SEARCHINFORM
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ПРОАКТИВНАЯ ЗАЩИТА ФАЙЛОВ



searchinform.ru

О чем этот документ

Информации много, без контроля она теряется. Сотрудники случайно или намерено удаляют важные файлы или вносят в них ненужные правки. Из-за этого происходят инциденты безопасности, в том числе утечки конфиденциальных документов – в 2025 году с ними столкнулись 46% российских компаний*, причем более чем в половине случаев терялись персональные данные, в трети – служебные регламенты и внутренняя документация, в четверти – данные клиентов и информация о сделках. Чтобы не разбираться с последствиями, лучше исключить вероятность нарушений заранее.

В этой книге мы:

- Разберем риски ИБ, которые возникают, когда документы не покидают пределы компании.
- Опишем инструменты для контроля угроз ИБ в файловых системах, их преимущества и недостатки.
- Сформулируем задачи, которые необходимо решать для оптимальной защиты файлов.
- Дадим рекомендации, как обезопасить конфиденциальные документы от нежелательного доступа и операций.
- Проиллюстрируем советы реальными примерами из ИБ-практики компаний.



По данным **исследования «СёрчИнформ» уровня ИБ в компаниях России в 2025 г.*

Что может произойти?

Универсальный риск при работе с конфиденциальной информацией – ее потеря. Это может произойти по нескольким причинам:

Утечка данных

Информация, не предназначенная для свободного распространения, покидает контролируемый периметр и попадает в распоряжение нежелательных лиц – конкурентов, мошенников, недоброжелательных СМИ, пользователей интернета и пр. Утечка не всегда связана с преднамеренной кражей информации – чаще (до 66% случаев*) это случайные инциденты. Например, сотрудники ошибаются адресатом в почте, или загружают рабочие файлы в публичное облачное хранилище, чтобы поработать с ними из дома.

Обратите внимание

Не всегда утечка подразумевает, что данные оказались вне компании. Отдельная категория инцидентов – нарушение целостности внутренних периметров доступа, например, когда информация для топ-менеджмента попадает к рядовым сотрудникам, или сведения, составляющие охраняемую законом тайну, оказываются на компьютерах, не прошедших специальную сертификацию. К ним относятся нарушения правил хранения и обработки информации, ошибки в распределении доступа к файлам, копирование или перемещение документов в общедоступные директории и пр.

Это чревато как минимум распространением слухов в коллективе и размыванием периметра контроля, как максимум – серьезным наказанием от регулятора, вплоть до уголовной ответственности.

По данным **исследования «СёрчИнформ» уровня ИБ в компаниях России в 2025 г.*

Модификация данных

В файл вносят изменения, которые искажают первоначальное содержание и ценность информации утрачивается. Например, если несколько сотрудников работают с разными копиями важного файла, кто-то может внести несогласованные правки или часть критичной информации не попадет в итоговую версию документа. Иногда серьезный ущерб может нанести даже опечатка.



Удаление данных

К этому может привести системный сбой, ошибка в работе с ПО и оборудованием. Частая история – когда сотрудники удаляют данные при увольнении, из мести или в попытке скрыть ошибки, недоработки или следы нарушений политик информационной или экономической безопасности.

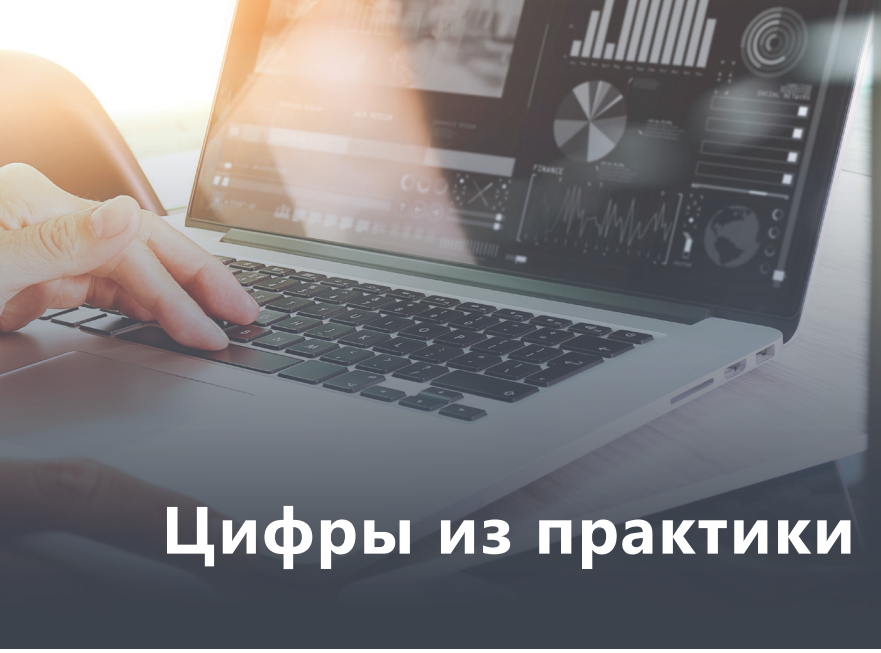
Нередко такие инциденты связаны с низкой ИТ-грамотностью сотрудников или непониманием, какую ценность в действительности представляет информация. Эти случаи контролировать сложно ввиду их непредсказуемости.

Отдельной задачей становится выявление признаков спланированных нарушений. Это могут быть:

- целенаправленные поиски информации ограниченного доступа сотрудниками, в обязанности которых не входит работа с такими данными;
- массовое копирование и перенос конфиденциальных файлов в непредназначенные для этого директории;
- подозрительные махинации: переименование, смена расширения файлов, помещение документов в архивы с паролем и др.

Такая активность с большой вероятностью указывает на подготовку к сливу информации. Служба информационной безопасности должна своевременно выявлять ее, чтобы предотвращать инциденты до того, как компания понесла ущерб.





**Данные собраны в рамках сервисного сопровождения компаний, внедривших или тестировавших «СёрчИнформ Файловый аудитор» («СёрчИнформ FileAuditor») в 2020-2025 гг.*

Цифры из практики

В каждой компании

обнаруживаются избыточные права доступа к файлам и папкам с конфиденциальной информацией, в том числе для учетных записей давно уволенных сотрудников.

Конфиденциальный документ без должного контроля попадает за пределы круга доверенных сотрудников в среднем

за 36 часов.

Через неделю круг сотрудников, получивших к нему доступ, расширяется **в 5 раз**, т.е. в 5 раз вырастает вероятность утечки.

Каждая третья компания

обнаруживает неучтенные копии критичных документов на компьютерах пользователей. В них вносят нерегламентированные правки, это порождает неразбериху и открывает поле для махинаций.

8 из 10 сотрудников

хранят файлы с паролями от рабочих аккаунтов на ПК. При их компрометации уязвимыми оказываются все корпоративные сервисы.



Как решать проблему?

Чтобы минимизировать риски, нужно навести строгий порядок в файловой системе. Задачу можно считать решенной, если у службы ИБ в любой момент времени есть ответы на следующие вопросы:

- 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?

Этого можно достичь двумя способами – организационными мерами и с помощью автоматизированных инструментов контроля.

В первом случае речь о внедрении в компании режима защиты информации. Для этого потребуется:

1. **Разработать положения о введении режима коммерческой тайны (КТ) и о защите информации.**

   В положении о КТ должны быть регламентированы хранение, обработка и маркировка сведений, относящихся к КТ. Например, правило хранить документы, содержащие конфиденциальные сведения, в защищенных хранилищах (например, сейфах или отдельных помещениях), а выдавать только при предъявлении документов, подтверждающих уровень доступа. Также важно отразить запрет передачи таких данных в любом формате посторонним, их публикации или нарушения правил их хранения, установленных положением.

2. **Закрепить в приложении к положению о КТ перечень сотрудников, которым будет доступна тайна.**

   Список должен включать имена или должности сотрудников и, при необходимости, их учетные записи в корпоративных системах. В положении также отражается порядок отнесения сведений к коммерческой тайне и право организации обеспечивать их защиту с помощью технических средств. Кроме того, уместно включить пункт о том, что организация имеет право контролировать все операции, связанные с обработкой, хранением, передачей, доступом, уничтожением информации, содержащей коммерческую тайну. Это нужно, чтобы в случае нарушения собрать доказательную базу для суда в ходе внутреннего расследования.

   Также в положении о КТ необходимо отразить, что работники несут ответственность за разглашение коммерческой тайны, предоставление к ней неправомерного доступа, несанкционированное изменение или уничтожение конфиденциальной информации, а также за убытки организации в случае таких инцидентов, в соответствии с действующим законодательством.

3. **Составить подробный перечень конфиденциальной информации** с максимально конкретными сведениями о типах, форматах таких данных и их отличительных признаках: от названий конкретных документов до целых категорий, например, «базы данных 1С», «служебная переписка» или «отчеты о приходах и расходах». Перечень должен быть включен в положение о КТ в качестве приложения.

4. **Нанести соответствующий гриф на все материальные носители, где хранится конфиденциальная информация.**

Гриф должен указание на обладателя такой информации: для юридических лиц это полное наименование и местонахождение, для индивидуальных предпринимателей – ФИО и место жительства. Помечать нужно не только все бумаги, но и каждую флешку или даже серверы (системы хранения данных) с такими данными. В электронные документы рекомендуется «зашивать» аналогичные метки – в защищенные поля, чтобы сотрудники не могли случайно или намеренно их удалить.

Обратите внимание

- *Файлы и бумаги, не попавшие в перечень и под гриф, тайной считаться не будут, даже если реально содержат конфиденциальные сведения. Так что работника, уволенного за их разглашение, могут восстановить на работе с компенсацией морального вреда и зарплаты за вынужденный прогул. То же касается отсутствия ознакомления сотрудников с актами о режиме КТ – в случае утечки в суде будет не доказать, что человек знал, что сведениями нельзя делиться.*
- *Некоторые сведения не могут относиться к коммерческой тайне в силу закона. Это, например, информация о зарплатах, об охране труда, о безопасности на предприятии. Соглашения об их неразглашении ничтожны.*

5. **С положением о КТ и перечнем сведений, составляющих КТ, необходимо под роспись ознакомить всех работающих и вновь нанимаемых сотрудников.**

Подпись сотрудников будет означать информированное согласие с правилами. Ознакомление сотрудников можно дополнить подписанием соглашений о неразглашении (NDA) или включением в трудовые договоры и должностные инструкции положений о неразглашении коммерческой тайны.

Подробнее о том, как ввести и обеспечить работу режима коммерческой тайны, рассказали в ***чек-листе.***



Контроль за соблюдением режима коммерческой тайны и реальную защиту конфиденциальных документов обеспечат автоматизированные средства для мониторинга и предотвращения опасных действий с файлами.

ВАЖНО:

Чтобы применение ИБ-средств не несло правовых рисков, регламентируйте ответственность сотрудников за нарушения и право компании на их контроль.

Читайте в наших материалах:

- Как внедрить средства контроля легитимно;
- Как использовать такие средства в служебных расследованиях.

Для **распределения прав доступа** к файлам и папкам часто используют **средства ОС и контроллеров домена (Active Directory и т.п.)**. Частично нужным функционалом обладают также платформенные средства – встроенные инструменты внутри СУБД, файловых систем, бизнес-приложений.

Как правило, они все работают по такому принципу:

- права распределяются по пользователям / группам
- права зависят от атрибутов файла (расположение, автор, имя, тип...)
- права распространяются на конкретные операции (чтение, изменение, копирование, удаление...)



Однако при таком подходе:

не учитывается содержимое и реальная ценность документов

Сотрудники могут исказить или удалить конфиденциальное содержимое из документа – или скопировать его в новый документ, не защищенный ограничениями доступа.

не исключаются риски

Пользователи с доступом могут переименовать, сменить расширение документа, переместить его в общедоступную директорию. Тогда меры защиты действовать перестанут, и информация будет скомпрометирована.

К тому же синхронизировать настройки доступа в разных ИТ-системах и хранилищах может быть непросто – а это создает бреши в безопасности. Поэтому оптимальнее использовать **специализированные средства.**

Системы аудита и защиты файловых ресурсов (DCAP-системы, от англ. data-centric audit and protection) специально созданы для обеспечения безопасности файлов с фокусом на данных. Они комплексно решают все актуальные задачи:

- **Обнаружение конфиденциальной информации, где бы она ни находилась:**

  все директории, неучтенные копии важных файлов, документы, формально не включенные в перечень КТ, но содержащие отсылки и выдержки из таких сведений, конфиденциальные файлы, замаскированные под иные объекты (изображения, аудио, видео и пр., в том числе с измененным расширением).

- **Категоризацию найденных данных по их содержимому:**

  бухгалтерская отчетность, персональные данные, документы с грифом, номера кредитных карт, файлы с паролями, договоры и пр. Присвоение меток по категориям, которые работают на уровне файловой системы и содержат сведения о контенте файла и необходимых для его защиты правилах. Метки должны наследоваться, быть защищены от удаления и повреждения и считываться иными приложениями и системами.

- **Архивирование критичных копий конфиденциальных документов**,

  чтобы обезопасить информацию от удаления и модификации, отслеживать историю редакций и проводить расследования нарушений. Архивы должны формироваться скрыто, методом теневого копирования, и храниться в изолированных защищенных директориях в зашифрованном виде.

Контроль за правами доступа к файлам.

Автоматическое отслеживание открытых ресурсов, файлов, доступных конкретному пользователю или группе, учетных записей с привилегированными правами, информации о владельцах файлов и истории изменений доступа – если файл или папка были перемещены или скопированы в новое месторасположение. Вычитка прав должна происходить без использования дополнительных инструментов, чтобы служба ИБ имела полную картину в единой консоли. Также необходимо контролировать действия администраторов по распределению пользовательских прав – например, с помощью интеграции с контроллерами домена.

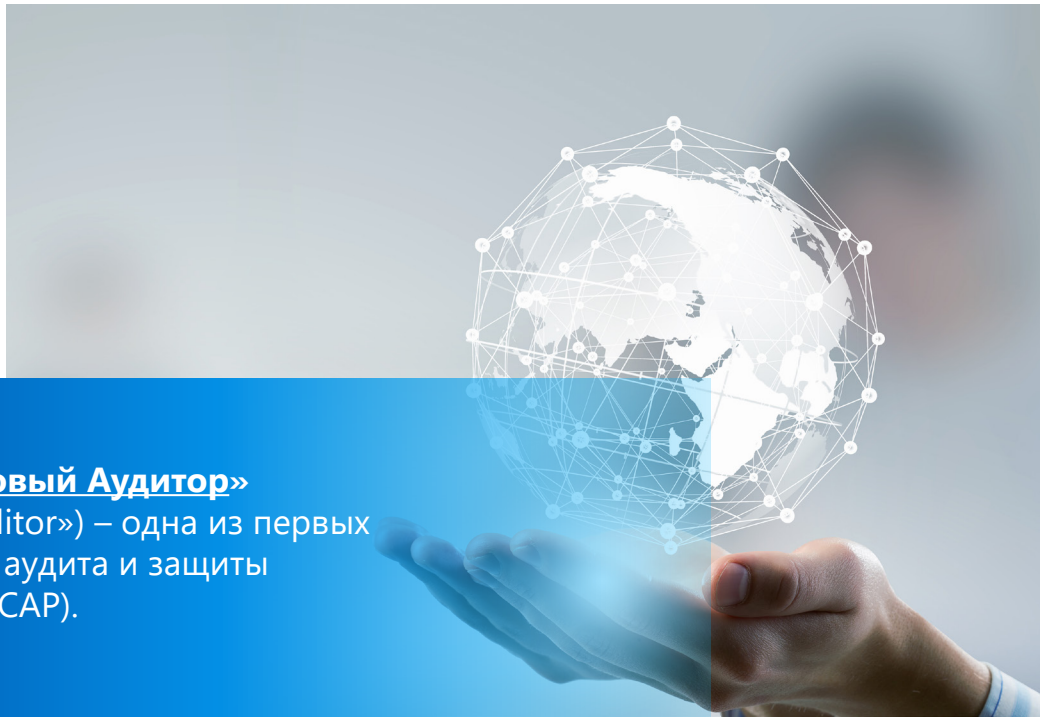
Аудит операций с файлами с возможностью заблокировать доступ.

Непрерывный сбор актуальной информации о «жизни» файла (создание, редактирование, перемещение, удаление и т.д.) и регистрация всех изменений в файловой системе. Автоматическое оповещение службы ИБ о нежелательных операциях, возможность ограничить доступ к файлу через любое приложение (почта, мессенджер, текстовый редактор и т.д.) для контроля нежелательной активности, чтения, правок и пересылки.

Уведомление пользователей об уровне конфиденциальности файлов.

Система должна помогать выполнить требования по оформлению и обработке документов, имеющих ограничительные грифы доступа.

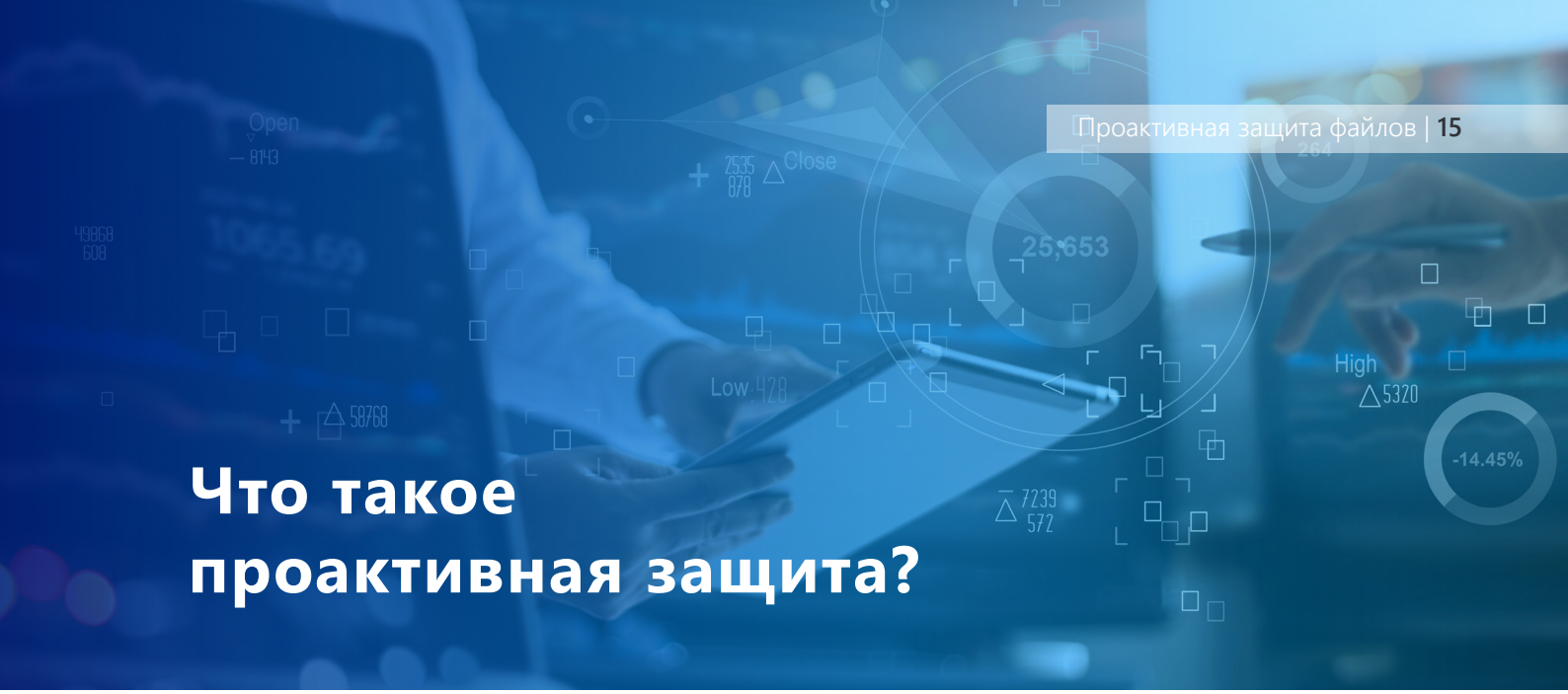
Кроме преимущества по функционалу, системы файлового аудита удобнее в работе. Они агрегируют всю важную информацию о жизненном цикле уязвимых данных в одной точке, совмещая возможности мониторинга и проактивного управления инцидентами безопасности. В идеальном случае они превосходят другие средства по быстродействию и меньше нагружают ИТ-инфраструктуру.



«СёрчИнформ Файловый Аудитор» («СёрчИнформ FileAuditor») – одна из первых отечественных систем аудита и защиты файловых ресурсов (DCAP).

Система помогает поддерживать порядок в файловых хранилищах и отвечает на ключевые вопросы: какие документы содержат критичную информацию, где они находятся и кто имеет к ним доступ. Она защищает коммерческую тайну, финансовую документацию и другие чувствительные данные, разграничивая к ним доступ, предотвращает нежелательные сценарии обработки критичных данных, а также страхует от их порчи и удаления.

Ключевое преимущество системы – функция контент-зависимого разграничения доступа, основанная на запатентованной технологии встраивания меток в файлы. Метки нельзя удалить, поэтому настроенные по ним политики защиты и ограничения обработки файлов действуют, пока в файле сохраняется защищаемый контент. Это обеспечивает реальную безопасность критичным документам в компании вне зависимости от их типа и расположения.



Что такое проактивная защита?

Это возможность заблаговременно предотвратить нежелательные события с файлами со стороны пользователей. В системах файлового аудита это реализовано за счет блокировки доступа к файлам. Важно, что это не обычное разграничение доступа – запреты учитывают содержимое документов, и работают не только внутри файловой системы, но и когда с файлами взаимодействуют сторонние приложения.

Вот, как это устроено:

1. Компания определяет круг доступа к данным и настраивает его средствами ОС. Разграничения работают для пользователей/ПК, но устанавливаются по формальным признакам (атрибутам, названию, расположению и т.п.) и не учитывают содержимое файлов и папок.

2. Система файлового аудита сканирует хранилища, классифицирует данные и автоматически присваивает документам метку категории. Метки ставятся сразу же, как файл с конфиденциальным содержимым появляется на ПК пользователя или в сетевом хранилище. Метки категорий описывают тип информации внутри файла: ПДн, выгрузки из БД, договоры и т.д.

«Файловый аудитор» *мониторит ПК сотрудников, локальные и сетевые СХД и облачные хранилища и анализирует содержимое найденных файлов. В системе со старта доступны 450+ готовых правил классификации документов, а также простые редакторы для создания собственных категорий. Также можно предоставить доверенным пользователям возможность проставлять метки конфиденциальности вручную – прямо из интерфейса офисных программ на своих ПК.*



3. Служба информационной безопасности настраивает доступы к файлам в системе файлового аудита: для выбранных категорий данных создают правила, кому, на каких ПК и в каких приложениях с ними разрешено или запрещено работать. Таким образом можно создать и контролировать безопасные сценарии обработки документов и надежно запретить все варианты нежелательного доступа к ним. Запреты и разрешения «записываются» в метку и наследуются вместе с ней.

4. Правила уточняются вручную, если есть необходимость защитить не целую категорию данных, а отдельный чувствительный документ. Например, владелец данных (топ-менеджер) или ИБ-специалист может поставить метку «Конфиденциально» прямо в интерфейсе текстового редактора – тогда пользователи без права работы с такой категорией данных, даже получив доступ к файлу, не смогут его прочесть.

Подробнее о том, как применять блокировки «Файлового аудитора» для ограничения доступа к файлам, рассказали в ***практической инструкции.***

В **«СёрчИнформ Файловый аудитор»** запреты/разрешения по меткам можно установить абсолютно для любых приложений – от браузера и почты до графического редактора или самописного корпоративного мессенджера. Ограничения работают на уровне получения данных из файловой системы, а потому не зависят от типа и версии ПО или ОС. Программа, для которой настроен запрет, просто не сможет открыть документ.

Функция блокировок по меткам в «Файловом аудиторе» работает по запатентованной технологии управления файловыми потоками. Такая проактивная защита – уникальная возможность решения, по сравнению с другими системами аудита файловых ресурсов (DCAP) и классическими средствами управления доступом к файлам.



Таким образом, можно заблокировать:

- Доступ к файлу посторонних;
- Нежелательные варианты обработки файла (например, открытие в веб-редакторах в браузере);
- Пересылку файлов по внешним и внутренним каналам (например, прикрепление во вложения в почтовом клиенте или приложении мессенджера)*.

Блокировки «СёрчИнформ Файловый аудитор» **работают для всех процессов**, то есть программа контролирует любое взаимодействие с конфиденциальными документами вне зависимости от того, где они хранятся. Это главный козырь систем аудита и защиты файловых ресурсов (DCAP) в сравнении с классическими инструментами мониторинга и управления доступом к данным.

** **«Файловый аудитор»** может автономно защищать файлы от «слива» путем запрета пользователям открывать их с помощью ПО с функциями отправки данных. Но для комплексного контроля лучше использовать профильные решения – например, систему защиты от утечек (DLP) **«СёрчИнформ КИБ»**. Она «понимает» метки конфиденциальности на файлах и блокирует их пересылку независимо от способа и канала, в том числе если содержимое копируют из файла и отправляют просто текстом. Решения бесшовно интегрируются и работают в одном интерфейсе – это упрощает работу и усиливает безопасность данных.*

Как это работает?

Рассмотрим, какие преимущества дают системы файлового аудита для защиты конфиденциальных документов, на примерах из практики клиентов «СёрчИнформ».

Обнаружение данных

В компании документы с грифом секретности должны были храниться строго на определенных компьютерах и не покидать их. Однако в работе сотрудники создавали неучтенные копии таких файлов, использовали выдержки из них и хранили их устаревшие версии в нарушение требований регулятора.

Вручную найти все такие случаи более чем на 1000 ПК не представлялось возможным. Чтобы избежать штрафа, с помощью «Файлового аудитора» компания проверила все файловые сервера и ПК сотрудников, выявила и устранила все нарушения.

Классификация данных

ИБ-служба компании обнаружила, что на файловом сервере нарушается установленная политика разграничения доступа. Критичные документы из скрытой для большинства пользователей папки периодически попадали в общую – по ошибке или незнанию сотрудников.

После установки «Файлового аудитора» выяснилось, что в общем доступе хранится до трети конфиденциальных файлов компании. Классификация уязвимой информации позволила ИБ-службе навести порядок в файловой системе и защитить важные документы.

Запрет нежелательного доступа

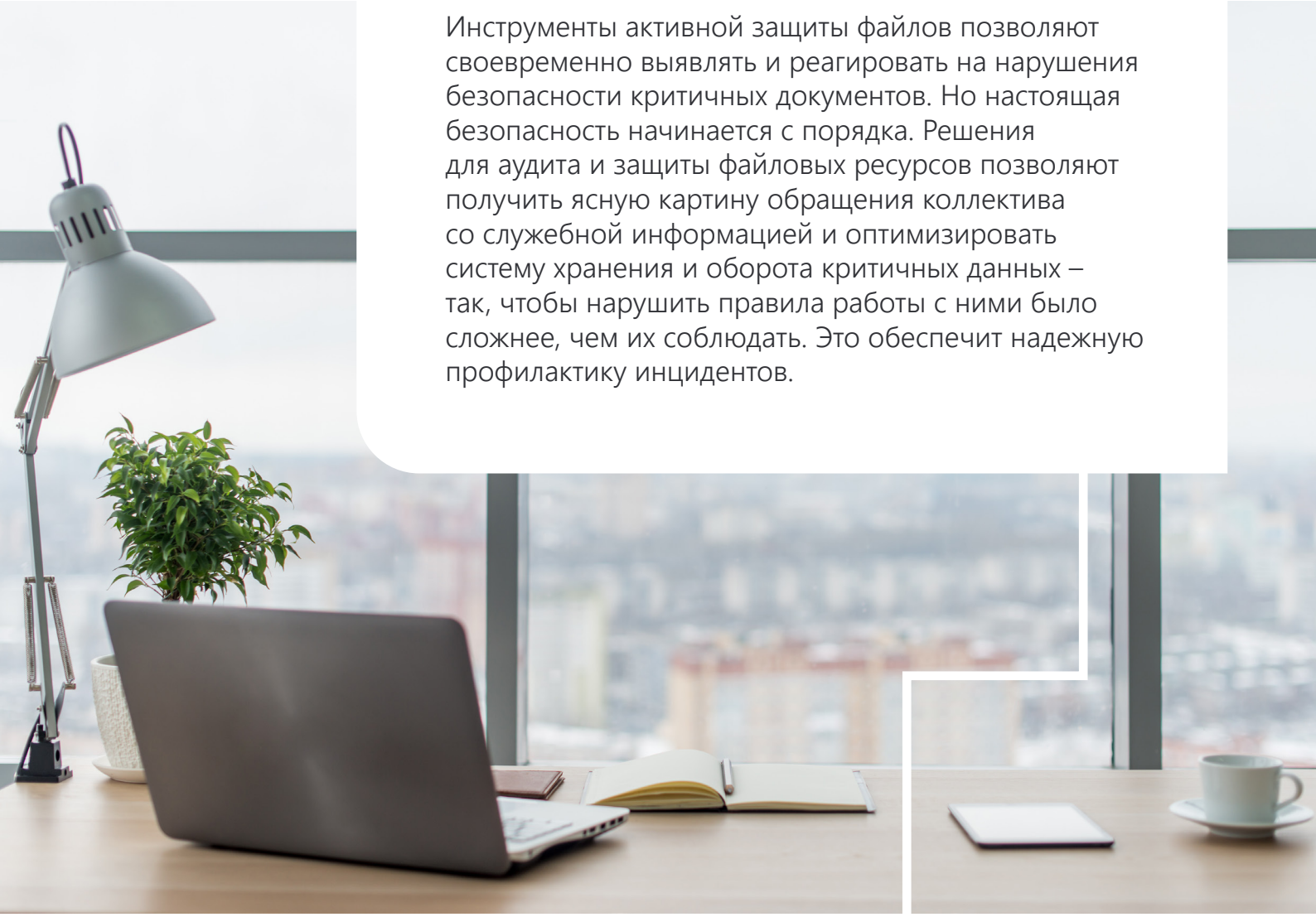
«СёрчИнформ Файловый аудитор» обнаружил, что системный администратор читает документы из категории «Для топ-менеджмента», пользуясь удаленным доступом к ПК генерального директора. Праздное любопытство в любой момент могло обернуться сливом данных.

Чтобы избежать угрозы, в «Файловом аудиторе» запретили доступ к таким файлам для всех, кроме членов совета директоров – в свой следующий «визит» за компьютер гендиректора сисадмин не смог открыть ни один интересный ему документ.

Мониторинг операций

Сотрудник компании анонимно передал СМИ информацию о внутренних проблемах предприятия. Найти информатора помог «СёрчИнформ Файловый аудитор». ИБ-служба создала фейковые документы и поместила их в папки с ограниченным доступом, из которых потенциально произошла утечка информации.

Программа зафиксировала, кто из сотрудников открывал поддельные документы, что позволило вычислить подозреваемого. Догадки ИБ-службы подтвердились, когда факты из подставных файлов попали в СМИ.



Инструменты активной защиты файлов позволяют своевременно выявлять и реагировать на нарушения безопасности критичных документов. Но настоящая безопасность начинается с порядка. Решения для аудита и защиты файловых ресурсов позволяют получить ясную картину обращения коллектива со служебной информацией и оптимизировать систему хранения и оборота критичных данных – так, чтобы нарушить правила работы с ними было сложнее, чем их соблюдать. Это обеспечит надежную профилактику инцидентов.

Закажите бесплатный 30-дневный тест **«СёрчИнформ Файловый аудитор»**. Даже в пилотный период вам будет доступно полнофункциональное ПО без ограничений по пользователям и функциональности. Вы узнаете, какие данные в ваших хранилищах требуют особого контроля – и сможете реально их защитить. Оставьте заявку **по ссылке**.

SEARCHINFORM
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

«СёрчИнформ» – ведущий российский разработчик средств информационной безопасности. Входит в ассоциации «РУССОФТ» и АПКИТ. Клиенты – более 4000 компаний по всей России и в 20+ странах мира.

В активе команды разработчиков – инструменты, которые позволяют комплексно контролировать источники внутренних угроз на всех уровнях информационной системы компании.



«СёрчИнформ КИБ»

Система защиты информации от утечки (DLP) «СёрчИнформ КИБ» блокирует утечки информации и обнаруживает признаки корпоративного мошенничества: откатов, боковых схем, саботажа, воровства.



«СёрчИнформ Файловый Аудитор»

Система аудита и защиты файловых ресурсов (DCAP) «СёрчИнформ Файловый Аудитор» («СёрчИнформ FileAuditor») классифицирует критичные данные, позволяет управлять доступом к ним и контролирует операции в файловой системе.



«СёрчИнформ Мониторинг безопасности»

Система управления инцидентами ИБ (SIEM) «СёрчИнформ Мониторинг безопасности» («СёрчИнформ SIEM») проводит мониторинг событий безопасности в корпоративной ИТ-инфраструктуре, выявляет сбои оборудования и ПО, признаки внешних атак и опасные действия пользователей.



«Аутсорсинг ИБ»

Сервис информационной безопасности по подписке без трудозатрат со стороны заказчика. ИБ-аналитик возьмет на себя мониторинг и реагирование на них, расследование инцидентов и отчеты перед заказчиком.



«СёрчИнформ КИБ» и другие инструменты внутренней ИБ можно развернуть в облаке. Компания получит защиту по подписке без единовременных затрат на закупку лицензий ПО и оборудования, на котором такой софт должен работать.

Больше аналитики и новостей безопасности читайте на сайте компании searchinform.ru, в телеграм-канале или в MAX.

Белые книги, памятки, чек-листы и результаты исследований можно посмотреть на сайте searchinform.ru в разделе «Практика и аналитика».