SEARCHINFORM

INFORMATION SECURITY

Комплексная защита от внутренних угроз

searchinform.ru

1995
сложилась команда «СёрчИнформ»

Москва, Россия
головной офис

2 000 000+
компьютеров под защитой продуктов «СёрчИнформ»

3 000+ клиентов по всей России и в 20+ странах

7 решений для комплексной защиты данных от угроз

2019
открытие направления
аутсорсинга DLP

2020
запуск услуги
DLP в облаке

65 вузов-партнеров в России и СНГ

Сертификат соответствия ФСТЭК
№4144 по требованиям безопасности информации № РОСС RU.0001.01БИ00

Лицензия ЦЛСЗ ФСБ России
№0015110 на осуществление разработки и производства средств защиты конфиденциальной информации

2016 продукты в Едином реестре российского ПО

2018 и 2020 лауреат национальной премии **«Цифровые вершины»**

Учебный центр «СёрчИнформ»:

6 курсов
повышения квалификации для ИБ-специалистов

2 курса
повышения ИБ-грамотности для рядовых пользователей

2020
«СёрчИнформ» - в топ-5 технологических компаний РФ по версии РВК «ТехУспех»

2017
DLP-система в «магическом квадранте»
Gartner Magic Quadrant
for Enterprise Data Loss Prevention

2020 SIEM-система – победитель конкурса
«Лучшие цифровые решения»

Продукты и услуги

СёрчИнформ КИБ

Защищает компанию от утечек конфиденциальной информации, корпоративного мошенничества и других инцидентов безопасности, связанных с человеческим фактором.

Контролирует все популярные каналы передачи данных, анализирует информацию, выявляет и предотвращает нарушения, предоставляет отчеты ИБ-службе.

Как КИБ помогает бизнесу

- Защищает конфиденциальные данные во время использования, хранения и перемещения.
- Блокирует нежелательные действия пользователей с чувствительной информацией.
- Выявляет факты корпоративного мошенничества и незаконные схемы обогащения за счет компании.
- Собирает детальную информацию о пользовательской активности за ПК для пошаговой реконструкции нарушения.
- Берет под контроль средства удаленного управления и виртуализации (TeamViewer, RAdmin, RDP).
- Шифрует данные, чтобы их нельзя было использовать за пределами компании.
- Сохраняет архив перехваченной информации, чтобы соблюдать требования регуляторов и проводить расследования.
- Предупреждает об аномалиях в сети, например, о копировании или удалении большого количества файлов.
- Следит за использованием рабочего времени и продуктивностью работы персонала.
- Анализирует настроения в коллективе и помогает управлять лояльностью.

КИБ в облаке

Чтобы бизнесу не приходилось выбирать между безопасностью, удобством и экономией средств, DLP-систему можно развернуть в облаке. Это не требует специального оборудования: КИБ собирает, обрабатывает и хранит данные в виртуальном пространстве. Такая схема внедрения подойдет компаниям без собственной IT-инфраструктуры, с филиалами в разных городах, с большим штатом удаленных сотрудников.

Перехват информации

КИБ состоит из модулей, каждый из которых контролирует определенный канал передачи информации.

MailController

Перехватывает отправленные и принятые письма, переданные в почтовых клиентах и через веб-сервисы, включая Gmail, Outlook.com, Yandex.Mail, Office 365. Фиксирует отправку информации на некорпоративную почту, email-адреса конкурентов. Блокирует передачу сообщений, если их содержание ставит под угрозу конфиденциальность корпоративной информации.

FTPController

Проверяет трафик, передаваемый через FTP- и FTPS-соединение, уведомляет ИБ-службу об инцидентах или блокирует соединение.

HTTPController

Защищает трафик, переданный по HTTP/HTTPS-протоколам. При необходимости блокирует веб-трафик, включая веб-мессенджеры, облачные сервисы, почту, блоги, форумы, соцсети и поисковые запросы. Продолжает контроль даже при использовании сервисов-анонимайзеров.

IMController

Перехватывает чаты, историю сообщений, звонки и списки контактов в мессенджерах: Skype, Telegram, Viber, WhatsApp, Lync/Skype For Business, ICQ 10, QIP, Slack и др. Контролирует переписку через веб-сервисы в соцсетях Facebook, «ВКонтакте», LinkedIn, «Одноклассники».

ProgramController

Собирает данные об активности пользователей за ПК и о времени, проведенном в приложениях, программах и на сайтах. Автоматически определяет, работает сотрудник или открыл программу «для вида». Сортирует веб-ресурсы по группам: знакомства, музыка, магазины, новости и др.

Помогает контролировать действия удаленных сотрудников.

PrintController

Инспектирует содержимое отправленных на печать документов: копирует текстовые файлы, сохраняет сканы в виде графического «отпечатка» и распознанного текста. Обнаруживает документы, заверенные печатью, позволяет контролировать печать бланков строгой отчетности.

MonitorController

Ведет фото- и видеорегистрацию действий за ПК. Собирает данные об открытых окнах и процессах, активных в момент съемки. При необходимости показывает информацию в режиме реального времени. Регистрирует изображения с веб-камеры для идентификации нарушителя.

Keylogger

Фиксирует клавиатурный ввод и данные, копируемые в буфер обмена. Позволяет перехватывать логины и пароли и отслеживать аккаунты сотрудника на «потенциально опасных» ресурсах. Определяет пользователей, вводивших с клавиатуры пароли к зашифрованным документам.

CloudController

Контролирует файлы, принятые и отправленные в облачные хранилища и файлообменные сервисы: Google Docs, Office 365, Evernote, iCloud Drive, Dropbox, Яндекс.Диск, Amazon S3, DropMeFiles, CMIS и др. Проверяет данные, уже хранящиеся в облаке. Перехватывает файлы, отправленные и полученные через TeamViewer, RealVNC, RAdmin, LiteManager. Контролирует документы, передаваемые через SharePoint.

DeviceController

Перехватывает и блокирует информацию, переданную на USB-накопители, внешние диски, CD/DVD, через RDP-сессии и камеры. Автоматически шифрует данные, записываемые на флешку. Обнаруживает, подключенные к ПК смартфоны (Android, Apple, BlackBerry, Windows Phone), анализирует их содержимое при подключении в режиме накопителя. Разграничивает доступ устройств к ПК.

MicrophoneController

С помощью любого обнаруженного микрофона записывает переговоры в офисе и за его пределами. Включает запись звука еще до авторизации пользователя в системе – при обнаружении речи, запуске процессов и программ, заданных политикой безопасности. Аудиопоток может быть преобразован в текст, по которому также выполняются заданные политики безопасности.

Центр управления

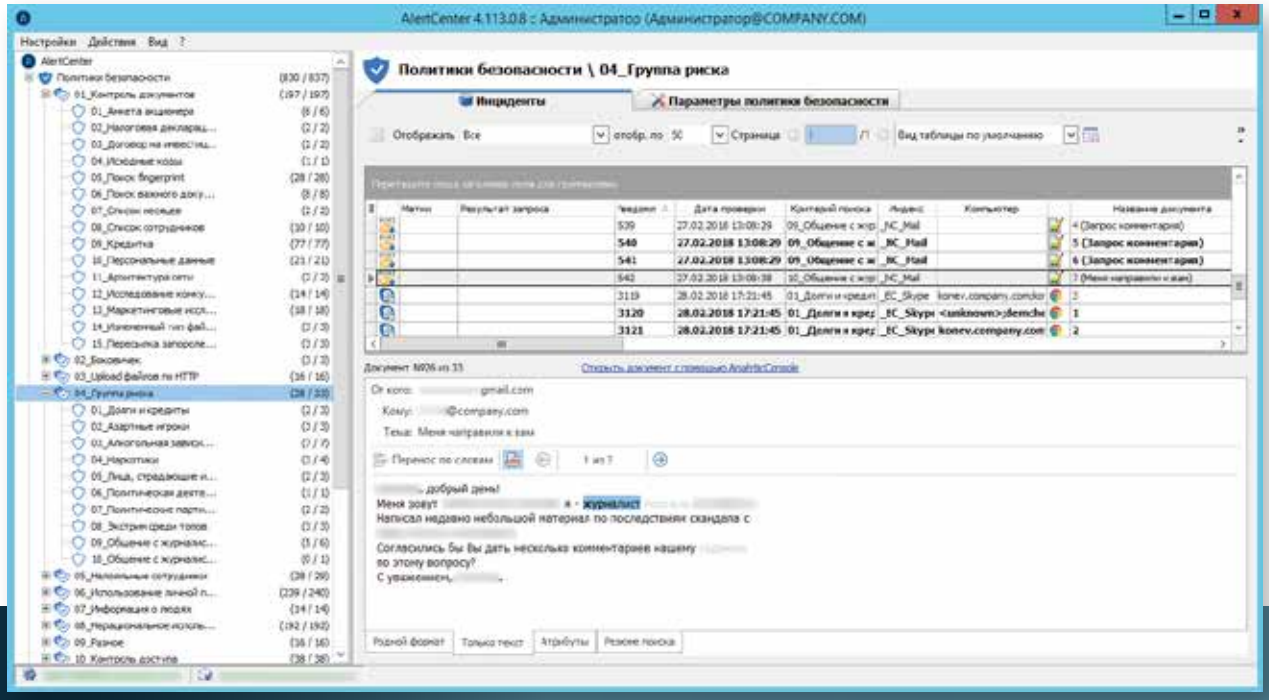
DataCenter

Управляет индексами и базами данных продуктов, администрирует уровни доступа, контролирует работоспособность комплекса и обеспечивает его взаимодействие со сторонними системами, например, AD, SOC, сервером исходящей почты.

AlertCenter

«Мозговой центр» системы, где настраиваются политики безопасности. В распоряжении ИБ-специалиста 250+ готовых политик, которые можно редактировать. Также в AlertCenter можно создавать собственные правила сканирования информации, настраивать расписание проверок и отправку уведомлений.

Просматривать инциденты можно через консоль AlertCenter, установленную на рабочем ПК сотрудника ИБ-службы, или через веб-интерфейс, доступный с ноутбука, планшета, смартфона.



Политики безопасности и просмотр результатов поиска в AlertCenter

Analytic Console

Служит для поиска и углубленного анализа собранных данных, а также для онлайн-наблюдения за компьютерами работников. В распоряжении ИБ-специалиста различные поисковые алгоритмы и предустановленные шаблоны отчетов.

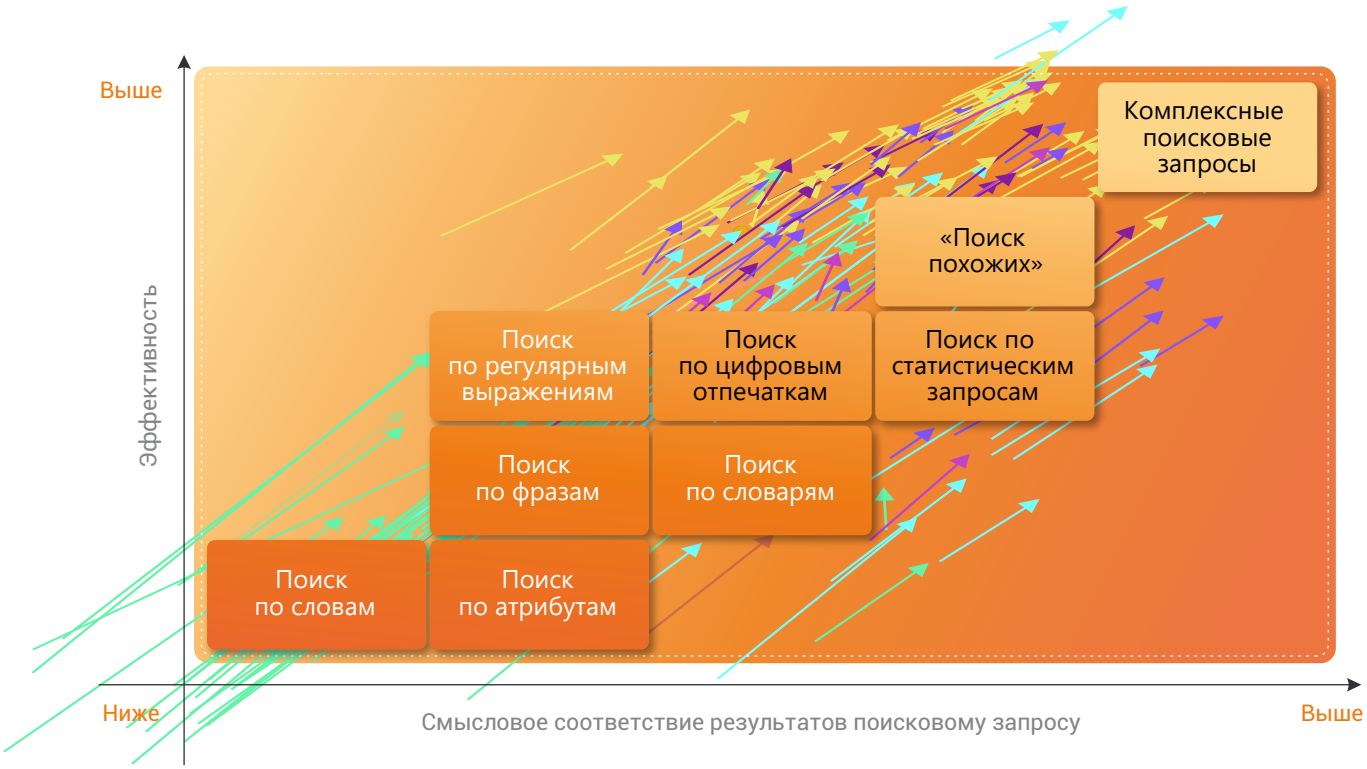
Просмотр отчетов, созданных в Analytic Console, **доступен** также **через веб-версию консоли**.

Аналитический модуль

Для эффективной работы ИБ-отдела необходим не только полный перехват по всем каналам, но и корректный поиск по собранной информации, ее анализ. Мощный аналитический модуль, разнообразные виды поиска, автоматизированный анализ графики и аудио позволяют одному специалисту по безопасности контролировать несколько тысяч работников.

Анализ текста

Разнообразие алгоритмов обеспечивает глубокую проверку текстовых сообщений и документов. Среди поисковых технологий есть уникальные. Например, запатентованный алгоритм для смыслового анализа «Поиск похожих», который находит конфиденциальные документы, похожие на поисковый запрос не только «технически», но и по смыслу. Поиск по сложным запросам объединяет несколько алгоритмов, связывая простые запросы логическими операторами И, ИЛИ и НЕ.



Анализ графики

Встроенная в КИБ OCR (система распознавания символов) анализирует содержимое изображений разных типов (фотографии, PDF-файлы, скан-копии). Система определяет документы установленных образцов: паспорта, банковские карты, водительские удостоверения и другие. Технология позволяет находить в архиве персональные, финансовые и любые другие чувствительные данные, даже если они передавались в формате отсканированных документов.

Анализ аудио

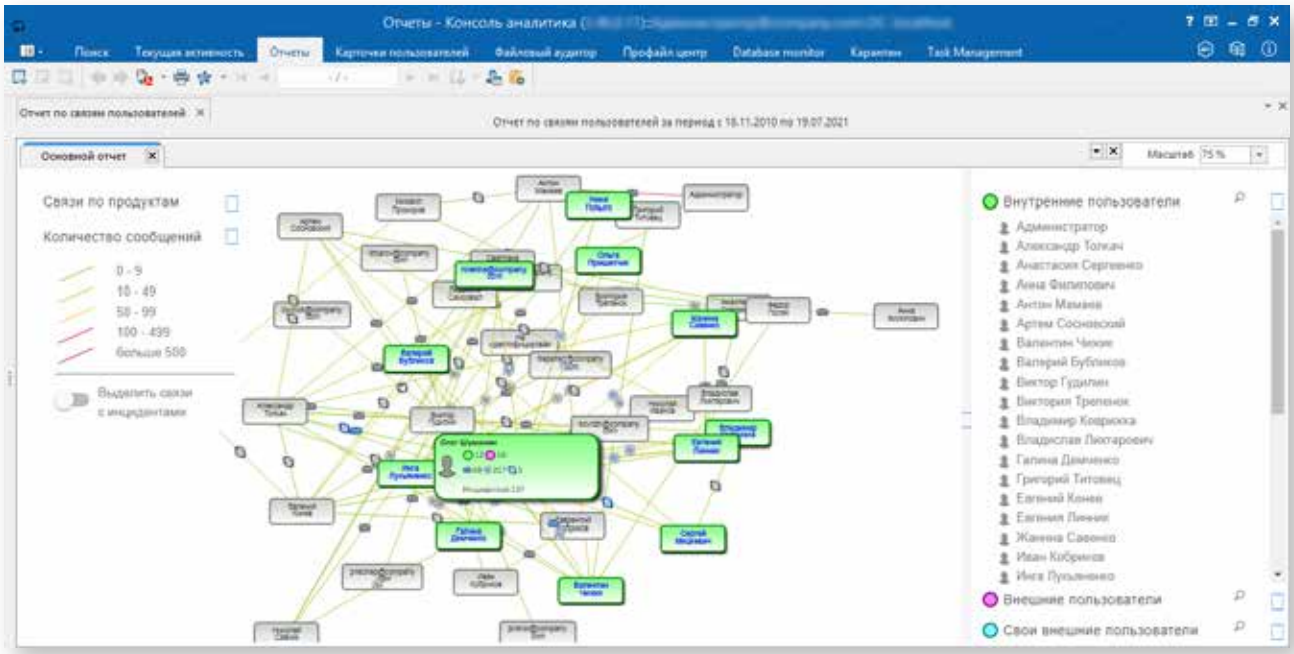
КИБ преобразовывает в текст перехваченные аудиозаписи и проверяет расшифровку на соответствие политикам безопасности. Запись переговоров активизируется при обнаружении речи или при запуске процессов и программ, заданных политикой безопасности.

Отчеты

Все события и связи внутри компании КИБ визуализирует в отчетах – в Консоли аналитика и веб-интерфейсе. В системе насчитывается 30+ базовых шаблонов. Мастер отчетов позволяет построить собственный отчет, не ограниченный критериями.

Отчет по связям пользователей

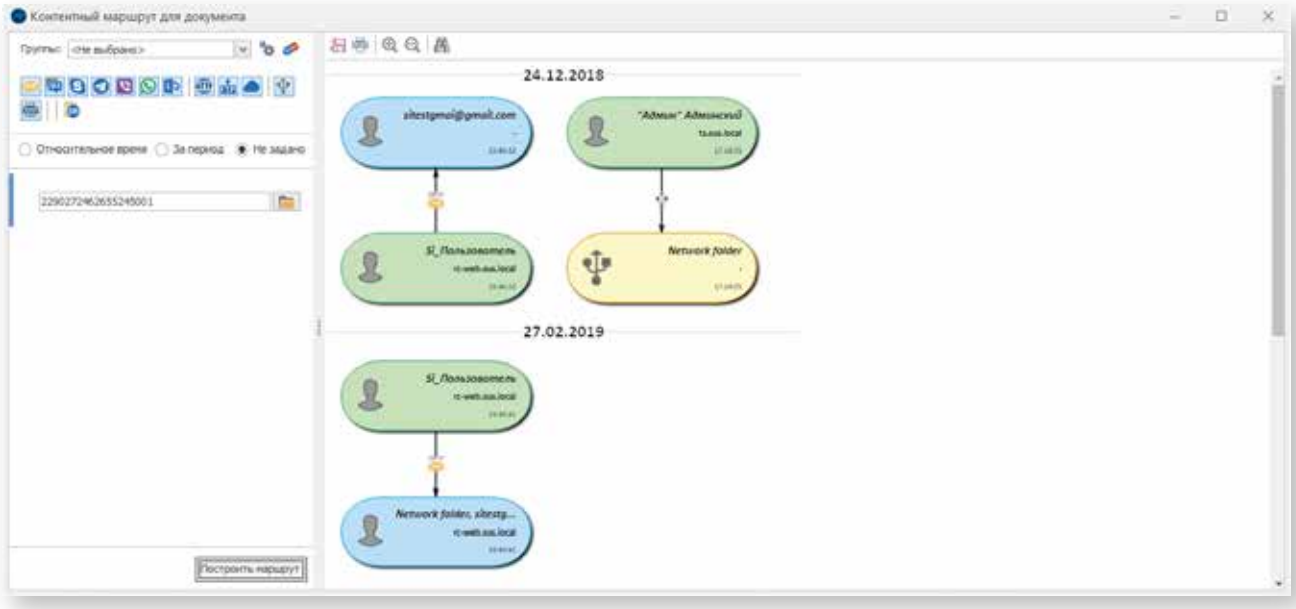
Отображает связи сотрудников между собой и с внешними адресатами в виде графа отношений. Позволяет увидеть активность пользователей по всем каналам коммуникации или по выбранной линии связи. Облегчает служебные расследования.



Граф отношений, построенный в веб-версии Консоли аналитика

Отчет о перемещении файла

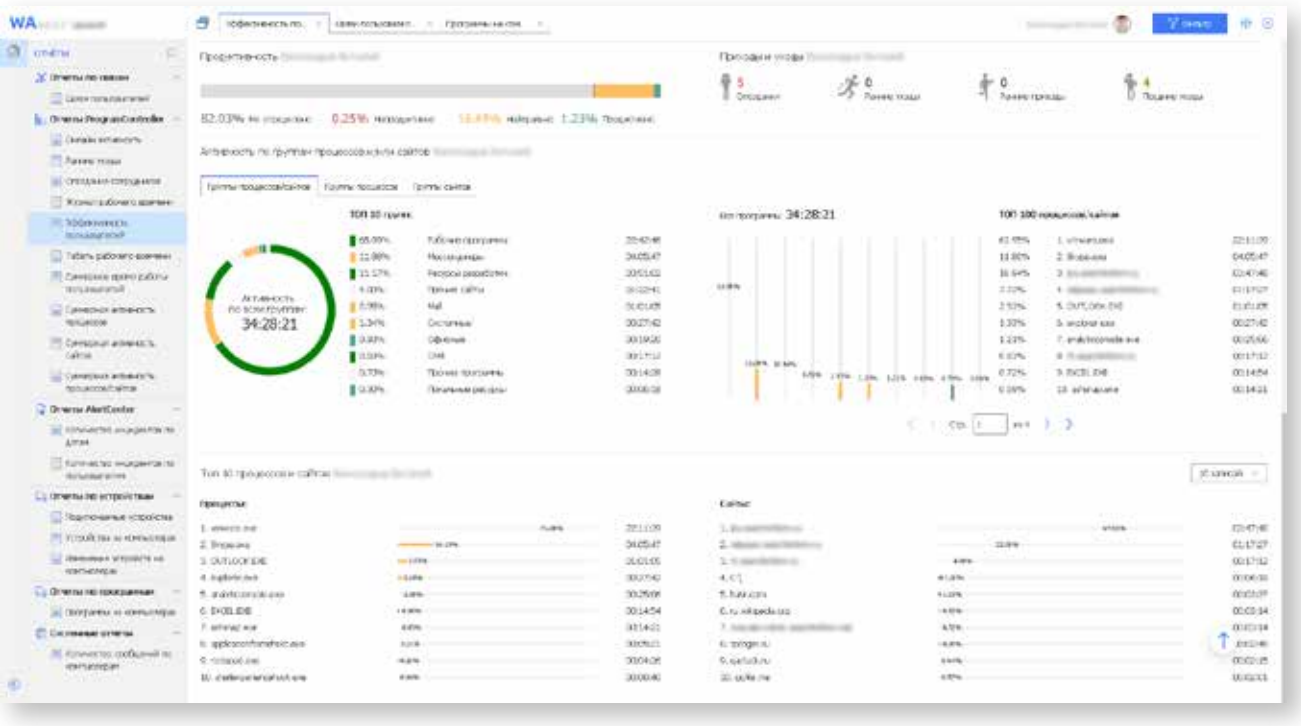
Делает прозрачным перемещение документа от отправителя к получателю по внутренним и внешним каналам связи. Позволяет оперативно установить автора документа, источник и пути распространения информации.



Контентный маршрут

Отчет по эффективности пользователей

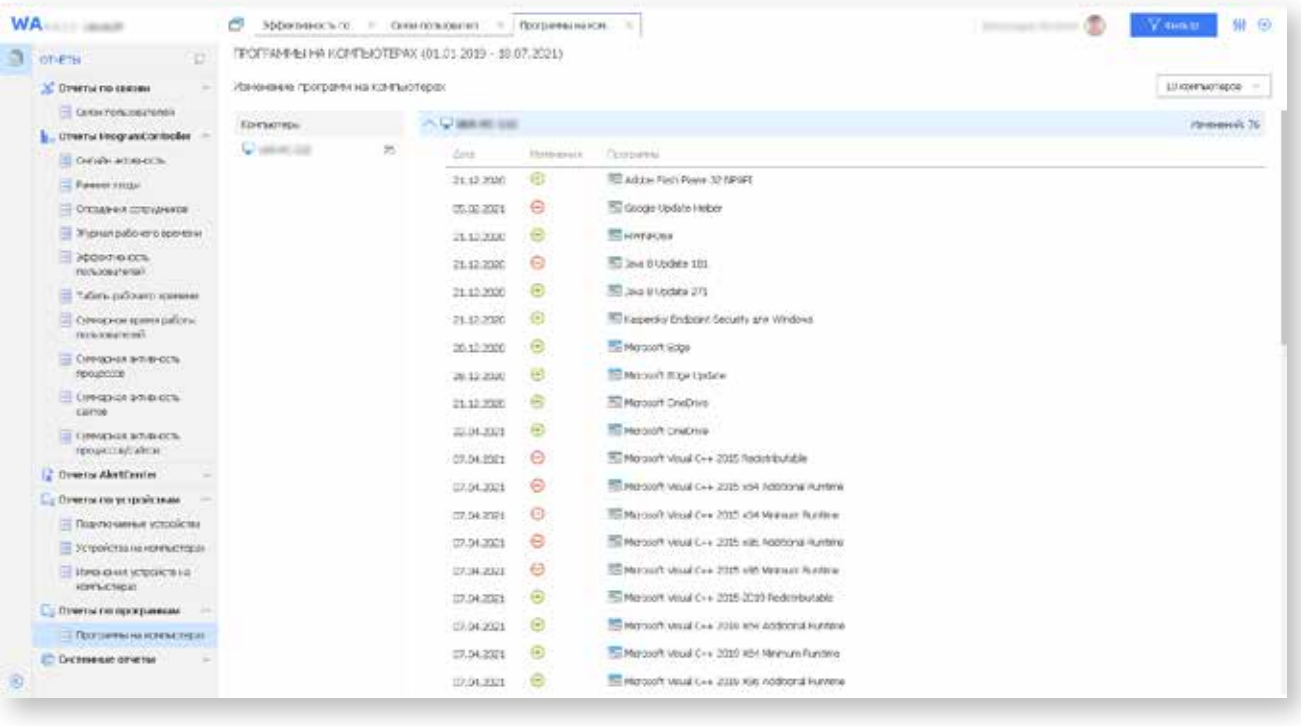
Отражает общую продуктивность сотрудников компании в виде диаграмм и рейтингов. Фиксирует частоту ранних уходов и приходов, количество опозданий. Визуализирует эффективность пользователей в течение рабочей недели в формате календаря.



Отчет по эффективности пользователя

Отчет по программам и устройствам

Упорядочивает данные об установке и удалении программ. Отражает изменения в устройствах, подключаемых пользователями к ПК, что облегчает инвентаризацию и страхует от краж и подмены оборудования.



Отчет по изменению программ на устройствах

Преимущества

Простое внедрение с сохранением структуры сети

Собственным IT-специалистам заказчика под силу инсталлировать КИБ за несколько часов. Внедрение не влияет на работу внутренних информационных систем компании.

Инструменты для пошагового расследования инцидентов

Запись переговоров и перехват содержимого мониторов в онлайн-режиме, аудит файловых операций, контроль клавиатурного ввода и видеосъемка в радиусе действия веб-камеры – встроенные компоненты системы позволяют восстановить нарушение по шагам.

Контентный маршрут документов

Наглядно показывает перемещение документов, указывает отправителя и получателей, а также каналы связи, использованные для передачи данных.

Визуализация связей между сотрудниками

Интерактивный граф отношений дает наглядное представление о круге общения и контактах по основным каналам коммуникации внутри компании и с внешними адресатами.

Мощный аналитический модуль

Позволяет быстро и гибко настраивать оповещения и анализировать информационные потоки. С помощью КИБ один специалист по безопасности может контролировать несколько тысяч сотрудников.

Комплексность решения

Многокомпонентная структура позволяет контролировать каналы утечек информации в комплексе или комбинировать модули в зависимости от потребностей, что снижает стоимость решения.

Возможность развертывания в облаке

Серверные, клиентские и агентские компоненты КИБ можно развернуть на облачной платформе («СёрчИнформ», Microsoft Azure или другого провайдера) без ущерба для функционала системы. Такой формат защиты данных экономит ресурсы на закупку и обслуживание «железа».

Адаптация для малых офисов и филиалов

Позволяет использовать систему в удаленных филиалах с небольшим количеством ПК и «узким» каналом связи. Данные фильтруются, обрабатываются, шифруются локально и только затем передаются на основной сервер.

Агенты контроля для российских ОС

КИБ работает под наиболее распространенными дистрибутивами Linux, включая российские ROSA Linux, GosLinux, Astra Linux, а также на РЕД ОС.

Интеграция с другими ИБ-продуктами

«СёрчИнформ КИБ» бесшовно интегрирован с SIEM, ProfileCenter, FileAuditor и Database Monitor, что многократно повышает уровень информационной безопасности компании, сокращает время реакции на инцидент, дает возможность максимально полно расследовать нарушения.

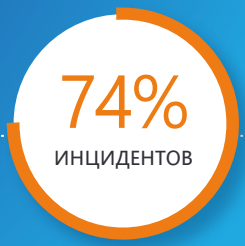
Отдел внедрения и Учебный центр

Опыт работы с 3 000+ компаниями из разных отраслей позволяет оперативно создавать уникальные наборы политик безопасности, ориентированные на актуальные задачи и специфику деятельности заказчиков.

«СёрчИнформ ProfileCenter»

74% инцидентов информационной безопасности* происходят по вине рядовых сотрудников.

Они нарушают правила и становятся инсайдерами умышленно или под давлением обстоятельств.



**По данным исследования уровня ИБ в российских и зарубежных компаниях в 2019 году.*

Задача ИБ-службы компании – смоделировать риск, предвидеть действия сотрудника и предотвратить инцидент.

Решить эту задачу помогает ProfileCenter – набор инструментов для анализа личности человека, прогнозирования его поведения, выявления сильных и слабых сторон и определения криминальных тенденций в характере.

Зачем профайлинг бизнесу

В бизнесе методы профайлинга используют для разоблачения мошенничества, управления кадрами, просчета рисков личности для окружающих или компании.

ProfileCenter выявляет:

- Криминальные тенденции и склонности.
- Основные черты характера, сильные и слабые стороны.
- Модель поведения в конфликтной ситуации.
- Роль сотрудника в коллективе, его социальные связи.
- Скрытое отношение к происходящему.
- Базовые эмоции.

«СёрчИнформ ProfileCenter» делает это автоматически – на основе данных, собранных DLP-системой.

Как работает ProfileCenter

ШАГ 1

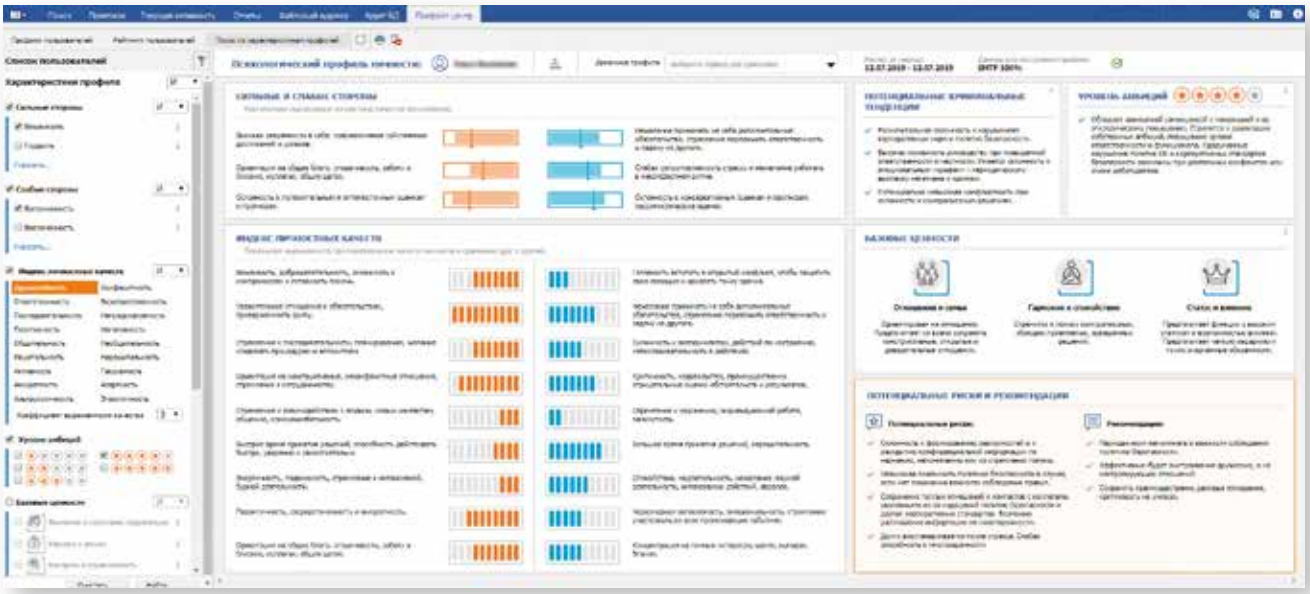
DLP собирает переписку сотрудника: исходящие письма, сообщения в Skype, WhatsApp, Telegram, других мессенджерах и соцсетях.

ШАГ 2

Модуль вычисляет базовые линии поведения и структуру мышления на основе оценки текста по 150+ критериям.

ШАГ 3

Результаты анализа отображаются в отчете с пояснениями и практическими рекомендациями.

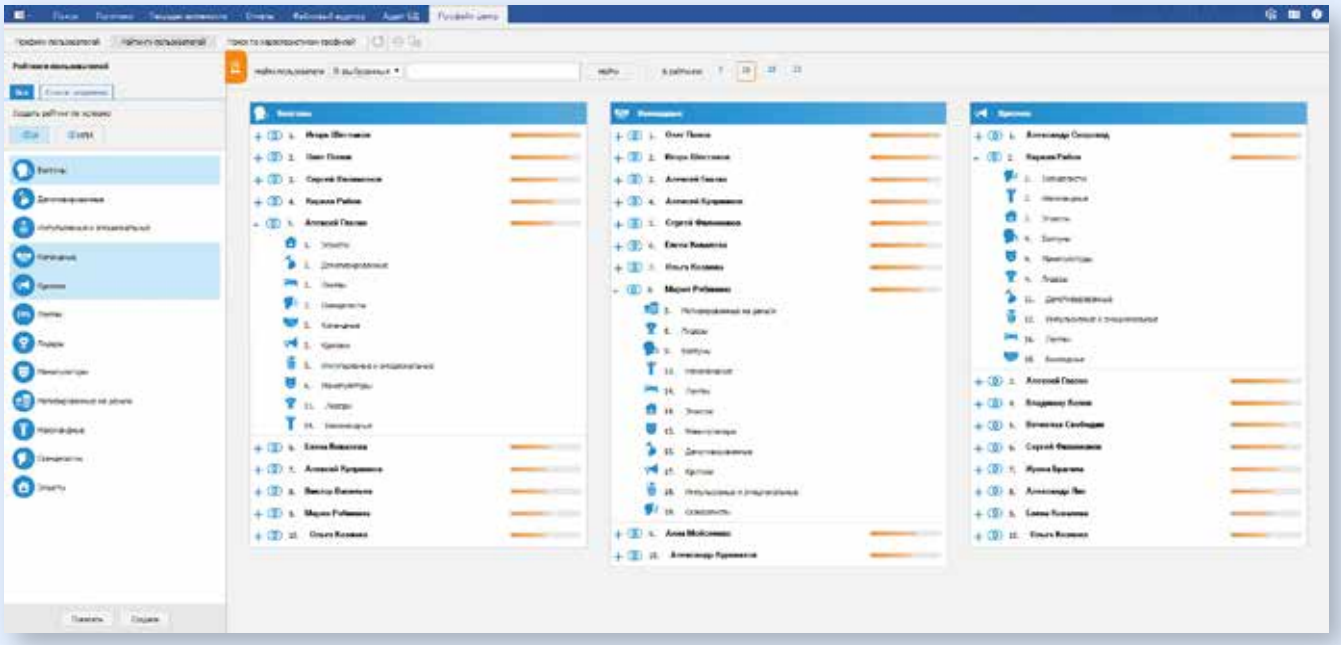


Психологический профиль личности

Помощь в принятии решений

Модуль дает практические рекомендации:

- На что обращать внимание в поведении сотрудника.
- Как сформировать эффективную команду.
- Наблюдать за сотрудником постоянно или время от времени.
- Насколько безопасно давать сотруднику доступ к конфиденциальной информации, финансовым активам и ценным ресурсам.
- Подходит или нет сотрудник на определенную должность.
- С кем в коллективе сохранять подчеркнуто деловые, формальные отношения, а с кем, наоборот, наладить дружеские связи.
- Кому из сотрудников достаточно профилактической беседы, а кого следует более сурово наказывать за нарушение правил.



Рейтинг пользователей

Преимущества

- Экономит расходы на эксперта-профайлера за счет автоматизации и быстрого анализа результатов.
- Анализирует данные, собранные DLP, актуальность которых выше, чем при открытом тестировании.
- Отслеживает изменения характеристик профиля в динамике.
- Не отвлекает персонал от работы и не нагнетает обстановку.
- Отражает перемены настроений в коллективе.

СёрчИнформ SIEM

IT-инфраструктура компании состоит из множества корпоративных систем: сетевых экранов, ОС, почтовых серверов, БД, сетевых устройств.

Многие из них – источники данных, которые интересны злоумышленникам, то есть нуждаются в особой защите.

- ПЕРВАЯ «КОРОБОЧНАЯ» SIEM.
- СОЗДАНИЕ ПОЛИТИК В 2 КЛИКА.

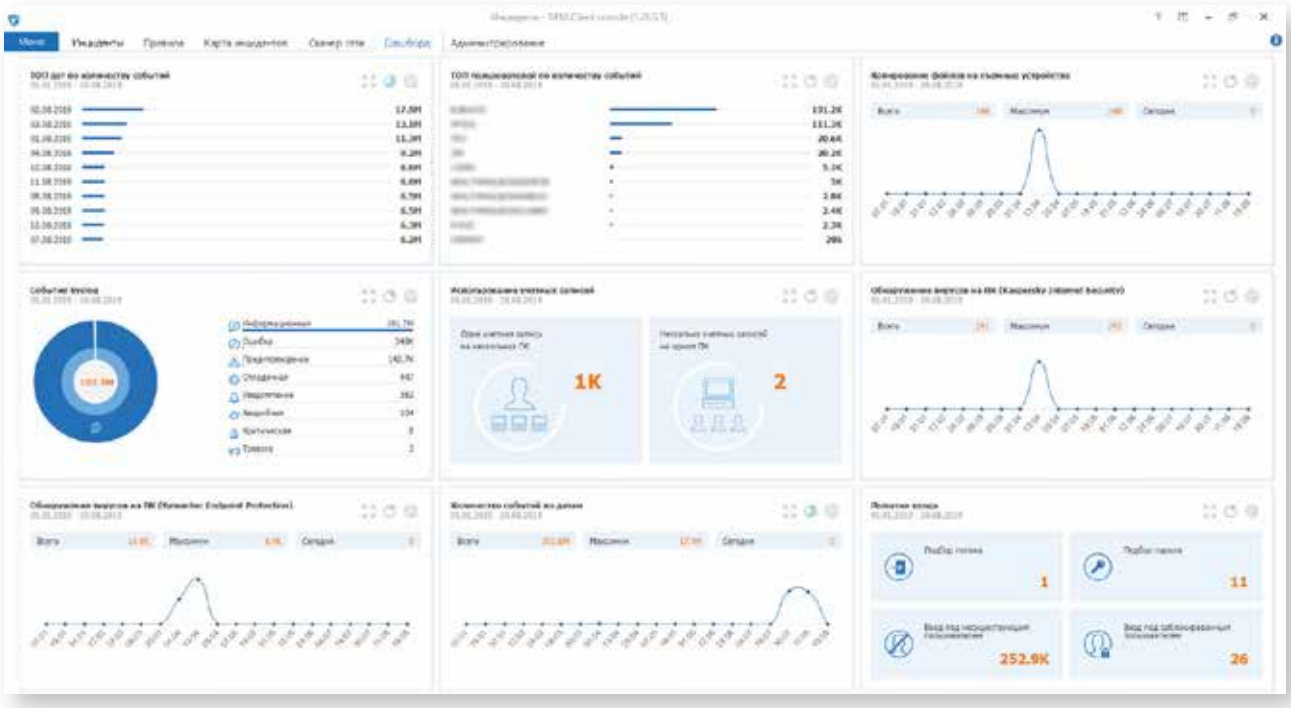
№1

Автоматический контроль событий безопасности

«СёрчИнформ SIEM» – система управления событиями информационной безопасности в реальном времени, помогает выявлять ИБ-инциденты и реагировать на них. Аккумулирует информацию из различных источников, анализирует ее, фиксирует инциденты и оповещает о них ИБ-службу.

«СёрчИнформ SIEM» выявляет:

- Вирусные эпидемии и отдельные заражения.
- Попытки несанкционированного доступа к данным.
- Подбор паролей к учетным записям.
- Активные аккаунты уволенных сотрудников, которые забыли удалить.
- Ошибки конфигурации оборудования.
- Нарушения допустимого температурного режима работы оборудования.
- Удаление информации с критически важных ресурсов.
- Использование корпоративных ресурсов в нерабочее время.
- Удаление виртуальных машин и снапшотов.
- Подключение к IT-инфраструктуре нового оборудования.
- Изменение групповых политик.
- Использование TeamViewer, удаленный доступ к корпоративным ресурсам.
- Критические события в средствах защиты.
- Другие ошибки и сбои в работе информационных систем.



Дашборд со статистикой событий

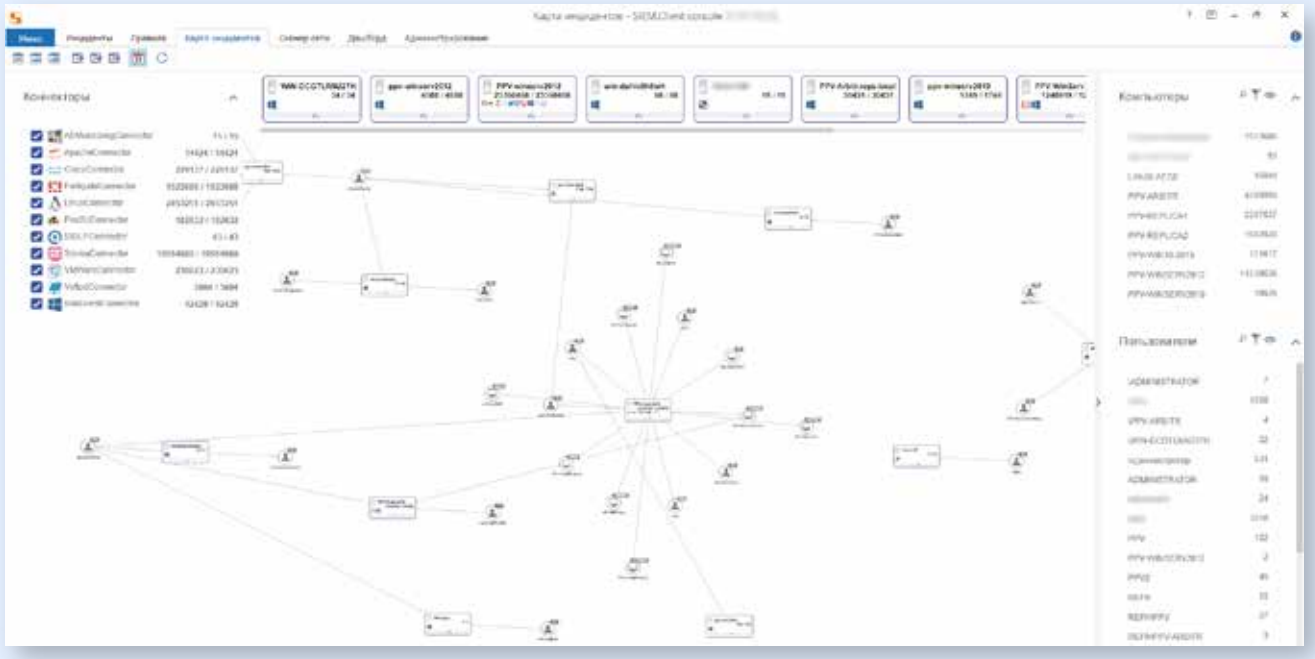
Предустановленные политики безопасности

После установки системы служба ИБ получает доступ к 300+ готовым правилам – политикам безопасности. Пользователи могут редактировать и настраивать уже существующие правила и создавать уникальные политики, выбирать источники из предустановленного списка и подключать собственные (функция «пользовательский коннектор»).

Политики безопасности «из коробки» используют следующие источники данных:

- операционные системы;
- почтовые серверы;
- контроллеры домена и рабочих станций;
- серверы и рабочие станции Linux;
- СУБД;
- DLP-системы;
- файловые серверы;
- среды виртуализации;
- антивирусы;
- межсетевые экраны и устройства комплексной сетевой безопасности;
- решения на платформе 1С;
- иные Syslog-источники.

Для поиска инцидентов в связке событий из разных источников можно настроить правила кросс-корреляции.



Карта инцидентов

Преимущества

- Быстрое внедрение без долгой предварительной настройки (ПО может быть введено в эксплуатацию за один день).
- Интеграция с DLP-системой «СёрчИнформ КИБ» повышает уровень информационной безопасности компании и дает возможность максимально полно расследовать инцидент, собрать доказательную базу.
- Простое использование: с программой справится специалист без IT-навыков, т.к. для создания правил корреляции и кросс-корреляции не нужно знать языки программирования.
- Невысокие требования к аппаратно-программным средствам и приемлемая даже для малого и среднего бизнеса ценовая политика.

СёрчИнформ FileAuditor

Объем данных в средней компании огромен. И некоторая их часть содержит конфиденциальные сведения: ПДн, финансовые отчеты, спецификации, чертежи и т.д. Каждая группа данных должна храниться, обрабатываться и распространяться по своим правилам.

Важные данные всегда на виду

«СёрчИнформ FileAuditor» – DCAP-решение (data-centric audit and protection) для автоматизированного аудита файловой системы, поиска нарушений прав доступа и отслеживания изменений в критичных данных. Защищает конфиденциальные документы от опасных действий сотрудников и наводит порядок в файловых хранилищах.

Как FileAuditor решает задачу контроля за безопасностью критичных данных:

Классификация чувствительных данных

Позволяет навести порядок в файловой системе: выделить в документообороте файлы, которые содержат критичную информацию, присвоить им метку определенного типа (ПДн, коммерческая тайна, номера кредитных карт и т.д.).

Архив критичных документов

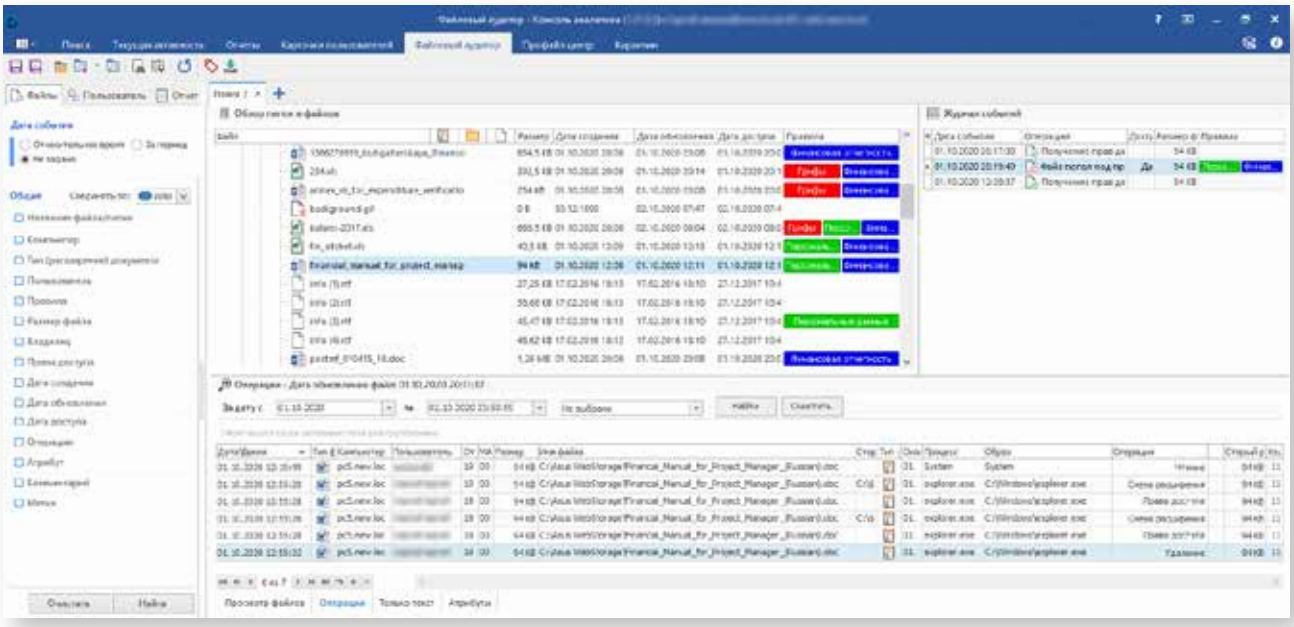
Делает теневые копии критичных файлов, найденных на ПК сотрудников, и сохраняет историю их редакций. Архив помогает в расследовании инцидентов, а теневые копии служат гарантией восстановления утраченной информации.

Аудит прав доступа

Контролирует права доступа к информации (полный доступ, редактирование, чтение, запись, чтение и изменение и др.). Отслеживает сотрудников, которые имеют неправомерный доступ к данным. Находит конфиденциальные файлы, хранящиеся с нарушением установленных правил (в открытом доступе, в общих сетевых папках, на ПК сотрудников и т.д.).

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.



Просмотр действий с файлом в режиме «Операции»

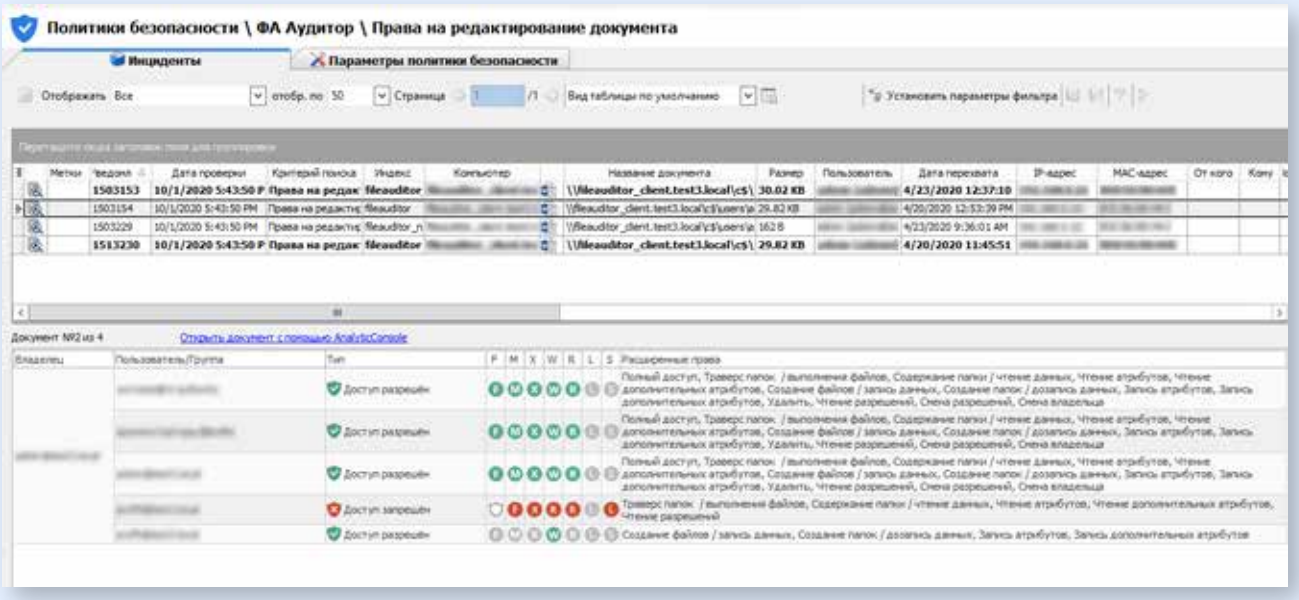
Анализ данных

Аналитический модуль FileAuditor визуализирует результаты сканирования файловой системы по заданным правилам. При настройке правил доступны разные виды поиска (по тексту, по атрибутам файлов, по регулярным выражениям, по словарю). Результаты поиска можно просмотреть в формате наглядных отчетов (по владельцам ресурсов, по правам доступа, по ошибкам) или в виде дерева.

Программа наглядно демонстрирует:

- дерево папок с указанием прав пользователей к каждому каталогу;
- операции с критичным файлами, даты их создания и модификации;
- маркировку файлов (секретный договор, секретные данные).

В AlertCenter можно настроить отправку уведомлений о нарушениях. Например, если FileAuditor найдет файл с чувствительной информацией на ПК сотрудника, у которого нет полномочий для его просмотра, специалист ИБ-службы получит автоматическое оповещение на email.



Сработки по политикам безопасности в AlertCenter

Собранная информация записывается в базы данных Microsoft SQL Server, а копии критичных файлов – в хранилище. Благодаря этому документы остаются доступными даже после удаления.

Преимущества

- Гибкая настройка правил избавляет службу ИБ от лишней работы, позволяя сосредоточиться на контроле только критичных данных.
- Отслеживание изменений документа – система сохраняет заданное число редакций, что помогает в служебных расследованиях.
- Возможность развертывания и работы в облаке.
- Контроль нагрузки на ПК и экономный расход «памяти» – проверка по расписанию; система дедупликации для экономии места и др.
- Проактивная защита файлов от изменений и пересылки – блокировки доступа к документам через любое приложение.
- Бесшовная интеграция FileAuditor с DLP расширяет функционал системы защиты от утечек данных.

СёрчИнформ TimeInformer

Присутствие сотрудника на работе не гарантирует, что он будет трудиться с полной отдачей. Работники часто устраивают перекуры и кофе-брейки, болтают с коллегами, сидят в с оцсетях, опаздывают или уходят раньше. В итоге работодатель оплачивает впустую потраченное время.

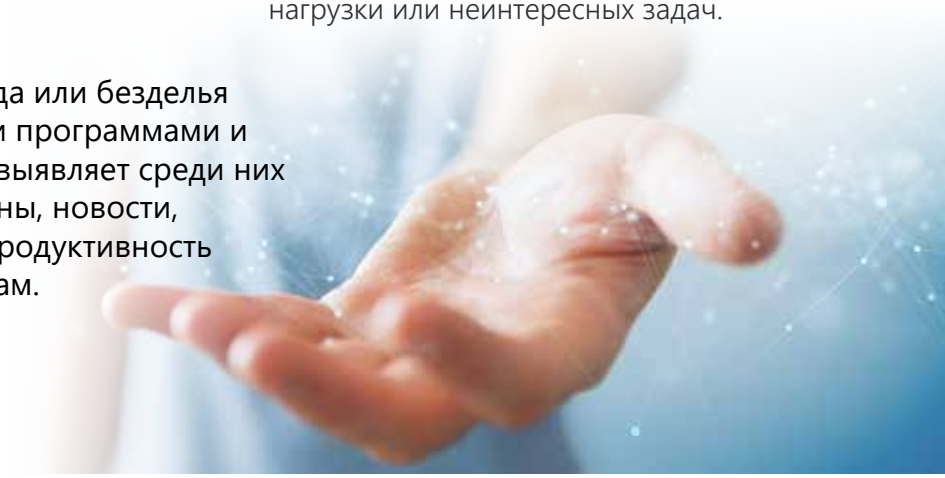
Тайная жизнь коллектива

TimeInformer – решение для мониторинга действий сотрудников за ПК, которое защищает бизнес от неэффективного труда и финансовых потерь, связанных с персоналом.

TimeInformer сканирует рабочие компьютеры и обнаруживает:

- **Нарушителей дисциплины** — поздно приходят, рано уходят, частят с перекурами и кофе-паузами;
- **Бездельников** — сидят в чатах, делают онлайн-покупки, отвлекаются на игры и частые перерывы;
- **Фрилансеров** — выполняют «левую» работу в часы, оплаченные компанией;
- **Недовольных** — настраивают коллектив против компании, выгорели от большой нагрузки или неинтересных задач.

Программа определяет время труда или безделья сотрудников, показывает, с какими программами и онлайн-ресурсами они работают, выявляет среди них сайты знакомств, интернет-магазины, новости, сериалы. И оценивает реальную продуктивность персонала по заданным параметрам.



SEARCHINFORM
INFORMATION SECURITY

Контроль в режиме реального времени

TimeInformer доступен для развертывания в облаке. Такой вариант не требует дополнительных затрат на закупку и обслуживание «железа».

Программа подключается к мониторам и микрофонам ПК и в режиме реального времени воспроизводит, что происходит на экранах ПК и в поле действия микрофона.

В онлайн-режиме можно записывать важные переговоры, а также увидеть, что на самом деле делает сотрудник за ПК в определенный отрезок времени. Служба ИБ может мониторить до 16 компьютеров одновременно.

Помощь в управленческих решениях

В программе доступно 33 шаблона отчетов, которые помогут обнаружить нарушителей и изменить загрузку людей так, чтобы поставленные бизнес-цели были достигнуты.

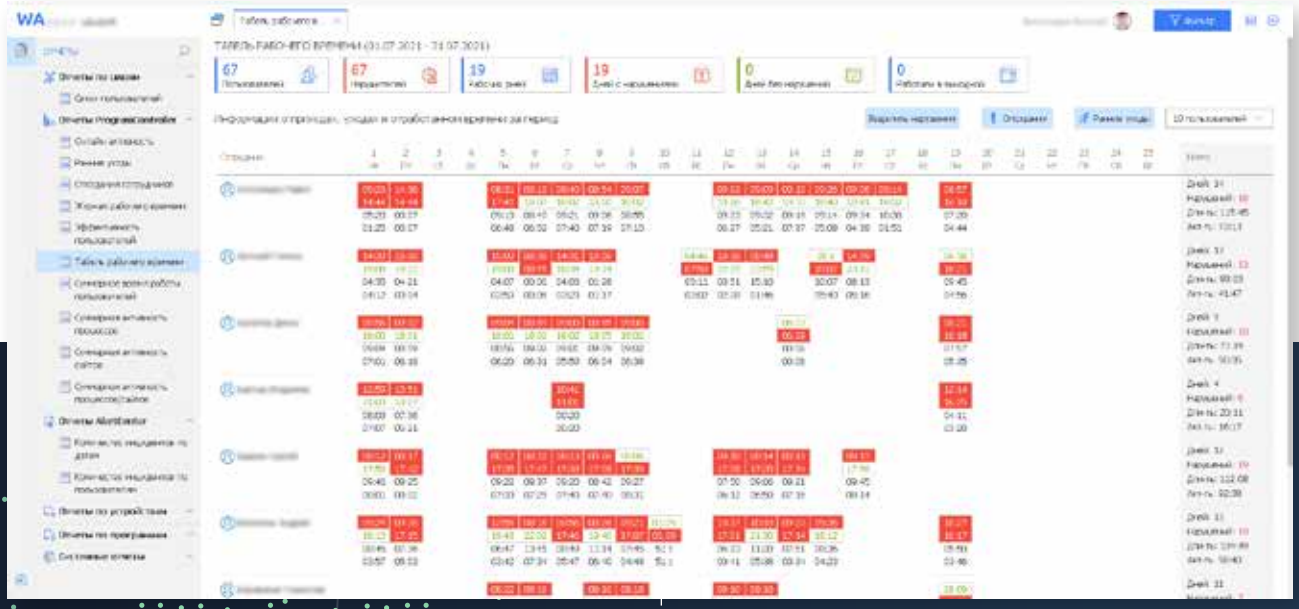
В TimeInformer доступны следующие группы отчетов:

- по активности пользователей в приложениях и на сайтах;
- по программам с историей установки и удаления ПО;
- по устройствам с данными об установленном на ПК оборудовании и изменениям в их комплектации.

Отчеты и оповещения можно настроить индивидуально. Уведомления о критичных нарушениях система высылает автоматически.

Удобство использования

Благодаря веб-интерфейсу контролировать персонал с помощью TimeInformer можно из любой точки мира. Права доступа к отчетам и административным функциям разграничиваются в зависимости от задач и должностных обязанностей. Автоматические оповещения о подозрительной активности сотрудников, при желании, можно получать на электронную почту.



Табель рабочего времени в веб-интерфейсе

Преимущества

- Защита от самостоятельного удаления с ПК и оповещение о подобных попытках.
- Контроль удаленных сотрудников, которые работают из дома или находятся в командировке.
- Наличие веб-интерфейса для доступа к результатам мониторинга вне офиса.
- Возможность интеграции с КИБ, что помогает при служебных расследованиях в отношении подозрительных сотрудников.

Аутсорсинг внутренней безопасности

Аутсорсинг информационной безопасности необходим компаниям, у которых нет выделенной службы безопасности либо недостаточно ресурсов для самостоятельного внедрения и обслуживания систем защиты данных.

Услуга позволяет решить проблему нехватки ИБ-кадров, минимизировать финансовые и трудовые затраты заказчика. Опытного ИБ-специалиста не нужно оформлять в штат, оплачивать ему отпуск и больничный, вкладываться в его обучение.

ИБ-аутсорсинг доступен для всех защитных решений от компании «СёрчИнформ». Некоторые из них можно развернуть в облаке, что избавляет компанию от затрат на закупку и обслуживание «железа».

	Можно взять на аутсорсинг?	Можно развернуть в облаке?
КИБ	+	+
ProfileCenter	+	+
SIEM	+	-
FileAuditor	+	+
TimeInformer	+	+

Как это работает

Персональный ИБ-аналитик настраивает систему в соответствии с задачами заказчика.

Заказчику предоставляются максимальные полномочия в системе.

Обнаружив инцидент, ИБ-аналитик связывается с заказчиком (способ связи оговаривается заранее).

ИБ-аналитик предоставляет заказчику отчеты по инцидентам за выбранный период (раз в день/неделю/месяц).

Заказчик может работать в системе совместно с ИБ-аналитиком или самостоятельно.

Заказчик может ставить персональному ИБ-аналитику конкретные задачи.

Задача – решение

Специалист заказчика контролирует этап развертывания программы, а также принимает управленческие решения по результатам полученных отчетов и расследованных инцидентов.

Краткий отчет по инцидентам					
№	Дата	Сотрудники связанные с инцидентом	Суть инцидента	Комментарии	Ссылка на документы
Конфиденциальная информация					
1		ФИО сотрудника	Сотрудник отправил с корпоративной почты на личную чертежи, принадлежащие компании.		ссылка на фактуру
2		ФИО сотрудника	Сотрудник выгрузил в облачное хранилище большое количество конфиденциальных документов, касавшихся дочерней компании.		ссылка на фактуру
3		ФИО сотрудника	Сотрудник скопировал на флешку базу данных, в которой содержались сведения о контрагентах компании.		ссылка на фактуру
4		ФИО сотрудника	Сотрудник компании скопировал на флешку файлы, содержащие программы для станков с ЧПУ.		ссылка на фактуру
5		ФИО сотрудника	Сотрудница скопировала на флешку проектную документацию.		ссылка на фактуру
6		ФИО сотрудника	Сотрудник бухгалтерии отправил с корпоративной почты на личную документы с информацией о зарплатах и премиях сотрудников компании.		ссылка на фактуру
Поиск работы					
7		ФИО сотрудника	Сотруднице на личную почту приходят письма от hh.ru с подходящими для неё вакансиями и информацией о просмотрах резюме.		ссылка на фактуру
8		ФИО сотрудника	Сотрудник с личной почты отправил анкету соискателя в компанию конкурента с просьбой рассмотреть его кандидатуру.		ссылка на фактуру
9		ФИО сотрудника	Сотрудница в социальной сети писала, что ищет работу в другом городе и в скором времени уволится из компании.		ссылка на фактуру
10		ФИО сотрудника	Из переписки в социальной сети стало ясно, что сотрудник планирует поработать пару месяцев и уволиться. К тому же играет в компьютерные игры в рабочее время и ведёт прямые трансляции (стримы) в интернете.		ссылка на фактуру
Подделка документов					
11		ФИО сотрудника	Сотрудник в графическом редакторе подделал счета и акты: изменил печать и подписи в договорах и допсоглашениях. По просьбе клиента сотрудник подделал сертификат соответствия на продукцию.		ссылка на фактуру
12		ФИО сотрудника	Сотрудник редактировал печать контрагента в графическом редакторе.		ссылка на фактуру
13		ФИО сотрудника	Сотрудник подделал командировочные документы.		ссылка на фактуру
14		ФИО сотрудника	Сотрудник компании с помощью графического редактора отредактировал в накладной вес поставляемого сырья.		ссылка на фактуру

Краткий отчет по инцидентам

Преимущества

- Обнаружение «болевых точек» компании за короткий период времени (первые результаты, как правило, получают в течение 1 месяца).
- Низкий порог входа: не нужно тратить несколько миллионов на лицензии ПО, оборудование, поиск и зарплату ИБ-специалиста, время на внедрение системы. Все это включено в ежемесячную подписку на ИБ-аутсорсинг.
- Непредвзятое отношение и профессиональный подход – специалист по ИБ-аутсорсингу не знает сотрудников компании лично, поэтому человеческий фактор при проведении расследований исключен.
- Использование опыта и базы знаний компании с более чем 3 000 клиентов. Персональный ИБ-аналитик сможет тонко настроить систему с учетом сферы деятельности компании, а также максимально эффективно использовать ее функционал.

Контакты

РОССИЯ

Москва (головной офис)

121069, Скатертный пер., 8/1, строение 1, этаж 2
Телефоны:
+7 (495) 721-84-06
+7 (495) 721-84-06, доб. 125 (техническая поддержка)
+7 (499) 703-04-57
Emails:
info@searchinform.ru – общие вопросы
support@searchinform.ru – технические вопросы
order@searchinform.ru – вопросы приобретения
pr@searchinform.ru – для прессы

Санкт-Петербург

Коломяжский пр-т, 27, Литер А, пом. 27Н
Телефоны:
+7 (812) 309-73-35
+7 (495) 721-84-06, доб. 119
Email: a.yanchuk@searchinform.ru

Екатеринбург

ул. Серафимы Дерябиной, 24, оф. 801
Телефоны:
+7 (495) 721-84-06, доб. 105, 117
+7 (343) 344-50-88
+7 (343) 344-51-38
Email: a.popov@searchinform.ru

Казань

ул. Островского, 57В, оф. 301–302
Телефоны:
+7 (495) 721-84-06, доб. 126
+7 (843) 206-07-43
+7 (965) 600-53-07
Email: t.latushkina@searchinform.ru

Новосибирск

ул. Владимировская, 2/1, оф. 109
Телефоны:
+7 (495) 721-84-06, доб. 106
+7 (913) 772-60-06
+7 (383) 280-46-57
Email: alena.bugaenko@searchinform.ru

Хабаровск

ул. Пушкина, 54, оф. 403
Телефоны:
+7 (495) 721-84-06, доб. 131
+7 (4212) 47-59-92
+7 (914) 427-98-60
Email: d.kirilenok@searchinform.ru

АРГЕНТИНА, Буэнос-Айрес

Гало 353, C1172ABG
Телефоны: +54 11 5984 2618
+54 911 5158 8557
Email: r.martinez@searchinform.com

БРАЗИЛИЯ, Сан-Паулу

Вила-Олимпиа, Руа Гомес де Карвальо 1356, оф.16
Телефон: +55 11 4380 1913
Email: v.prestes@searchinform.com

ВЕЛИКОБРИТАНИЯ, Лондон

Телефон: +44 (0) 203 808 4340
Email: uk@searchinform.com

КАЗАХСТАН, Алматы

ул. Ауэзова, 84, оф. 200
Телефоны: +7 (777) 239-30-36
+7 (727) 222-17-95
Email: d.stelchenko@searchinform.ru

ЮАР, Центурион

Блок 32, Кембриджский офисный парк,
ул. Баухиния, 5, Хайвелд технопарк, Центурион, 0157
Телефон: +27 12 683 8816
Email: jorina@searchinform.com