SEARCHINFORM

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

КОНТУР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SEARCHINFORM
INFORMATION SECURITY

1995
год основания компании

Москва, Россия
головной офис

6 филиалов
в Российской Федерации

10 представительств
за рубежом

1700+
количество клиентов

1 000 000+
количество компьютеров под контролем DLP-системы

2006
первый релиз DLP-системы

2010
открытие Учебного центра

2011
первая серия конференций Road Show SearchInform

2014
первый релиз программы учета рабочего времени TimeInformer

2015
статус резидента «Сколково»

2016
Единый реестр российского ПО

2016
первый релиз «СёрчИнформ SIEM»

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

Сертификат соответствия ФСТЭК России №3598 по требованиям безопасности информации № РОСС RU.0001.01БИ00

Контур информационной безопасности

«Контур информационной безопасности СёрчИнформ» (КИБ) – инструмент класса DLP, который защищает компанию от действий инсайдеров и утечек конфиденциальной информации. Задача КИБ – обнаружить утечку на этапе планирования и предупредить инцидент.

Как работает «КИБ СёрчИнформ»?

Контролирует информационные потоки

Проверяет входящий и исходящий трафик на соответствие политикам безопасности и не позволяет конфиденциальной информации покинуть пределы компании. Инспектирует содержимое писем и документов, пересылаемых по электронной почте. Следит за соблюдением политик безопасности при общении сотрудников в социальных сетях, мессенджерах, блогах, на форумах, в комментариях на сайтах.

Контролирует ресурсы компании и хранимую информацию

Следит за появлением, перемещением, изменением конфиденциальных документов на локальных рабочих станциях и в местах общего доступа. Защищает от несанкционированных операций с файлами. Контролирует запись на внешние устройства и печать документов.

Контролирует сотрудников

Система упрощает работу специалистам ИБ-отдела и помогает «улавливать» общие настроения в коллективе. Определяет неформальных лидеров, нелояльных и негативно настроенных работников, сотрудников в поиске новой работы. Устанавливает источники сплетен и факты непрофессионального поведения. Контролирует нагрузку и продуктивность сотрудников, находит нарушителей трудовой дисциплины.

«КИБ СёрчИнформ» состоит из модулей, каждый из которых защищает определенный канал передачи информации. Заказчики комбинируют модули в зависимости от приоритетных задач.

Для успешной борьбы с утечками информации, вызванными как халатностью, так и целенаправленными действиями сотрудников, необходимо контролировать все информационные потоки. Модули КИБ контролируют максимальное количество каналов и при комплексном использовании обеспечивают наиболее надежную защиту.

Компоненты системы

MailController

Перехватывает корпоративную почту, работающую по протоколам IMAP, POP3, SMTP, NNTP, WebMail, MAPI. Фильтрует сообщения по отправителю, получателю, теме, дате и другим атрибутам, производит контентный анализ текста письма и вложенных файлов.

Проверяет на соответствие политикам безопасности исходящие и входящие письма, переданные в почтовых веб-сервисах:

- Mail.ru
- Рамблер/почта
- Gmail
- Outlook.com
- Яндекс.Почта
- Office 365 и др.

Модуль позволяет блокировать почту, переданную по протоколу SMTP или через веб-интерфейс.

HTTPController

Перехватывает и индексирует файлы и сообщения, передаваемые по HTTP/HTTPS–протоколам. Контролирует данные, отправленные через браузер в чаты, блоги, форумы, социальные сети (POST-запросы). «Сканирует» запросы поисковой системы (GET-запросы).

Модуль проверяет на соответствие политикам безопасности:

- записи в блогах и на форумах;
- данные, отправленные через формы обратной связи;
- веб-чаты;
- посты в социальных сетях.

Контроль продолжается в штатном режиме, даже если сотрудники пользуются сервисами-анонимайзерами.

IMController

Перехватывает чаты, историю сообщений и списки контактов в популярных мессенджерах, включая:

- Mail.Ru Агент
- ICQ
- Viber
- QIP
- Lync/Skype For Business
- Telegram и др.

Берет под контроль переписку через веб-сервисы в социальных сетях:

- Google+
- ВКонтакте
- Facebook
- Одноклассники
- Мой мир и др.

SkypeController

Контролирует переписку, звонки, SMS и файлы, отправленные через чат. «Подтягивает» историю сообщений, даже если пользователь вел переписку вне офиса. Это помогает расследовать инциденты, произошедшие до установки DLP-системы в компании.

FTPController

Контролирует каналы передачи большого объема информации и предупреждает утечку «тяжелых» файлов, например, баз данных, программного обеспечения, сканированных документов, проектной документации, детализированных чертежей.

Модуль проверяет на соответствие политикам безопасности трафик, передаваемый через обычное (FTP) и шифрованное (FTPS) соединение.

MonitorController

Снимает скриншоты и записывает видео происходящего на экране, а также ведет фото- и видеорегистрацию действий за компьютером с помощью веб-камеры, которая фиксирует происходящее в поле обзора. Фиксация событий сопровождается информацией об открытых окнах и процессах, активных в момент съемки.

Настройки модуля позволяют:

- Выбрать интервал, качество и цветность скриншотов, режим работы с двумя мониторами.
- Задать расписание «по событию», когда скриншоты снимаются при посещении определенных сайтов или запуске программ, например, Skype или CRM.
- Блокировать клавишу PrintScreen и ограничить пользователю возможность создавать снимки экрана.
- Задать формат изображения (фото или видео) и расписание съемки с помощью веб-камеры.

Модуль поддерживает работу в режиме реального времени:

LiveView открывает доступ к содержимому экранов.

LiveCam дает возможность контролировать поведение пользователей.

CloudController

Контролирует файлы, принятые и отправленные в облачные хранилища. Способ перемещения информации не имеет значения: модуль перехватывает данные в программах-клиентах и веб-сервисах.

Модуль отслеживает облачные и файлообменные сервисы:

- Google Docs
- Office 365
- Evernote
- iCloud Drive
- SharePoint
- Amazon S3
- Dropbox
- Яндекс.Диск
- DropMeFile и др.

MicrophoneController

Предназначен для записи переговоров сотрудников в офисе и за его пределами, в командировке и на деловой встрече. Запись производится с помощью любого обнаруженного микрофона.

Настройки модуля позволяют:

- Выбрать качество и длительность записи, параметры шумоподавления.
- Включать запись звука при запуске процессов и программ, которые заданы политикой безопасности.
- Включать запись звука при обнаружении речи (алгоритм Voice Activity Detection).
- Прослушивать переговоры в режиме реального времени (функция LiveSound).
- Вести запись переговоров до авторизации пользователя в системе, в таком случае включенный компьютер становится пассивным средством сбора информации.

PrintController

Инспектирует содержимое отправленных на печать документов. Текстовые файлы копируются, скан-копии перехватываются в виде графического «отпечатка» и распознанного текста.

Функции модуля позволяют:

- Собирать статистику печати на сетевых и локальных принтерах.
- Обнаруживать документы, заверенные печатью.
- Контролировать печать бланков строгой отчетности.
- Оценивать целевое использование принтера.
- Вести электронный архив распечатанных документов.

ProgramController

Собирает данные об активности и времени, проведенном в приложениях. Автоматически определяет, работает сотрудник или открыл программу «для вида». Ведет статистику посещения: подсчитывает время, проведенное на сайтах.

Модуль автоматически сортирует интернет-ресурсы по тематическим группам: знакомства, музыка, онлайн-магазины, новости, биржи труда и т.д. В системе уже распределены по категориям более 1 млн сайтов, и количество постоянно растет. Каждые 10 минут модуль собирает и обрабатывает неизвестные ресурсы, распределяя по категориям.

Индексация рабочих станций

Модуль обнаруживает конфиденциальные документы, которые хранятся с нарушением политик безопасности: на рабочих станциях, выделенных серверах и местах общего хранения. Система проводит аудит данных в папках общего доступа (Shares), на жестких дисках компьютера (Local System) и общих ресурсах на платформе SharePoint.

Функции модуля позволяют:

- Выбирать область индексации: папка в сети, отдельный компьютер, диск или папка на локальной станции.
- Находить и переиндексировать новую или измененную информацию.
- Искать в индексе по содержимому удаленных файлов.

FileController

Контролирует операции с файлами, которые хранятся на серверах и в общих сетевых папках. Регистрирует любые манипуляции пользователей с файлами, в том числе:

- открытие;
- копирование;
- редактирование;
- изменение формата;
- удаление и другие операции.

DeviceController

Перехватывает информацию, передаваемую пользователем на съемные устройства. Контролирует использование USB-накопителей, внешних дисков, CD/DVD-дисков, камер, сканеров и принтеров, Bluetooth-адаптеров и других подключаемых устройств.

Настройки модуля позволяют:

- Блокировать доступ к устройствам или портам.
- Блокировать доступ к папкам или локальным дискам.
- Считать содержимое подключенного USB-накопителя.
- Запретить запуск ПО со съемных носителей.
- Зашифровать данные, записываемые на устройства (таким образом информацию нельзя прочесть за периметром компании).
- Создавать «белые списки», чтобы исключить из мониторинга устройства, пользующиеся доверием.

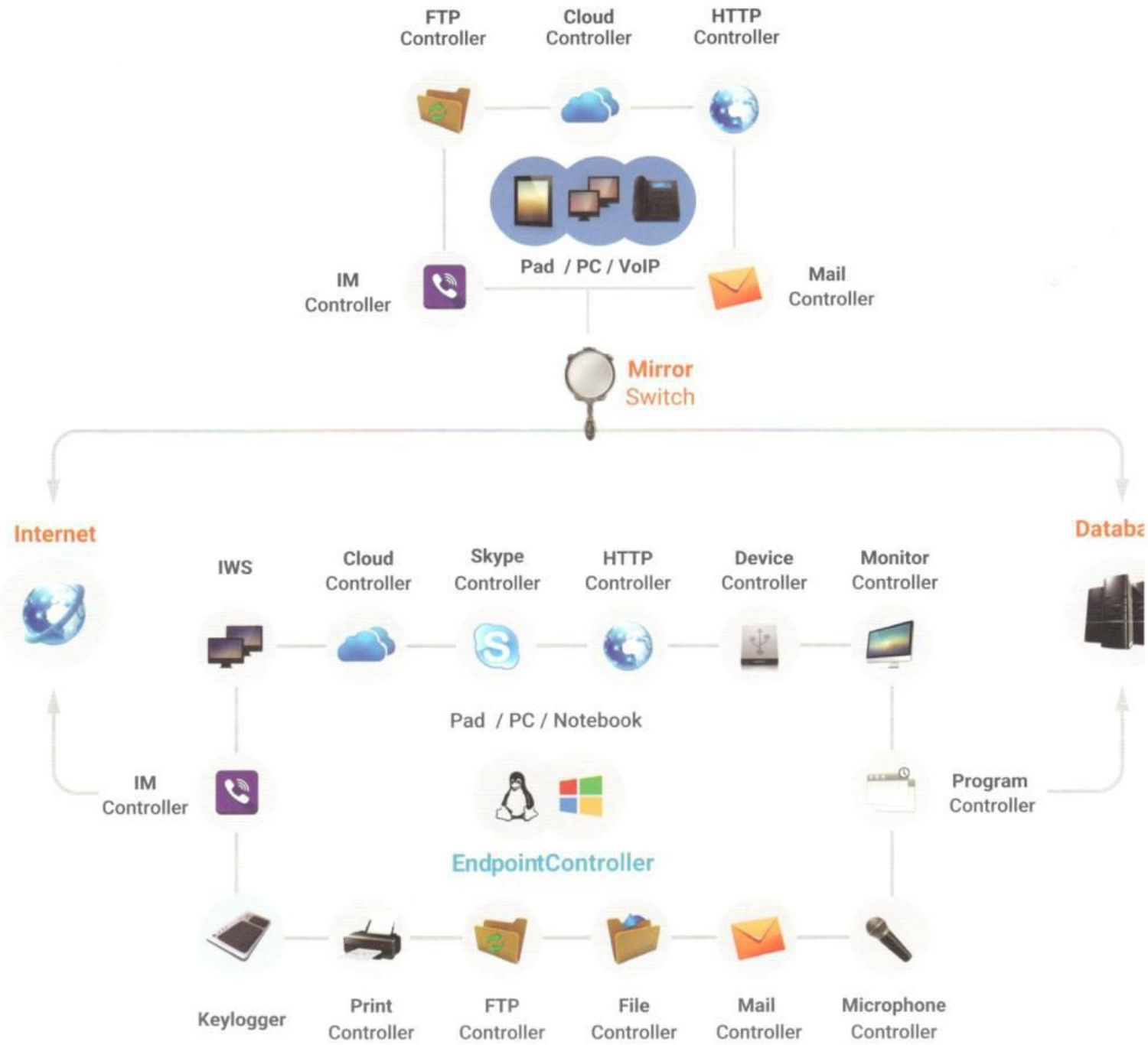
Реализована возможность полной или частичной блокировки, когда данные на USB-накопителях, внешних винчестерах и картах памяти разрешается использовать для чтения, при этом запрещены другие операции (создание, копирование, переименование, запись).

Keylogger

Фиксирует нажатия клавиш на клавиатуре и информацию, копируемую в буфер обмена. Позволяет перехватывать логины и пароли и отслеживать аккаунты сотрудника на «потенциально опасных» ресурсах. Модуль определяет пользователей, вводивших с клавиатуры пароли к зашифрованным документам.

Основные функции:

- перехват нажатий клавиш;
- перехват нажатий функциональных клавиш;
- перехват текста из буфера обмена.



Интеграция с доменной структурой Windows

Учетная запись Windows идентифицирует пользователя, который работал за компьютером: изменял или копировал файлы, отправлял письма через веб-браузер, переписывался в мессенджерах и социальных сетях от чужого имени. Интеграция с доменной структурой Windows помогает в расследовании инцидентов, составлении отчетов активности работников и подразделений.

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.

Ни один компонент системы не хранит и не отправляет данные в открытом виде: в «КИБ СёрчИнформ» реализовано принудительное шифрование при передаче между агентами и сервером. Связь между серверными, агентскими и клиентскими компонентами происходит в рамках заданных настроек. Отправка данных за пределы периметра исключена.

AlertCenter

«Мозговой центр» системы. В AlertCenter задаются политики безопасности. Модуль по заданному расписанию или по команде проводит поиск по массиву перехваченной информации и в случае нарушения политик безопасности уведомляет ИБ-специалиста.

ReportCenter

Собирает статистику и отображает статистические данные в виде емких по содержанию, удобных для восприятия отчетов. ReportCenter генерирует отчеты в виде таблиц, диаграмм и временного графика, а также в виде графа отношений, который наглядно демонстрирует связи по основным каналам коммуникации с внешним миром и внутри коллектива. Просмотр отчетов доступен через веб-интерфейс.

DataCenter

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

В DataCenter реализована возможность разграничения прав доступа к перехваченной информации пользователей, групп пользователей и компьютеров. Таким образом офицер безопасности работает только с теми данными, которые относятся к закрепленным за ним отделам.

Аналитический модуль

Контроль информационных потоков и перехват данных – только часть функциональности DLP-системы. Чтобы проанализировать массив информации и обнаружить инцидент, необходимы мощные поисковые и аналитические инструменты.

Поисковые механизмы «КИБ СёрчИнформ» позволяют эффективно работать со всеми видами конфиденциальной информации, содержащейся в перехваченных данных.

Возможности анализа разных типов данных

Поиск по видеозаписи активности пользователя

Позволяет находить нужные фрагменты по активности пользователя. Достаточно выбрать потенциально опасное событие, например, запуск программы – и начать просмотр записи с конкретного отрезка.

Анализ и категоризация изображений

Интегрированный в «КИБ СёрчИнформ» инструмент на основе технологии оптического распознавания символов классифицирует данные, которые циркулируют внутри компании. Классификаторы помогают определить документы установленных образцов: паспорта, банковские карты, водительские удостоверения и другие.

Проверка подлинности изображений

Система обнаруживает различные способы подделки изображений: клонирование, перенос и вставку фрагментов; добавление и удаление деталей; создание изображения паспорта с помощью специального ПО. Результаты экспертизы предоставляются в виде графических эскизов с указанием места подделки.

Распознавание речи

Технология распознавания речи позволяет контролировать содержание переговоров сотрудников. Система преобразовывает аудиозаписи в текст и проверяет расшифровку на соответствие политикам безопасности. Вся процедура локальна: данные не покидают корпоративной сети.

Поисковые алгоритмы «КИБ СёрчИнформ»

1. **Поиск по словам и фразам**

   Обнаруживает документы с заданными словами, их формами и синонимами. Проверяет документ на совпадение по словосочетаниям и устоявшимся определениям. Учитывает порядок слов и расстояние между ними. Алгоритм поиска с опечатками принимает в расчет слова с ошибками: неверными, лишними и недостающими буквами.

2. **Поиск по тематическим словарям**

   Выявляет документы и сообщения на определенную тему: наркомания, откаты, терроризм, шпионаж, фриланс, поиск работы. Редактор параметров поиска позволят вставить готовый словарь из файла.

3. **Запатентованный алгоритм «Поиск похожих»**

   Интеллектуальные возможности поиска позволяют контролировать конфиденциальные документы даже в том случае, если они были предварительно отредактированы. В качестве поискового запроса используются как фрагменты, так и документы целиком. В результате выявляются документы, похожие на поисковый запрос не только «технически», но и по смыслу.

4. **Поиск по атрибутам**

   В качестве поискового запроса выступают различные параметры: протокол передачи данных; доменный пользователь; IP-адрес; название, тип и размер файла; шифрованное сообщение и другие атрибуты.

5. **Поиск по регулярным выражениям**

   Находит документы с однотипными данными по шаблону, например, номера телефонов, серии и номера паспортов, банковские реквизиты, ФИО и т.д.

6. **Поиск по цифровым отпечаткам**

   Выявляет документы и файлы, имеющие сходство с заданным эталоном. Технология позволяет создать библиотеку конфиденциальных документов-образцов и автоматически следить за операциями с похожими документами.

7. **Статистические запросы**

   Позволяют выявлять нетипичное поведение пользователей и инциденты на основании количественных показателей. Поиск учитывает количество и объем файлов, записанных на внешнее устройство; количество отправленных писем и количество адресатов в одном письме; количество сообщений и собеседников в мессенджерах и другие показатели.

8. **Комплексные запросы**

   Пользователь задает сложный алгоритм поиска, используя простые запросы, объединенные логическими операторами И, ИЛИ и НЕ.

Политики безопасности

«Контур информационной безопасности 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:

- контроль откатов и взяточничества;
- выявление негативных настроений и сговоров в коллективе;
- определение групп риска (проблемы с алкоголем, наркотиками, крупные долги и т.д.);
- контроль персональных данных (паспорта, номера банковских карт и др.);
- выявление общения с конкурентами, с уволенными сотрудниками;
- посещение запрещенных сайтов;
- антитеррористические политики и др.

Отраслевые политики безопасности

Учитывают сферу деятельности компании:

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

Индивидуальные политики безопасности

Специалисты «СёрчИнформ» бесплатно разрабатывают политики безопасности, необходимые для соблюдения корпоративного регламента, внутренних инструкций, локального законодательства или для решения специфической задачи клиента.

Профайлинг

DLP-система проверяет перехваченную информацию в соответствии с политиками безопасности и составляет **характеристику документа**. Например, отмечает, что в документе содержатся конфиденциальные данные или указание на сотрудника из группы риска.

Профайлинг – инструмент психологической диагностики – работает со структурой перехваченной информации, анализирует действия и составляет **характеристику пользователя**.

Методика профайлинга основана на принципах нетестовой психодиагностики и помогает:

- определить актуальные ценности, убеждения сотрудника;
- выявить криминальные тенденции в характере;
- составить прогноз поведения в нормальных, критических и стрессовых ситуациях;
- разработать компенсационные меры;
- рационально применять базовые психологические принципы подбора, отбора, увольнения сотрудников, исходя из требований безопасности.

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 детального расследования инцидентов

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

Архив перехваченной информации

Открывает неограниченные возможности для расследований, существенно упрощает восстановление цепочки событий и позволяет при необходимости расследовать инцидент в соответствии с новыми политиками безопасности.

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.

Разграничение прав доступа

Производится на уровне DLP, отменить его невозможно ни на локальном, ни на доменном уровне.

Агенты контроля для ОС Linux

«КИБ СёрчИнформ» интегрирован с российскими операционными системами Astra Linux, ROSA Linux и GosLinux.

Контроль содержимого рабочих станций и общедоступных сетевых ресурсов

Позволяет отслеживать появление конфиденциальной информации в местах, для этого не предназначенных.

Комплексность решения

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

Контроль в реальном времени

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

Контроль ноутбуков

Позволяет выявить утечку информации через ноутбуки, которые сотрудники используют вне корпоративной сети, например, дома или в командировках.

Адаптация для малых офисов и филиалов

Позволяет использовать систему в удаленных офисах с небольшим количеством компьютеров и «узким» каналом связи. Фильтрация, обработка, сжатие и шифрование данных происходят локально, только после этого информация передается на основной сервер.

Отдел внедрения и учебный центр

Опыт работы с более чем 1700 компаниями 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. 112, 126
+7 (843) 212-43-12
+7 (843) 212-43-13
+7 (965) 600-53-07
Email: t.latushkina@searchinform.ru

Новосибирск

ул. Владимировская, 2/1, оф. 109
Телефон: +7 (495) 721-84-06, доб. 106
Email: n.sorokin@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

БЕЛАРУСЬ

Минск

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

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

БЕНИЛЮКС

Телефон: +31 6 44 78 62 93
Email: ay@searchinform.com

БЛИЖНИЙ ВОСТОК

Телефон: +44 (0) 207 043 7152
Email: sy@searchinform.com

ВЕЛИКОБРИТАНИЯ

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

ЛАТИНСКАЯ АМЕРИКА

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