



staffcop®

Расследование инцидентов внутренней безопасности

Мониторинг
Анализ
Оповещение
Блокировка

О компании



Компания «Атом Безопасность» - аккредитованный российский разработчик IT-решений в области информационной безопасности и контроля действий персонала.

Более 10 лет мы разрабатываем программные решения для расследования инцидентов внутренней информационной безопасности. Среди наших клиентов представители крупного, среднего и малого бизнеса, коммерческие предприятия и государственные службы.

Подтверждена совместимость:



10+ лет в информационной безопасности

200 000+ ПК под защитой Staffcor

20+ отраслей бизнеса и промышленности, в которых мы работаем

3 000+ клиентов в 40+ странах мира



Минцифры
России

«Атом безопасность» внесена в Единый реестр IT-компаний Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации с регистрационным номером 9965 запись №95 от 15.03.2019 г.

Staffcor внесен в Единый реестр российского ПО под №8828.



ФСТЭК
России

Сертификат ФСТЭК №4234. Соответствует требованиям документов: Требования к СКН, Профиль защиты СКН (контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ. СКН. П4. ПЗ), ЗБ.

О Staffcop



Система для расследования инцидентов внутренней информационной безопасности Staffcop состоит из двух частей: сервера и службы-агента.

Агент запускается на рабочих станциях сотрудников или терминальных серверах, собирает данные действий пользователя и события, передает и сохраняет их на сервере для обработки и визуализации. В дальнейшем сервер позволяет собирать, анализировать, обрабатывать, визуализировать и осуществлять поиск информации.

Staffcop может работать как в рамках локального закрытого периметра, так и с учетом компьютеров, находящихся за его пределами, в том числе и на ПК сотрудников, которые работают удаленно.

Для кого



Собственникам
бизнеса



IT специалистам



ИБ специалистам



HR

С помощью Staffcop вы сможете



Расследовать

1. Инциденты информационной безопасности.
2. Причины неэффективной работы.



Выявлять

1. Мошеннические схемы внутри компании.
2. Нелояльных сотрудников, работающих на конкурентов.



Предупреждать

1. Утечки конфиденциальной информации.
2. Саботаж рабочих процессов.
3. Конфликтные ситуации в коллективе.



Блокировать

1. Копирование на съемные носители.
2. Пересылку конфиденциальной информации.
3. Доступ к нерегламентированным ресурсам.

Как работает Staffcop?



1 Сбор данных

Агент собирает все активные события на рабочих станциях, и передает их на сервер для последующего расследования, анализа, оповещения и принятия решения.

2 Анализ

Визуальный и статистический анализ данных для выявления отклонений в поведении пользователей, поиска инцидентов, инсайдеров и нелояльных сотрудников.

3 Расследование

Поиск по всем данным с помощью фраз и регулярных выражений, корреляций событий. Технология «drill-down» позволяет находить данные, очищенные от информационного шума в несколько кликов.

4 Оповещение

Автоматическое оповещение о нарушении политики безопасности, опасной и непродуктивной деятельности сотрудников.

5 Блокировка

Операций с файлами по контенту и цифровым меткам.
Доступа к съемным носителям информации.
Запуска приложений и доступа к сайтам, использование WiFi сети.

Подходит для импортозамещения

Серификат ФСТЭК
и ТИ ФСБ

Поддержка Linux, PostgreSQL,
ClickHouse, Jatoba

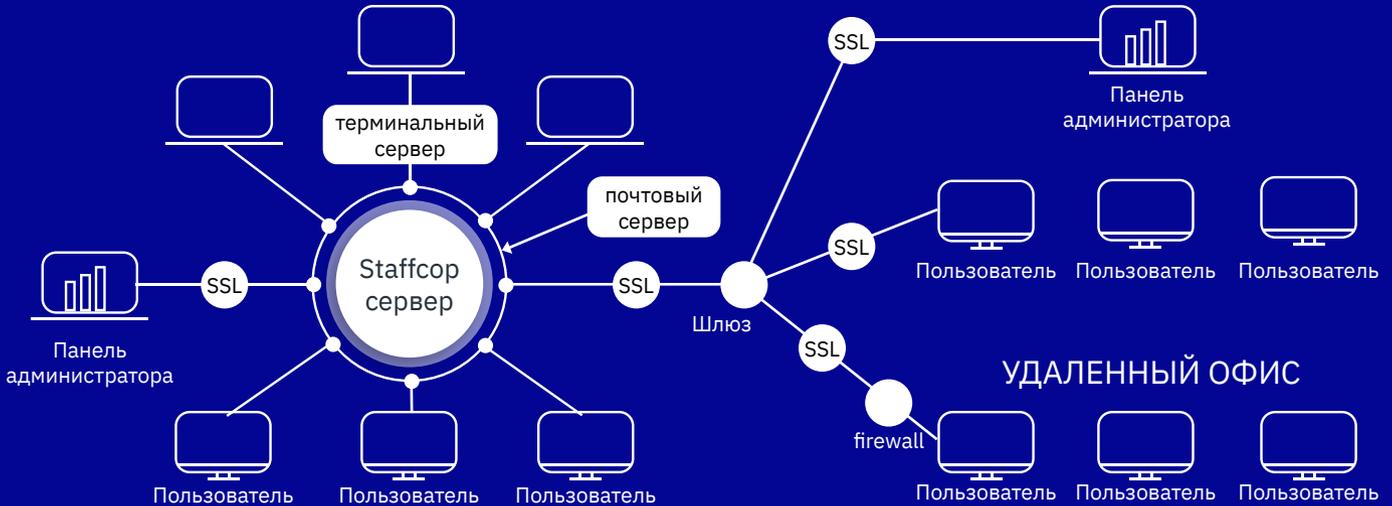
Реестр отечественного
ПО

Работает на СПО,
защищен от санкций

ЛОКАЛЬНАЯ СЕТЬ

Работает в локальных, распределенных и смешанных сетях любой сложности.

ИНТЕРНЕТ



1 Сервер работает на операционной системе Linux (Astra, Ubuntu) и может быть установлен как на физическом, так и на виртуальном сервере.

2 При отсутствии связи, данные собираются в зашифрованной локальной базе данных агента и при восстановлении связи будут передаваться небольшими пакетами на сервер.

3 Контроль ведется на рабочих станциях, терминальных серверах, VDI. Агент работает на операционных системах Windows, Linux, MacOS*.

**Функциональность агента на разных операционных системах отличается*



Единый веб-интерфейс

Доступ к данным, отчетам и настройкам осуществляется через единый веб-интерфейс.



Современные технологии

В основе лежит OLAP - технология обработки данных для построения многомерных отчетов «на лету» и обработки огромных объемов данных за секунды.



Горизонтально масштабируется

Staffcop эффективно работает как с несколькими компьютерами, так и с тысячами рабочих станций.



Возможности интеграции

Открытое API.
Получение данных от СКУД.
Сбор данных с почтового сервера.

Контроль всех каналов и событий

Снимки и запись с веб-камер

Снимки и запись с веб-камеры, установленной на компьютере пользователя, для визуальной идентификации.

Мониторинг посещенных сайтов и социальных сетей

Длительность пребывания.
Контроль переписки.
Перехват поисковых запросов.

Контроль e-mail переписки

IMAP, SMTP, MAPI, POP3 и шифрованные аналоги. Контроль отправки сообщений и передачи файлов через сервисы веб-почты.

Контроль съемных носителей

Фиксация времени подключения и отключения, теневое копирование, блокировка по «черным»\«белым» спискам.

Контроль ввода данных

Запись нажатия клавиш на клавиатуре с целью предотвращения утечки данных. Копирование данных в буфер обмена.

Инвентаризация

Программного обеспечения и железа

Запись аудио с микрофона и колонок

Запись аудио с микрофона и колонок компьютера и возможность сопоставления ее с любыми событиями.



Контроль рабочего стола

Снимки экранов всех мониторов пользователя по событиям и интервалам времени, запись видео рабочего стола.

Удаленное подключение

Просмотр нескольких рабочих столов с быстрой навигацией по ним. Перехват управления рабочей сессии.

Контроль печати

Отслеживание файлов, отправляемых на печать, регистрация пользователя и времени отправки.

Перехват сообщений в мессенджерах

Telegram, Skype, Teams, Bitrix24 и др. Фиксация времени отправки или получения сообщения, адресата, содержание, и вложенных файлов.

Контроль пользовательской активности

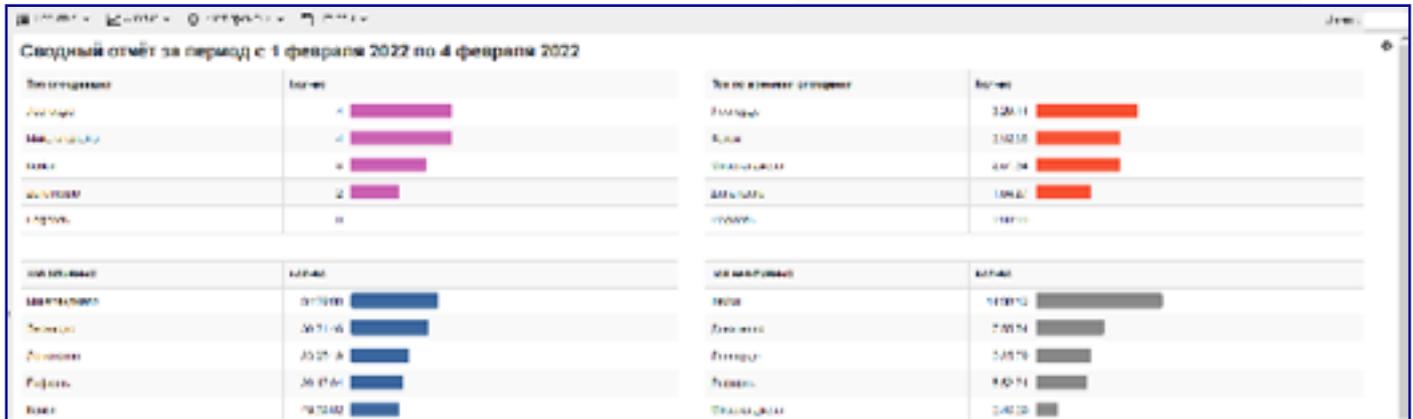
Контроль пользовательской сессии, локальной и удаленной, логирование входа и выхода из системы.

Мониторинг доступа к файлам

Создание теневых копий файлов, отправляемых за пределы рабочей станции.

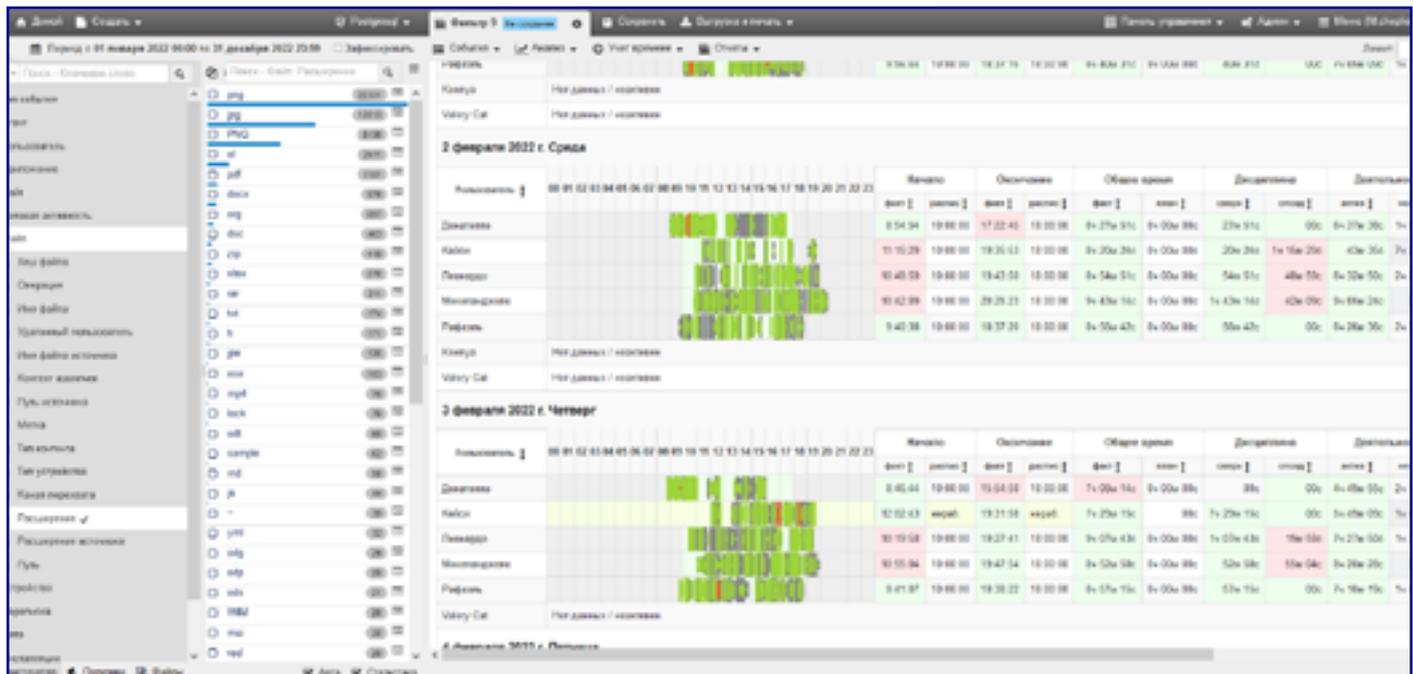
Наглядная статистика

- Опоздания
- Простои на работе
- Активное время за компьютером
- Продуктивное время
- Время, затраченное на личные нужды
- Статистика по сотрудникам и отделам



Гибкая настройка раписаний и категоризации

Для разных категорий сотрудников можно настроить те программы и сайты, которые требуются им для выполнения задач, и те, которые «противопоказаны» к использованию. А так же задавать уникальное расписание.



Staffcop умеет в автоматическом режиме по расписанию отправлять подробный отчет в pdf или excel по электронной почте.

Табель учета активного времени
Отчетный период с 1 февраля 2022 по 28 февраля 2022

Пользователь	Отчеты по неделям														Итого		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	Среднее время	Максимальное время	Время
Иванов	10	17	10	19	20	21	20	20	24	28	26	27	26	20	20	28	200
Петров															0	0	0
Сидоров															0	0	0
Смирнов															0	0	0
Васильев															0	0	0
Кузнецов															0	0	0
Лебедев															0	0	0
Новиков															0	0	0
Попов															0	0	0
Соловьев															0	0	0
Тихонов															0	0	0
Федотов															0	0	0
Харьков															0	0	0
Цыганов															0	0	0
Чайков															0	0	0
Шаров															0	0	0
Щербаков															0	0	0
Юрьев															0	0	0
Яковлев															0	0	0

Возможности интеграции

- Открытая API позволяет дополнять данными SIEM-систему для осуществления комплексного анализа и обработки инцидентов.
- Возможность интеграции IMAP с почтовым сервером позволяет контролировать и анализировать рабочие коммуникации и передаваемую информацию.
- Получение данных сетевого трафика со стороны шлюзового решения посредством интеграции на основе ICAP.
- Синхронизация с Active Directory на основе LDAP позволяет дополнить профиль пользователя данными. Возможность группировать и анализировать данные по отделам, формировать отчеты руководителям.
Для доменных пользователей возможно предоставить доступ к системе с определенными правами и установить агенты контроля в рамках данной инфраструктуры.
- Для комплексного анализа рабочего дня сотрудников система позволяет дополнять расписание данным табеля отсутствия из 1С.
- Для проведения анализа нахождения сотрудников на рабочем месте реализована интеграция со СКУД.

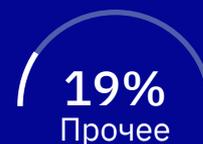
Блокировки

Staffcop позволяет производить следующие блокировки в режиме «черных» или «белых» списков на компьютерах и терминальных серверах:

- Блокировки запуска процессов и приложений.
- Блокировка доступа к сайтам.
- Блокировка USB-устройств по задаваемым группам и Hardware ID.
- Ограничение записи на съемные носители.
- Блокировка буфера обмена при передаче контента в другое приложение.
- Блокировка операций с файлами по контенту, атрибутам и цифровым меткам.
- Блокировка подключения к Wi-Fi сетям.
- Блокировка носителей информации при превышении порога передачи данных.

Повышение эффективности труда

Немного статистики и вычислений



Мы опросили около 20 компаний, использующих Staffcop, в которых суммарно 4500 сотрудников, работающих за ПК, и составили картину распределения рабочего времени среднестатистического сотрудника.

Отвлекающие от работы программы и сайты могут быть заблокированы.

Блокировки могут быть назначены лично для сотрудника, для отдела или для всех.

Потери от оплачиваемой непродуктивной деятельности и опозданий 10 сотрудников, со средней заработной платой 50 000 Р.

285 000 Р в месяц или 3 420 000 Р в год.

Почему Staffcor?

Кроссплатформенный

Уникальные функции мониторинга рабочих станций и терминальных серверов под управлением Windows, Linux и MacOS систем.

Оптимальная стоимость покупки и владения

Минимальные требования к «железу», разумная стоимость, как результат - низкая стоимость приобретения, внедрения и эксплуатации.

Быстрый

Высокая скорость на больших объемах данных за счет использования современных баз данных ClickHouse и PostgreSQL на технологии OLAP-кубов.

Отечественный

Нас уже выбрали многие предприятия из ВПК, госсектора, крупные коммерческие и производственные организации.



Многомерные аналитические отчеты, схемы коммуникаций и движения информации с возможностью перехода от общего к частному.



Подробная документация, оперативная и компетентная техническая поддержка. Команда проекта оказывает комплексную поддержку с начального этапа тестирования.



Работа в любых сетевых инфраструктурах подойдет для контроля распределенной филиальной сети, удаленных офисов и сотрудников.



Мониторинг и управление рабочими местами из единого веб-интерфейса, возможность просто и безопасно организовать доступ из любой точки мира.



Staffcor подходит для выполнения банковских ГОСТов, приказов ФСТЭК России, и работе в критической информационной инфраструктуре. Staffcor подходит для выполнения ряда требований в соответствии с ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций и ФСТЭК приказ ведомства №35 от 20.02.2020 об обеспечении безопасности КИИ.

Пробуйте бесплатно

Дистрибутив и подробная документация на сайте www.staffcop.ru



Быстро

Развертывание пилотного проекта обычно занимает не более одного дня.

Легко

Требуется минимум усилий и ресурсов для запуска.

Комплексно

Вы сможете оценить сразу весь комплекс решаемых задач и принять правильное решение.

Полное техническое сопровождение на этапе тестирования!

Стоимость

Лицензия

Гибкая политика лицензирования согласно тарифного плана*

Обновления

Входят в стоимость тарифного плана

Техническая поддержка (стандарт)

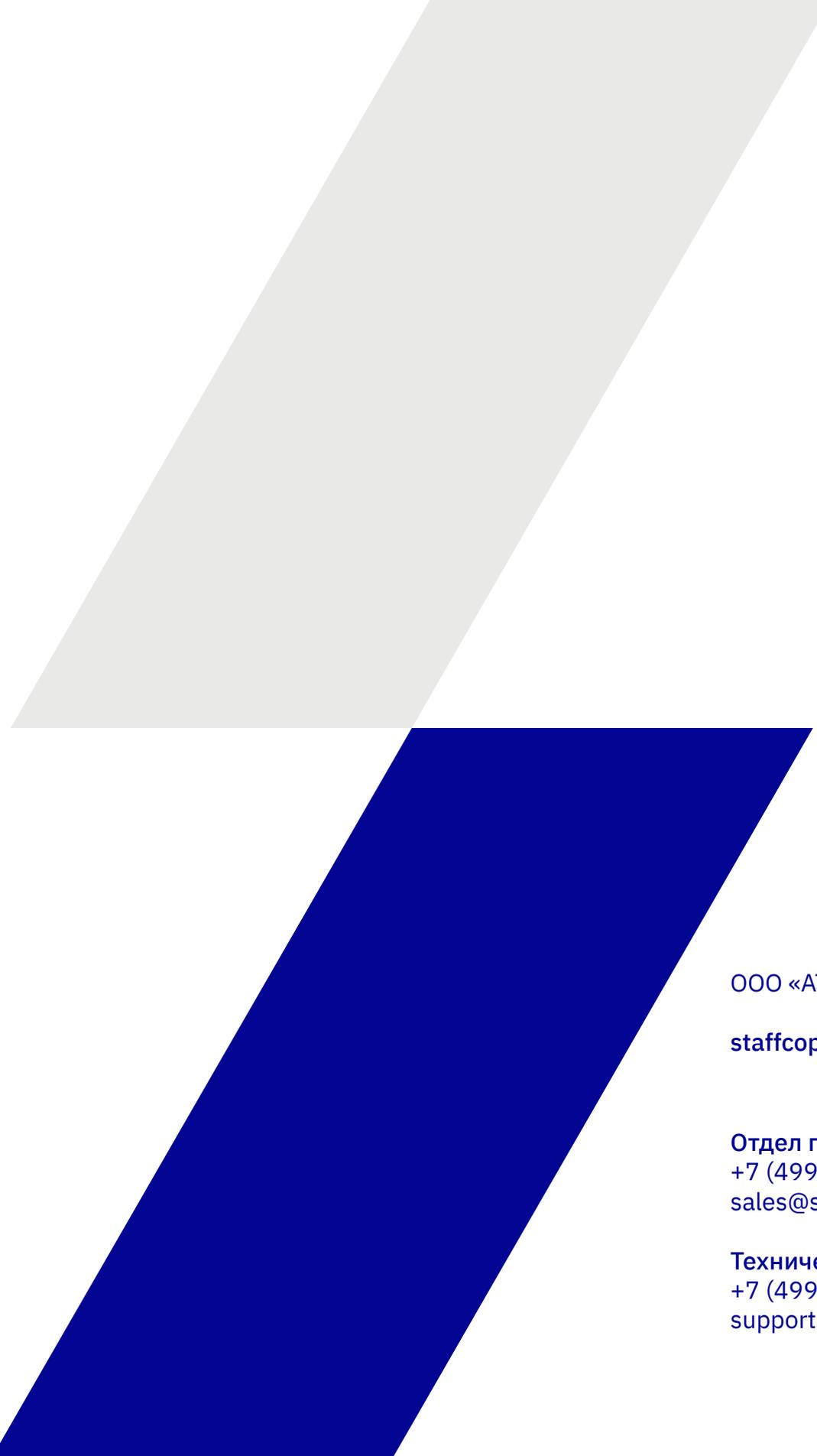
Входит в стоимость тарифного плана

Тарифный план: лицензия, обновления, техническая поддержка



Модуль рабочей станции - Агент Staffcop имеет плавающий характер, то есть Агента можно переносить на другие устройства без потери предоставленного неисключительно права и ранее накопленных данных неограниченное количество раз в течении срока действия лицензии. Установленный Агент осуществляет мониторинг активных учётных записей. При отсутствии учетных записей Агент осуществляет мониторинг самой рабочей станции.

*Условия тарифных планов, в том числе на продление технической поддержки и доступа к обновлениям уточняйте у вашего менеджера.



ООО «АТОМ БЕЗОПАСНОСТЬ»

staffcop.ru

Отдел продаж

+7 (499) 653 71 52

sales@staffcop.ru

Техническая поддержка

+7 (499) 638 28 09

support@staffcop.ru