Контроль действий пользователей в информационной среде компании.

Кандыбович Дмитрий
Генеральный директор ООО Атом Безопасность

ООО Атом Безопасность

— ФСТЭК 3Б Требованиям к средствам контроля съёмных носителей информации по 4 классу
— Тематические исследования на соответствие временных требованием к программному обеспечению, используемому в автоматизированных системах ИТКС специального назначения (ТИ 69 Центр ФСБ России)
— Команда 60+
— Сколково
— 100 серверных компонентов в месяц, общее покрытие за год 94000 АРМ
— 82 мероприятия по СНГ

Технопарк Новосибирского Академгородка

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

Минкомсвязь России

Риски от инсайдеров

- **Нецелевое использование рабочего времени**



- **Расходы при утечке конфиденциальной информации**



STAFFCOP

Комплексное решение по информационной безопасности,
учёту рабочего времени и контролю эффективности сотрудников

учет рабочего времени

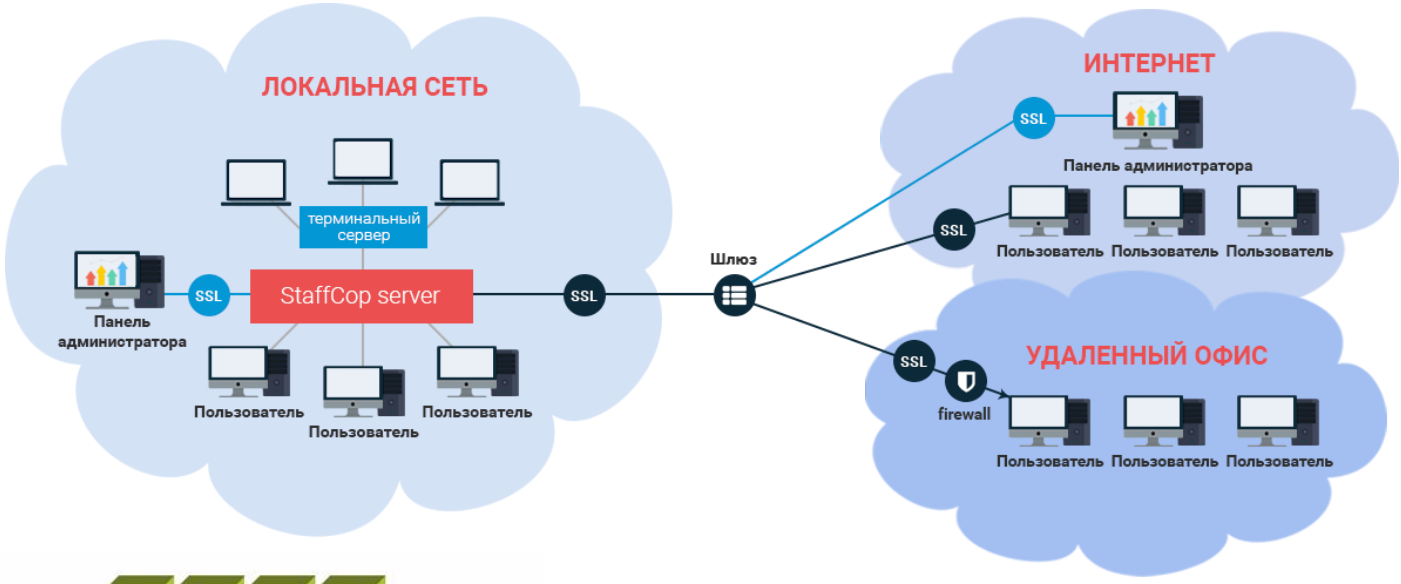
эффективность персонала

информационная безопасность

расследование инцидентов

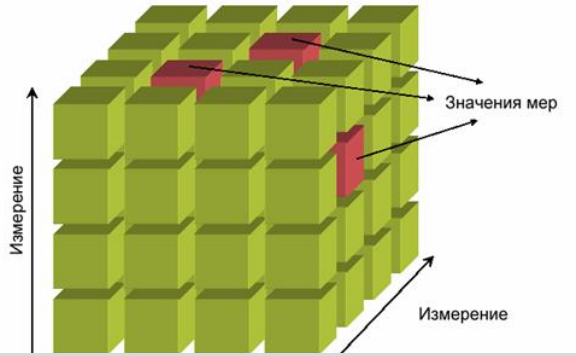
www.staffcop.ru

Современные архитектурные решения



1. Толстый клиент. Мониторинг рабочих станций внутри локальной сети

2. Saas технологии. Централизованный контроль удаленных офисов и распределенной филиальной сети



OLAP технология. OnLine Analytical Processing — оперативный анализ данных

www.staffcop.ru

Тотальный контроль

Декодирование сервисов веб-почты и социальных сетей:

— mail.ru, yandex.ru, gmail.com…
— VK, FB, Одноклассники, LinkedIn…

Почтовые протоколы:
— SMTP / SMTPs
— IMAP
— POP3 / POP3s
— MS Exchange

Передача гипертекстовой информации и файлов:
— HTTP / HTTPs
— FTP / FTPs

Интернет-мессенджеры
— Skype
— ICQ, QIP, Jabber (XMPP)
— Mail.ru Agent
— Yahoo и другие

USB-порты
— контроль и блокировка

Теневое копирование файлов
— из электронной почты
— со съемных носителей
— переданных через интернет
— отправленных на печать

www.staffcop.ru

Расследование инцидентов ИБ

Конструктор многомерных отчетов

позволяет «налету» получить необходимый набор данных. Поиск по ключевым словам и регулярным выражениям до минимума сократит время расследования инцидента.

Поиск по словам и регулярным выражениям

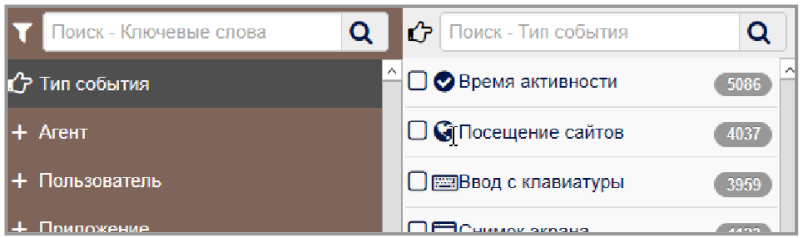
позволяет «на лету» получить необходимый набор данных. Поиск по ключевым словам и регулярным выражениям до минимума сократит время расследования инцидента,

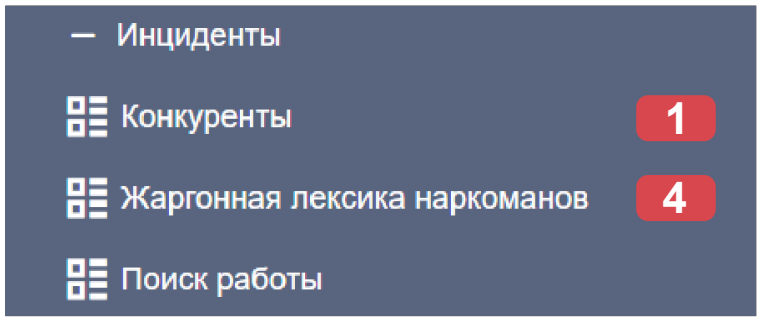
Множество графов и диаграмм

для выявления аномального поведения, анализа изменений интенсивности событий. Линейные, круговые и тепловые диаграммы, графы взаимосвязей.

www.staffcop.ru

Современные инструменты обнаружения угроз и оповещения





Анализатор угроз

Автоматический анализ данных на предмет подозрительных событий.

Контентный анализ файлов

Парсинг файлов на наличие в них конфиденциальной или потенциально опасной информации.

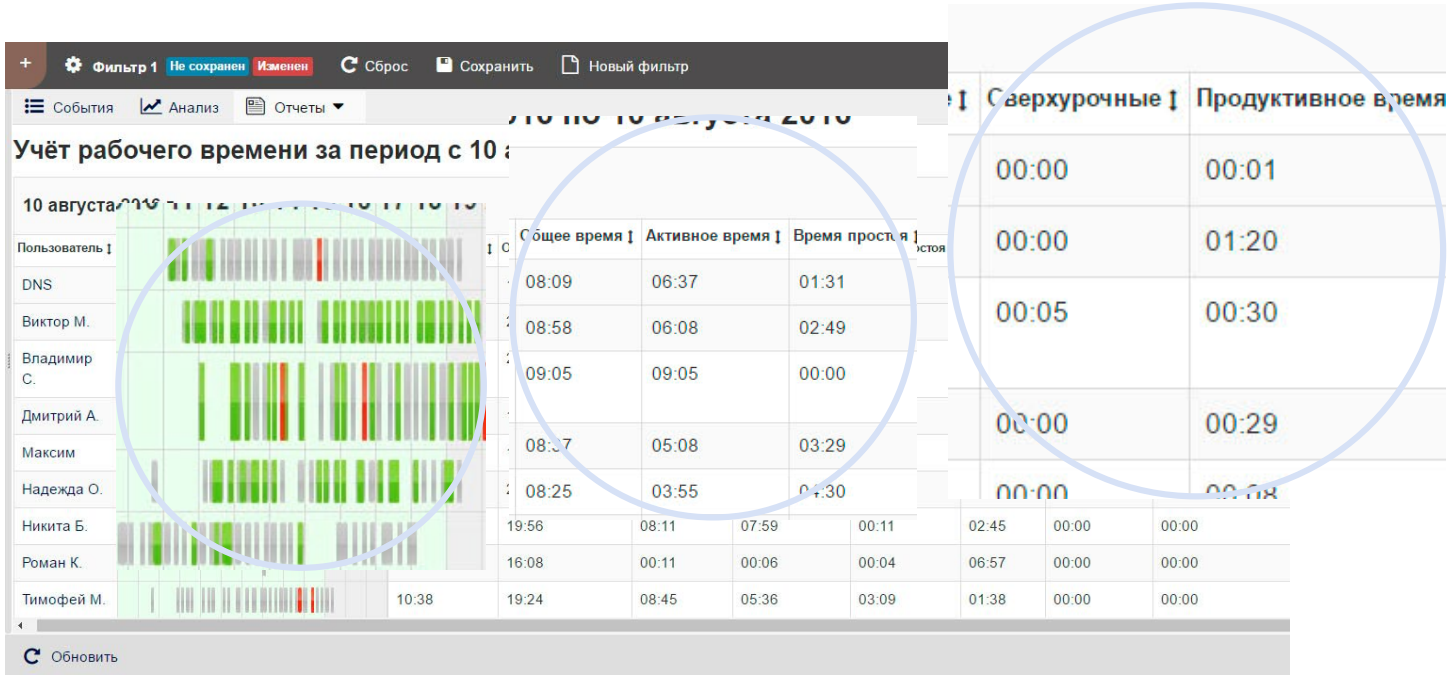
Система оповещений

Уведомления о нарушениях появляются как в панели администрирования, так и могут быть немедленно отправлены по электронной почте.

www.staffcop.ru

Учёт рабочего времени и оценка его эффективности

- Продуктивная деятельность
- Непродуктивная деятельность
- Нейтральная деятельность
- Не было активности



STAFFCOP

www.staffcop.ru

Удаленное управление и администрирование ПК

Мониторинг

— удаленный рабочий стол
— сетевой трафик
— процессы и приложения
— установка и удаление ПО

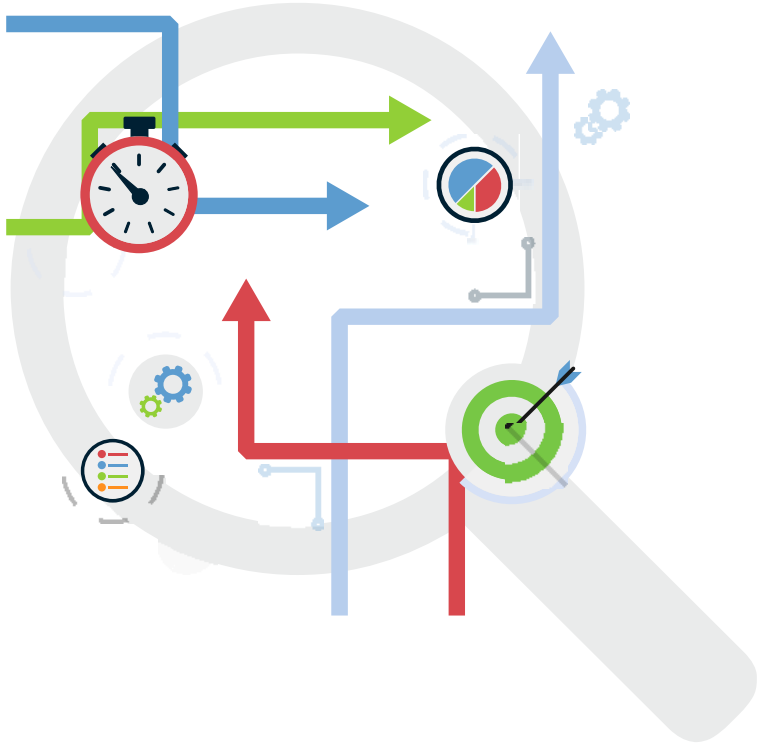
Блокировки

— приложений и сайтов
— съемных USB-устройств

Инвентаризация ПО и «железа»

www.staffcop.ru

Оптимизация бизнес-процессов

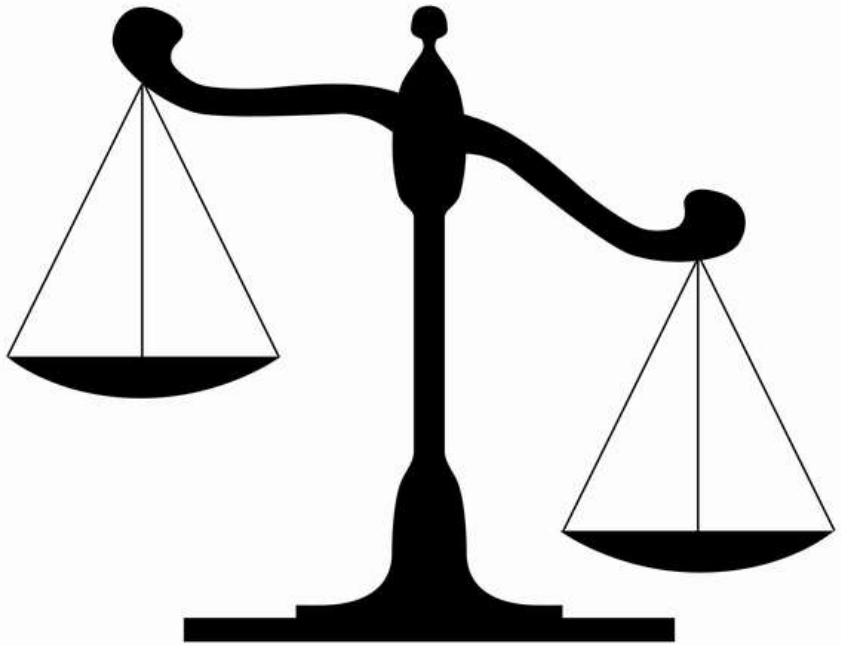


Со StaffCop легко контролировать ваши бизнес-процессы, находить «узкие» места и выявлять блокирующие факторы, а также расследовать причины их появления.

Отслеживать реальный KPi сотрудников, например, для менеджеров продаж - это может быть количество отправленных коммерческих предложений и договоров, количество контактов с клиентами и поставщиками.

Проблемы организации мониторинга

Правовые



Что говорит закон?

С одной стороны:

Конституция РФ Статья 23

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

УК РФ Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

1. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан - наказывается штрафом …, либо обязательными работами …, либо исправительными работами

Изменение ФЗ 138 УК РФ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О внесении изменения в статью 138[1] Уголовного кодекса Российской Федерации

Статья 1

Дополнить статью 138[1] Уголовного кодекса Российской Федерации (Собрание законодательства Российской Федерации, 1996, № 25, ст. 2954; 2011, № 50, ст. 7362; 2015, № 24, ст. 3367; 2016, № 27, ст. 4258; 2017, № 31, ст. 4799) примечанием следующего содержания:

«**Примечание.** Под специальными техническими средствами, предназначенными для негласного получения информации, в настоящем Кодексе понимаются приборы, системы, комплексы, устройства, специальный инструмент и программное обеспечение для электронных вычислительных машин и других электронных устройств, независимо от их внешнего вида, технических характеристик, а также принципов работы, которым намеренно приданы качества и свойства для обеспечения функции скрытного (тайного, неочевидного) получения информации либо доступа к ней (без ведома ее обладателя).».

Президент
Российской Федерации

Что говорит закон?

С другой стороны:

Гражданский кодекс Статья 1470. Служебный секрет производства

1. Исключительное право на секрет производства, созданный работником в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя (служебный секрет производства), принадлежит работодателю.

Трудового кодекса РФ статья 15

"Трудовые отношения - отношения, основанные на соглашении между работником и работодателем о личном выполнении работником за плату трудовой функции (работы по определенной специальности, квалификации или должности), подчинении работника правилам внутреннего трудового распорядка при обеспечении работодателем условий труда, предусмотренных трудовым законодательством, коллективным договором, соглашениями, трудовым договором.

Соответствие 21 приказу ФСТЭК

ЗНИ.2	**Управление доступом к машинным носителям информации**
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации
ЗНИ.7	Контроль подключения машинных носителей информации
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных

www.staffcop.ru

Соответствие приказу ФСТЭК России “Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации”. (относится напрямую к 187 ФЗ)

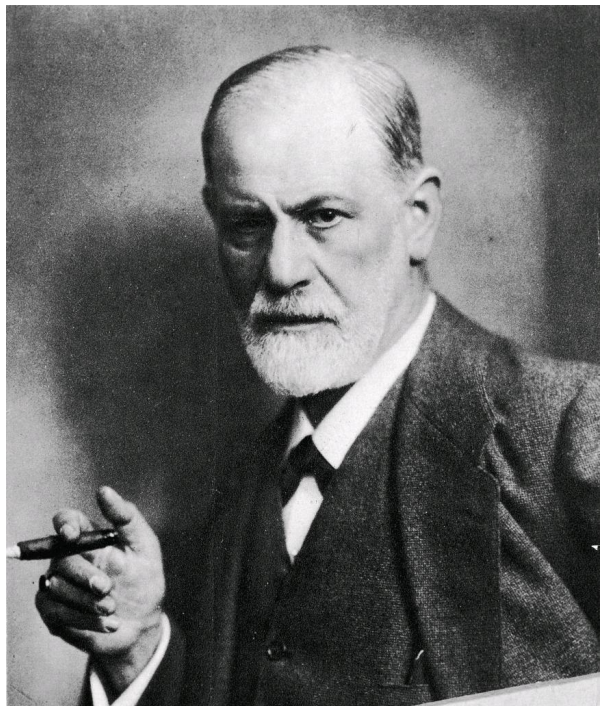
ЗНИ.6	**Контроль ввода-вывода информации на машинные носители информации**
ЗНИ.7	Контроль подключения машинных носителей информации
АУД.5	Контроль и анализ сетевого трафика
АУД.9	Анализ действий пользователей
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенным к использованию
ЗИС.17	Защита информации от утечек
УКФ.4	Документирование данных об изменениях в конфигурации

Обязательные действия перед началом мониторинга

- Определить и довести до работников правила использования средств хранения, обработки и передачи информации
- Разработать и довести до работников регламент проведения мониторинга
- Получить согласие работников на проведение мониторинга использования им средств хранения, обработки и передачи информации
- Включить положения об обязательстве работника соблюдать правила использования средств коммуникации и согласие на мониторинг в трудовой договор (дополнительное соглашение к трудовому договору)

Проблемы организации мониторинга

Этические и психологические



- Проявление потенциального недоверия
- Пределы вмешательства
- Возможный доступ к частной жизни
- Возможность злоупотреблений
- Несоответствие заявленных целей контроля фактическим

STAFFCOP

Windows Server 2008 R2

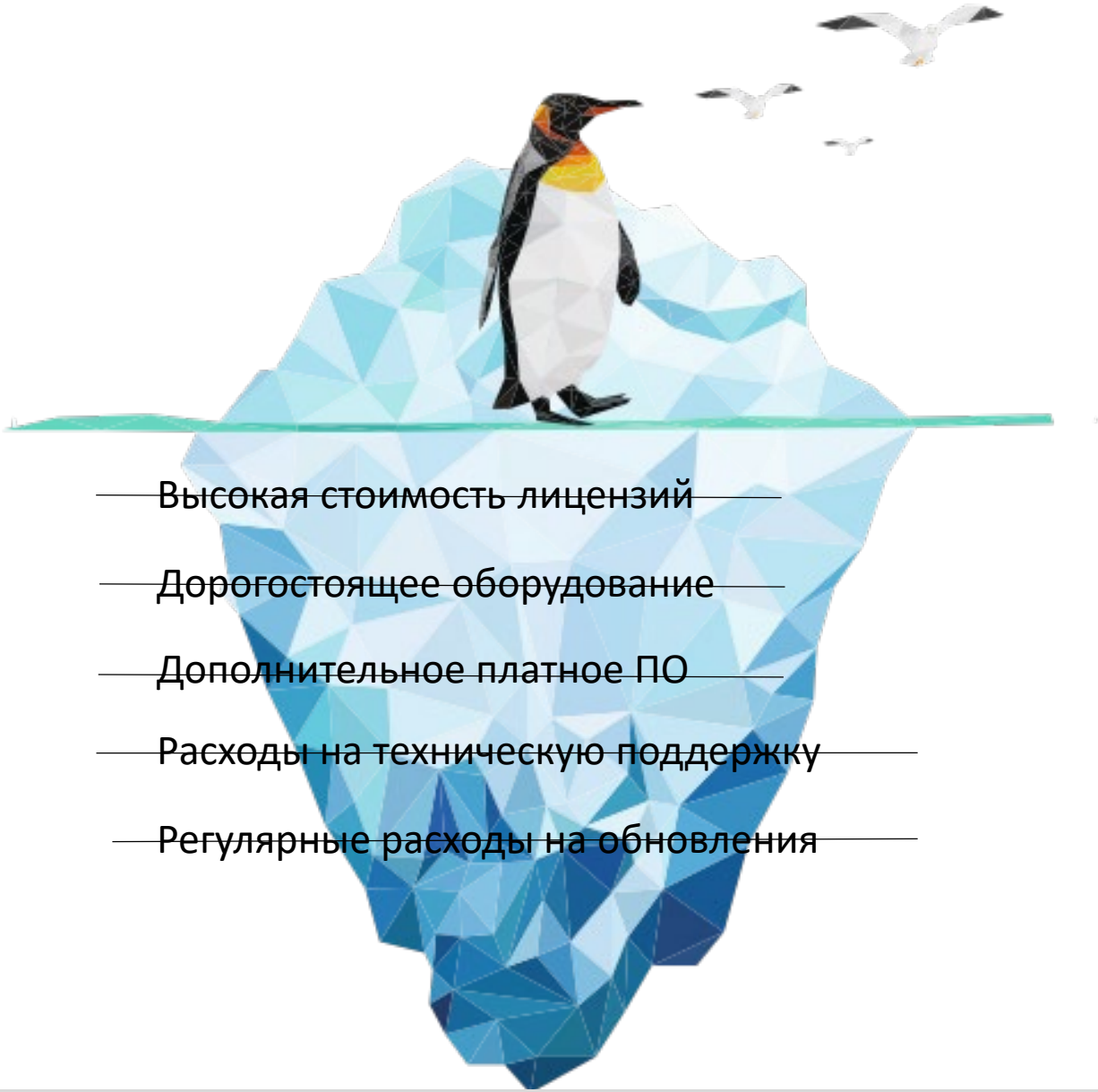
Microsoft SQL Server

ubuntu

PostgreSQL

Бесплатная поддержка
в течение года

Бессрочные лицензии



- ~~Высокая стоимость лицензий~~
- ~~Дорогостоящее оборудование~~
- ~~Дополнительное платное ПО~~
- ~~Расходы на техническую поддержку~~
- ~~Регулярные расходы на обновления~~

Спасибо за внимание!

Дмитрий Кандыбович
Генеральный директор
ООО Атом Безопасность

+79139152137
sales@staffcop.ru
Staffcop.ru