

DLP-Система

Falcongaze SecureTower®

Спикер:

Роман Клименко

Руководитель представительства Falcongaze
в УФО и Республике Казахстан



СТАТИСТИКА ПО УДАЛЁННОЙ РАБОТЕ НА 2020 ГОД

Количество удалённых работников увеличилось в **8 раз** по сравнению с 2019

(По данным ВЦИОМ и Social Buisness Group)

52%

работников во всем мире работают дома хотя бы раз в неделю

18%

людей работают удаленно полный рабочий день

16%

компаний нанимают исключительно удаленных работников

ЧЕМ ГРОЗИТ ОТСУТСТВИЕ КОНТРОЛЯ НАД СОТРУДНИКАМИ?



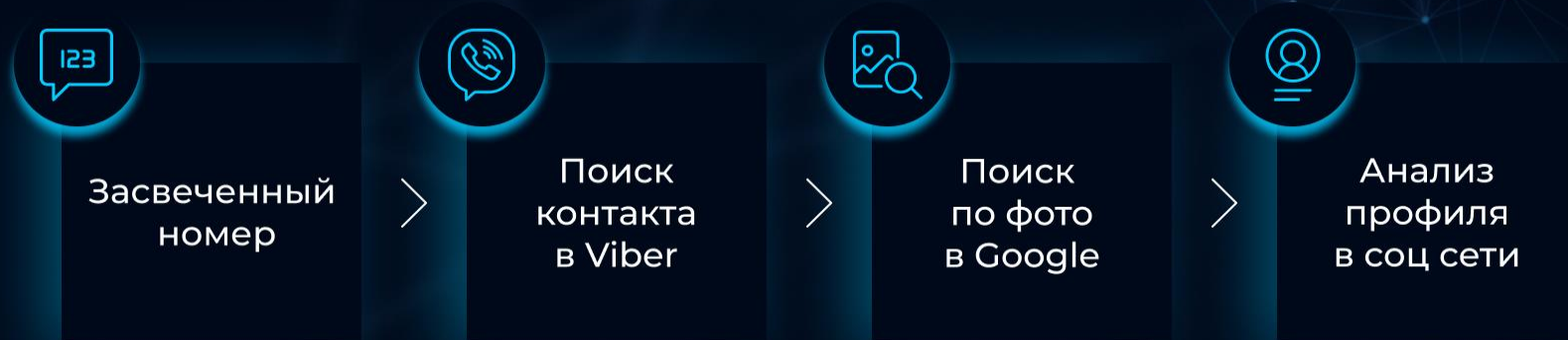
УДАЛЕННЫЕ РАБОТНИКИ МОГУТ:

- Пренебрегать рабочими обязанностями и проявлять халатность
- Заниматься личными делами во время своего рабочего дня
- Украсть информацию и продать её конкурентам
- Допустить случайную утечку данных

ПОСЛЕДСТВИЯ ОТСУТСТВИЯ КОНТРОЛЯ ЗА СОТРУДНИКАМИ



КЕЙС 1: ИДЕНТИФИКАЦИЯ НЕИЗВЕСТНОГО КОНТАКТА СОТРУДНИКА ЧЕРЕЗ ЗАСВЕЧЕННЫЙ НОМЕР И ОБНАРУЖЕНИЕ УТЕЧКИ ИНФОРМАЦИИ



🕒 **Наблюдение за сотрудником**

КЕЙС 2: СЛИВ ВХОДЯЩИХ КЛИЕНТОВ СТРАХОВОЙ КОМПАНИИ - КОНКУРЕНТУ



Статистика
по входящим
клиентам



Круг
общения
менеджера
(связи)



E-mail

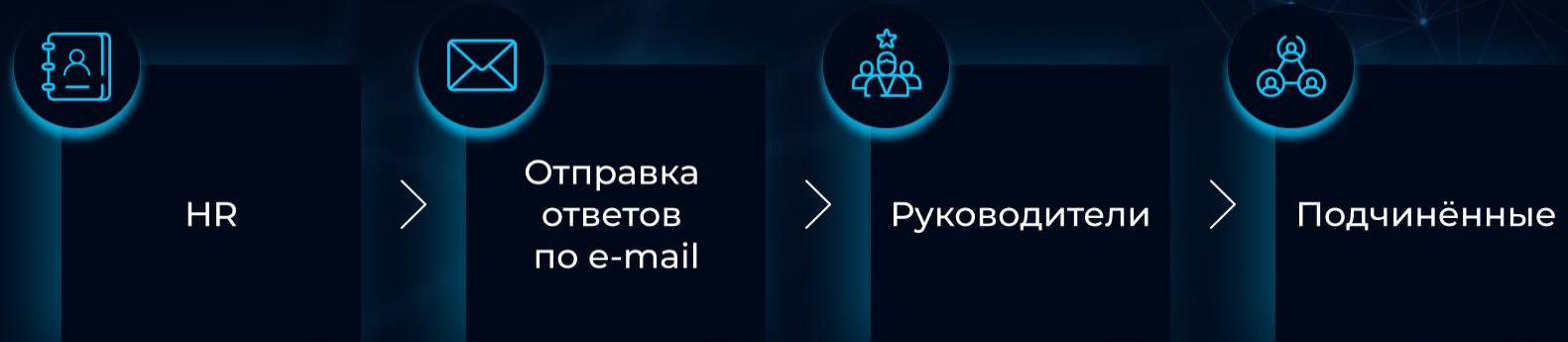


Принтер



Анализ коммуникации

КЕЙС 3: ЗАВЫШЕНИЕ РЕЗУЛЬТАТОВ АТТЕСТАЦИИ СОТРУДНИКОВ



 **Анализ коммуникации**

ОБНОВЛЕНИЕ SECURE TOWER В 2021



Категоризация сайтов и приложений

Блокировка посещения сайтов, запуска приложений, поиска правила безопасности

Настройка правила блокировки

Название: Новое правило блокировки 1

Описание:


Условия блокировки по хеш-сумме файлов

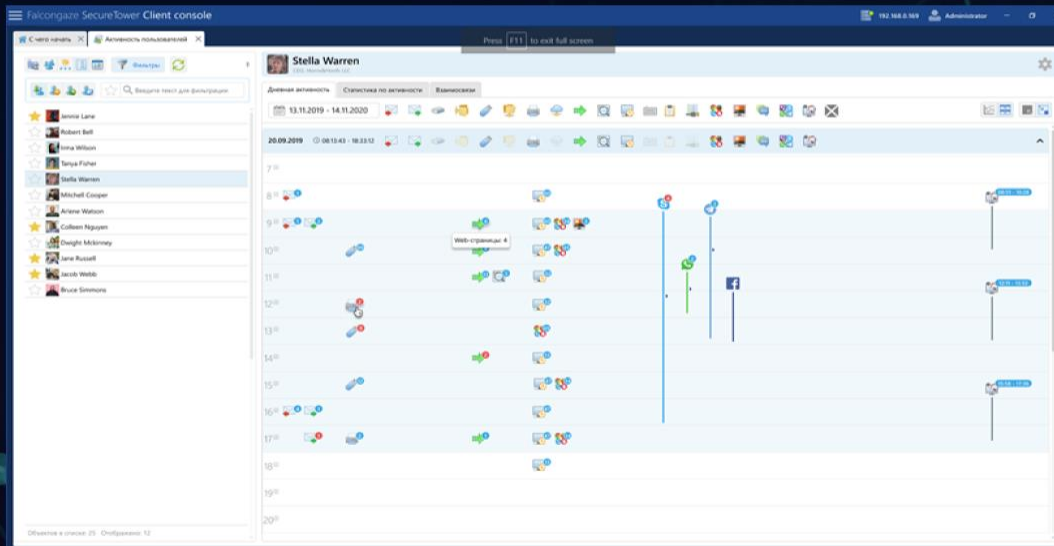
Выберите операцию, применяемую к условиям в блоке: И Или Не (отрицание)

Категория сайтов Равно Введите текст для фильтрации

[\[Добавить условие\]](#) [\[Добавить блок\]](#) [\[Обратить блок\]](#)

ОБНОВЛЕНИЕ SECURE TOWER В 2021

 **2** Новый режим отображения информации



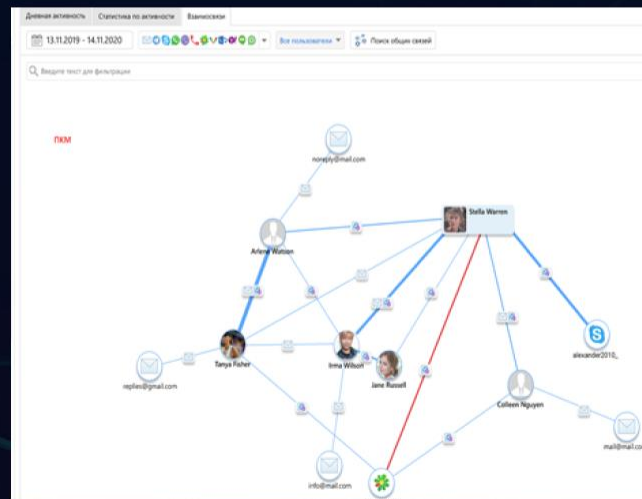
ОБНОВЛЕНИЕ SECURE TOWER В 2021

3 Добавление графа многие ко многим

6.4



6.5



ОБНОВЛЕНИЕ SECURE TOWER В 2021

4 Конструктор отчетов

Конструктор отчетов

1 Общее 2 3 4

Укажите название отчета

ТОП-отчет

Пользователи
Сводный отчет
Политики безопасности
Активность приложений
Браузер-активность
Табель

ТОП-отчет

Scalix Mailbox	30
Scalix Mailbox	24
Scalix Mailbox	24
Scalix Mailbox	22
Scalix Mailbox	20
Scalix Mailbox	18
Scalix Mailbox	16
Scalix Mailbox	14
Scalix Mailbox	12

Отчет об активности определенного количества пользователей, для которых характерны экстремальные значения показателей по выбранному типу отчетности.

Далее Отмена

Конструктор отчетов

1 2 Настройки 3 4

Параметры отчета

Представление отчета: [Иконки]

Число результатов: 20 Тип сортировки: По убыванию

Среднеустойчивый Количество инцидентов безопасности

Статус инцидентов: Ложное срабатывание

Конструктор отчетов

1 2 3 Фильтры 4

Период формирования отчета

Интервал дат: 16.08.2019 16.08.2019

Учитьте текущий день при построении отчета

Фильтр по пользователям

Строить отчет по всем пользователям

Строить отчет только по указанным пользователям

Планировщик рассылки

Добавить Удалить

1 2 3 4 Рассылка

Параметры отчета

Формат: *.pdf Ориентация: Короткая

Подписчики на уведомления

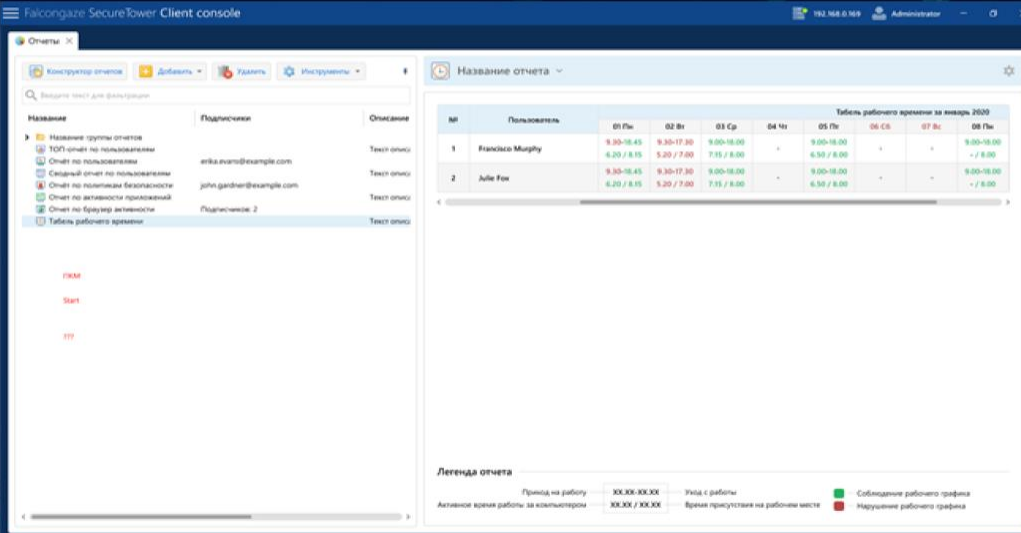
Добавить Удалить

Планировщик рассылки

Добавить Удалить

ОБНОВЛЕНИЕ SECURE TOWER В 2021

5 Табель рабочего времени



The screenshot displays the 'SecureTower Client console' interface. On the left, a sidebar lists various report types under the heading 'Отчеты'. The main area shows a selected report titled 'Табель рабочего времени за январь 2020'. The report is presented as a table with columns for days of the week and rows for individual users. A legend at the bottom explains the symbols used in the table, such as 'XX:XX-XX:XX' for work periods and 'XX:XX / XX:XX' for absence periods.

№	Пользователь	Табель рабочего времени за январь 2020							
		01 Пн	02 Вт	03 Ср	04 Чт	05 Пт	06 Сб	07 Вс	08 Пн
1	Francisco Magru	9:30-18:45 6:20 / 8:15	9:30-17:30 5:20 / 7:00	9:00-18:00 7:15 / 8:00	-	9:00-18:00 6:50 / 8:00	-	-	9:00-18:00 -/ 8:00
2	Lidia Fox	9:30-18:45 6:20 / 8:15	9:30-17:30 5:20 / 7:00	9:00-18:00 7:15 / 8:00	-	9:00-18:00 6:50 / 8:00	-	-	9:00-18:00 -/ 8:00

Легенда отчета

- Принял на работу: XX:XX-XX:XX
- Ушел с работы: XX:XX / XX:XX
- Время присутствия на рабочем месте: [Green Box]
- Соблюдение рабочего графика: [Green Box]
- Нарушение рабочего графика: [Red Box]

ОБНОВЛЕНИЕ SECURE TOWER В 2021



6 Возможности анализа динамики

The screenshot displays the FortiGate Secure Tower Client console interface, illustrating various dynamic analysis features:

- Summary Dashboard:** Shows overall system status with metrics like "Инциденты за сегодня" (12 тыс) and "Инциденты за неделю" (2 тыс).
- Incident List:** A table listing incidents with columns for "Подписчик" (Subscriber), "Инцидент" (Incident), and "Угроза" (Threat). It includes details like "1839 / 1 0...", "578 / 556", and "42 / 41".
- Search Results:** A "Введите текст для фильтрации результатов" (Enter text to filter results) section showing search results for incidents, including details like "19 марта 2020 г. 9:05:45 - 10:29:33" and "Правило безопасности: 2. Рассылка резюме".
- User Profile:** A "Локальный пользователь: Васильева Надежда" (Local user: Vasileva Nadezhda) profile view, showing "Информация об удалённом пользователе" (Information about the remote user) and "Сообщений: 25" (Messages: 25).
- Task List:** A list of tasks such as "Повышение привилегий / запуск специализированной...", "Запуск скриптов / командных интерпретаторов", and "Использование ПО для администрирования / RAT".
- Activity Log:** A log of system events, including "Запись большого количества файлов на USB" (Recording a large number of files on USB) and "Отправка большого количества писем" (Sending a large number of emails).

ОБНОВЛЕНИЕ SECURE TOWER В 2021

7 Контроль буфера обмена

The screenshot shows the 'Falcongaze SecureTower Client console' search interface. At the top, there are search tabs: 'С чего начать', 'Поиск информации', and 'Комбинированный поиск'. Below the tabs are search actions: 'Искать', 'Добавить в избранное', 'Показать избранное', and 'Экспорт/Импорт'. The search parameters are set to 'Интервал поиска: Последние 30 дней' and 'Количество результатов: 500 результатов'. A note indicates the available search interval is '04.04.2020 - 25.11.2020'. The search criteria are for 'Группы Active Directory' with the condition 'И'. The search terms are 'Буфер обмена' (Type: 'Текст') and 'Буфер обмена' (Operation: 'Копирование в буфер обмена'). A dropdown menu for 'Тип данных' is open, showing options: 'Текст', 'Изображения', 'Файл', 'Прочие данные', 'Копирование в буфер обмена', and 'Вставка из буфера обмена'. At the bottom, there are links to 'Добавить условие', 'Добавить шаблон', 'Добавить блок', and 'Обратить блоком'.

ОБНОВЛЕНИЕ SECURE TOWER В 2021

8 Блокировка буфера обмена по контенту

Создание правил для блокирования, копирования и вставки из буфера по контенту, которые могут быть применены к разным профилям

Настройка правила блокировки

Название: Новое правило блокировки 2

Описание:

Аудит заблокированных данных Сохранить теневую копию блокируемых данных

Выберите операцию, примененную к условиям в блоке: И Или Не (отрицание)

Операция: Копирование в буфер обмена

И: Текст: Все указанные слова

И: Контролируемые данные: Файл

[Добавить условие](#) [Добавить блок](#) [Ограничить блокики](#)

Блокирование осуществляется только при включении контроле буфера обмена

Сохранить Отмена

ОБНОВЛЕНИЕ SECURE TOWER В 2021

➤ 9 Агент на Linux



ОБНОВЛЕНИЕ SECURE TOWER В 2021

➤ 10



Скорость построения отчётов выросла

в 100 раз

ОБНОВЛЕНИЕ SECURE TOWER В 2021

➤ 11 Добавлен контроль



CMS Bitrix24



LinkedIn



Zoom



Skype



WhatsApp

ПОЛНОЕ БЕСПЛАТНОЕ СОПРОВОЖДЕНИЕ



Техническое

Внедрение, настройка и техподдержка системы



Практическое

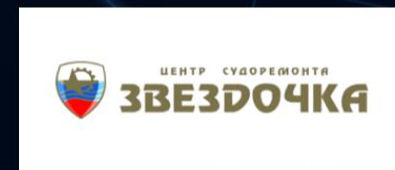
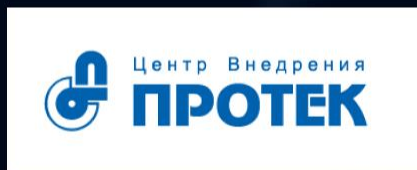
Обучение и помощь в поиске утечки информации



Юридическое

Консультации и рекомендации по внедрению системы

НАШИ КЛИЕНТЫ



Роман Клименко

Директор регионального
представительства ООО «ФалконГейз»
в УФО и Республике Казахстан

 + 7 (343) 339 41 42 доб. 8001

 + 7 (963) 035 42 48

 r.klimenka@falcongaze.ru

 fg-sale12

 www.falcongaze.ru

