Контроль действий пользователей в информационной среде компании. Итоги 2019.

Кандыбович Дмитрий
Генеральный директор ООО Атом Безопасность

STAFFCOP

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

учет рабочего времени

эффективность персонала

информационная безопасность

расследование инцидентов

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 50+
— Сколково
— 100 серверных компонентов в месяц, общее покрытие за год 94000 АРМ
— 82 мероприятия по СНГ

www.amtestlab.ru CERTIFIED AM TEST LAB REG # 00158 02/2016 PC MAGAZINE RUSSIAN EDITION BEST 2010 SOFT

infosecurity RUSSIA

BIS SUMMIT 2018

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

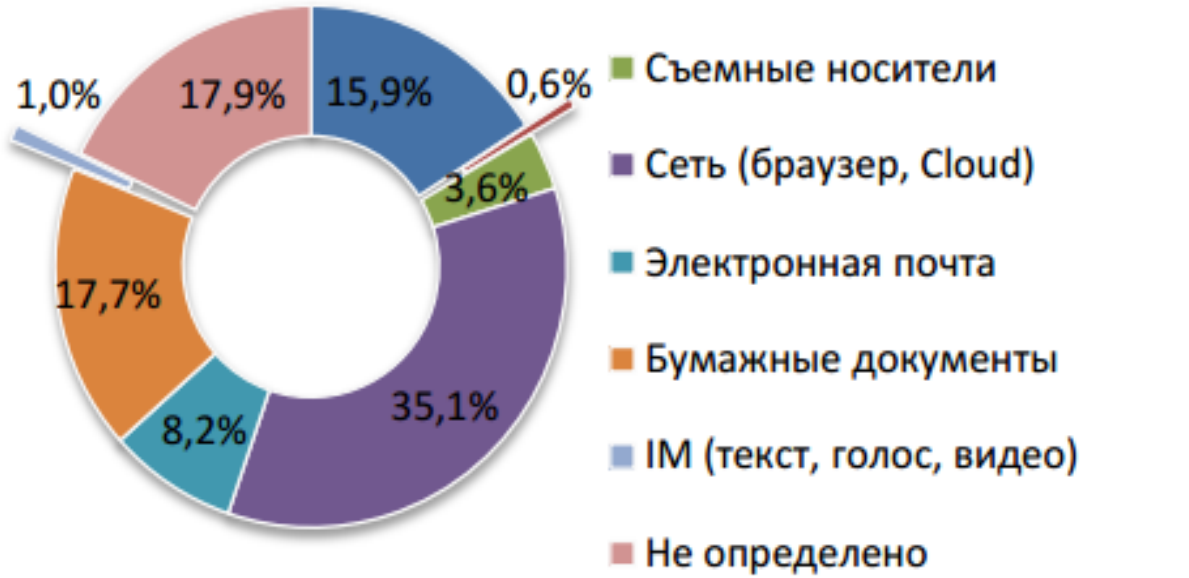
Минкомсвязь России

Статистика распределения угроз 2018 год

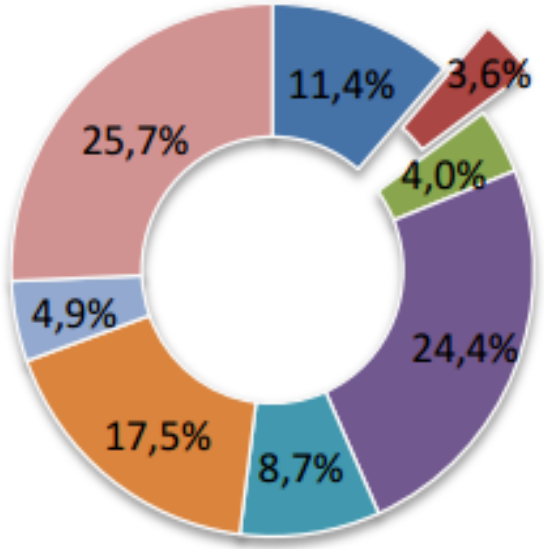
*по данным Аналитического отчёта Anti Malware

Статистика каналов утечек

2017



2018



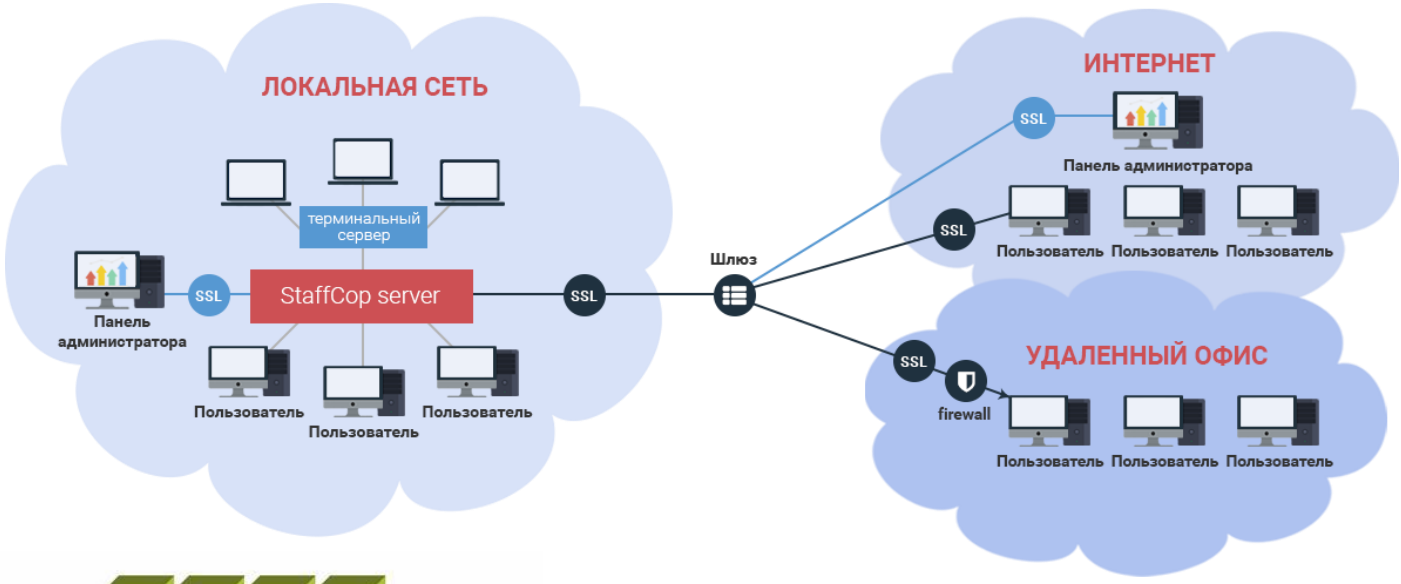
*по данным Аналитического отчёта InfoWatch

Что на рынке

- Контроль сьёмки с телефона
- UEBA
- Профайлинг
- Контроль графических объектов, чертежей
- Интеграция данных из сторонних источников

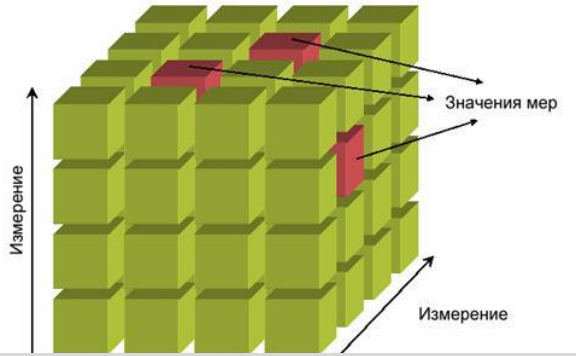
www.staffcop.ru

Современные архитектурные решения



1. **8000 ПК на один сервер**

2. **Промежуточные сервера, консоль управления инцидентами**



OLAP технология. OnLine Analytical Processing — оперативный анализ данных

STAFFCOP

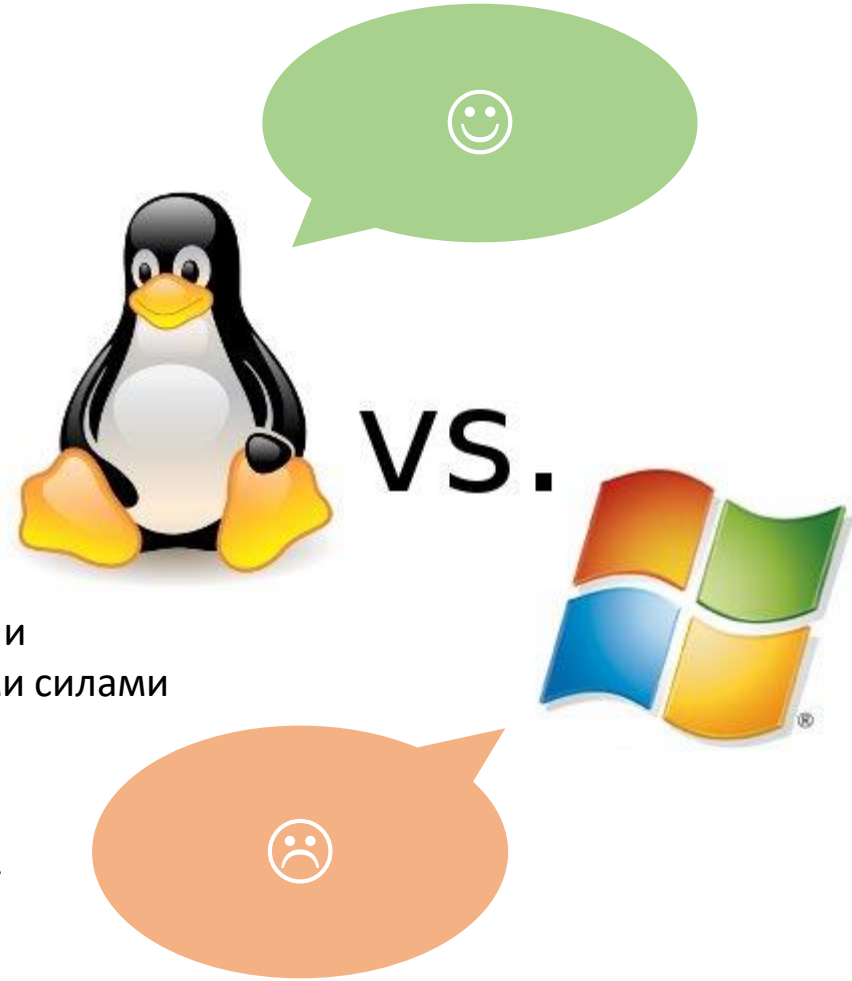
www.staffcop.ru

Linux

— бесплатно

— менее требователен к «железу»

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



Windows

— дорогие лицензии

— дорогое обслуживание

— высокие требования к «железу»

ubuntu

PostgreSQL

Windows Server 2008 R2

Microsoft SQL Server

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

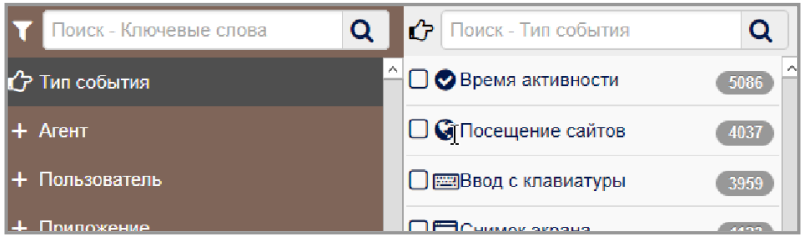
позволяет «на лету» получить необходимый набор данных. Поиск по ключевым словам и регулярным выражениям до минимума сократит время расследования инцидента,

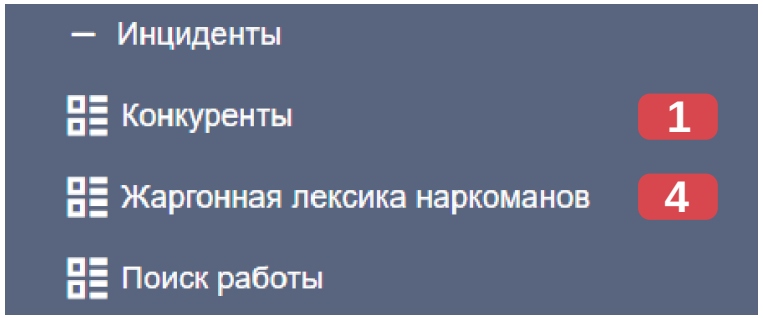
Множество графов и диаграмм

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.

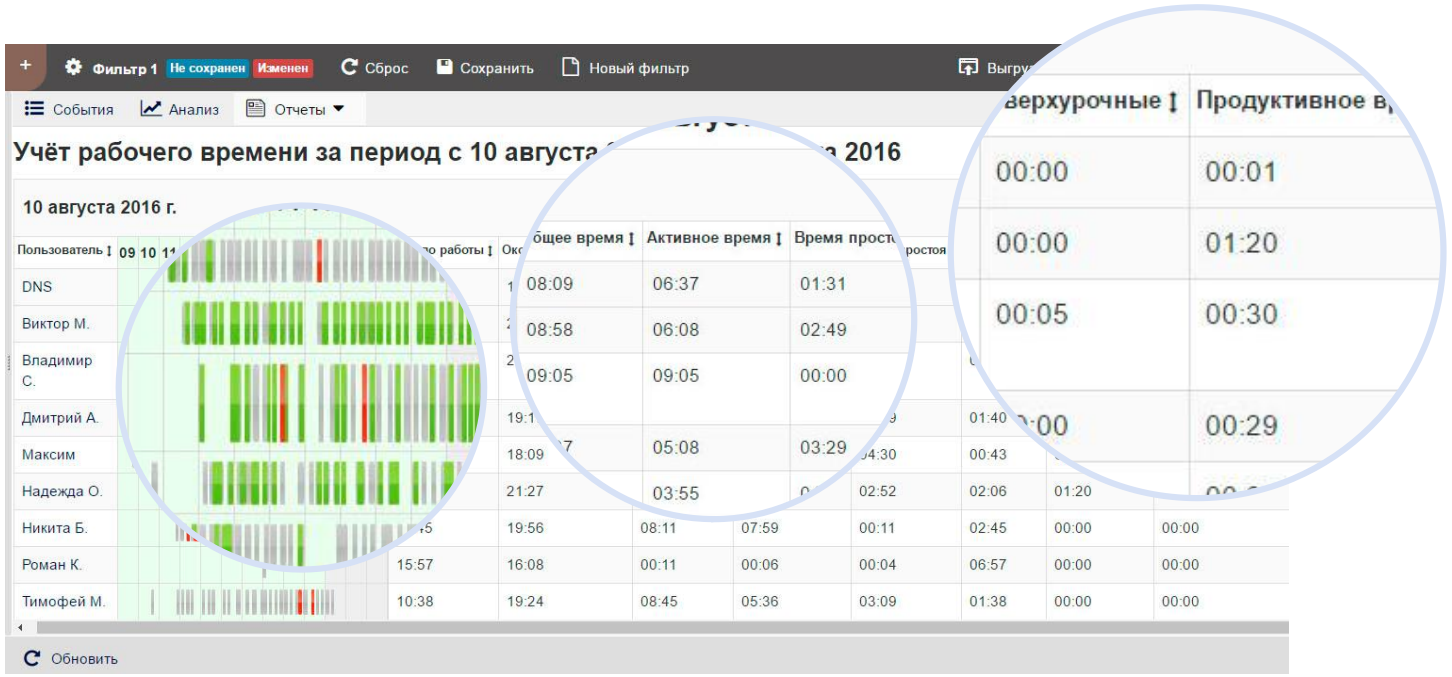
Система оповещений

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



www.staffcop.ru

Удаленное управление и администрирование ПК

Интеграция с SIEM

Мониторинг

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

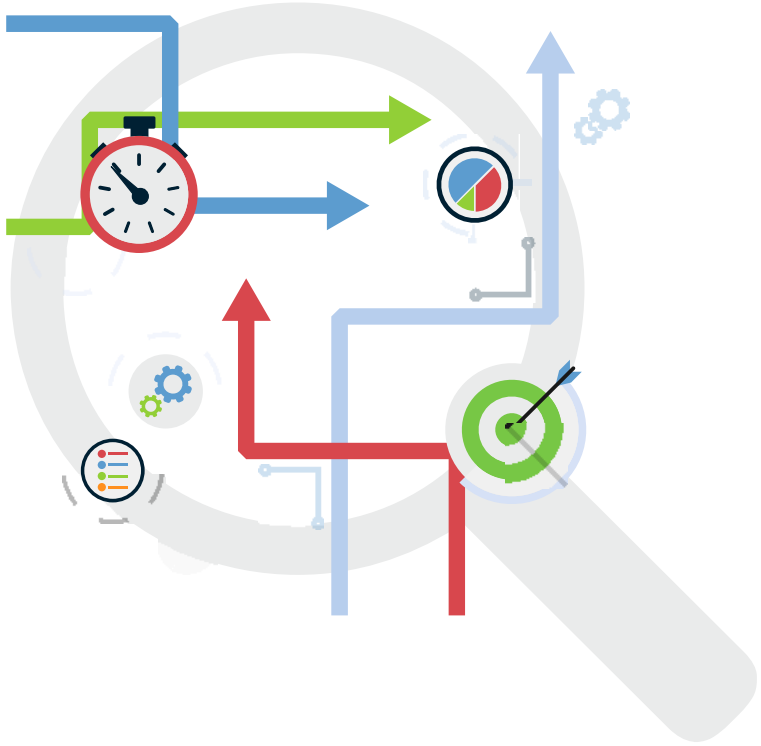
Блокировки

— 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.

Куда движемся

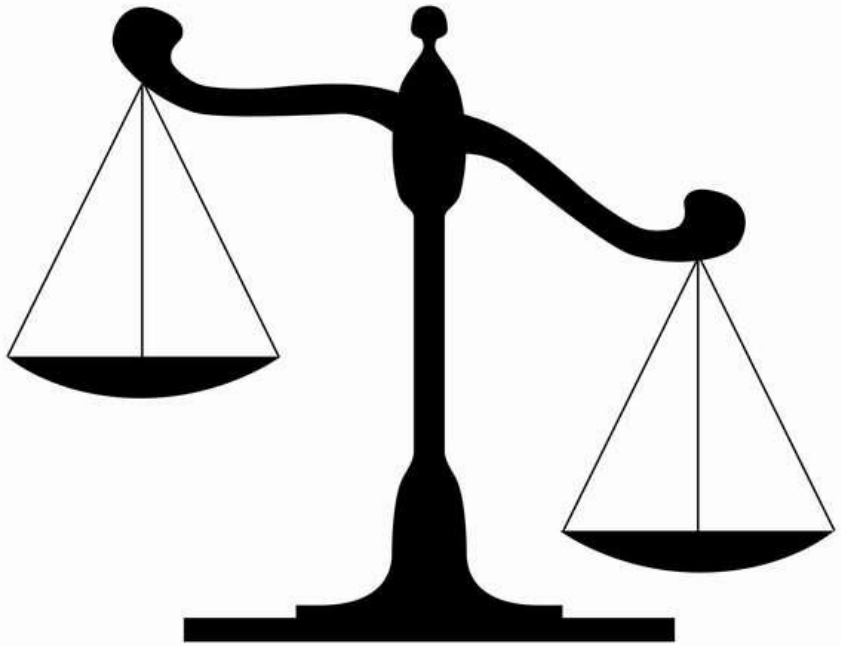
Нейронные сети:

- **Звук**
- **Скриншоты**
- **Теневые копии**
- **Снимки с веб камеры**
- **Переписки**

Досье пользователя

Проблемы организации мониторинга

Правовые



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

Легализация. 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)

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

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

Обоснование внедрения

Спасибо за внимание!

Дмитрий Кандыбович
Генеральный директор
ООО Атом Безопасность

+79139152137
sales@staffcop.ru
Staffcop.ru