SEARCHINFORM

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1995
Год основания компании

Москва, Россия
головной офис

2000+ клиентов в 17 странах

1 200 000+
компьютеров под защитой DLP-системы

6 филиалов в России

6 представительств за рубежом

Статус резидента инновационного фонда **«Сколково»** 2015

Участник

Первый релиз DLP-системы
«КИБ СёрчИнформ»
2006

Первый релиз программы учета рабочего времени
TimeInformer
2014

Первый релиз
«СёрчИнформ SIEM»
2016

Первый релиз модуля
«КИБ СёрчИнформ ProfileCenter»
2018

Первая серия конференций
Road Show SearchInform

2011 в России

2018 в странах **Латинской Америки, Ближнего Востока и Африки**

Сертификат соответствия ФСТЭК

№3598 по требованиям безопасности информации №РОСС RU.0001.01БИ00

Лицензия ЦЛСЗ ФСБ России

№0015110 на осуществление разработки и производства средств защиты конфиденциальной информации

2016 Реестр российских разработчиков ПО

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

Открытие
Учебного центра
2010

Контур информационной безопасности

«Контур информационной безопасности СёрчИнформ» (КИБ) защищает от утечек конфиденциальной информации, мошенничества и других инцидентов в компании. КИБ контролирует максимальное количество каналов передачи данных, анализирует содержание информационных потоков, выявляет аномалии и нарушения и предупреждает о них специалиста по безопасности.

Благодаря встроенным аналитическим инструментам система берет под контроль человеческий фактор и обеспечивает комплексную защиту активов и репутации компании.

Как «КИБ СёрчИнформ» помогает бизнесу

Защищает конфиденциальные данные от утечек во время использования, хранения и перемещения.

Выявляет факты корпоративного мошенничества и незаконные схемы обогащения за счет компании.

Сохраняет архив перехваченной информации, что позволяет соблюдать требования регуляторов и проводить расследования.

Следит за использованием рабочего времени и продуктивностью работы персонала.

Анализирует настроения в коллективе и помогает управлять лояльностью.

Ведет постоянный аудит мест хранения и обнаруживает конфиденциальные данные, где бы они ни находились.

Предупреждает об аномалиях в сети, например, копировании на съемные устройства или удалении большого количества файлов.

Упрощает инвентаризацию ПО и оборудования.

Шифрует данные, таким образом их нельзя использовать за пределами компании.

Открывает доступ к веб-камере, микрофону и экрану рабочего ПК для наблюдения в онлайн-режиме, например, если нужно подтвердить подозрения.

Модульная архитектура, масштабируемость и гибкость системы позволяют «КИБ СерчИнформ» подстраиваться под нужды конкретного бизнеса и решать нестандартные задачи.

Компоненты системы

«КИБ СёрчИнформ» состоит из модулей, каждый из которых защищает определенный канал передачи информации. Заказчики используют модули в комплексе для наиболее полной защиты и комбинируют компоненты в зависимости от приоритетных задач.

MailController

Проверяет на соответствие политикам безопасности исходящие и входящие письма, переданные в почтовых клиентах и через веб-сервисы, включая Gmail, Outlook.com, Yandex.Mail, Office 365 и другие. Блокирует почту, переданную по протоколам SMTP и ICAP. Перехватывает личную почту (входящие, исходящие, черновики), просматриваемую на рабочем ПК через веб-интерфейс.

FTPController

Проверяет трафик, передаваемый через обычное (FTP) и шифрованное (FTPS) соединение, и предупреждает утечку «тяжелых» файлов, например, баз данных, программного обеспечения, сканированных документов, проектной документации, детализированных чертежей.

CloudController

Контролирует файлы, принятые и отправленные в облачные хранилища. Перехватывает данные в программах-клиентах и веб-сервисах. Отслеживает облачные и файлообменные сервисы: Google Docs, Office 365, Evernote, iCloud Drive, SharePoint, Dropbox, Яндекс.Диск, Amazon S3, DropMeFiles и другие.

SkypeController

Контролирует переписку, звонки, СМС и файлы, отправленные через чат. «Подтягивает» историю сообщений, даже если пользователь вел переписку вне офиса.

IMController

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

HTTPController

Перехватывает и индексирует файлы и сообщения, передаваемые по HTTP/HTTPS-протоколам. Контролирует данные, отправленные через браузер в чаты, блоги, форумы, соцсети. «Сканирует» запросы поисковой системы.

Продолжает контроль в штатном режиме, даже если сотрудники пользуются сервисами-анонимайзерами.

FileController

Контролирует операции с файлами, которые хранятся на серверах и в общих сетевых папках. Регистрирует открытие, копирование, редактирование, удаление, изменение формата и другие операции пользователей с файлами.

PrintController

Инспектирует содержимое отправленных на печать документов. Текстовые файлы – копирует, скан-копии перехватывает в виде графического «отпечатка» и распознанного текста. Обнаруживает среди документов заверенные печатью и контролирует печать бланков строгой отчетности. Ведет архив распечатанных документов.

ProgramController

Собирает данные об активности и времени, проведенном в приложениях. Автоматически определяет, работает сотрудник или открыл программу «для вида».

Суммирует время, проведенное на сайтах. Автоматически сортирует веб-ресурсы по группам: знакомства, музыка, магазины, новости, биржи труда и т.д. Каждые 10 минут собирает и распределяет по темам неизвестные ресурсы. Более 1 млн сайтов распределены по категориям в системе по умолчанию.

Индексация рабочих станций

Обнаруживает конфиденциальные документы, которые хранятся с нарушением политик безопасности на рабочих станциях, выделенных серверах и в местах общего хранения. Проверяет папки общего доступа (Shares), жесткие диски компьютеров (Local System) и общие ресурсы на платформе SharePoint.

Находит и переиндексирует новую или измененную информацию. Ищет в индексе по содержимому удаленных файлов.

MonitorController

Снимает скриншоты и записывает видео активности на экране. Ведет фото- и видеорегистрацию действий за компьютером с помощью веб-камеры, которая фиксирует происходящее в поле обзора. Дополняет снимки и видео данными об открытых окнах и процессах, активных в момент съемки.

Обеспечивает мониторинг в режиме реального времени:

LiveView открывает доступ к содержимому экранов.

LiveCam дает возможность контролировать поведение пользователей.

DeviceController

Перехватывает данные, передаваемые на USB-накопители, внешние диски, CD/DVD, камеры, сканеры и другие подключаемые устройства.

Блокирует доступ к устройствам и портам, папкам и локальным дискам. Контролирует запуск ПО со съемных носителей. Шифрует данные, записываемые на устройства, таким образом, информацию нельзя прочесть за пределами компании.

Полностью или частично блокирует подключения. Например, разрешает чтение с запретом других операций с файлами на USB-накопителях, внешних винчестерах и картах памяти. Ведет «белые» списки, чтобы исключить из мониторинга устройства, пользующиеся доверием.

Keylogger

Фиксирует клавиатурный ввод и данные, копируемые в буфер обмена. Перехватывает логины и пароли, что позволяет отслеживать аккаунты на потенциально опасных ресурсах. Определяет пользователей, которые вводили с клавиатуры пароли к зашифрованным документам.

MicrophoneController

С помощью любого обнаруженного микрофона записывает переговоры в офисе и за его пределами. Включает запись звука при обнаружении речи (алгоритм Voice Activity Detection), при запуске процессов и программ, заданных политикой безопасности. Функция LiveSound позволяет прослушивать переговоры в режиме реального времени.

Включает запись переговоров еще до авторизации пользователя в системе, так что компьютер становится пассивным средством сбора информации.

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

«КИБ СёрчИнформ» имеет как базовые поисковые алгоритмы (**поиск по словам и фразам**), так и сложные виды поиска:

- **Поиск по тематическим словарям** выявляет документы и сообщения на определенную тему (наркомания, откаты, терроризм, шпионаж, фриланс, поиск работы).
- **Поиск по атрибутам** в качестве поискового запроса использует различные параметры (протокол передачи данных, доменный пользователь, IP-адрес, название, тип и размер файла и другие атрибуты).
- **Поиск по регулярным выражениям** находит документы с однотипными данными по шаблону, например, номера телефонов, серии и номера паспортов, банковские реквизиты, ФИО и т.д.
- **Поиск по цифровым отпечаткам** выявляет документы и файлы, схожие с заданным эталоном. Позволяет создать библиотеку документов-образцов и следить за операциями с похожими документами.
- **Статистические запросы** выявляют нетипичное поведение пользователей и инциденты на основании количественных показателей. Поиск учитывает количество и объем файлов, записанных на внешнее устройство; количество отправленных писем и другие показатели.
- **Запатентованный алгоритм «Поиск похожих»** служит для смыслового анализа. Поиск выявляет конфиденциальные документы даже в том случае, если их отредактировали. В результате находятся документы, похожие на поисковый запрос не только «технически», но и по смыслу.
- **Комплексные запросы** позволяют задавать сложный алгоритм поиска, используя простые запросы, объединенные логическими операторами И, ИЛИ и НЕ.

Анализ графики

Система определяет тип изображений, которые циркулируют внутри компании: фотография или скан-копия – и категоризирует файлы. Встроенная OCR (система распознавания символов) определяет документы установленных образцов: паспорта, банковские карты, водительские удостоверения и другие.

В «КИБ СёрчИнформ» предусмотрена опция проверки подлинности изображений. Система распознает и выделяет на изображении участки, которые были изменены любым способом, включая клонирование, перенос и вставку фрагментов; добавление и удаление деталей; создание изображения с помощью специального ПО.

Анализ аудио

Позволяет контролировать содержание голосовых коммуникаций. Система преобразовывает аудиозаписи в текст и проверяет расшифровку на соответствие политикам безопасности. Вся процедура локальна: данные не покидают корпоративной сети.

В КИБ есть возможность активировать запись при обнаружении речи или при запуске процессов и программ, заданных политикой безопасности.

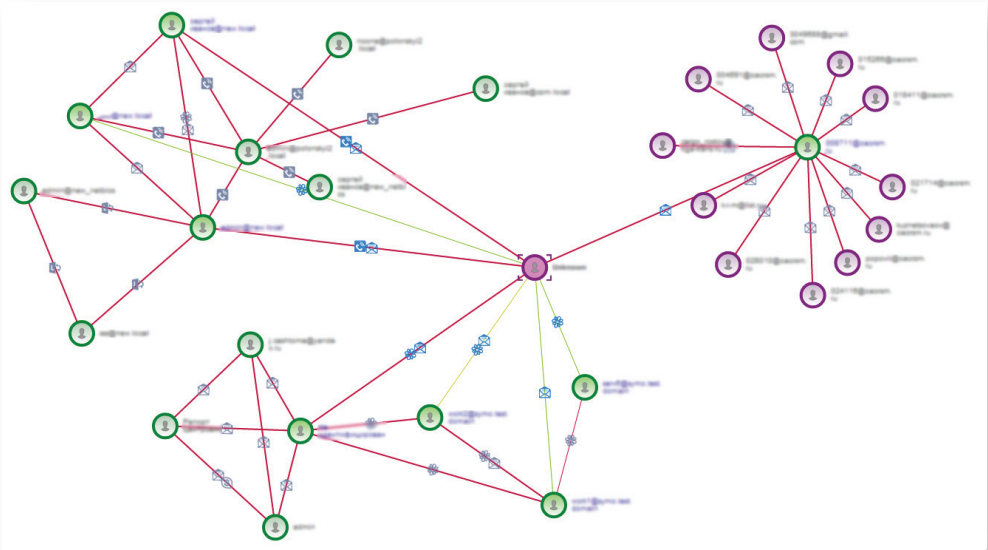
Отчеты

«КИБ СёрчИнформ» визуализирует все события и связи внутри компании в виде отчетов по активности пользователей и ИБ-инцидентам.

В системе насчитывается более 100 базовых шаблонов. Мастер отчетов позволяет построить собственный отчет, не ограниченный критериями. Просмотр доступен через веб-интерфейс.

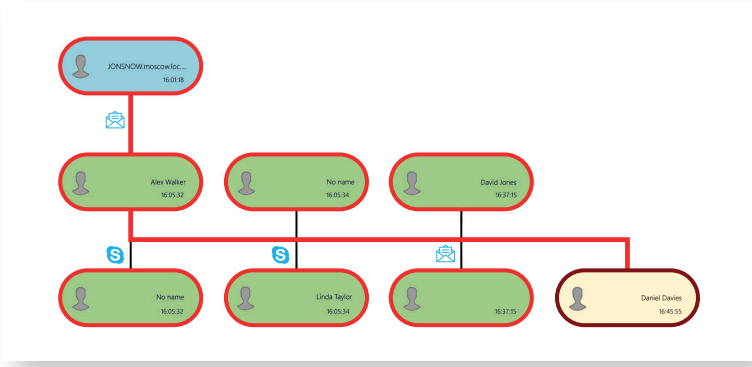
Отчет по связям пользователей

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



Отчет по контентным маршрутам

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



Отчеты по программам и оборудованию

Отражает изменения в комплектующих и устройствах, подключаемых пользователями к ПК. Это облегчает инвентаризацию и страхует от краж и подмены оборудования. Отчеты по программам упорядочивают данные об установке и удалении программ.

Расследование инцидентов

Архив перехваченной информации

Система сохраняет архив всех коммуникаций пользователей. Причем не просто «складывает» информацию, но позволяет эффективно с ней работать. ИБ-специалисты формируют полноценные аналитические выборки, сочетая технологии анализа метаданных с контентным анализом.

Навигация по видеозаписи действий пользователя

Система находит нужные фрагменты по активности пользователя. Достаточно выбрать потенциально опасное событие, например, запуск программы – и просмотреть записи с конкретного отрезка.

Профилирование пользователей

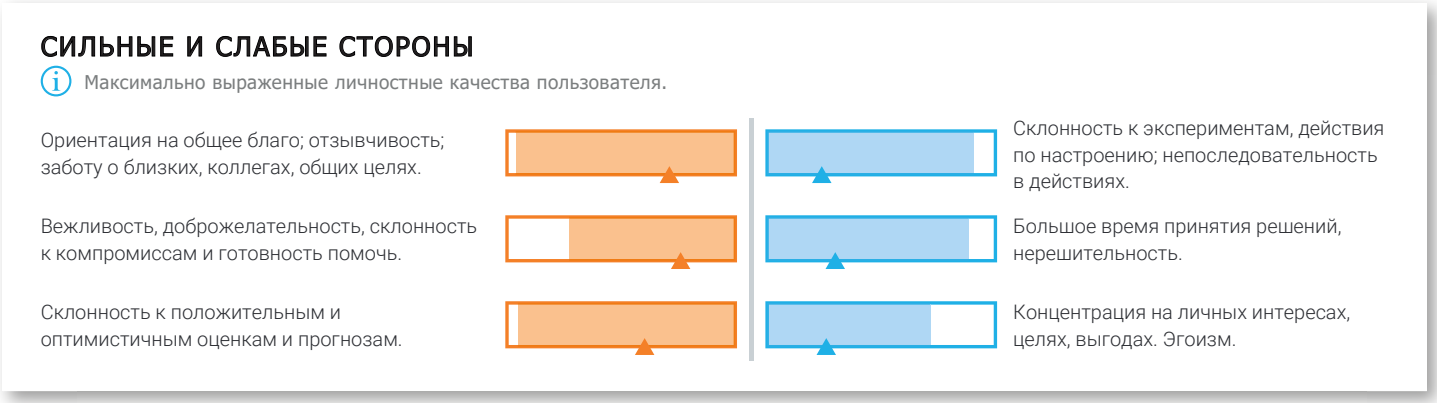
Часто до инцидента ничего в поведении сотрудника не выдает в нем инсайдера. Тогда как для специалистов по безопасности важно предвидеть действия в той или иной ситуации – и предотвратить инцидент.

Оперативно оценить личностные качества, составить комплексный психологический портрет сотрудника и спрогнозировать риски, связанные с человеческим фактором, – задачи, которые решает автоматизированный модуль профайлинга «КИБ СёрчИнформ ProfileCenter» (ProfileCenter).

Модуль черпает данные из DLP-системы «КИБ СёрчИнформ» и анализирует исходящие письма, сообщения в Skype, Viber, WhatsApp, Lync, Telegram, других мессенджерах и социальных сетях. На основании оценки текста по более чем 70 критериям ProfileCenter определяет:

- Черты характера, базовые эмоции, сильные и слабые стороны личности.
- Склонности и криминальные тенденции.
- Актуальную мотивацию и потребности.
- Уровень лояльности и надежности.
- Роль сотрудника в коллективе и степень влияния на коллег.

Модуль анализирует каждого сотрудника, сравнивает с окружением и дает рекомендации в соответствии с психологическим типом личности. Результаты отображаются в отчете с пояснениями и рекомендациями.



Часть отчета «КИБ СёрчИнформ ProfileCenter»

Архитектура системы

Компоненты «КИБ СёрчИнформ» располагаются на двух платформах – сетевой и агентской:

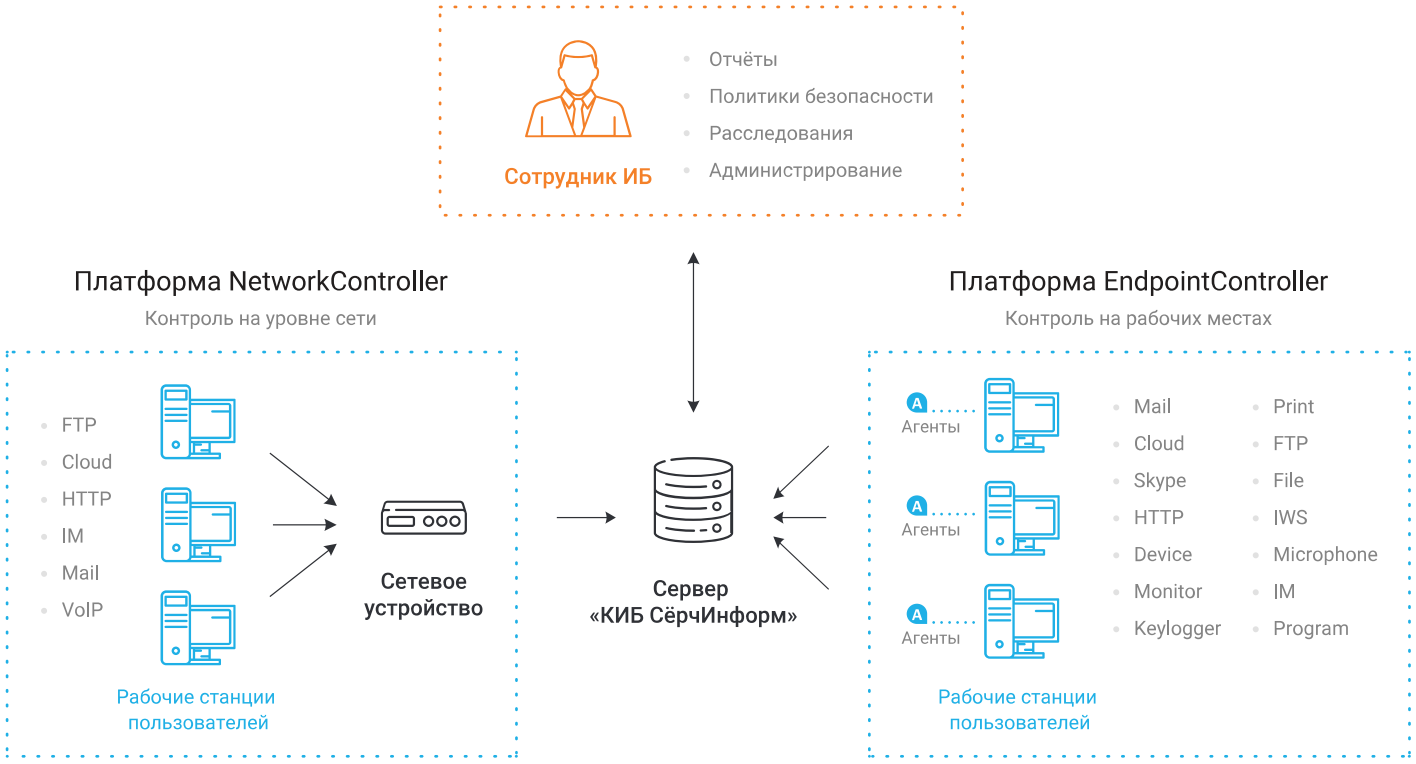
SearchInform NetworkController

перехватывает данные на уровне зеркалируемого трафика без влияния на работу корпоративной сети.

SearchInform EndpointController

фиксирует действия пользователей на конечных точках с помощью модулей-агентов и передает данные на сервер по интернету или внутренней сети.

Между агентами и сервером реализовано принудительное шифрование. Отправка конфиденциальных данных за пределы периметра исключена.



DataCenter

Управляет индексами и базами данных продуктов, контролирует работоспособность комплекса и обеспечивает взаимодействие со сторонними системами, например, SIEM, SOC, сервером исходящей почты.

В DataCenter задаются параметры разграничения прав доступа. Офицер безопасности работает только с теми данными, которые относятся к его зоне ответственности.

AlertCenter

«Мозговой центр» системы, где настраиваются политики безопасности. По расписанию или по команде сканирует перехваченную информацию и уведомляет ИБ-специалиста о нарушениях.

Analytic Console

Служит для поиска по перехваченным данным, контроля активности пользователей, работы с психологическими профилями и изучения отчетов.

Политики безопасности

«КИБ СёрчИнформ» включает **более 250** готовых политик безопасности. Решение позволяет создавать специфические политики, что гарантирует полноту контроля любого вида данных, нуждающихся в защите.

Универсальные политики безопасности актуальны для любой организации:

- раскрытие схем мошенничества;
- раскрытие фактов незаконного обогащения за счет компании;
- выявление негативных настроений и контроль лояльности в коллективе;
- определение групп риска (сотрудники с зависимостями, крупными долгами и т.п.);
- контроль персональных данных (паспорта, номера банковских карт и т.п.);
- предупреждение общения с конкурентами, уволенными сотрудниками;
- посещение запрещенных сайтов;
- вербовочные уязвимости, антитеррористические политики и другие.

Отраслевые политики безопасности учитывают сферу деятельности компании:

- банки и финансы;
- добывающая и химическая промышленность;
- транспорт и логистика;
- газо-, электро- и водоснабжение;
- строительство, связь;
- государственное управление и социальная сфера;
- сфера услуг и т.д.

Индивидуальные политики безопасности

Специалисты «СёрчИнформ» бесплатно разрабатывают политики безопасности, необходимые для соблюдения корпоративного регламента, внутренних инструкций, локального законодательства и для решения специфических задач клиента.

Преимущества «КИБ СёрчИнформ»

Простое внедрение с сохранением структуры сети

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

Мощный аналитический модуль

Позволяет быстро и гибко настраивать оповещения и анализировать информационные потоки без привлечения сторонних специалистов.

Инструменты для пошагового расследования инцидентов

Запись переговоров, перехват содержимого мониторов, аудит файловых операций, контроль клавиатурного ввода – встроенные компоненты системы позволяют восстановить нарушение по шагам.

Архив перехваченной информации

Существенно упрощает восстановление цепочки событий и позволяет при необходимости расследовать инцидент в соответствии с новыми политиками безопасности.

Контроль человеческого фактора

Построение психологических профилей позволяет оценить потенциальный риск, прогнозировать поведение в нормальных, критических и стрессовых обстоятельствах в данном коллективе, предвидеть действия в той или иной ситуации – и предотвратить инцидент.

Визуализация связей между сотрудниками

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

Контроль в реальном времени

«КИБ СёрчИнформ» подключается к монитору, микрофону и веб-камере, чтобы фиксировать нарушения в онлайн-режиме.

Контроль содержимого рабочих станций и общедоступных сетевых ресурсов

Система своевременно предупредит о появлении конфиденциальной информации в местах, для этого не предназначенных.

Комплексность решения

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

Разграничение прав доступа

Права доступа распределяются по ролевой модели. В зависимости от роли: аудитор безопасности, администратор, аналитик или руководитель – формируется индивидуальный режим доступа к настройкам системы, перехваченным данным, инцидентам и отчетам.

Гарантии безопасности в территориально распределенных компаниях

В удаленных филиалах с небольшим количеством ПК и «узким» каналом связи с головным офисом, когда нет возможности развернуть полноформатную DLP-систему, данные фильтруются, обрабатываются, шифруются локально и только затем передаются на основной сервер.

Агенты контроля для ОС Linux

«КИБ СёрчИнформ» работает под наиболее распространенными дистрибутивами, включая российские: ROSA Linux, GosLinux, Astra Linux.

Отдел внедрения и Учебный центр

Опыт работы с более чем 2 000 компаний из разных отраслей позволяет оперативно создавать уникальные наборы политик безопасности, ориентированные на актуальные задачи и специфику деятельности заказчиков.

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., 27, лит. 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
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) 201-69-86
Email: d.kirilenok@searchinform.ru

АРГЕНТИНА

Буэнос-Айрес

пр-т Леандро Н. Алем 896, C1001AAQ
Телефоны:
+54 11 5984 2618
+54 911 5158 8557
Email: r.martinez@searchinform.com

БЕЛАРУСЬ

Минск

ул. Измайловская, 30
Телефон: +375 (29) 649-77-79
Email: ab@searchinform.ru

БРАЗИЛИЯ

Сан-Паулу

Вила-Олимпиа, Руа Гомес де Карвальо 1356, оф.16
Телефоны:
+55 11 9 8973 2037
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 (495) 721-84-06, доб. 137
+7 (727) 222-17-95
Email: d.stelchenko@searchinform.ru