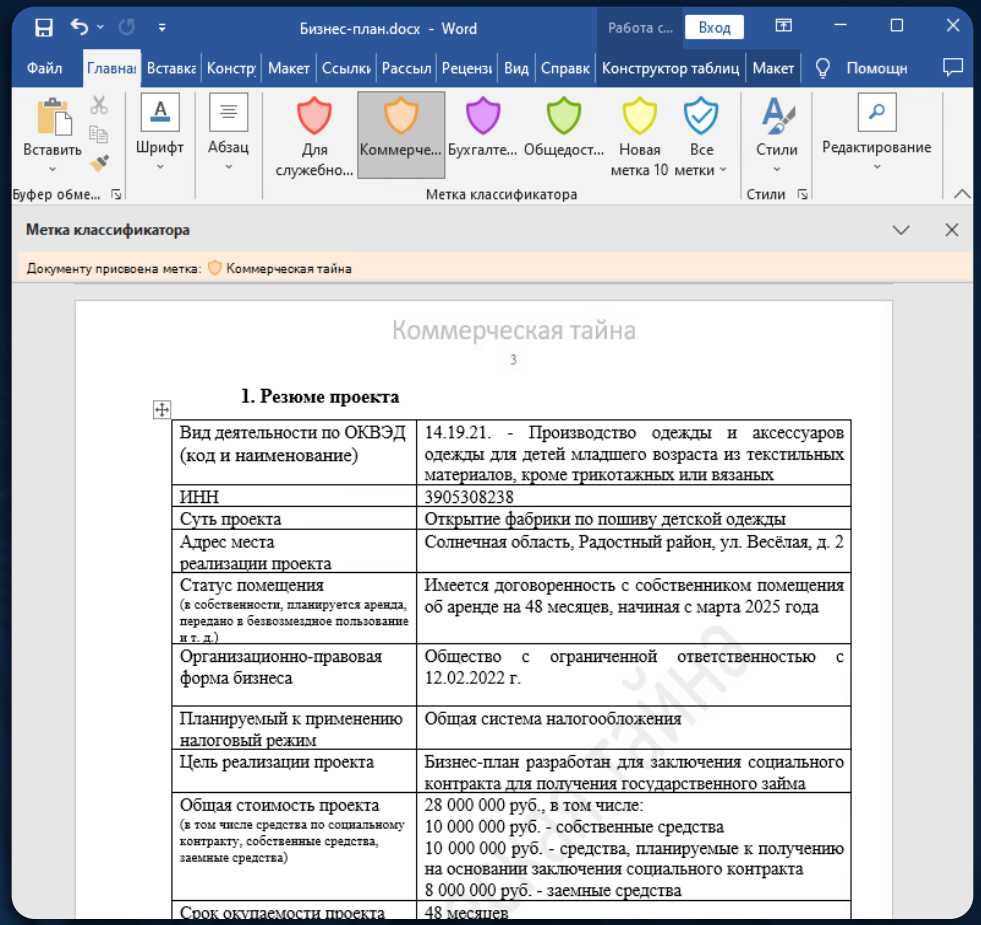
SEARCHINFORM

- **Автоматическая классификация**
  Система анализирует содержимое файлов и ставит на них метки в зависимости от класса. «Из коробки» доступны **450+ готовых правил** классификации, можно создать свои.

- **«Ручная» классификация**
  Можно выводить на документы **графические метки** с указанием статуса конфиденциальности, предоставить пользователям право ставить их самостоятельно. Это позволяет выполнить требования к режиму КТ в цифровой инфраструктуре



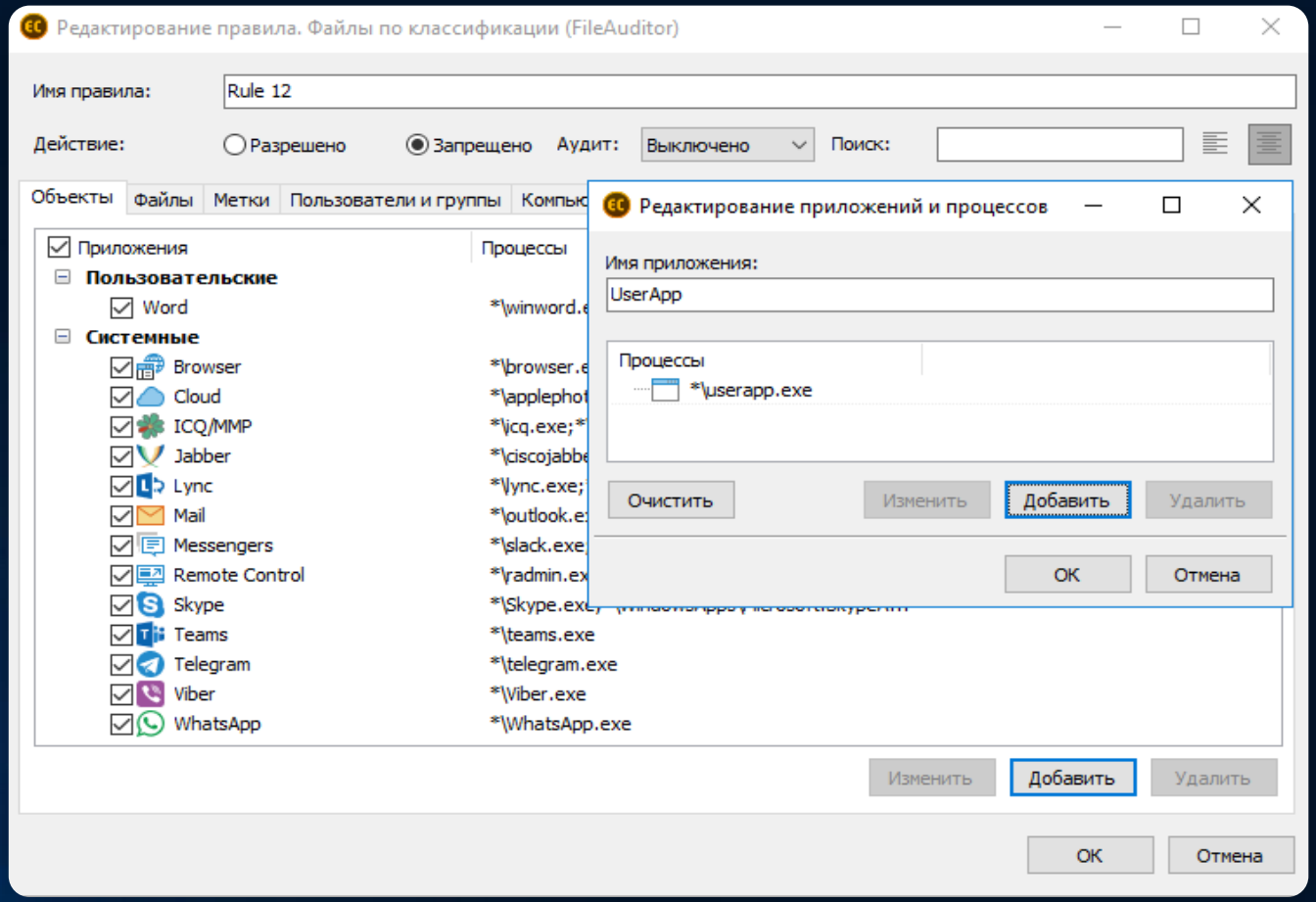
Метки **«Файлового аудитора»** вшиваются в альтернативный файловый поток и остаются на документе, пока в нем есть защищаемый контент. Это делает защиту надежной.



ФАЙЛОВЫЙ АУДИТОР:
КОНТЕНТ-ЗАВИСИМОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА

- **Блокировки по меткам классификации**
  Запрет действует не на папку / тип файла, а на конкретный контент.

- **Запрет применяется к процессам**
  Можно создать безопасные сценарии работы с файлом в разрешенных приложениях или полностью запретить доступ к нему нежелательным пользователям.



SEARCHINFORM

ПОЛНЫЙ КОНТУР ЗАЩИТЫ

SEARCHINFORM

Оптимизация нагрузки

- «Файловый аудитор» анализирует контент файла и ставит метку классификации.
- КИБ получает сведения о файле через метку – системе не нужно анализировать его повторно.
- КИБ быстрее блокирует / фиксирует инцидент с передачей файла.

Усиление контроля

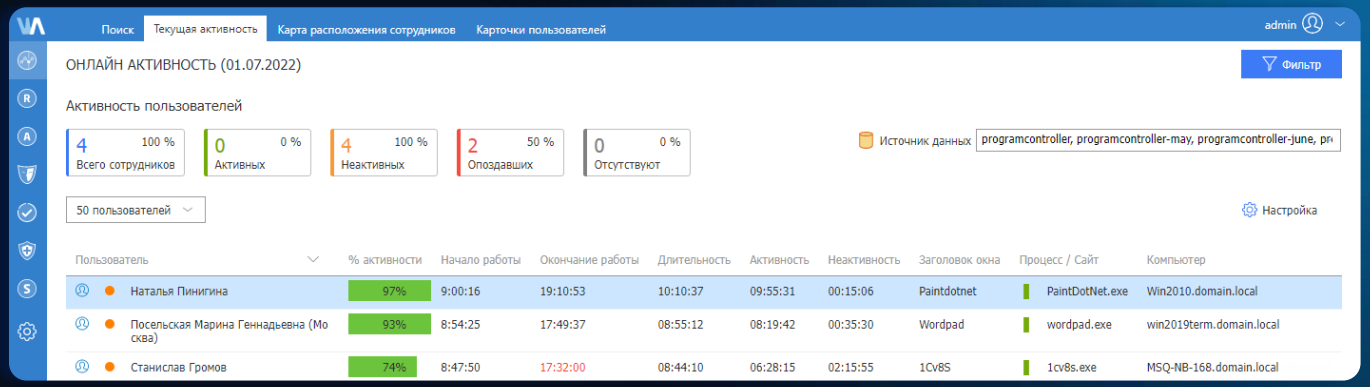
- «Файловый аудитор» контролирует доступ к файлу **внутри компании** и минимизирует риск утечки.
- «СёрчИнформ КИБ» контролирует передачу контента за пределы файла и передачу файла **за пределы компании.**

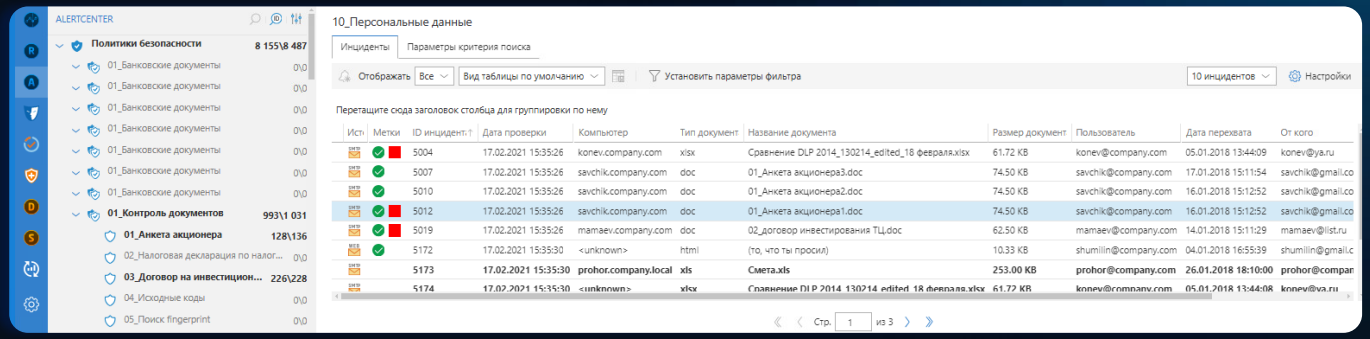
Системы работают в едином интерфейсе и управляются из одного центра. Это обеспечивает сквозной контроль на всех этапах жизненно цикла корпоративных данных и удобство работы ИБ-специалистов.

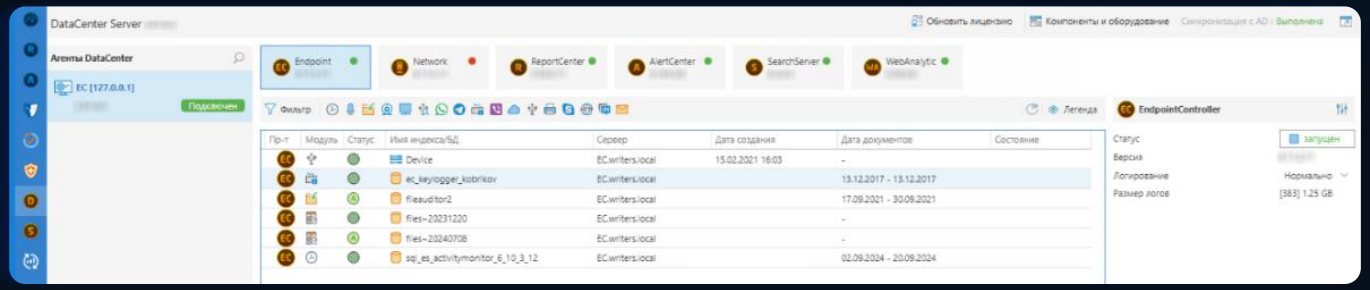


ВСЯ АНАЛИТИКА в одной консоли

- Поиск в веб-интерфейсе;
- Центр обнаружения инцидентов (AlertCenter);
- Центр отчетов (ReportCenter);
- Менеджер задач;
- Центр управления (DataCenter);
- Почтовый карантин;
- Карточки пользователей;
- Текущая активность.









SEARCHINFORM

ИННОВАЦИОННОСТЬ И УНИКАЛЬНОСТЬ

SEARCHINFORM

Проблемы

- Инспекция файловых ресурсов с помощью штатных средств ОС либо вручную неэффективна. Система защиты от утечек не дает возможностей аудита данных в системе.
- Средства аудита и защиты файлов не дают достаточных возможностей для предотвращения, пресечения и расследования внутренних ИБ-нарушений.
- Для обеспечения внутренней ИБ необходимо внедрение СЗИ нескольких классов. Возникают барьеры:
  - Отсутствие интеграции СЗИ между собой, с ОС и прикладным ПО;
  - Чрезмерные затраты на внедрение нескольких СЗИ;
  - Снижаются возможности защиты в разнородной ИТ-инфраструктуре.

Решение

- Комплекс «СёрчИнформ КИБ» и «СёрчИнформ Файловый аудитор» – первая на рынке единая платформа, сочетающая функции обеих систем.
- Системы отвечают требованиям к импортозамещению, позволяют выполнить:
  - Более 50 требований ГОСТ 57580.1
  - Требования к защите коммерческой тайны
  - п. 5.2.2, 5.2.3 Положения Банка России № 851-П
  - п. 1.11, 1.12 Положения Банка России № 757-П
  - п. 1.4.1 Положения Банка России № 821-П

  и иные требования
- Системы позволяют дополнительно решать задачи контроля целевого использования ИС организации, рабочего времени пользователей, предотвращения нарушений общей и экономической безопасности.

ЭКОНОМИЧЕСКИЙ И СОЦИАЛЬНЫЙ ЭФФЕКТ



- Минимизация рисков утечек экономически ценных сведений, ноу-хау, персональных данных.
- Снижение рисков нарушений экономической безопасности в организациях.
- Снижение риска штрафов за ИБ-нарушения.
- Выполнение нормативных требований: 152-ФЗ, 187-ФЗ, приказов ФСТЭК России № 239, 21, Положений Банка России № 757-П, 821-П, 851-П, ГОСТ Р 57580.1.
- Повышение доверия к электронному взаимодействию и цифровым сервисам, повышение доверия к организациям (в т.ч. финансовым учреждениям)
- Сокращение риска ИКТ-преступлений за счет снижения объема скомпрометированных данных.

SEARCHINFORM

РЕШЕНИЯ «СЁРЧИНФОРМ» УЖЕ ЗАЩИЩАЮТ:

























SEARCHINFORM

ЭКСПОРТНЫЙ ПОТЕНЦИАЛ

SEARCHINFORM

4 000+ клиентов в

20+ странах

3 000 000+

ПК под защитой
решений «СёрчИнформ»



СПАСИБО ЗА ВНИМАНИЕ!

SEARCHINFORM

https://max.ru/id7704306397_biz

https://vk.com/securityinform

https://rutube.ru/channel/26067088/

Практика и аналитика

https://searchinform.ru/practice-and-analytics/

E-mail: info@searchinform.ru