APSdigital

searchinform

ИБ-АУТСОРСИНГ

Передача задач информационной безопасности профессионалам

Защита бизнеса от рисков, связанных с персоналом

«СёрчИнформ» сегодня

30
лет в IT

3 000 000+
ПК под защитой продуктов «СёрчИнформ»

4 000+
клиентов по всей России

6
решений для комплексной защиты бизнеса

20+
стран мира

Реестр отечественного ПО

Продукты «СёрчИнформ» входят в Реестр отечественного программного обеспечения.

Рекомендованы к внедрению

Решения «СёрчИнформ» рекомендованы к внедрению и тиражированию в регионах Минпромторгом РФ, Минцифры РФ и Аналитическим центром при Правительстве России.

ПРОБЛЕМА

Бизнес теряет деньги из-за:

- воровства
- откатов
- боковых продаж
- кражи клиентов
- саботажа
- шпионажа
- внезапных увольнений
- утечек данных: клиентских баз, условий работы с поставщиками и др.

РЕШЕНИЕ

Передать задачи ИБ на аутсорсинг

и предотвратить риски и угрозы, связанные с персоналом, без больших затрат.

Комплексный подход к информационной безопасности

DLP «СёрчИнформ КИБ»

Борьба с утечками, мониторинг и анализ данных.

DCAP «СёрчИнформ FileAuditor»

Аудит файловой системы, поиск нарушений прав доступа и отслеживание изменений в критичных данных.

«СёрчИнформ ProfileCenter»

Система профилирования сотрудников: оценка психологической атмосферы в коллективе и обнаружение деструктивного поведения.

«СёрчИнформ TimeInformer»

Мониторинг действий сотрудников за ПК; предупреждает бизнес о неэффективной работе и опозданиях.

Что входит в услугу

1

Защитные системы по подписке

Готовый набор ИБ-инструментов без покупки лицензий.

2

Работа внештатного аналитика

Опытный специалист по ИБ ведёт мониторинг и расследования.

3

Облачный сервер для установки ПО

Развёртывание решений в облаке — без нагрузки на вашу инфраструктуру.

Как работает ИБ-аутсорсинг?

Сотрудники поставщика услуги:

+ Договор + NDA

1. Разворачивают в облаке DLP, DCAP и систему профилирования сотрудников.
2. Устанавливают агенты на ПК сотрудников: перехватывают информацию и активность за рабочим местом. Персонал не видит программу и не может её выключить.
3. Настраивают систему под задачи клиента: выявление мошенничества, контроль рабочего времени, мониторинг групп риска и т. п.
4. Решают все технические вопросы и сопровождают работу системы.
5. Следят за событиями в корпоративной сети клиента и проводят расследования инцидентов.
6. Формируют и отправляют заказчику отчёты, взаимодействуют по результатам.

Кто работает с инцидентами?

ИБ-аналитик

Сотрудник поставщика услуги — специалист по информационной безопасности. Он оценивает корпоративные риски, связанные с персоналом, анализирует действия пользователей в системе и следит за использованием рабочего времени.

Всё это помогает предотвратить утечки данных, мошенничество, саботаж и другие инциденты.

Контроль популярных каналов передачи данных

DLP

- Электронная почта
- Социальные сети
- Форумы и блоги
- Мессенджеры: VK Teams, Skype, Zoom, Телеграм, WhatsApp и др., в том числе российские
- Бумажные носители
- Flash-накопители и другие съёмные устройства

Больше об инструментах: что перехватывают

MailController

Электронная почта, включая черновики Outlook и входящую через веб-браузер.

IMController

Чаты, изображения, файлы, звонки в десктопных и web-версиях соцсетей и мессенджеров.

HTTPController

Сообщения (Post/Get запросы) на форумах, в блогах, чатах, службах веб-почты, а также из боковой панели браузерных IM-клиентов.

CloudController

Информация в облачных хранилищах.

Сливы по любви

— Какими ты видишь наши отношения через 5 лет?
— Мы будем сливать базы данных конкурентам.

Что произошло: Сработала политика безопасности о пересылке базы данных на внешнюю почту.

Расследование: Письма с базами отправляла одна из сотрудниц, а получал их её супруг, бывший в сговоре с конкурентами. Действия «семейного подряда» нанесли фирме ущерб порядка 50 миллионов рублей.

Не верь глазам своим

Что произошло: В компании по продаже стройматериалов сотрудник создал своё ИП и предлагал действующим клиентам закупку материалов через него на «выгодных» условиях.

Расследование: Мошенник использовал web-почту для отправки клиентам коммерческих предложений с невыгодными условиями от имени компании-работодателя, своего ИП и сторонних организаций.

Записи с монитора: Сотрудник сам формировал КП: в одних повышал цену, в своих — добавлял скидки. С помощью фоторедактора вставлял печати и подписи.

Распространённая схема с фальсификацией печатей и подписей с помощью фоторедакторов.

Свой-чужой

Что произошло: Практически во всех закупках выигрывала одна и та же компания, КП от которой не поступало. У этого поставщика цена всегда была чуть ниже, а отсрочка платежа — чуть больше.

Расследование: Проверили всех сотрудников, связанных с закупками, и их каналы связи. Один из них вёл переписку в WhatsApp и почте с этим поставщиком — в перехват попали все КП к предстоящим закупкам.

Анализ перехвата: Записи из интернет-браузеров и видео с монитора показали: сотрудник имел доступ на торговую площадку с двух аккаунтов — работодателя и поставщика.

Больше об инструментах: что перехватывают

MonitorController

Снимки экранов по расписанию или событию; рабочие столы в реальном времени; запись видео экрана; фиксация в поле обзора веб-камеры; распознавание попыток сфотографировать экран.

ProgramController

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

Keylogger

Перехватывает нажатия клавиш (логины, пароли и т. д.) и данные из буфера обмена. Входит в состав MonitorController.

Сокращение непродуктивного времени

Вводные

Торговая компания, штат 50 человек.

Средняя зарплата — 64 600 ₽/мес.

До внедрения ИБ-аутсорсинга непродуктивное время составляло **32%.**

Результат

После ввода контроля и разъяснительных бесед непродуктивное время сократилось до **16%.**

Экономия компании — **6 201 600 ₽ в год.**

Год услуги ИБ-аутсорсинга на это число сотрудников обошёлся в **1 875 674 ₽.**

Больше об инструментах: что перехватывают

FTPController

Перехватывает документы, переданные и полученные по протоколу FTP, через обычное или зашифрованное (SSL) соединение — FileZilla, Serv-U, vsFTPd, freeFTPd и др.

MicrophoneController

Записывает разговоры сотрудников в офисе и в командировках через любой обнаруженный микрофон (гарнитура, ноутбук и т. д.).

PrintController

Контролирует содержимое всех документов, отправленных на печать. Печать можно заблокировать по содержанию, типу файла или количеству страниц.

DeviceController

Отслеживает подключение внешних устройств, контролирует записываемые данные, позволяет запретить запись или зашифровать информацию.

Штрафы за утечку персональных данных

Федеральный закон от 30.11.2024 № 420-ФЗ (вступил в силу 30.05.2025)

Утечка	Впервые	Повторно
Менее 10 тыс. записей / менее 1 тыс. граждан	150–300 тыс. ₽	300–500 тыс. ₽
10–100 тыс. записей / 1–10 тыс. граждан	3–5 млн ₽	1–3% выручки (20–500 млн ₽)
100 тыс.–1 млн записей / 10–100 тыс. граждан	5–10 млн ₽	1–3% выручки (25–500 млн ₽)
Более 1 млн записей / более 100 тыс. граждан	**10–15 млн ₽**	1–3% выручки (25–500 млн ₽)
Персональные данные специальных категорий	**10–15 млн ₽**	1–3% выручки (25–500 млн ₽)

Штраф для предприятий и ИП

Комплексная защита существенно минимизирует риски инцидентов. Но если утечка всё же произошла, компания с помощью ИБ-средств докажет, что виновен конкретный человек, — и сможет снять с себя ответственность.

APSdigital

searchinform

DCAP

Аудит файловой системы, поиск нарушений прав доступа и отслеживание изменений в критичных данных

«СёрчИнформ FileAuditor»: возможности

1 Наводит порядок в файловой системе

- Поиск в общем документообороте информации, подлежащей защите.
- Классификация файлов по типу содержимого: персданные, номера карт, информация ограниченного доступа.
- Теневое копирование критичных данных и истории последних изменений каждого документа.

2 Контролирует работу с файлами

- Аудит прав доступа к папкам и файлам; контроль групп сотрудников, работающих с данными ограниченного доступа.
- Мониторинг операций с файлами: кто, когда и как с ними взаимодействовал.
- Блокировка опасных действий: редактирование, чтение, пересылка и др. в любых приложениях.

Найти виновного и наказать

Что произошло: Был уволен ИТ-специалист. Перед уходом он оставил себе лазейку, а через полгода удалённо стёр массив данных, почистив логи в AD, и, казалось, «замёл» следы.

Расследование: Обнаружено удалённое подключение к файловому серверу. Все действия злоумышленника зафиксировал FileAuditor. Удалённые файлы оперативно восстановили из теневых копий.

Итог: Ущерб оценили в 1,5 млн ₽. Данные DLP стали доказательством в суде, вина доказана: бывший сотрудник получил условный срок, ущерб взыскан в полном объёме.

Полезно в новых законодательных условиях!

Отображение местоположения компьютеров

Контроль сотрудников вне офиса

Доступен контроль удалённых сотрудников и сотрудников в командировках — с точным определением, где находятся их рабочие ПК.

APSdigital

searchinform

«СёрчИнформ ProfileCenter»

Система профилирования сотрудников

Отчёт инцидентов: угрозы безопасности

По итогам 2 недель / месяца ИБ-аналитик предоставляет отчёт об инцидентах.

Дата	Суть инцидента
Наркотики	
10.01	Сотрудник с другом во «ВКонтакте» договариваются о поездке к дилеру, у которого оставили заявку на 2 грамма.
Отправка корпоративных документов с личной почты	
11.01	Сотрудница с личной почты отправила должностную инструкцию (для внутреннего пользования) сотруднику другой компании, куда планирует перейти.
Боковые схемы	
15.01	Сотрудница загрузила в личное облако счета-фактуры и накладные организаций, где значится руководителем и главным бухгалтером.
Подделка документов	
19.01	Сотрудник в графическом редакторе подделал счета и акты: изменил печати и подписи в договорах; подделал сертификат соответствия.
ИП и подработки	
21.01	В личной почте сотрудника велось обсуждение изготовления продукции, аналогичной продукции компании, без оформления документов.

Отчёт инцидентов: рабочее время и ресурсы

Нерациональное использование рабочего времени

- Просмотр фильмов в рабочее время — от 2 до 5 часов в день.
- Просмотр сериала: за 11 рабочих дней суммарно 24 ч 55 мин.
- Посещение посторонних сайтов (auto.ru, pikabu.ru) — до 3 часов в день.
- За 22 рабочих дня — порядка 60 часов на сторонних сайтах.

Нецелевое использование рабочего оборудования

- Сотрудница распечатала учебники по химии — 1254 страницы.
- Сотрудница распечатала журналы по вязанию — 260 страниц.

Что на выходе?

ИБ-аутсорсинг за короткий срок (первые результаты — обычно за 2 недели – 1 месяц) помогает увидеть «болевые точки» компании:

- Какие сайты сотрудники посещают с рабочих ПК (соцсети, кино, игры?).
- Как используют рабочее время (открывают программы только для вида?).
- Что обсуждают в мессенджерах (боковые схемы, откаты, махинации?).
- Что копируют на устройства (флешка с клиентской базой перед увольнением?).
- Есть ли в компании сотрудники из групп риска (например, главный бухгалтер – игроман?).

Преимущества аутсорсинга ИБ

1 Бесплатный тест 30 дней

Полная картина происходящего в компании без финансовых вложений. ИБ-аналитик определит актуальные риски на основе опыта 4 000+ клиентов.

2 Непредвзятость

Специалист не знает сотрудников лично — человеческий фактор исключён. Все действия аналитика логируются, заказчик может проверить работу на любом этапе.

3 Профессиональный подход

ИБ-специалист с опытом в разных сферах расследует инцидент, выявит виновных и предоставит доказательства.

4 Бесперебойность

Работа без больничных, увольнений и отпусков — защита не прерывается ни на день.

APSdigital

searchinform

Доверьте информационную безопасность вашей компании профессионалам!

Алексей Ивахин

+7 902-927-45-46
t.me/alexfull24
ceo@apsdigital.ru