

Лабораторный практикум

МОНИТОРИНГ СЕТЕВОЙ И КОМПЬЮТЕРНОЙ АКТИВНОСТИ
ПОЛЬЗОВАТЕЛЕЙ. Ч.2

при помощи Консоли пользователя Falcongaze SecureTower

Цель практического занятия: Научиться работе с Клиентской консолью **Falcongaze SecureTower** для проведения расследований и предупреждения инцидентов информационной безопасности организации, освоить инструмент создания статистических отчетов о компьютерной и сетевой активности пользователей. Научиться использовать инструменты системы для наблюдения за активностью пользователей в режиме реального времени и для мониторинга файловых систем.

Оборудование и настройки: ПК, включенный в рабочую группу компьютеров (локальный компьютер с установленным комплексом **Falcongaze SecureTower**).

Содержание практикума

Общие сведения.....	3
Порядок выполнения работы.....	3
1. Запуск Консоли пользователя SecureTower Client Console.....	3
2. Создание отчетов о пользовательской активности при помощи Центра отчетности SecureTower.....	4
3. Мониторинг файловых систем.....	7
4. Мониторинг в реальном времени.....	8

Рекомендации по выполнению работы

Изучите теоретическую часть лабораторного практикума, изложенную в разделе **Общие сведения**, перед выполнением практических заданий.

Выполнять задания лабораторного практикума следует строго в соответствии пунктами, как указано в разделе **Порядок выполнения работы**. Шаги и задания, помеченные «*», выполняются по указанию преподавателя.

После каждого шага или при возникновении вопросов о выполнении задания сравните результат на экране с соответствующим рисунком. Для быстрого получения помощи в работе с программой, а также получения дополнительной информации используйте команды меню *Помощь* либо обратитесь к преподавателю.

Чтобы проверить, насколько хорошо Вы усвоили материал, в конце работы ответьте на контрольные вопросы.

Общие сведения

Для получения статистической информации об активности пользователей сети служит компонент комплекса Центр отчетности. Инструменты Центра отчетности позволяют строить и просматривать предустановленные отчеты и настраивать параметры любого предустановленного отчета, используя его как шаблон для создания нового отчета. Отчет по пользователю - это удобный инструмент для мгновенного построения отчетов о количественных показателях активности отдельных сотрудников для получения более детальной статистической информации. Предустановленные Топ-отчеты - это готовые к использованию отчеты более чем по 30 количественным показателям компьютерной и сетевой активности пользователей, разделенные по типам данных. Отчеты по центру безопасности позволяют получить сводную статистику по срабатыванию правил безопасности, сформированным в Центре безопасности. Сводные отчеты позволяют получить данные о статистических показателях выбранного круга пользователей за определенный промежуток времени в форме сводной таблицы.

Помимо ретроспективного анализа данных система позволяет производить мониторинг действий пользователей на рабочих местах в режиме реального времени. Мониторинг осуществляется путем удаленного подключения и просмотра видеоизображения рабочего стола компьютера и прослушивания аудиосигнала, поступающего на микрофон либо другое аудиозаписывающее устройство рабочей станции.

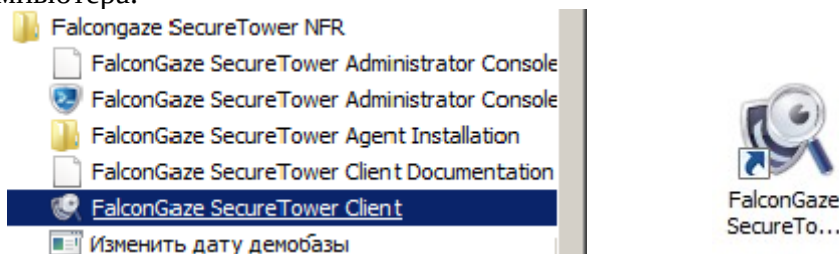
В дополнение к перечисленным инструментам, система поддерживает возможность поиска файлов, представляющих интерес в рамках обеспечения информационной безопасности, в файловых системах контролируемых рабочих станций. Поиск файлов может производиться вручную с помощью инструмента Мониторинг файловых систем либо в автоматическом режиме на основе предварительно настроенных банков хэшей файлов.

Порядок выполнения работы

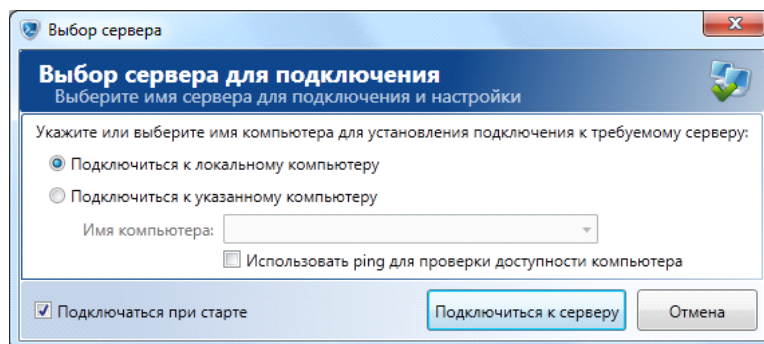
1. Запуск Консоли пользователя SecureTower Client Console


Алгоритм действий

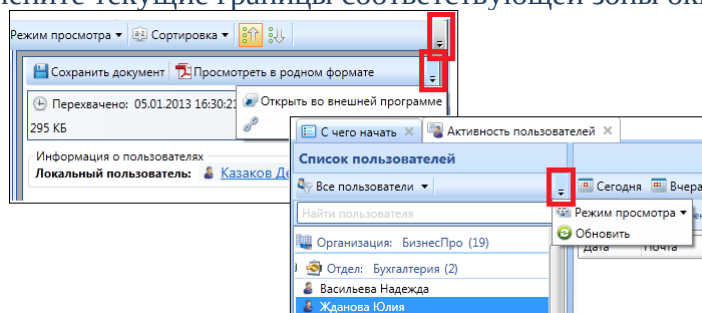
1.1 Запустите Клиентскую консоль, используя ярлык консоли, размещенный в папке *Falcongaze SecureTower NFR* в меню *Пуск* либо используйте ярлык консоли на рабочем столе компьютера.



1.2 В открывшемся диалоговом окне выберите *Подключиться к локальному компьютеру* и нажмите кнопку **Подключиться к серверу**.



Внимание! Если окно одного из компонентов Консоли пользователя находится в свернутом состоянии, то некоторые пункты меню могут быть скрыты. Для доступа к скрытым пунктам нажмите кнопку , расположенную в панелях инструментов вкладок компонентов, либо измените текущие границы соответствующей зоны окна.




2. Создание отчетов о пользовательской активности при помощи Центра отчетности SecureTower

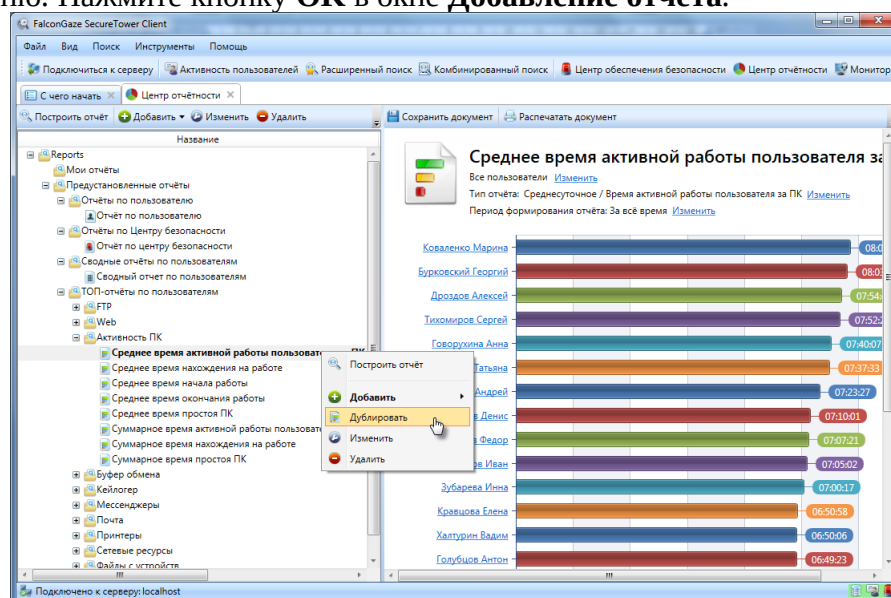
Алгоритм действий

2.1 Перейдите в Клиентскую консоль. В главном окне Консоли пользователя наведите курсор мыши на зону компонента **Центр отчетности** и перейдите в окно компонента, нажав левую клавишу мыши.

2.2 *Нажмите кнопку **Обновить отчеты** на панели команд окна **Центр отчетности** (требуется в случаях, когда система была установлена менее суток назад, т.к. автоматическое обновление отчетов выполняется в ночное время).

2.3 Разверните содержимое папки **Активность ПК**, нажав кнопку  слева от папки, и выберите предустановленный топ-отчет **Среднее время активной работы пользователя за ПК** в списке. Дважды кликните по имени отчета либо нажмите кнопку **Построить отчет** на панели команд окна. Изучите результаты.

2.4 Кликните на имени топ-отчета **Среднее время активной работы пользователя за ПК** правой клавишей мыши и выберите команду **Дублировать** в контекстном меню. Нажмите кнопку **ОК** в окне **Добавление отчета**.



1.1.1 Переместите вновь созданную копию топ-отчета в папку **Мои отчеты**. Для перемещения наведите курсор на имя топ-отчета в списке, нажмите левую клавишу мыши и, удерживая клавишу, перемести курсор на папку **Мои отчеты**.

1.1.2 Выберите перемещенный топ-отчет **Среднее время активной работы пользователя за ПК-2** в списке и нажмите кнопку **Изменить** на панели команд окна либо выберите соответствующий пункт в контекстном меню топ-отчета.

1.1.3 В поле **Название отчета** введите *“Среднее время активной работы пользователей за два рабочих дня”*.

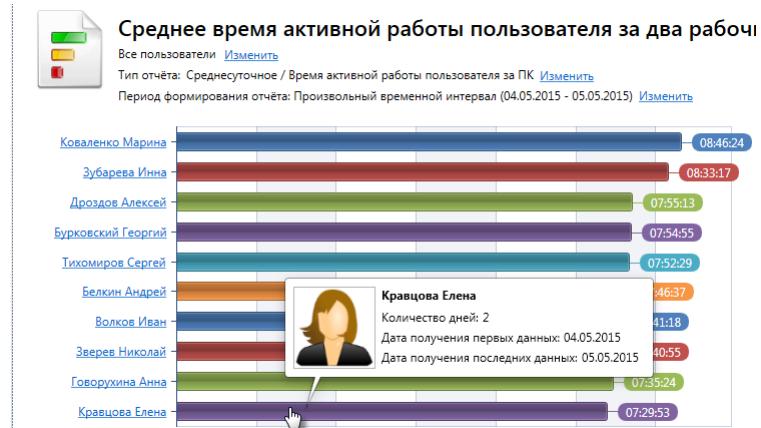
1.1.4 Установите количество топ-пользователей равное **10** в поле **Количество топ-пользователей**.

1.1.5 Выберите пункт **Произвольный временной интервал** в разделе **Отчет за определенный временной период**.

1.1.6 Задайте временной интервал, соответствующий первым двум дням предыдущей рабочей недели.

1.1.7 Нажмите **ОК** для завершения.

2.5 Постройте измененный отчет. Для получения развернутой информации по каждой позиции на диаграмме, наведите указатель мыши на столбец либо перейдите по ссылке в имени пользователя на шкале.



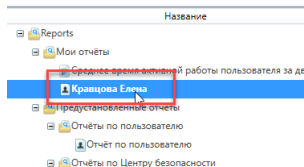
2.6 Выберите папку **Мои отчеты**, нажмите **Добавить** на панели команд Центра отчетности и выберите пункт **Отчет по пользователю**.

1.1.8 В окне добавления отчета введите имя *Кравцова Елена* в поле **Название отчета**.

1.1.9 Выберите из списка **Пользователь** соответствующее имя пользователя.

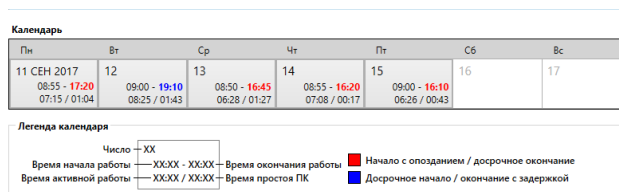
1.1.10 Нажмите **ОК**.

Результат: Новый отчет отображается в папке **Мои отчеты** в списке отчетов.



2.7 Постройте вновь созданный отчет.

2.8 Перейдите в раздел отчета **Активность пользователя за компьютером**. Обратите внимание на факты систематического нарушения рабочего графика пользователем.



2.9 Нажмите кнопку **Сохранить** на панели команд зоны просмотра отчетов и сохраните отчет по пользователю Елена Кравцова в отдельный PDF-файл с произвольным названием в папку Student на рабочем столе компьютера, нажав соответствующую кнопку в панели меню открывшегося окна.

Результат: Отчет по пользователю сохранен в папку Student.

2.10 *Удалите все созданные вами отчеты, используя кнопку **Удалить** на панели команд окна Центр отчетности.

2.11 *Нажмите кнопку Настройки и очистите все поля формы. Сохраните изменения.

2.12 Закройте вкладку Центр отчетности.

3. Мониторинг файловых систем

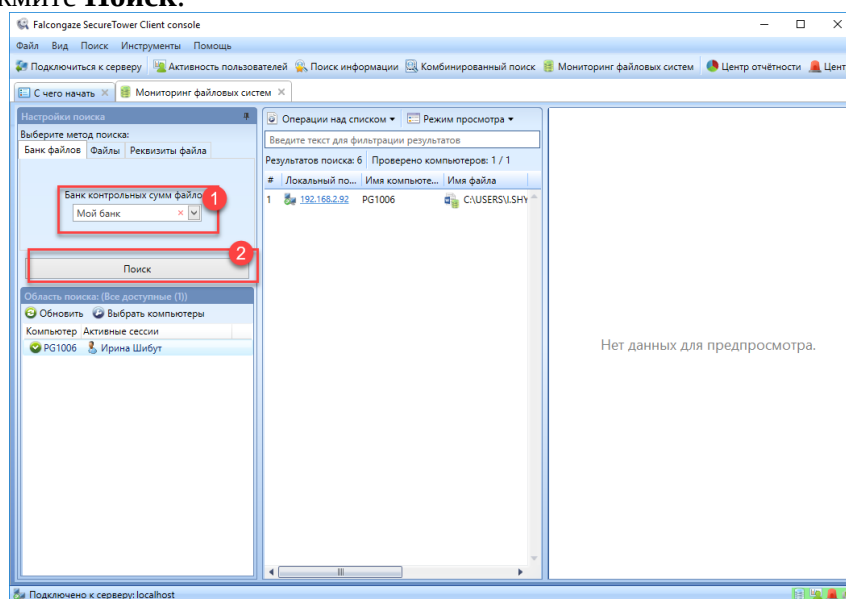
Алгоритм действий

3.1 В главном окне Консоли пользователя наведите курсор мыши на зону компонента **Мониторинг файловых систем** и перейдите в окно компонента, нажав левую клавишу мыши.

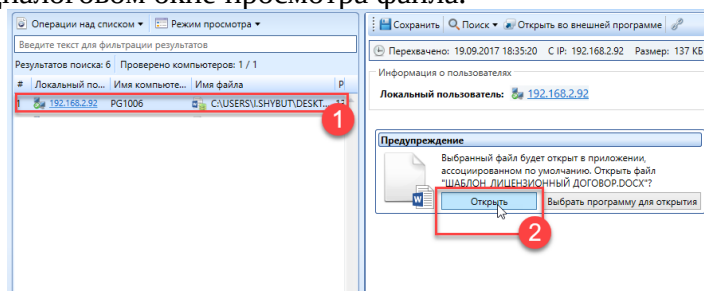
3.2 Выполните поиск совпадений с файлами ранее созданного банка хэшей. Для этого:

3.2.1 В окне мониторинга в списке **Банк контрольных сумм файлов** выберите **Мой банк**.

3.2.2 Нажмите **Поиск**.



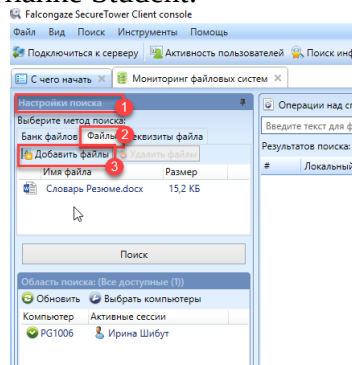
3.2.3 Кликните по строке записи результата в списке результатов поиска и нажмите **Открыть** в диалоговом окне просмотра файла.



Результат: Найденный файл соответствует файлу-источнику, добавленному в банк хэшей при настройке индексирования ранее.

3.3 Выберите закладку **Файлы** на панели **Настройки поиска**.

3.3.1 Нажмите **Добавить файлы** и выберите файл *Словарь резюме.docx*, расположенный на рабочем столе в папке Student.



3.3.2 Нажмите **Поиск**.

Результат: В ходе мониторинга найден файл *Словарь резюме.docx*, расположенный на рабочем столе в папке Student.

3.4 Закройте вкладку мониторинга файловых систем.

4. Мониторинг в реальном времени

Алгоритм действий

4.1 Запустите Консоль Администратора и подключитесь к локальному компьютеру.

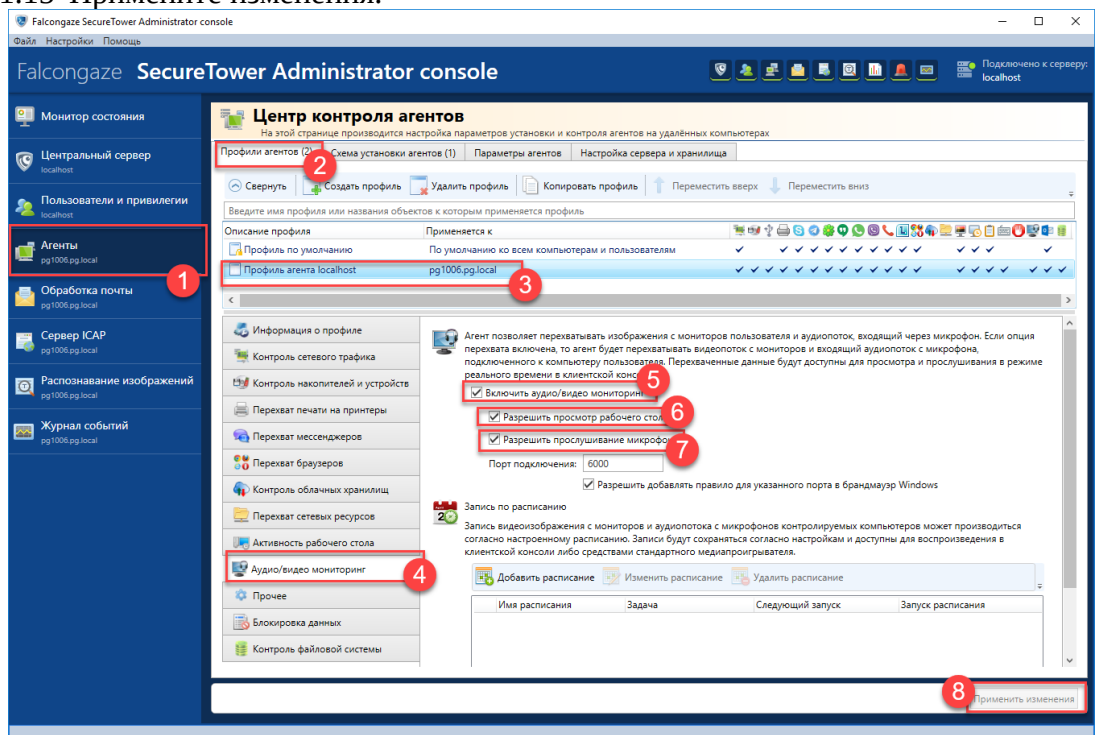
1.1.11 Выберите вкладку **Агенты** на боковой панели консоли.

1.1.12 На вкладке **Профили агентов** выберите профиль локального компьютера в списке профилей.

1.1.13 Выберите закладку **Аудио/видео мониторинг** в зоне настроек профиля и отметьте опции **Включить аудио/видео мониторинг**, **Разрешить просмотр рабочего стола**, **Разрешить прослушивание микрофона**.

1.1.14 Изучите раздел **Запись по расписанию** самостоятельно.

1.1.15 Примените изменения.



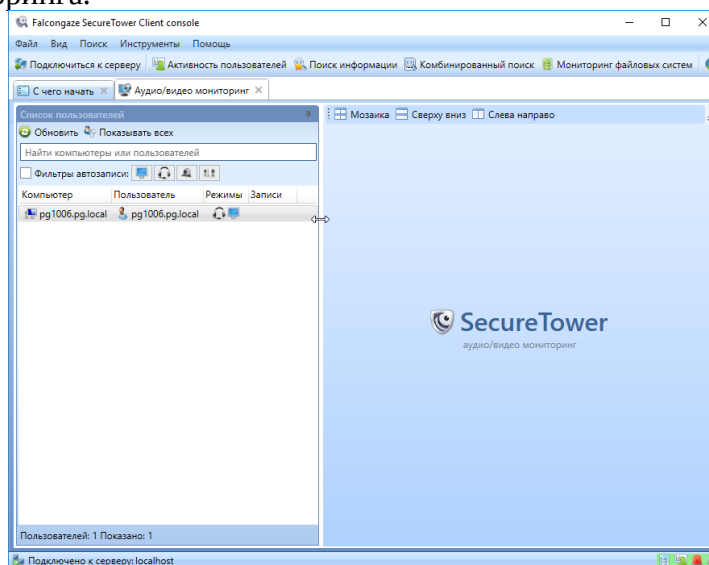
Результат: Мониторинг активирован.



4.2 Перейдите в Консоль пользователя.

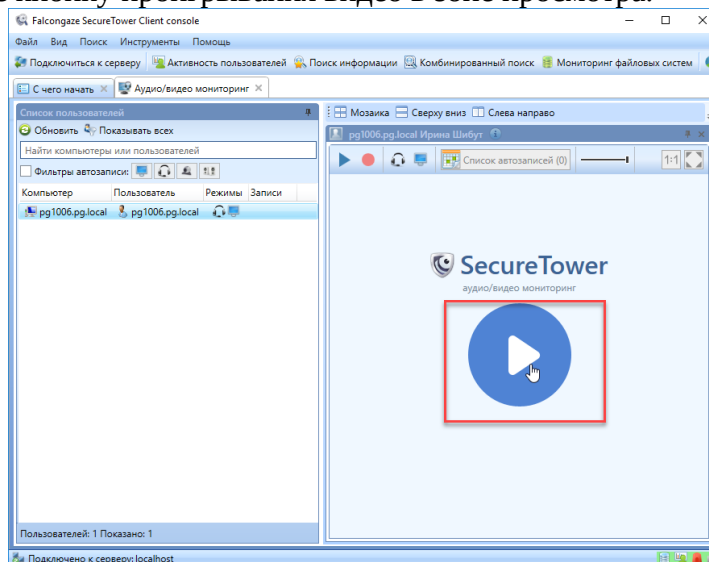
4.3 В главном окне Консоли пользователя наведите курсор мыши на зону компонента **Аудио/видео мониторинг** и перейдите в окно компонента, нажав левую клавишу мыши.

4.4 Убедитесь, что локальный компьютер отображается в списке компьютеров, доступных для мониторинга.



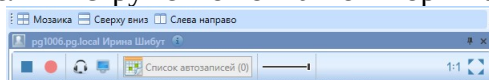
4.5 Дважды кликните по имени компьютера в списке.

4.6 Нажмите кнопку проигрывания видео в зоне просмотра.

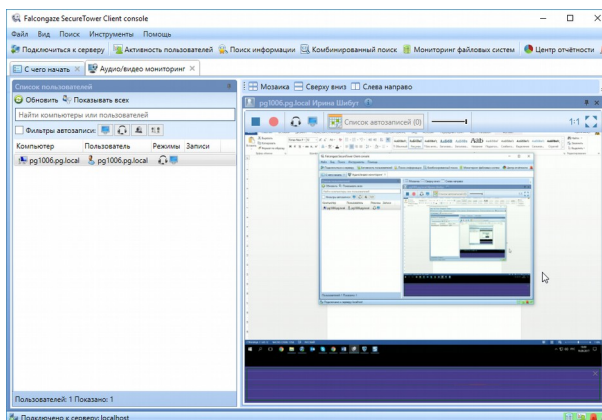


4.7 Убедитесь, что отображаемое видео соответствует вашим действиям на рабочем столе локального компьютера.

4.8 Изучите возможности встроенного проигрывателя самостоятельно. Для этого используйте кнопки панели инструментов окна мониторинга.



Результат: Воспроизводимое видео соответствует действиям пользователя на локальном компьютере.



4.9 Вернитесь в Консоль администратора и отключите аудио/видео мониторинг в профиле настроек, а также отключите опцию индексирования рабочих станций пользователя на вкладке **Параметры агентов** для снижения нагрузки на систему. Примените изменения.

Контрольные вопросы

1. Какой инструмент Консоли пользователя позволяет провести комплексный (и качественный и количественный) анализ статистики по выбранному направлению активности пользователя в сети?
2. Перечислите виды активности, по которым доступно построение статистических отчетов для отдельного пользователя сети организации.
3. Как получить информацию о соблюдении режима рабочего дня пользователя?
4. Для чего выполняется индексирование файловых систем компьютеров?
5. Возможно ли выполнить поиск произвольного файла в файловой системе контролируемого компьютера? Например, файла, выбранного пользователем, или с указанным именем или расширением.
6. Возможно ли записать видео рабочего стола пользователя вручную?
7. Позволяет ли система производить автоматическую запись результатов мониторинга компьютеров пользователей?