«Контур информационной безопасности СёрчИнформ»:

контроль всех потоков информации
и предотвращение утечек

SEARCHINFORM
INFORMATION SECURITY

Что это?

«Контур информационной безопасности СёрчИнформ» (КИБ) – инструмент, который позволяет защитить бизнес от внутренних угроз в несколько шагов:

1. Берёт под контроль все информационные потоки.
2. Проверяет содержимое переписок и вложений.
3. Оповещает о нарушениях политик безопасности.
4. Помогает расследовать инциденты и предупреждать утечки.

Задача КИБ: выявить утечку на этапе планирования и предотвратить её.

Как работает система?

Программа контролирует:

Каналы связи

электронную почту
мессенджеры, облачные
хранилища и т.д.

Действия сотрудников

занятость за компьютером,
запись данных на USB,
печать документов

Хранимую информацию

ее нахождение в сетевых
папках, на «разрешенных»
ПК и т.д.

Компоненты «КИБ СёрчИнформ»

КИБ состоит из модулей, каждый из которых контролирует свой канал передачи информации. Система показывает, какой путь проходят данные, и делает прозрачными все коммуникации.

SEARCHINFORM
INFORMATION SECURITY

Модули «КИБ СёрчИнформ»

MailController

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

SkypeController

Перехватывает чаты, звонки, SMS и файлы в Skype.

IMController

Перехватывает чаты в социальных сетях (VK, Facebook и т.д.) и мессенджерах (Viber, Telegram и т.д.), а также входящие и исходящие сообщения с популярных сайтов на платформе Mamba (mamba.ru, meebo.com и т.д.).

Модули «КИБ СёрчИнформ»

FTPController

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

HTTPController

Перехватывает сообщения (Post/Get запросы), передаваемые на интернет-форумы, блоги, чаты, службы веб-почты или при помощи браузерных IM-клиентов.

CloudController

Контролирует содержимое облачных хранилищ (Яндекс.Диск, Google Диск, Dropbox и т.д.).

Модули «КИБ СёрчИнформ»

MonitorController

- Делает снимки экранов рабочих компьютеров по расписанию или событию (запуск программы/процесса и др.).
- Отображает рабочие столы в режиме реального времени.
- Записывает видео происходящего на экране.

MicrophoneController

Записывает разговоры сотрудников как в офисе, так и в командировках через любой обнаруженный микрофон (в гарнитуре, ноутбуке и т.д.).

Режимы:

- непрерывная запись;
- запись при запуске определенных программ/процессов;
- запись только речи (алгоритм VAD);
- вещание в режиме онлайн.

Модули «КИБ СёрчИнформ»

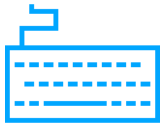
PrintController

Контролирует содержимое документов, отправленных на печать. Модель принтера не важна, поскольку перехват осуществляется на уровне ОС.

DeviceController

Отслеживает факт подключения внешних устройств к компьютеру, контролирует данные, записываемые на носители. Дает возможность запретить запись или зашифровать информацию, чтобы обеспечить конфиденциальность.

Модули «КИБ СёрчИнформ»



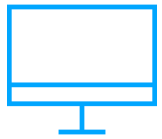
Keylogger

Перехватывает нажатия клавиш (логины, пароли и т.д.), а также информацию, скопированную в буфер обмена. Входит в состав MonitorController.

ProgramController

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

Модули «КИБ СёрчИнформ»



Индексация рабочих станций

Позволяет отслеживать наличие конфиденциальной информации на рабочих станциях, файл-серверах и в местах общего хранения.

FileController

Контролирует операции с файлами, которые хранятся на серверах и в общих сетевых папках. Регистрирует все действия, совершаемые пользователями с файлами: открытие, копирование, изменение, удаление и т.д.

Архитектура «КИБ СёрчИнформ»

Все модули системы размещаются на двух платформах. Их комплексное использование оптимально:

NetworkController контроль на уровне сети	**EndpointController** контроль на уровне ПК
Зеркалирует трафик на уровне корпоративной сети (коммутатора).	Фиксирует действия сотрудников с помощью установленных на ПК программ-агентов.
MailController, IMController, HTTPController, FTPController, CloudController	MailController, IMController, SkypeController, DeviceController, FTPController, PrintController, HTTPController, FileController, MonitorController + Keylogger, MicrophoneController, ProgramController, CloudController, Индексация рабочих станций

Как КИБ анализирует данные?

«Мозговой центр» системы – **AlertCenter** – проверяет данные, перехваченные всеми компонентами. Чтобы обнаружить подозрительные слова, фразы и действия, КИБ использует **8 видов поиска.**

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

SEARCHINFORM
INFORMATION SECURITY

Умный поиск и автоматизация

Поиск по видеозаписи активности пользователя

Чтобы быстро найти нужный фрагмент, достаточно выбрать потенциально опасное событие, например, запуск программы – и начать просмотр записи с конкретного отрезка.

Анализ и категоризация изображений

КИБ 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: перенос и вставку фрагментов; добавление и удаление деталей и др. В результатах экспертизы указаны места подделки.

Распознавание речи

Позволяет контролировать содержание переговоров сотрудников. Аудиозаписи автоматически преобразуются в текст и проверяются в соответствии с политиками безопасности. Процедура локальна: данные не покидают корпоративной сети.

Политики безопасности КИБ «СёрчИнформ»

«КИБ СёрчИнформ» включает более 250 политик безопасности, готовых к работе:

- **Универсальные политики безопасности**

Подходят любой компании независимо от сферы деятельности: контроль откатов и взяточничества; выявление негативных настроений в коллективе и т.д.

- **Отраслевые политики безопасности**

Учитывают особенности конкретной сферы деятельности: добывающая промышленность; газо-, электро- и водоснабжение; строительство; торговля; транспорт и логистика и т.д.

- **Индивидуальные политики безопасности**

Политики, которые специалисты «СёрчИнформ» бесплатно разрабатывают под запросы клиента.

Больше, чем контроль

Как только система обнаружила инцидент, специалист по безопасности получает оповещение. Теперь он приступает к расследованию: КИБ поможет выявить детали нарушения и круг лиц, причастных к инциденту.

Кроме того, DLP-система делает прозрачными все бизнес-процессы. **Более 30 отчетов** подсказывают, как оптимизировать работу компании:

- **Статистические отчеты** (показывают занятость, активность и продуктивность сотрудников).
- **Отчеты о связях пользователей** (дают понимание кругов общения).
- **Отчеты по оборудованию и ПО** (упрощают инвентаризацию и облегчают мониторинг программного обеспечения).

ProfileCenter в КИБ

Новый инструмент КИБ позволяет работать с человеческим фактором. Система анализирует всю информацию о пользователе и составляет его **психологический профиль**:

- характер и намерения;
- ценности и убеждения;
- личностные качества;
- уровень лояльности;
- криминальные тенденции;
- наклонности и др.

ИБ-служба использует профиль при решении задач информационной безопасности:

- ✓ Для расчета человеческих (кадровых) рисков и профилактики преступлений.
- ✓ Для прогнозирования поведения работников в нормальных, критичных и стрессовых ситуациях.
- ✓ Для определения истинных намерений и мотивации сотрудников.
- ✓ Для предупреждения инцидентов ИБ.
- ✓ Для пресечения противоправных действий в отношении организации.

6 доводов в пользу КИБ для вашего бизнеса

Установка займет всего 2-3 часа

С ней справятся штатные IT-специалисты. Клиентам не придется предоставлять внутренние документы компании-разработчику.

Внедрение не нарушит рабочие процессы

Установка DLP не потребует изменений в структуре локальной сети. Внедрение продукта не грозит простоем в работе или изменением налаженных процессов.

Система защитит данные и вне офиса

КИБ защищает информацию, даже если сотрудники работают из дома или в командировках.

6 доводов в пользу КИБ для вашего бизнеса

Гибкое лицензирование

DLP-система «КИБ СёрчИнформ» многокомпонентна. Заказчику не обязательно оплачивать «полный пакет»: можно «собрать» только необходимые модули.

Бесплатная пробная версия на 30 дней

Можно попробовать продукт и оценить его полезность. Возможности бесплатной версии не ограничены, так что уже на этапе тестирования вы выявите больные места своего бизнеса.

Постоянная поддержка отдела внедрения

«СёрчИнформ» обучает работе с КИБ и оказывает поддержку: мы готовы решить вашу проблему и ответить на любые вопросы по телефону или в Skype 5 дней в неделю. Бесплатная версия КИБ также сопровождается поддержкой.

Технические преимущества КИБ

1 **Уникальные технологии контентного анализа**

Система учитывает смысловую схожесть, и распознает даже отредактированные конфиденциальные документы.

2 **Архив перехваченной информации**

КИБ сохраняет всю перехваченную информацию. Её всегда можно проверить в соответствии с новыми политиками безопасности. Архив не ограничен как по времени, так и по объему.

3 **Инструменты для расследований и наличие доказательств нарушений**

Программный комплекс не просто фиксирует нарушения, но и собирает доказательства: противоправные действия подкрепляются скриншотами, аудио- и видеозаписями.

4 **Контроль в реальном времени**

Программный комплекс позволяет подключиться к монитору и микрофону конкретного сотрудника и проследить за его действиями в реальном времени.

Технические преимущества КИБ

5 **Прозрачность связей внутри компании и за ее пределами**

Продукт анализирует связи сотрудников между собой и с внешними адресатами. Карта взаимодействий помогает проводить расследования.

6 **Полная картина активности**

Подробная запись действий пользователя в ПО, аудит операций файловой системы, нажатых клавиш, аудио- и видеозапись действий дают полное видение активности пользователей.

7 **Контроль содержимого ПК и сетевых ресурсов**

С «КИБ СёрчИнформ» офицеры безопасности могут отслеживать появление конфиденциальной информации в местах, для этого не предназначенных.

8 **Отчеты по программному обеспечению и оборудованию**

Система упрощает инвентаризацию и облегчает мониторинг ПО. Это оптимизирует работу IT-отдела и страхует компанию от расходов.

Технические преимущества КИБ

9 **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 это информация передается на основной сервер.

10 **Агенты контроля для ОС Linux**

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

«КИБ СёрчИнформ» уже защищает:

«СЁРЧИНФОРМ» СЕГОДНЯ

6 филиалов в России
и **11 представительств** за рубежом

11 лет на рынке DLP, **21** год в IT

Более **2000** клиентов в **16** странах мира

Более **1 200 000** ПК под защитой «КИБ СёрчИнформ»

«КИБ СёрчИнформ» включен в **Реестр отечественного ПО**

23 уголовных дела выиграно клиентами против инсайдеров

В 2017 году «КИБ СёрчИнформ» **вошел в «магический квадрант» Gartner**

SEARCHINFORM
INFORMATION SECURITY

Сохранность конфиденциальных данных вашей компании зависит от вас!

+7 (495) 721-84-06
info@searchinform.ru
searchinform.ru