Как контролировать сотрудников в информационной среде компании

13 февраля 2020 Ростов-на-Дону

Андрей Арбатский
представитель StaffCop в Москве

ООО Атом Безопасность

— 12 лет разработки приложений контроля сотрудников
— Академгородок Новосибирск, резиденты Технопарка
— Высокотехнологичная компания с опытной командой разработчиков-профессионалов в области ИБ

Технопарк Новосибирского Академгородка

STAFFCOP

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

учет рабочего времени

эффективность персонала

информационная безопасность

расследование инцидентов

удаленное администрирование

Угрозы безопасности информации

- Внешние
- Кража информации
- Промышленный шпионаж

- Внутренние
- Инсайдеры
- Непреднамеренная потеря данных

Риски от инсайдеров

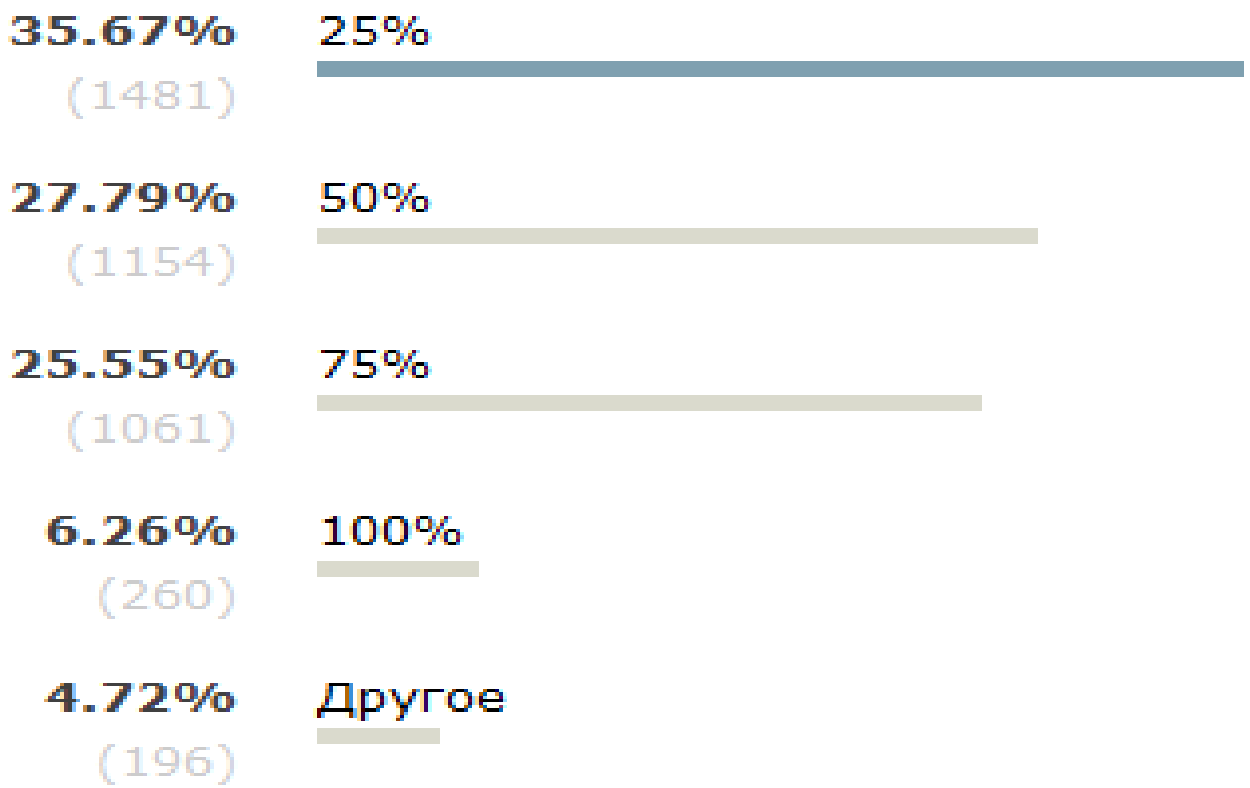
- Нецелевое использование рабочего времени



- Расходы при утечке конфиденциальной информации



Какой процент рабочего времени вы реально работаете, а не бездельничаете?



опрос посетителей сайта habrahabr.ru

Проблема в людях.
Как обезопасить бизнес?

Политика запретов

- Риск в обнаружении утечки информации по факту.
- Ложные срабатывания.
- Дискредитация методов и инструментов СБ.
- Долго и дорого.

STAFFCOP

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

учет рабочего времени

эффективность персонала

информационная безопасность

расследование инцидентов

удаленное администрирование

Проблемы организации мониторинга

Технические

STAFFCOP

Дорого

— дорожан

— дополнит

— аутсорс (у кажд

— услуги интеграторов

Длинно

окументации

— эксплуатация до результата

Крупный проект – длинный проект

КОГДА ПРИБЫЛЬ?

И всё?

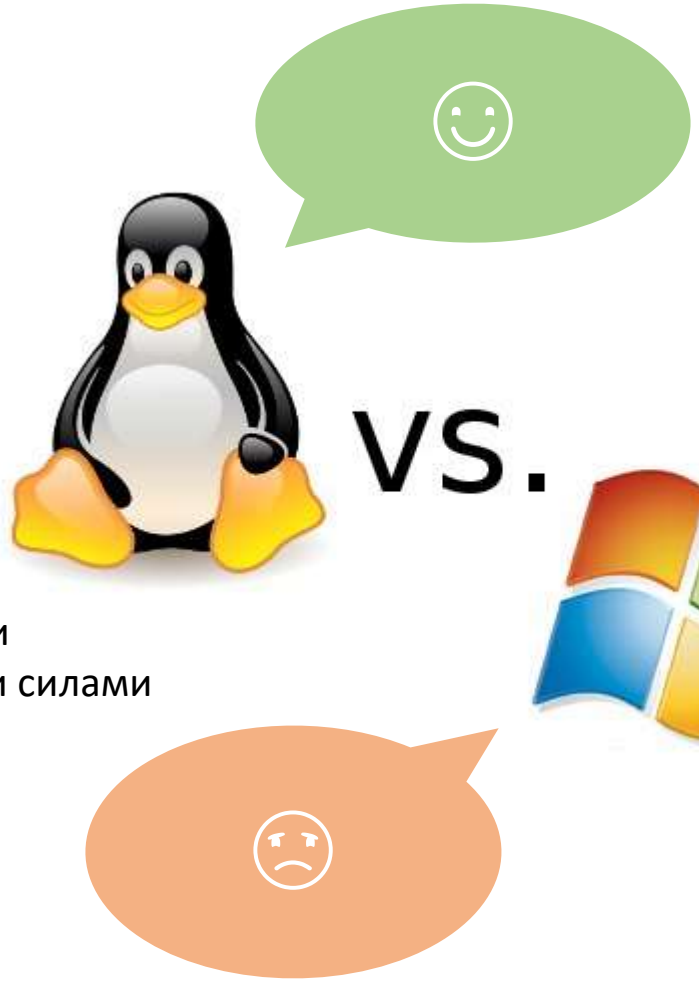
STAFFCOP

Linux

— бесплатно

— менее требователен к «железу»

— заказчик может в любой момент забрать проект себе и доработать его собственными силами



ubuntu

PostgreSQL

Windows

— дорогие лицензии

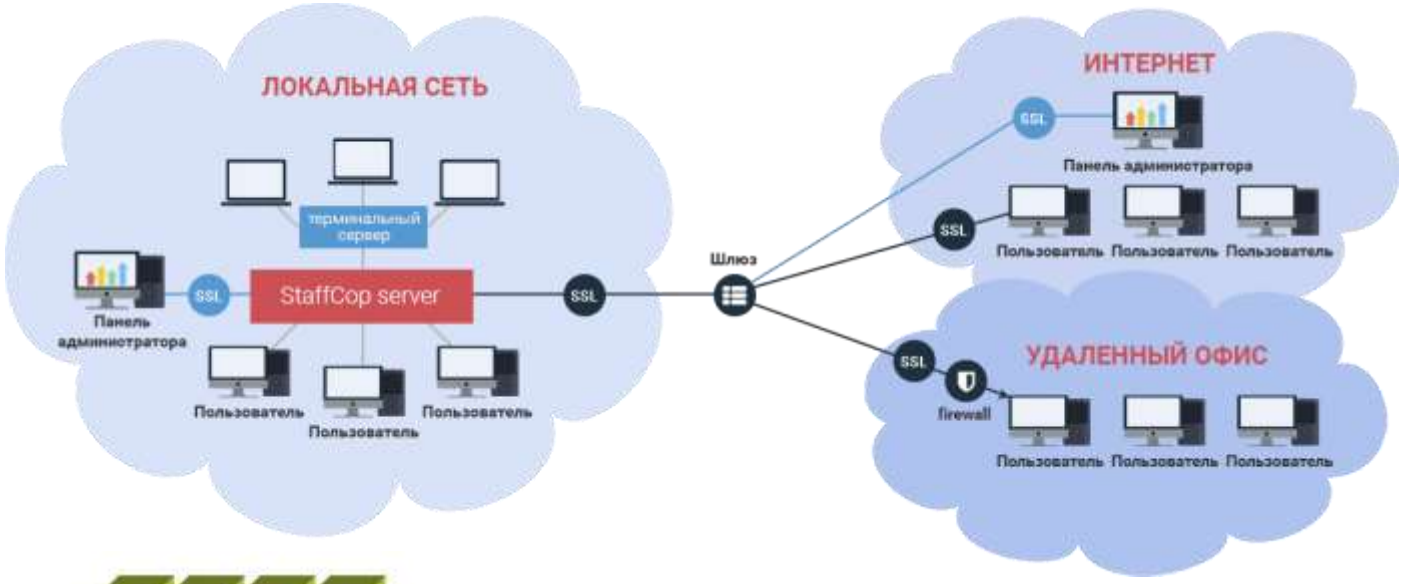
— дорогое обслуживание

— высокие требования к «железу»

Windows Server 2008 R2

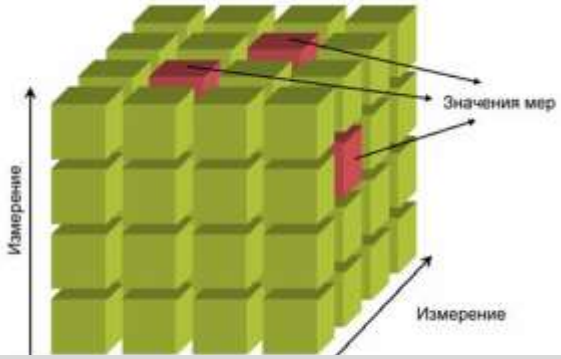
Microsoft SQL Server

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

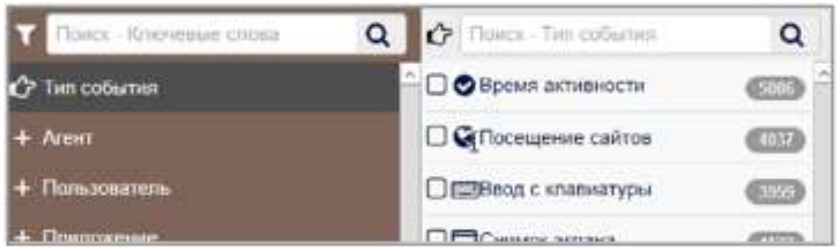
Тотальный контроль

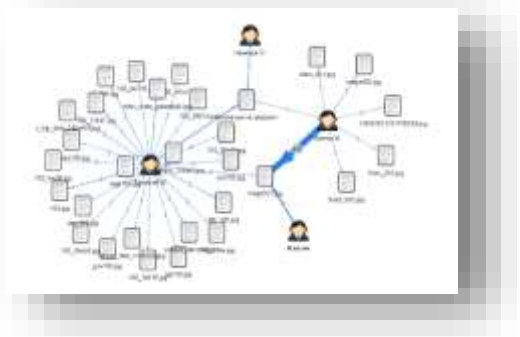
Декодирование сервисов веб-почты и социальных сетей:
— mail.ru, yandex.ru, gmail.com…
— VK, FB, Одноклассники, LinkedIn…
Почтовые протоколы:
— SMTP / SMTPs
— IMAP
— POP3 / POP3s
— MS Exchange
Передача гипертекстовой информации и файлов:
— HTTP / HTTPs
— FTP / FTPs
Интернет-мессенджеры
— Skype
— ICQ, 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

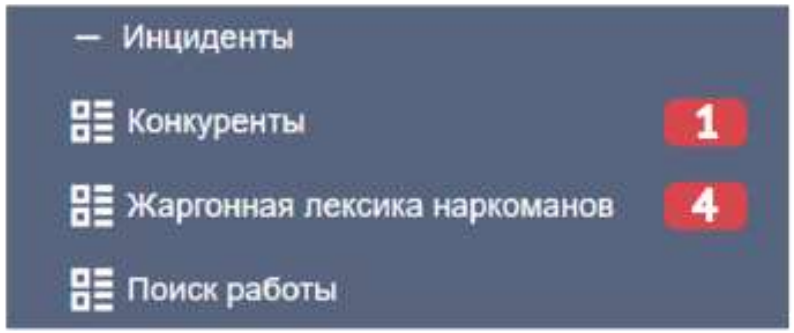
Современные инструменты обнаружения угроз и оповещения

Проблематика:

- Утечка конфиденциальной информации
- Распространение секретных документов и неправомерный доступ к ним
- Уничтожение документов
- Изменение/Подмена документа
- Поведенческие Аномалии







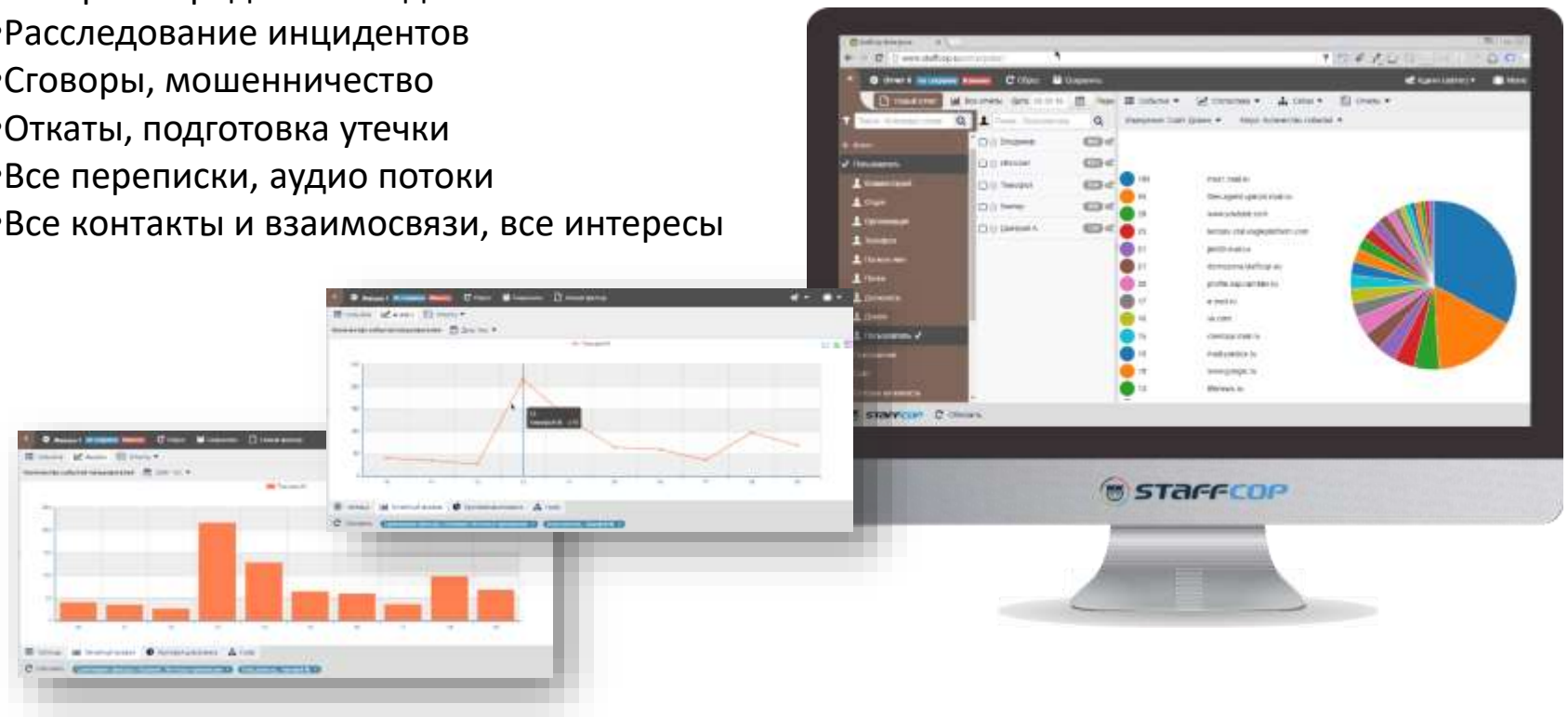
Инструменты:

- Создание теневых копий
- Графы взаимосвязей
- Анализатор угроз
- Контентный анализ файлов
- Система оповещений

Расследование инцидентов ИБ

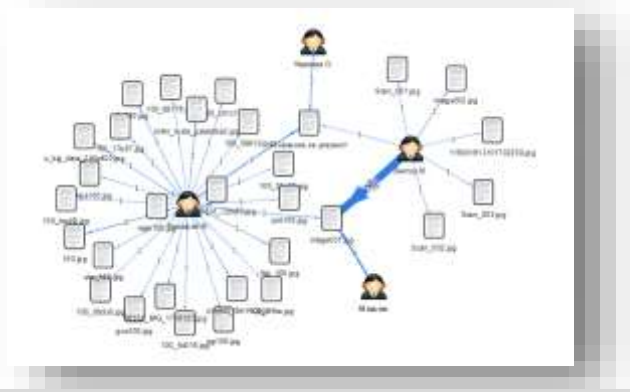
Всё под контролем:

- Контроль вредоносной деятельности
- Расследование инцидентов
- Сговоры, мошенничество
- Откаты, подготовка утечки
- Все переписки, аудио потоки
- Все контакты и взаимосвязи, все интересы



Инструменты:

- Тотальный контроль
- Инструменты поиска по словам и регулярным выражениям
- Контроль аудио потоков и метаданных
- Контроль взаимосвязей и переписок
- Множество графов и диаграмм

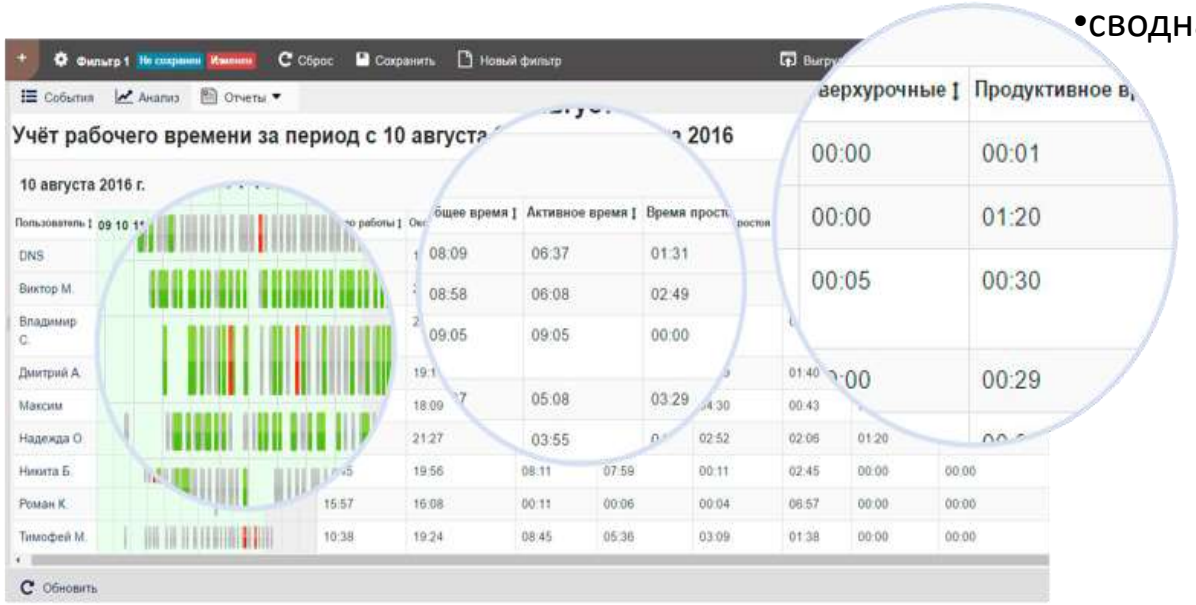


Учет рабочего времени и оценка его эффективности

Фиксация:
- опозданий/переработок
- работы с программами
- сайты в интернете
- присутствие на рабочем месте

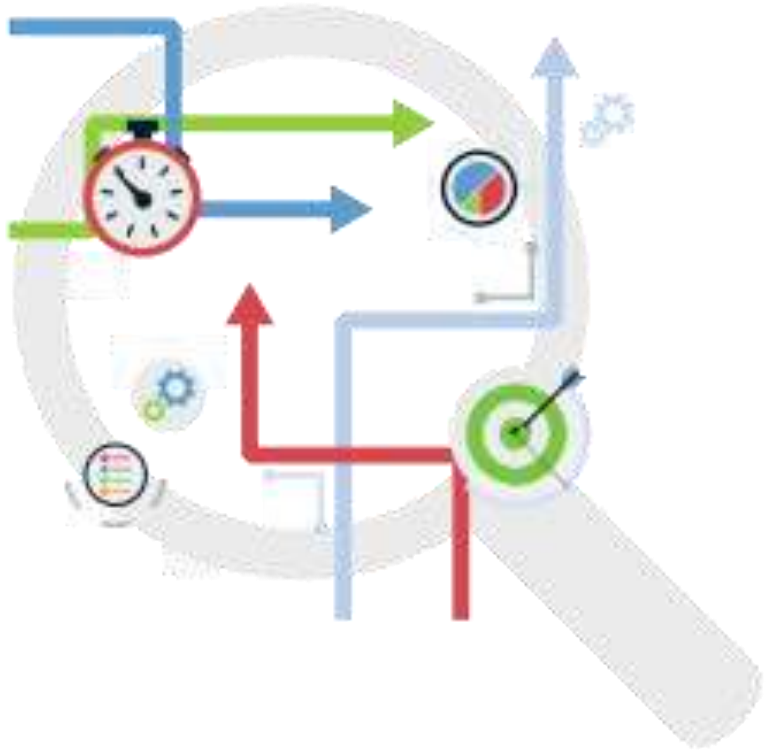
Статистика:
- выявление реального KPI
- контроль пиков активности
- контроль нецелевой переписки
- поиск новой работы
- определение лояльности сотрудников

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



Инструменты:
- отчёты в разных формах
- рейтинги
- граф взаимосвязи
- выделение важного в 2 клика
- сводная статистика

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.

Удаленное администрирование

Мониторинг

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

Блокировки

— приложений и сайтов
— съемных USB-устройств

Инвентаризация ПО и «железа»

От 2000 руб. за покрытие 1 рабочего места!

Бессрочные лицензии и гибкая политика лицензирования

На opensource-решениях и не требует дополнительного платного программного обеспечения.

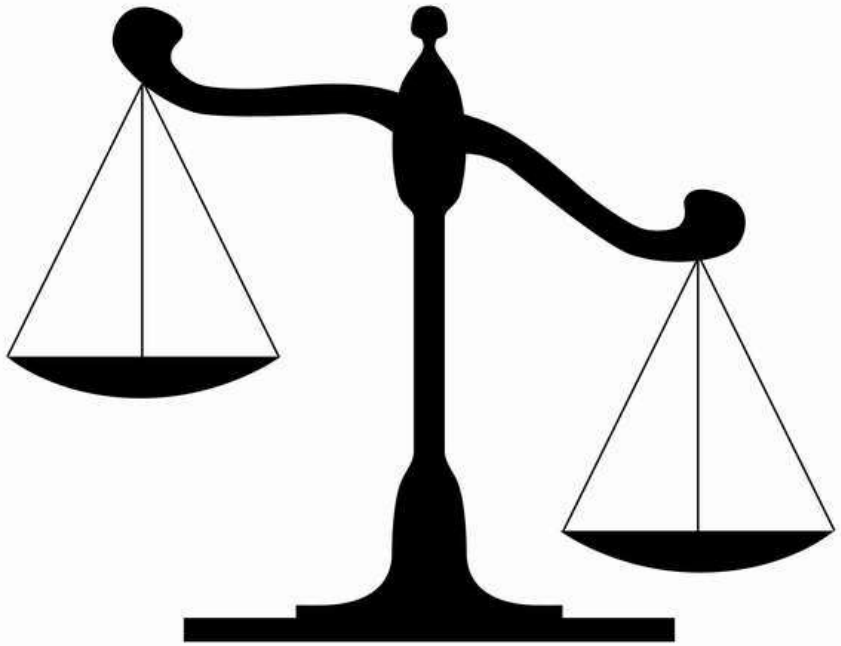
OLAP-куб снижает требования к «железу» сервера

97% внедрений StaffCop окупились менее чем за 2 месяца

Полноценное техническое сопровождение с начального этапа тестирования.

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

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.

Разграничение личной и служебной информации

На рабочем месте:

- Компьютер и телефон – для выполнения должностных обязанностей, а не для личных целей
- Владелец электронного почтового ящика, абонент телефонной сети – организация, а не физическое лицо
- Работник ведет не личную переписку, а выполняет трудовые обязанности и указания работодателя
- Весь бумажный документооборот ведется через канцелярию, фактически с перлюстрацией

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)

Спасибо за внимание!

Андрей Арбатский
компания Атом Безопасность

+7.903.628.8208
a.arbatskiy@staffcop.ru
andrey.arbatskiy