



staffcop®

Новый уровень внутренней безопасности

Система для расследования инцидентов
внутренней информационной 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 Staffcop

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.

Staffcop 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

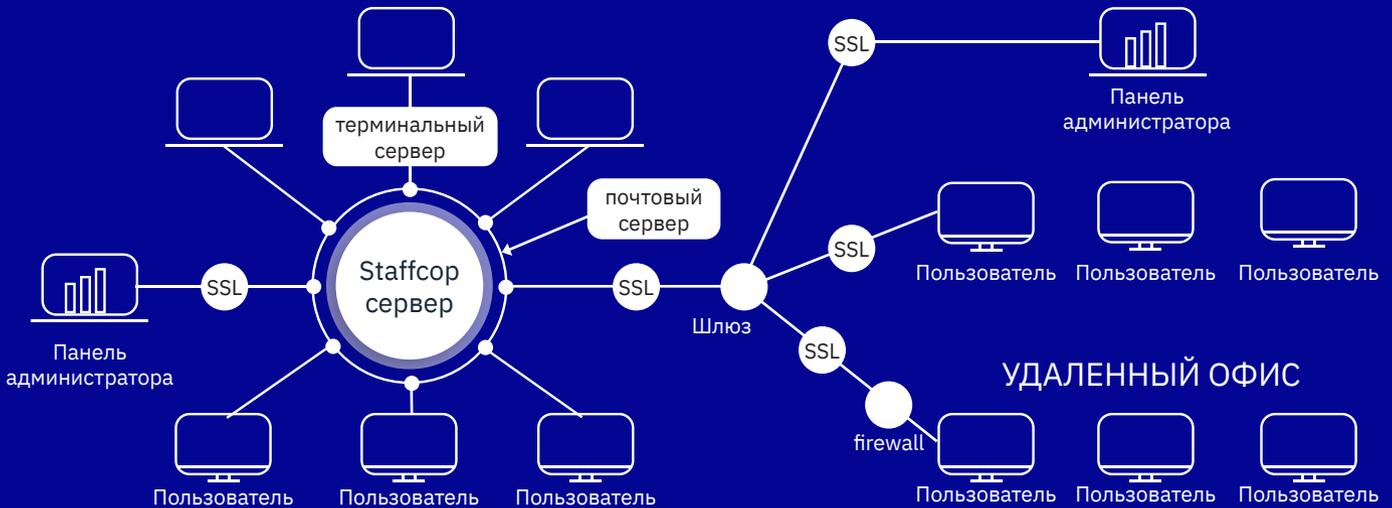
Реестр отечественного
ПО

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.

Аналитические возможности

- Широкий функционал по анализу регистрируемых событий и собранной информации.
- OLAP (интерактивный анализ данных) - технология отображения данных, заключающаяся в подготовке информации на основе больших массивов данных.
- Корреляция событий и данных по различным измерениям, для построения многомерных отчетов в несколько кликов.
- Возможность работать в гибридном режиме с подключением СУБД ClickHouse, что позволяет увеличить скорость обработки данных на сервере со слабыми характеристиками.

Гибкий и интерактивный конструктор отчетов и фильтров

Система позволяет создавать новые фильтры и отчеты, для поиска и анализа информации, используется прием последовательного наложения ограничивающих фильтров. Наложение каждого фильтра в режиме реального времени отсекает лишнюю информацию, что позволяет находить данные в 2-3 клика.

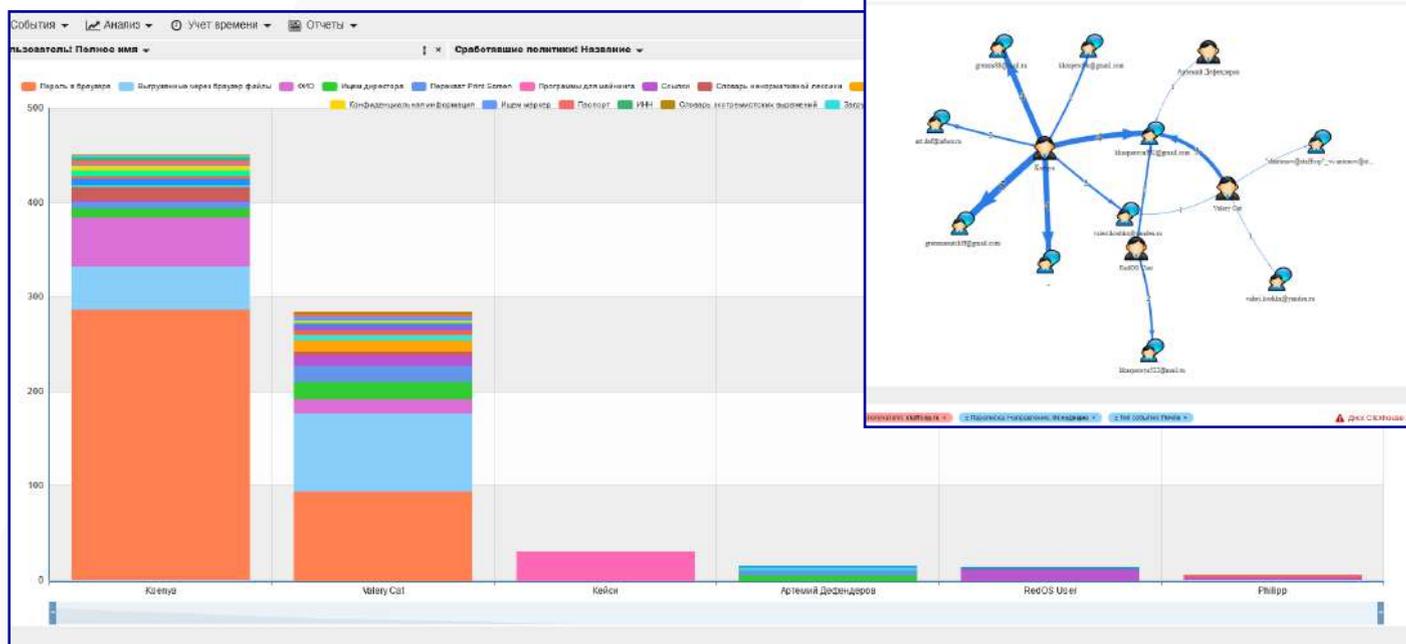
The screenshot displays a security analysis interface. On the left, there is a sidebar with various filters and search options. The main area shows a table of events with columns for 'Серверное время', 'Компьютер', 'Пользователь', 'Приложение', 'Получатели', 'Контент', 'Размер', and 'Ссылка с'. Below the table, a detailed view of a selected event is shown, including fields for 'Пользователь', 'Имя файла', 'Путь', 'Получатели', 'Формат', 'Источник', 'Комментарий', 'RID', 'Размер', and 'Содержимое'.

Серверное время	Компьютер	Пользователь	Приложение	Получатели	Контент	Размер	Ссылка с
2022-03-03 11:49:19	DESKTOP- R3932SU	Ксения	svchost.exe	Ксения	Скачать grafik.doc	37,4 Кб	Ит
2022-03-02 18:13:32	DESKTOP- R3932SU	Ксения	svchost.exe	Андрей_Арибагидий_Сергей_Нурович Андрей_Ворожей_Филипп_Воловичев Виктор_Турин_Максим_Юрьевич Anton_Bogush Оксана_Линия_Александр Василий_Павел_Александр_Константинович Феликс_Викторович Александр_Татьяна_Сергей_Дмитриев Эрнесто_Чарльз_Александр_Челван Ксения_Ксенья_Смирнова	Скачать 11Debug_AgentLog	68 Кб	Ит

Пользователь: Ксения
Имя файла: grafik.doc
Путь: grafik.doc
Получатели: Ксения
Формат: Plain
Источник: Ит
Комментарий: особый контроль
RID: 404
Размер: 37,4 Кб
Содержимое: РАСЧЕТНАЯ БЕЗОПАСНОСТЬ
Наймодель:

График взаимосвязей и анализ аномалий

Различные формы визуального анализа позволяют сформировать и наглядно отобразить перепику сотрудников, перемещение файлов, аномалии в рамках активности пользователя.



Учет рабочего времени

Staffcop не только фиксирует начало, перерывы и окончание рабочего дня, но и показывает детальную картину активности сотрудников.

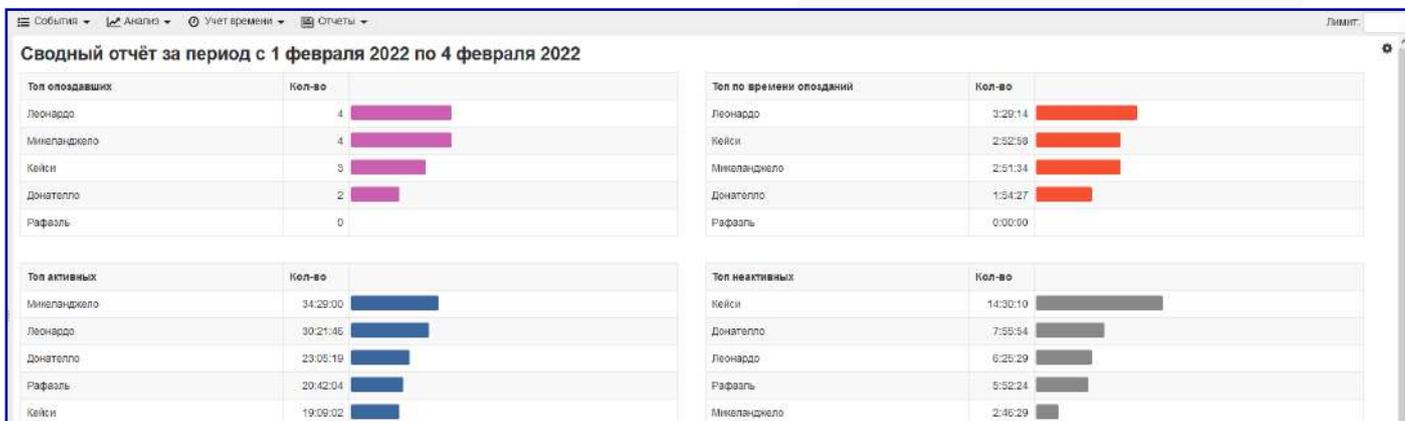
Уникальные алгоритмы определения активности позволяют максимально точно учитывать проведенное время в приложениях и на сайтах.

Учёт рабочего времени за период с 7 февраля 2018 по 7 февраля 2018

7 февраля 2018 г.																														
Компьютер ↓	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Начало ↓	Окончание ↓	Общее время ↓	Активное ↓	Простой ↓	
inparc																									11:25	19:51	8:26:22	7:09:40	1:16:42	
Продуктивность																														
Информационная безопасность																										2:27:48 (34.40%)				
Почтовые приложения																										2:11:37 (30.63%)				
Офисные приложения																										0:57:28 (13.28%)				

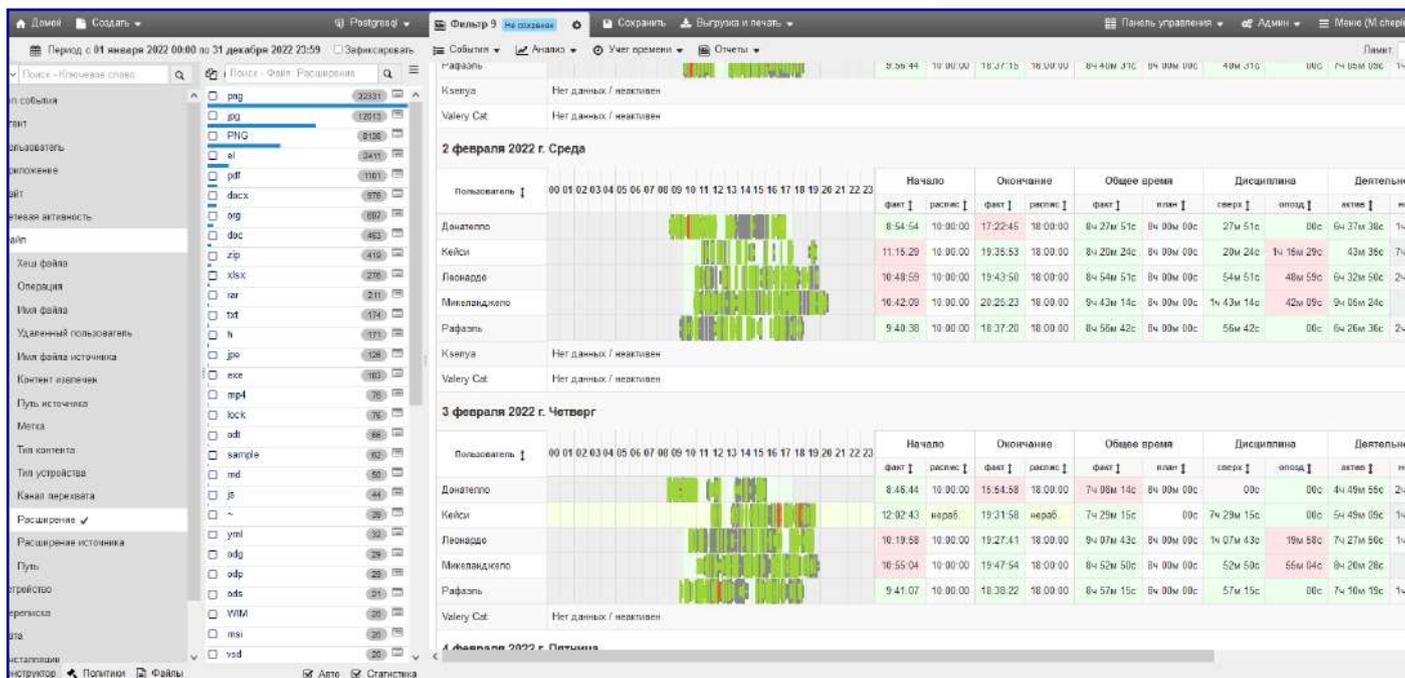
Наглядная статистика

- 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
Отчётный период с 1 февраля 2022 по 28 февраля 2022

Пользователь	Отметки по числам месяца																За		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	к	I половину месяца	II половину месяца	месяц
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	дни	дни	дни
Ксепуя						06м 58с				20м 20с			24м 52с				0	3	3
Vakely Call						21м 29с							03м 15с				0	3	3
Донателло	5ч 40м 21с	6ч 37м 38с	4ч 49м 56с	6ч 57м 25с													4	0	4
Кайси	5ч 35м 28с	43м 36с	5ч 45м 09с	6ч 59м 50с													23ч 05м 19с	00с	23ч 05м 19с
Леонардо	6ч 28м 45с	6ч 32м 50с	7ч 27м 50с	7ч 52м 21с													4	0	4
Микеланджело	8ч 31м 50с	0ч 05м 24с	8ч 20м 28с	8ч 31м 19с													30ч 21м 46с	00с	30ч 21м 46с
Рафаэль	7ч 05м 08с	6ч 29м 36с	7ч 10м 19с												13м 01с		4	0	4
																	20ч 05м 05с	00с	20ч 05м 05с

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.

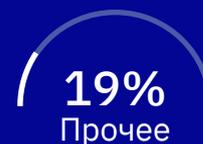
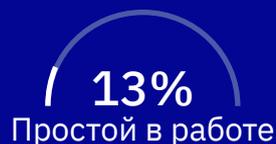
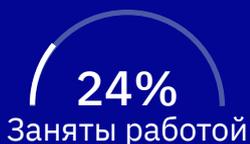
Блокировки

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

Бессрочная и срочная лицензия

Гибкая политика лицензирования.

Бесплатные обновления

В течение 12 месяцев с момента приобретения.

Бесплатная техподдержка

Оперативная, и компетентная техподдержка в течение 1 года бесплатно.

Политика лицензирования

Что лицензируем

Лицензии на пользователей



Рабочая станция



Учетная запись

Виды лицензий

Срочная
3, 12, 24 мес.

Бессрочная

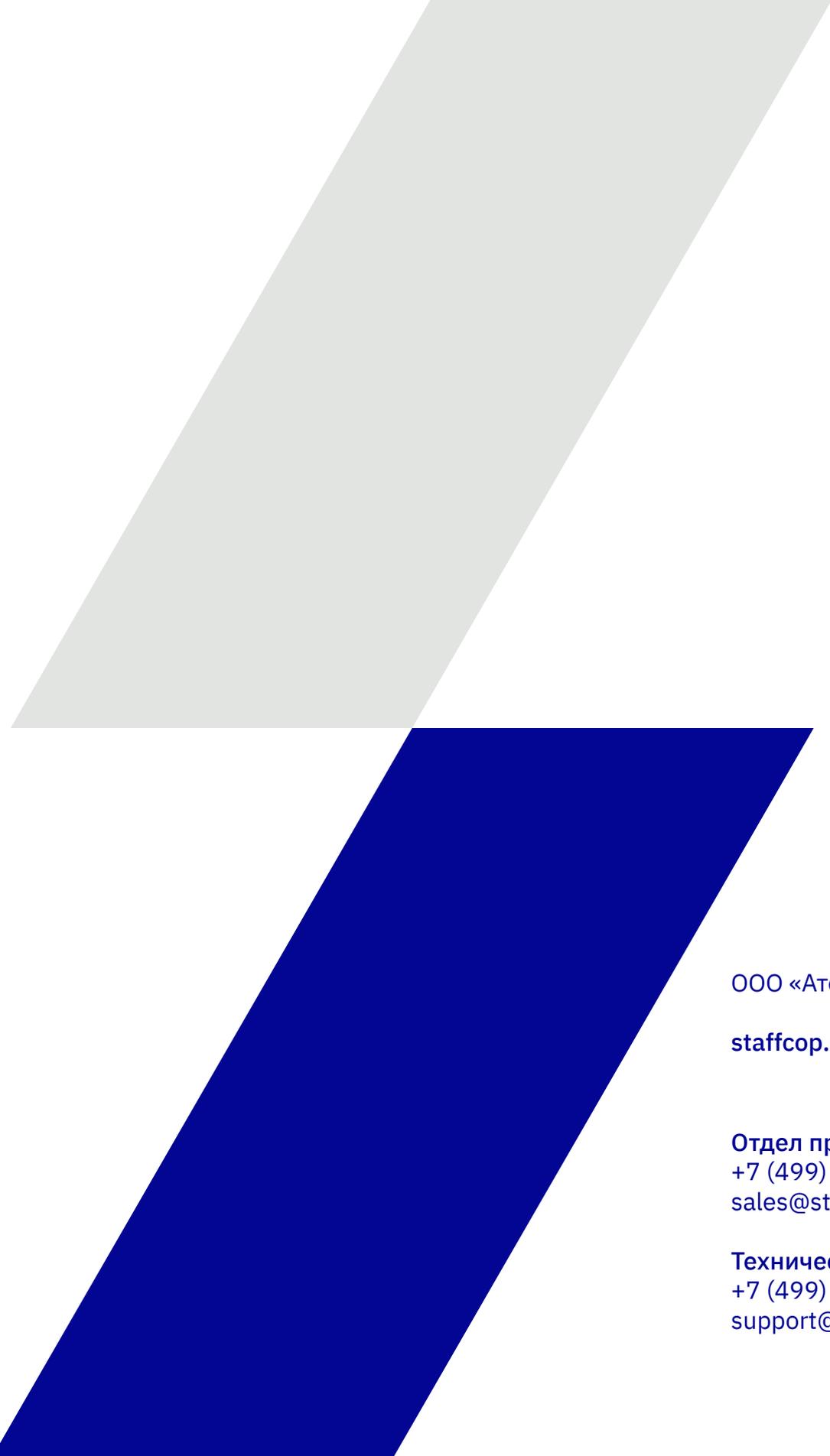
Тех. поддержка (стандарт) и обновления

Включено в стоимость

Включено в стоимость на 1 год

Агент мониторинга Staffcop имеет плавающий характер, предусмотрена возможность переносить агент на другие ПК без потери лицензии и архива данных. Установленный агент на рабочей станции осуществляет мониторинг активных учётных записей. При отсутствии учётных записей пользователей агент осуществляет мониторинг самой рабочей станции.

Бесплатная техническая поддержка и доступ к обновлениям программы предоставляются на срок лицензирования, но не более 12 месяцев с момента покупки. Тарифы на продление технической поддержки и доступа к обновлениям уточняйте 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