Контроль действий сотрудников в информационной среде компании. «Подводные камни», технические и юридические аспекты

6 февраля 2020 г., Уфа

Юрий Основский
Руководитель группы технической поддержки (московское отделение)
ООО «Атом Безопасность»

ООО Атом Безопасность

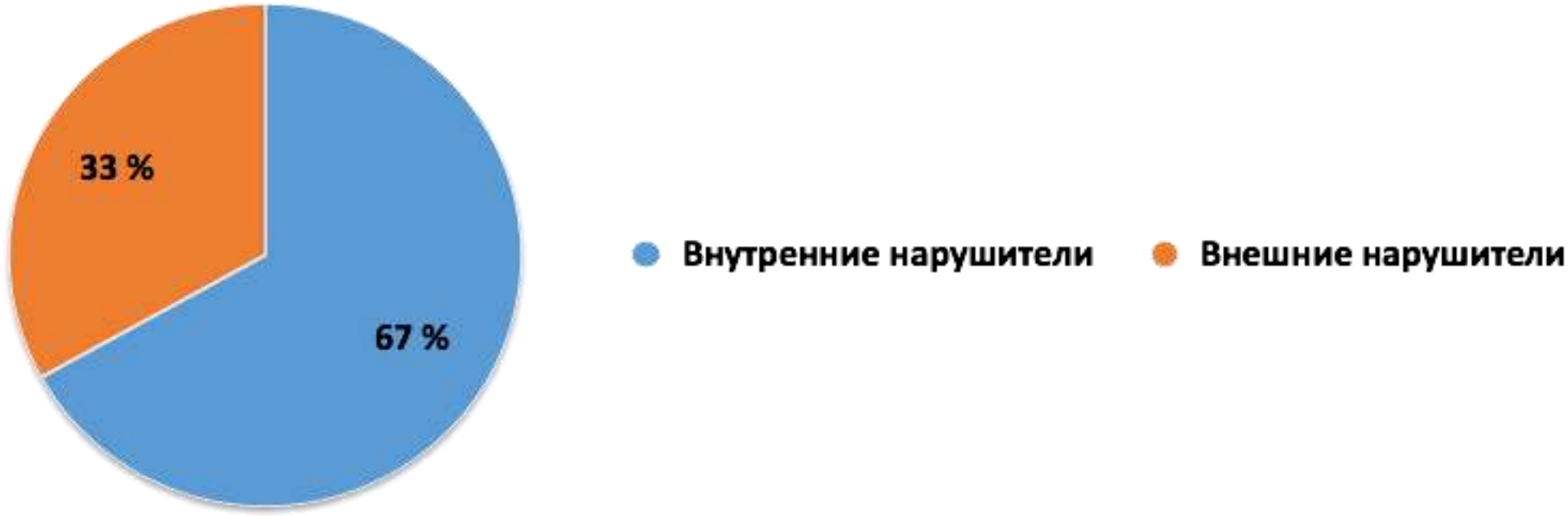
— 10 лет разработки приложений контроля сотрудников
— Академгородок Новосибирск, резиденты Технопарка
— Высокотехнологичная компания с опытной командой разработчиков-профессионалов в области ИБ

Угрозы безопасности информации

- Внешние
- Кража информации
- Промышленный шпионаж

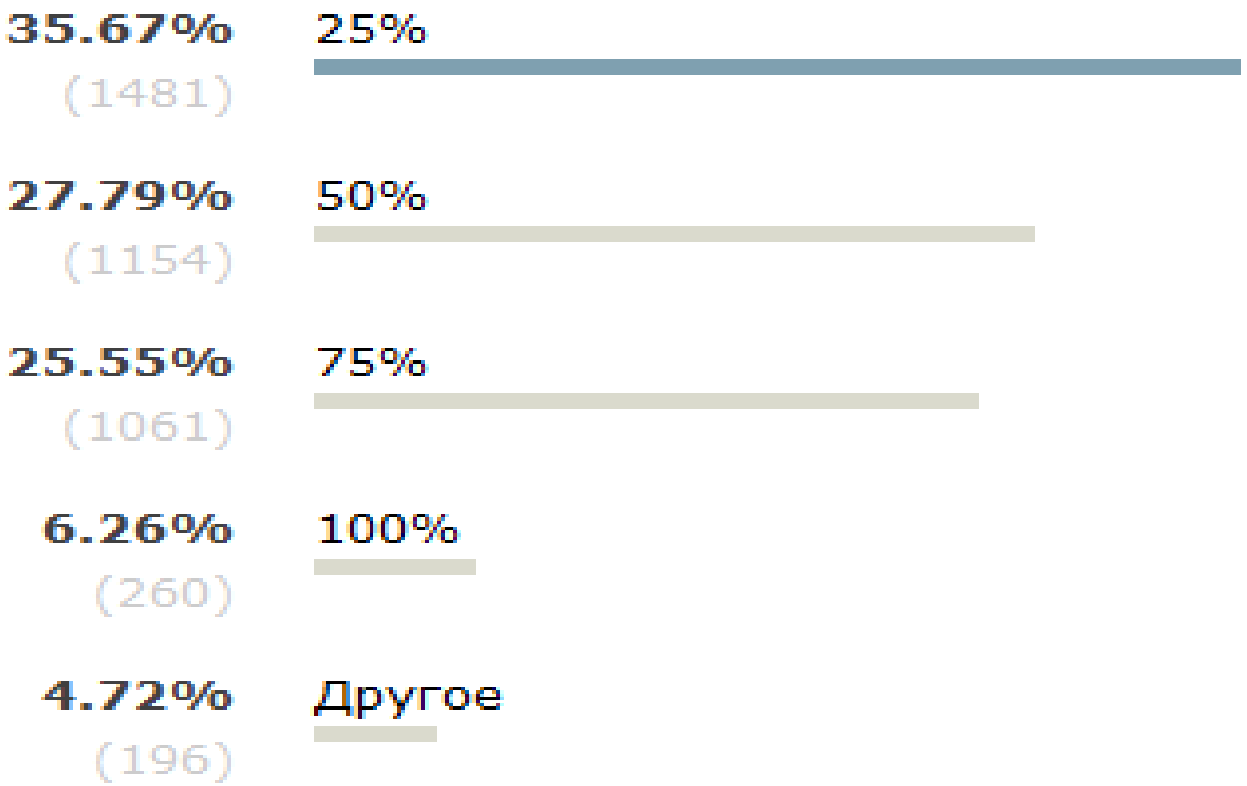
- Внутренние
- Инсайдеры
- Непреднамеренная потеря данных

Статистика распределения угроз



*по данным InfoWatch

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



опрос посетителей сайта habrahabr.ru

100 сотрудников
средний оклад 30 000 ₽
ФОТ = 3 000 000 ₽/месяц

25% вхолостую
теряем до 750 000 рублей!
ежемесячные потери
+
недополученная прибыль
от неэффективной работы

Подведём итоги

1. Утечка конфиденциальной информации может нанести серьёзный материальный ущерб, а также привести к потере репутации компании
2. Нецелевое использование рабочего времени сотрудниками обходится организации достаточно дорого
3. Необходим инструмент, который позволит понять, как расходуется рабочее время, чтобы определить направления для оптимизации!

STAFFCOP

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

учет рабочего времени

эффективность персонала

информационная безопасность

расследование инцидентов

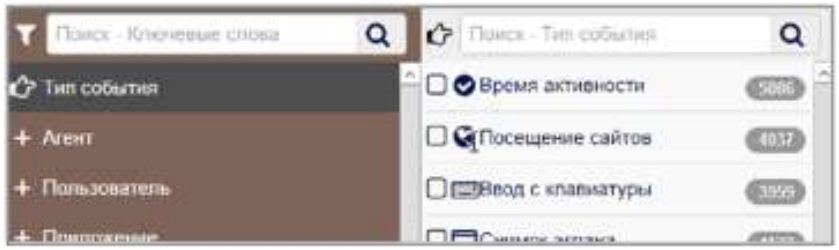
Тотальный контроль

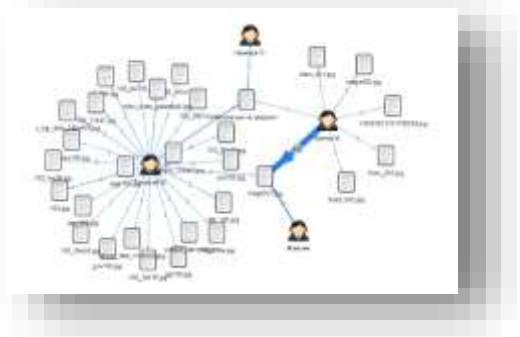
Декодирование сервисов веб-почты и социальных сетей:
— mail.ru, yandex.ru, gmail.com…
— VK, FB, Одноклассники, LinkedIn…
Почтовые протоколы:
— SMTP / SMTPs
— IMAP
— POP3 / POP3s
— MS Exchange
Передача гипертекстовой информации и файлов:
— HTTP / HTTPs
— FTP / FTPs
Интернет-мессенджеры
— Skype
— ICQ,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

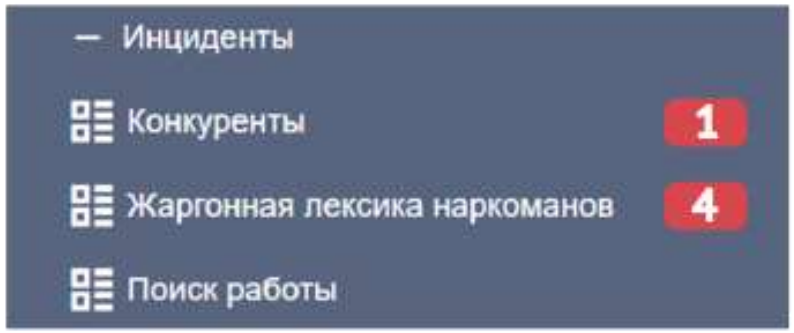
Современные инструменты обнаружения угроз и оповещения

Проблематика:

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







Инструменты:

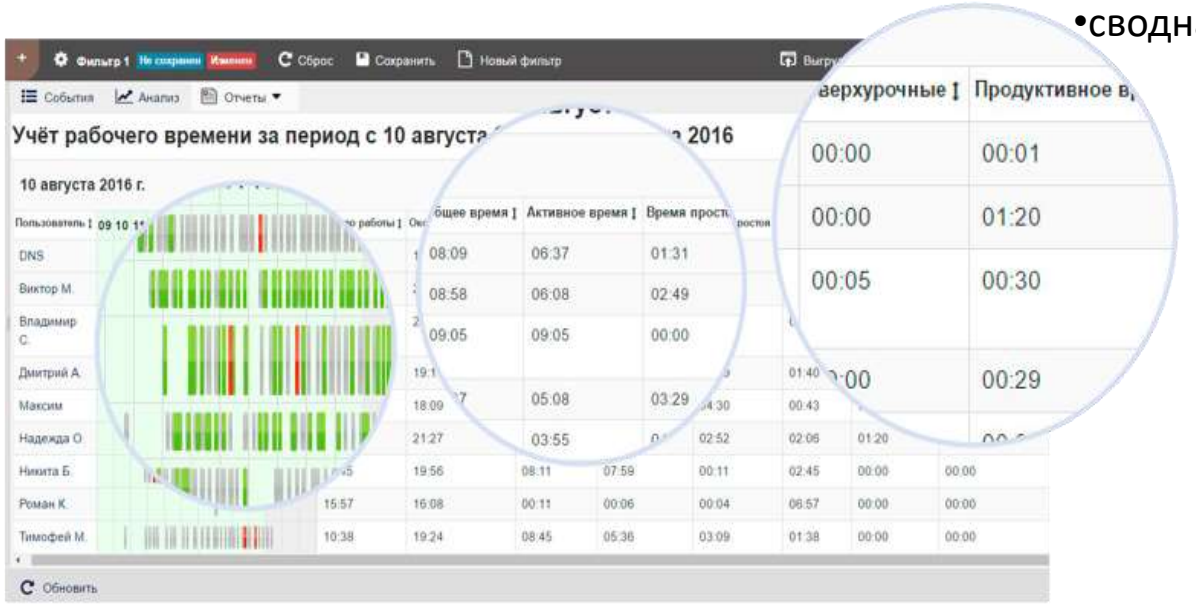
- Создание теневых копий
- Графы взаимосвязей
- Анализатор угроз
- Контентный анализ файлов
- Система оповещений

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

Удалённое администрирование

Мониторинг

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

Блокировки

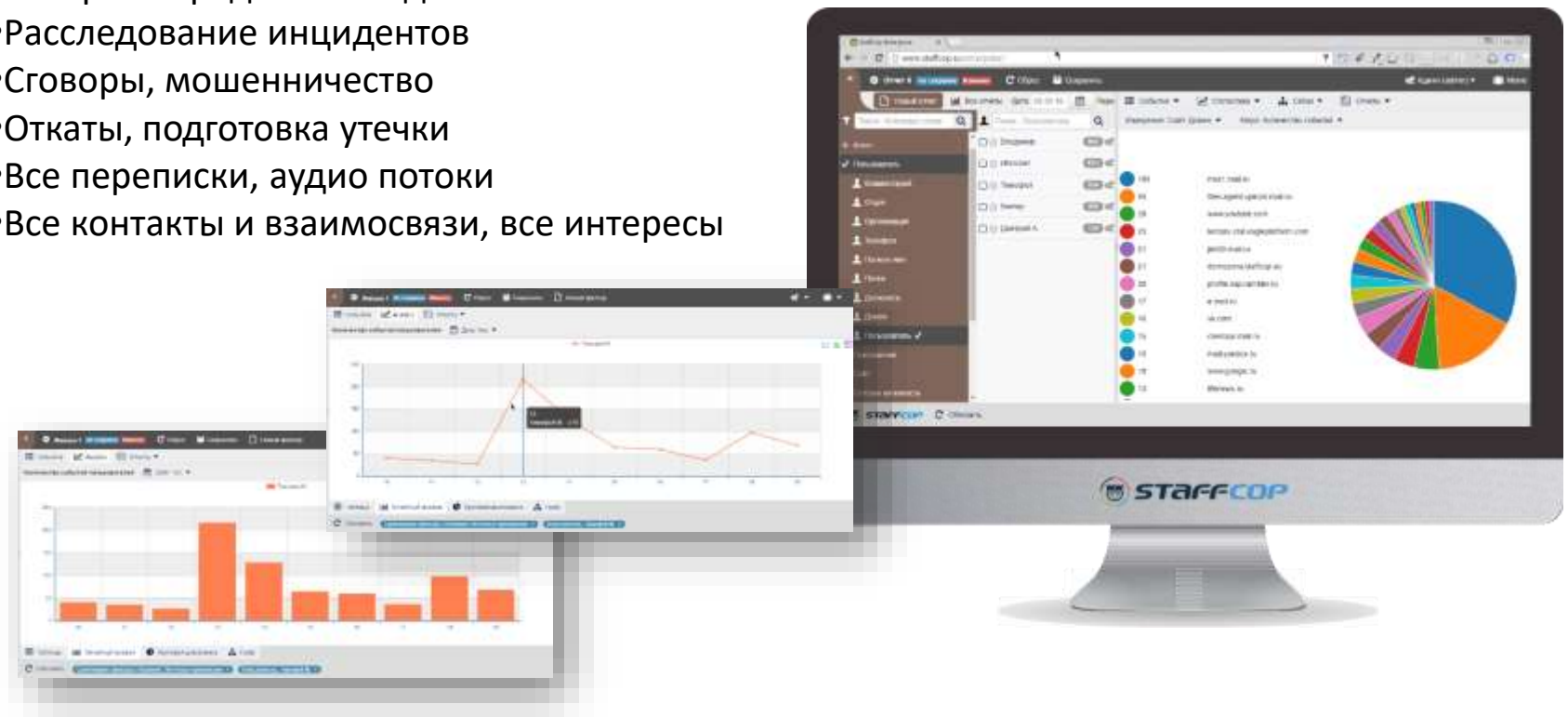
— приложений и сайтов
— съемных USB-устройств

Инвентаризация ПО и «железа»

Расследование инцидентов ИБ

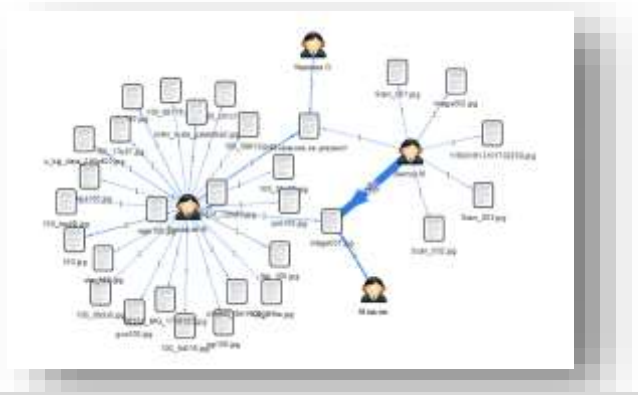
Всё под контролем:

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



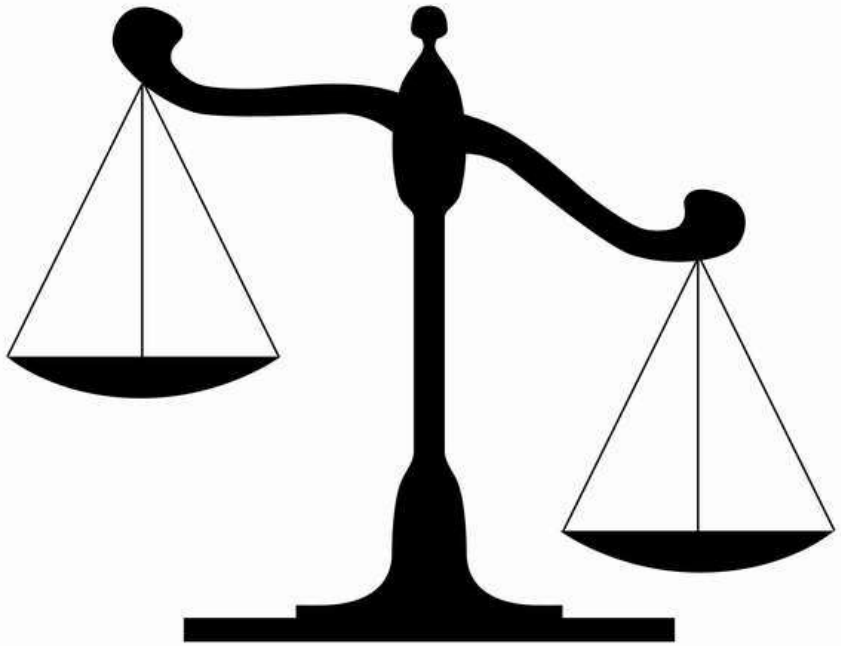
Инструменты:

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



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:

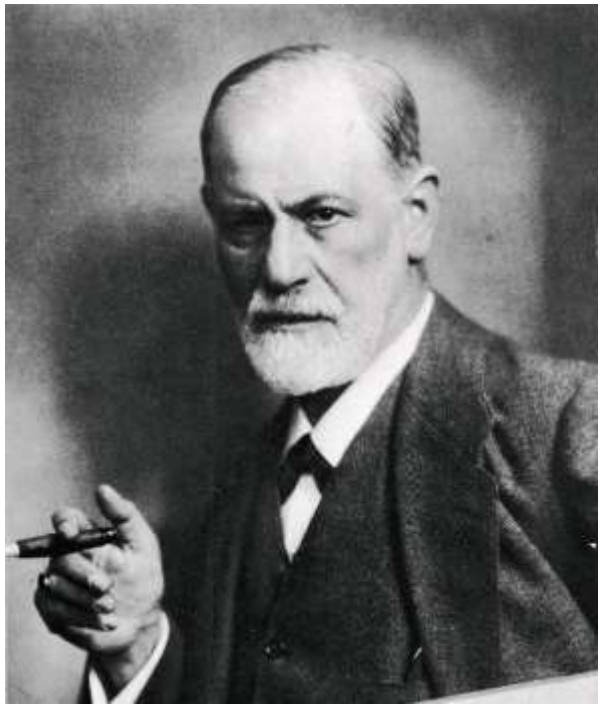
- Компьютер и телефон – для выполнения должностных обязанностей, а не для личных целей
- Владелец электронного почтового ящика, абонент телефонной сети – организация, а не физическое лицо
- Работник ведет не личную переписку, а выполняет трудовые обязанности и указания работодателя
- Весь бумажный документооборот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

Проблемы организации мониторинга

Этические и психологические



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

Требования к контролю:

- честность (порядочность)
- профессиональная компетентность
- объективность
- конфиденциальность

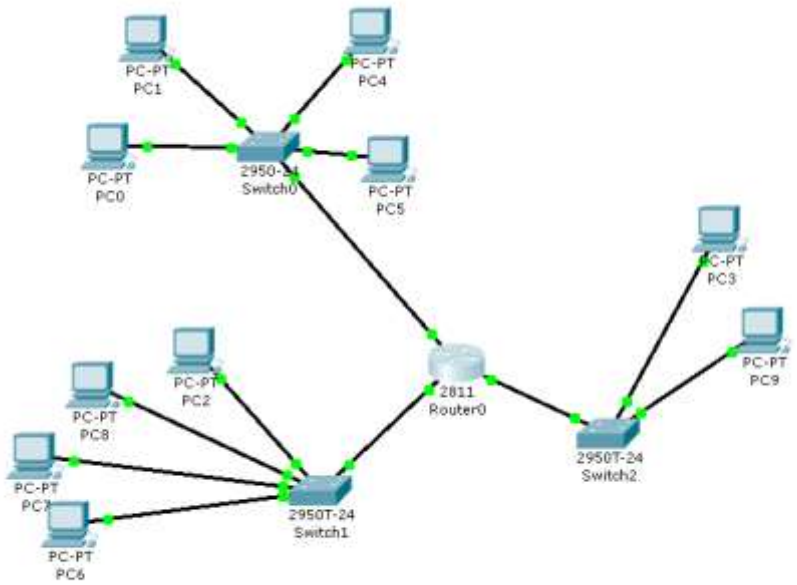
Проблемы организации мониторинга

Технические

Настройка антивирусных приложений

- Исключение файлов и папок агента из анализируемых антивирусом
- Настройка файерволла антивируса
- Постоянный мониторинг работы антивируса
- Проверка работоспособности агента после обновлений антивируса

Настройка маршрутизации



- Прозрачность маршрутизатора на 80 (для веб-интерфейса) и 443 (для агента) портах
- Рекомендуется использование VPN как более надёжного способа организации каналов
- Номера портов могут быть изменены для большей безопасности

Спасибо за внимание!

Дмитрий Кандыбович
руководитель
компании Атом Безопасность

+7.913.915.2137
sales@staffcop.ru
Staffcop.ru

Юрий Основский
Руководитель группы технической поддержки (московское отделение) ООО «Атом Безопасность»

+7 (499) 638-28-09 доб. 237
y.osnovskiy@staffcop.ru