**Федеральное государственное автономное образовательное учреждение высшего образования**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ «ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Московский институт электроники и математики им. Тихонова

Департамент электронной инженерии

**ОТЧЕТ**

**О ПРАКТИЧЕСКОЙ РАБОТЕ №8**

по дисциплине «Программные и аппаратные средства защиты информации»

**Программный комплекс «Стахановец»**

Студент гр. БИБ201

Шадрунов Алексей

Дата выполнения: 18 июня 2023 г.

Преподаватель:

Перов А. А.

«___» _____ 2023 г.

Москва, 2023

**Содержание**

## 1 Цель работы

Цель: изучить программный комплекс «Стахановец» и приобрести навыки работы с комплексом, настройки политик и мониторинга активности.

## 2 Ход работы

### 2.1 Установка комплекса

Для разворачивания комплекса понадобится виртуальная машина. Попробуем развернуть с помощью опции Быстрая установка «в один клик» (Windows). В таком режиме база и серверная часть устанавливаются автоматически, что подходит для небольшой конфигурации и знакомства с комплексом.

Установка серверной части осуществляется автоматически (Рисунки 1-2).

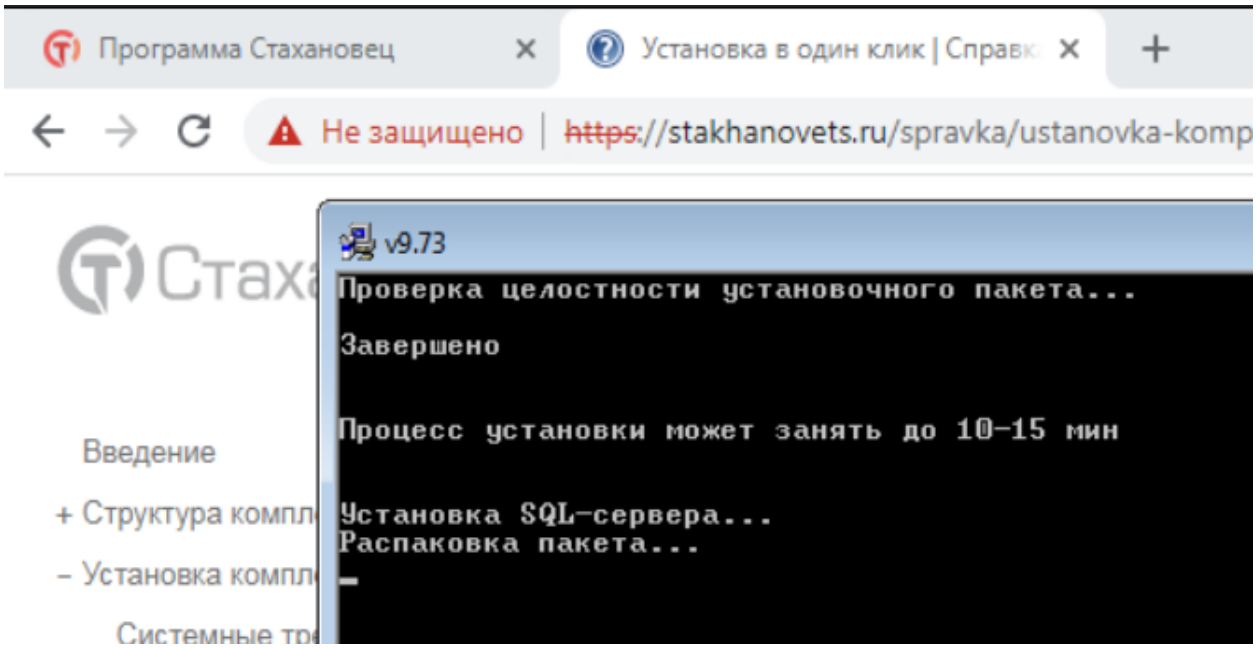


Рисунок 1 – Установка серверного компонента

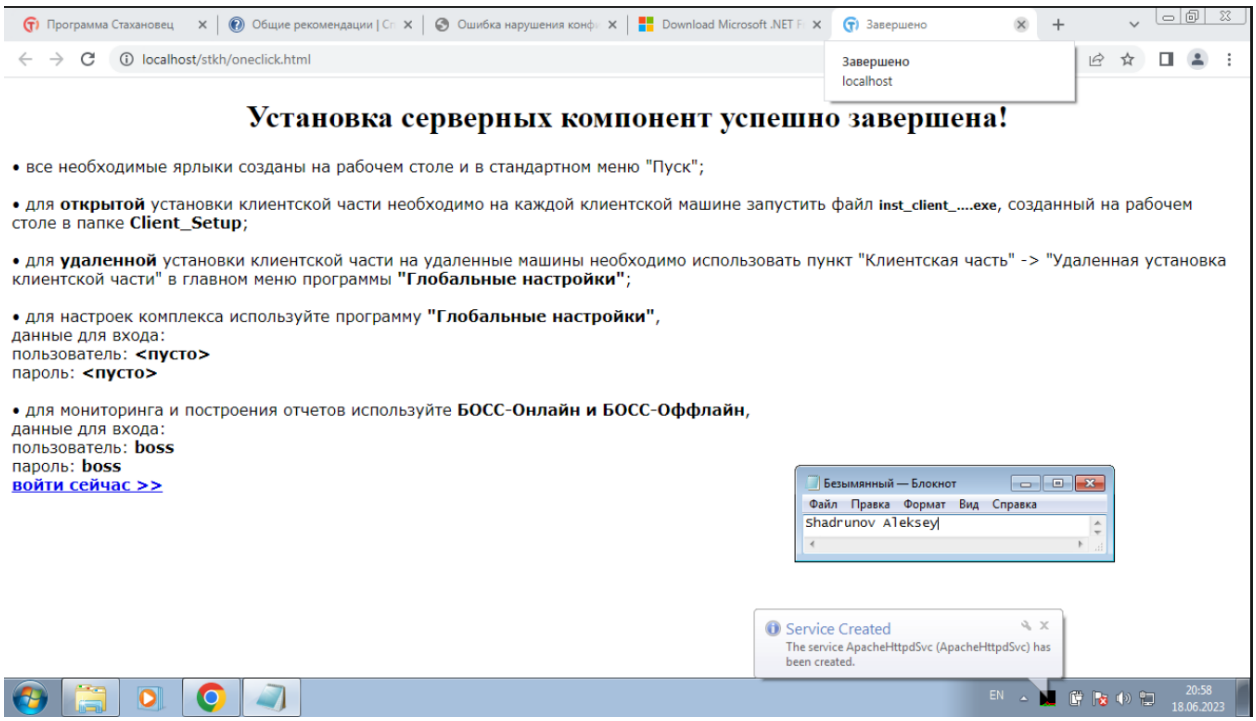


Рисунок 2 – Завершение установки

Затем в ручном режиме устанавливаем клиентский компонент. После установки видим сообщение о запуске подслушивания (Рисунки 3-4).

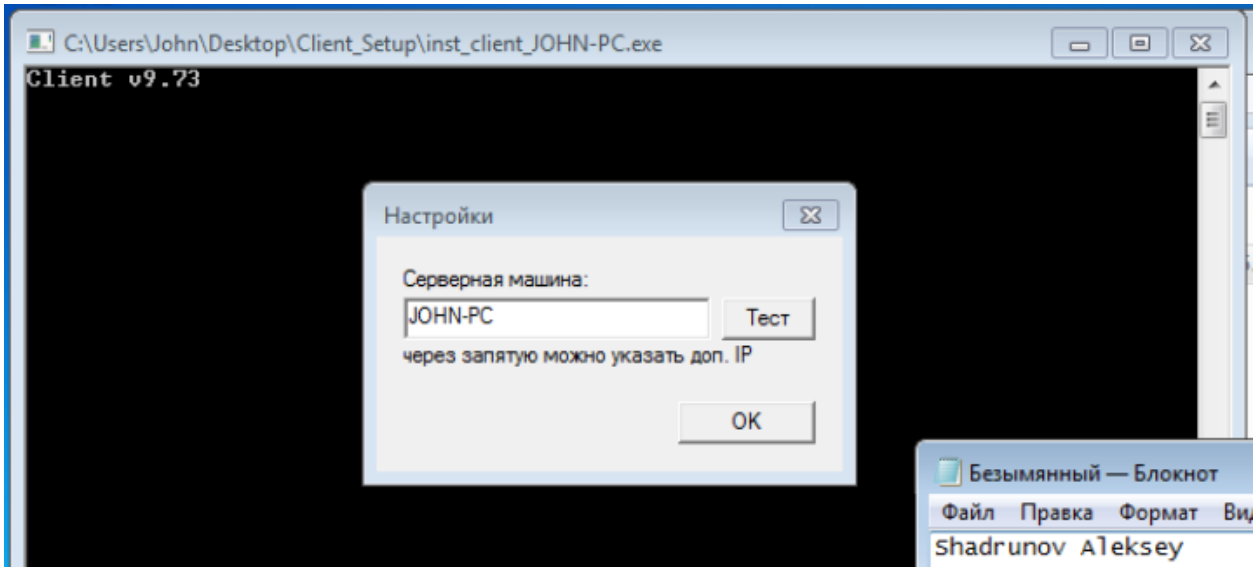


Рисунок 3 – Установка клиентского компонента

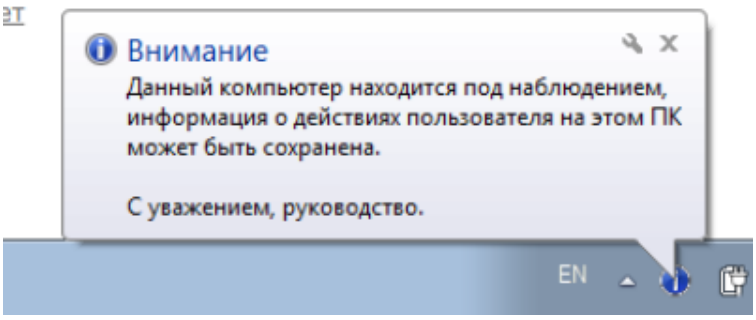


Рисунок 4 – Уведомление пользователя можно скрыть

После установки администратор может войти в два компонента — босс-онлайн и босс-офлайн (Рисунок 5).

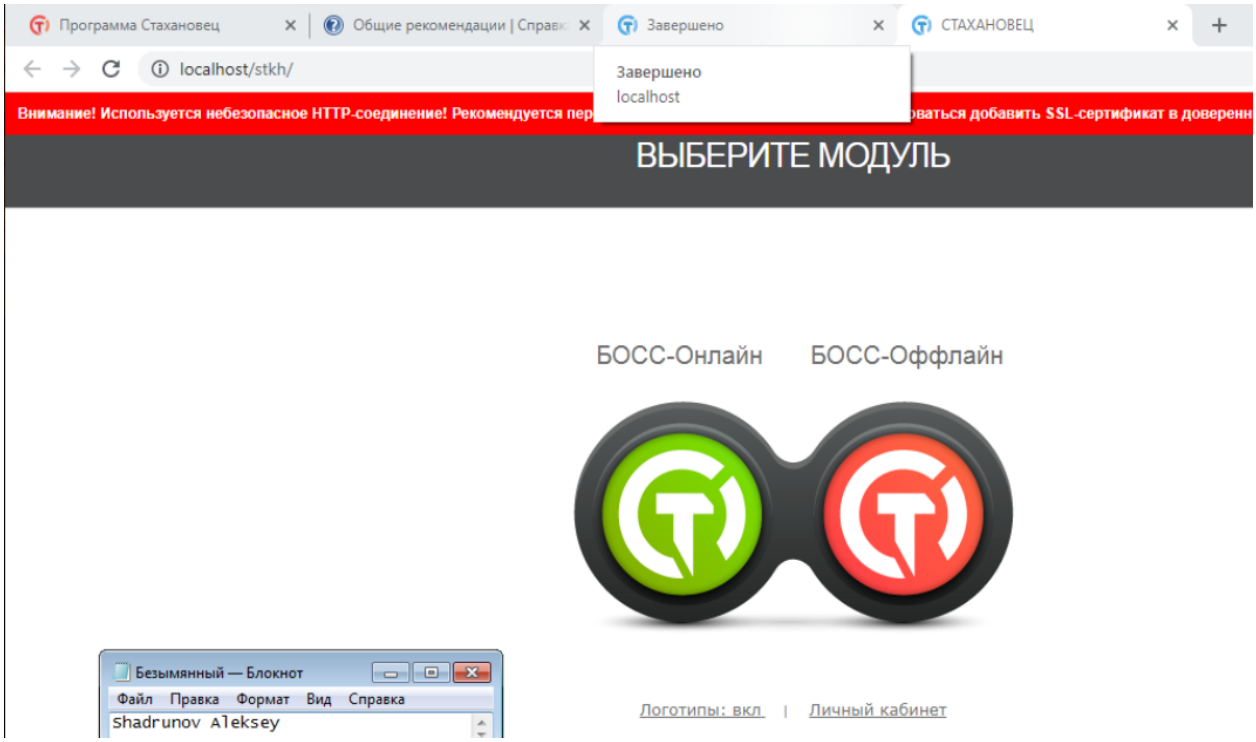


Рисунок 5 – Босс

## 2.2 Исследование возможностей для обеспечения информационной безопасности

Выберем функциональные возможности для защиты информационной безопасности и контроля персонала.

### 2.2.1 Запрет использования программ

Можно указать списки приложений для запрета или разрешения соответственно. Каждое приложение должно указываться с новой строки и представлять собой либо полный путь к исполняемому файлу, либо только сам exe-файл без пути, или описание приложения (название из его оригинального поля Description). В случае попадания приложения под запрет запуска будет выдано сообщение в трее на машине пользователя и само приложение будет закрыто.

Например, так можно заблокировать запуск потенциально нежелательных программ, например, мессенджеров, в которых работник может переслать файлы за пределы организации, или такое устаревшее программное обеспечение, как Internet Explorer (Рисунок 6).

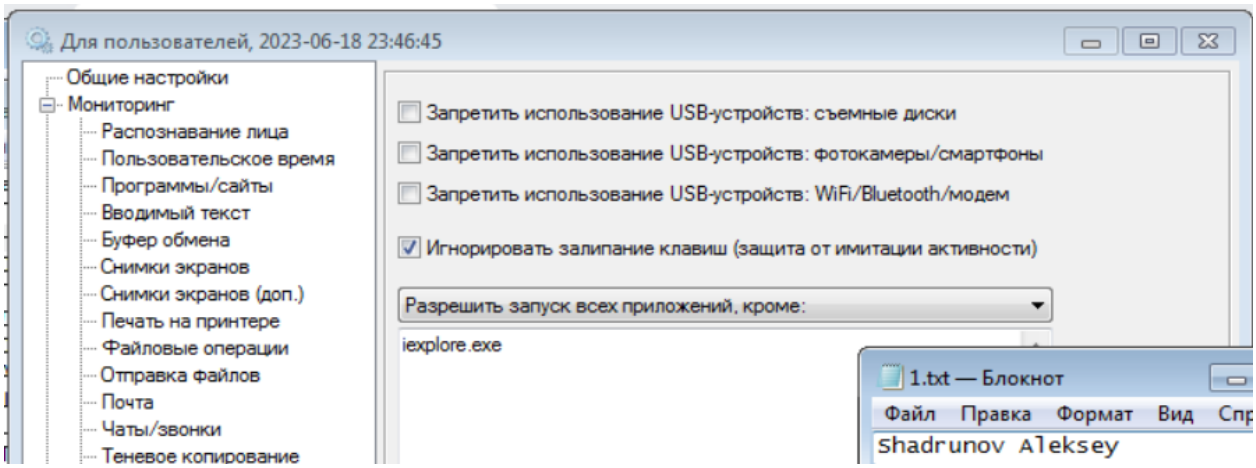


Рисунок 6 – Блокировка iexplorer.exe

### 2.2.2 DLP для печати документов

Если пользователь будет совершать то или иное действие с определенными объектами, в тексте которых присутствуют одно или несколько совпадений из списка чувствительности, то будет сформировано событие, которое может быть далее записано в отчет "События" и выдано мгновенное уведомление в БОСС-Онлайн. События настраиваются на вкладке "События". Также существует возможность запретить те или иные действия.

Для настройки DLP для печати документов включим соответствующую галочку в глобальных настойках. Система будет срабатывать на выражения из списка

чувствительности, например, "Совершенно секретно".

Для работы DLP также необходимо включить соответствующие опции мониторинга на одноименных вкладках настроек (то есть Мониторинг -> Печать на принтере), а также включить теневое копирование на клиенте и на сервере.

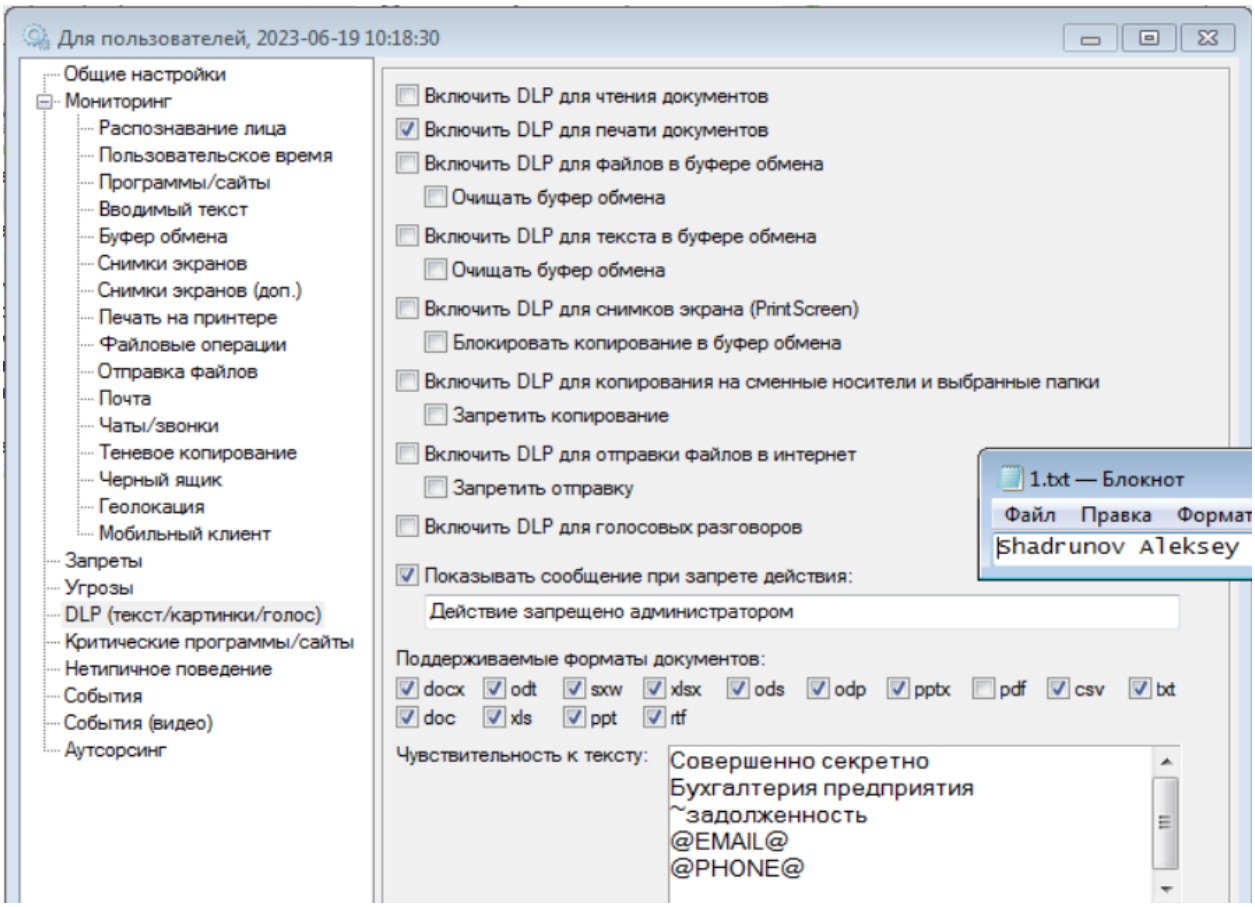


Рисунок 7 – DLP для печати документов

### 2.2.3 DLP для документов в буфере обмена

DLP для документов в буфере обмена работает схожим образом с DLP для печати. Настраиваем, как на рисунках 8-9. Не забываем включить мониторинг.

Этот способ защиты может быть полезен для защиты конфиденциальности данных, точнее, для защиты от нежелательного копирования.

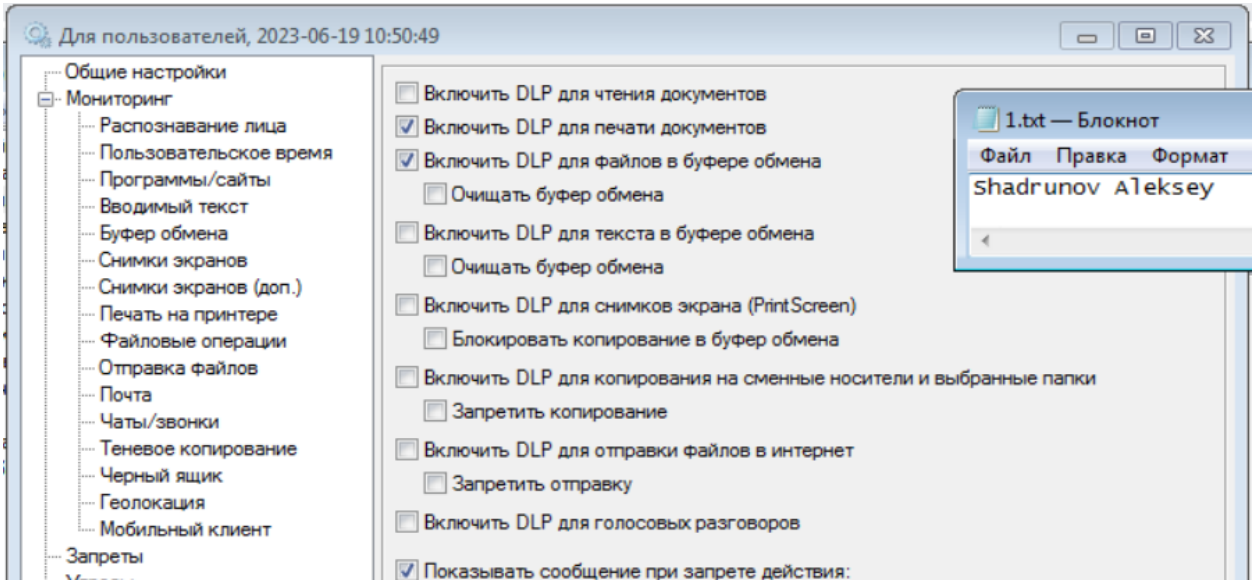


Рисунок 8 – DLP для текста в буфере обмена

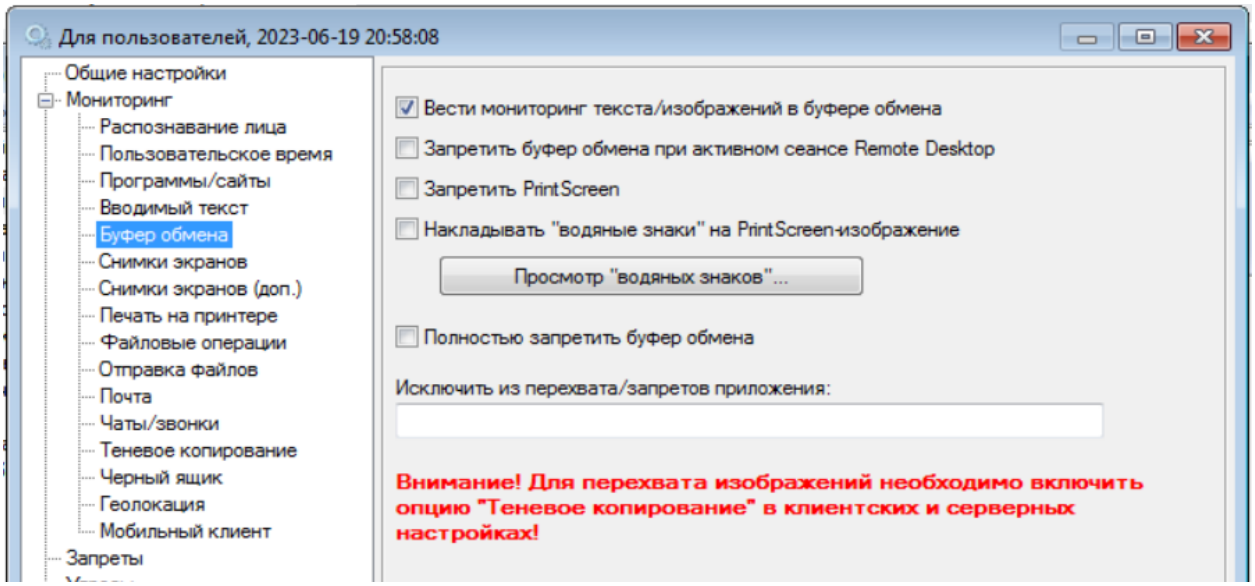


Рисунок 9 – Мониторинг текста в буфере обмена

### 2.2.4 Ограничения в критичных программах

Если в компании используются приложения или сайты, копирование или фотографирование данных из которых крайне нежелательно, то имеет смысл использовать ограничения в критичных программах. При запуске пользователем программы/сайта из списка будут происходить запреты/действия из отмеченных. Также при возникновении запрета будет сгенерировано событие.

Выбираем запретить PrintScreen и запретить буфер обмена в программе Word (Рисунок 10).

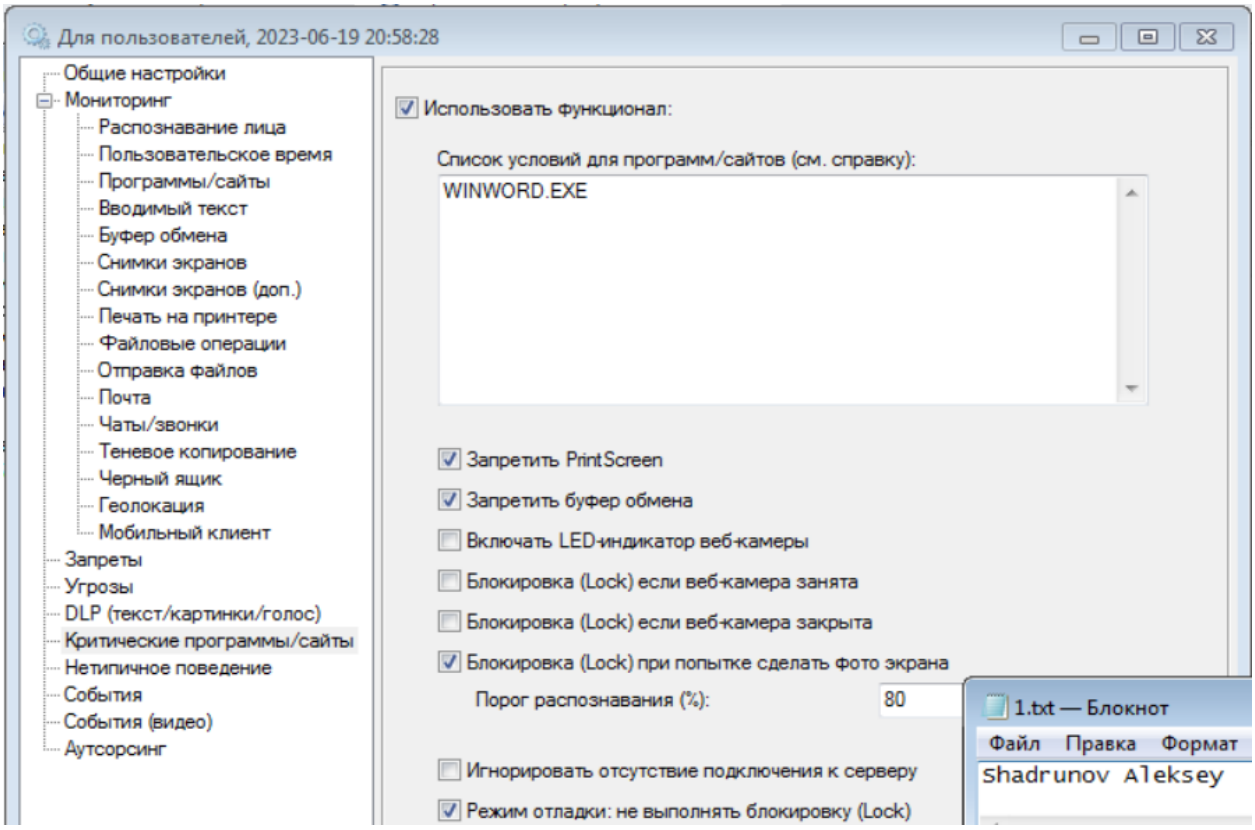


Рисунок 10 – Ограничения в критичных программах

### 2.2.5 Нетипичное поведение

На этой Нетипичное поведение настраивается возможность отслеживания нетипичного поведения сотрудника по ряду критериев. Можно задать интервал отслеживания — время наблюдения, в течение которого ведется подсчет всех остальных критериев. Если в течение данного времени любой из критериев превысил указанное в настройках значение, то происходит событие. Также необходимо включение соответствующих настроек на вкладках "Теневое копирование", "Файловые операции", "Буфер обмена", "Отправка файлов", "Программы/сайты".

Подобный поведенческий анализ позволяет выявлять подозрительную активность сотрудников и предотвращать действия, направленные на нарушение конфиденциальности или целостности каких-либо защищаемых данных.

Установим контроль за копированием и удалением любых файлов (Рисунок 11).

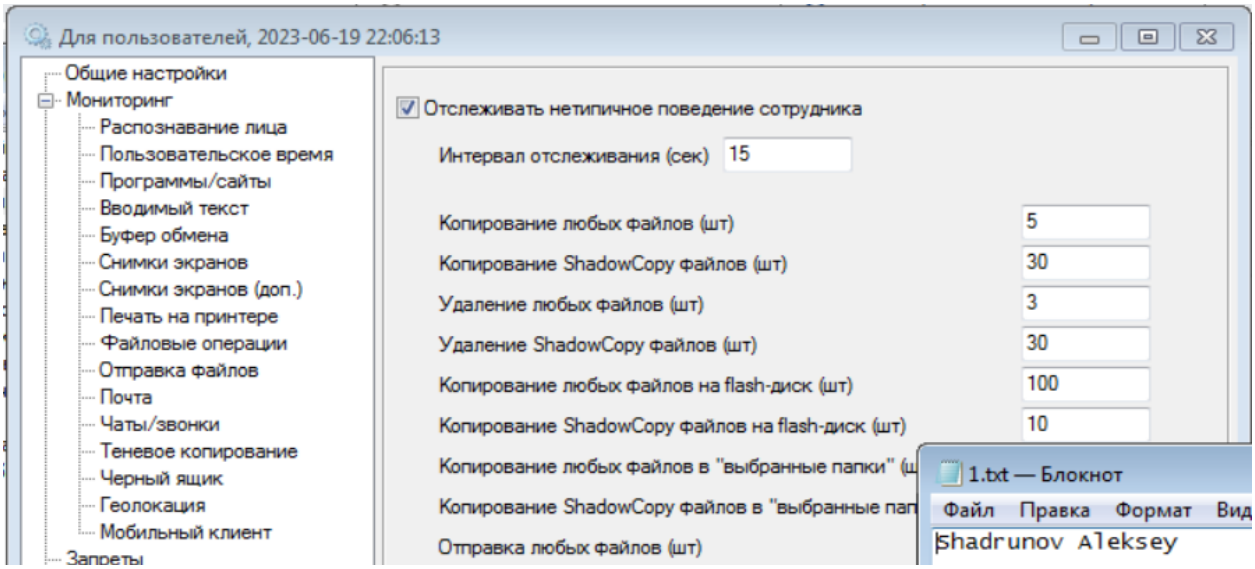


Рисунок 11 – Нетипичное поведение

### 2.2.6 Пользовательское время

Перейдём к настройкам контроля сотрудников. Для включения опции контроля пользовательского времени нужно зайти на соответствующую вкладку в глобальных настройках и включить эту функцию (Рисунок 12). Эта опция позволяет следить, в какое время был активен пользователь и в каких программах работал, а затем строить отчёты.

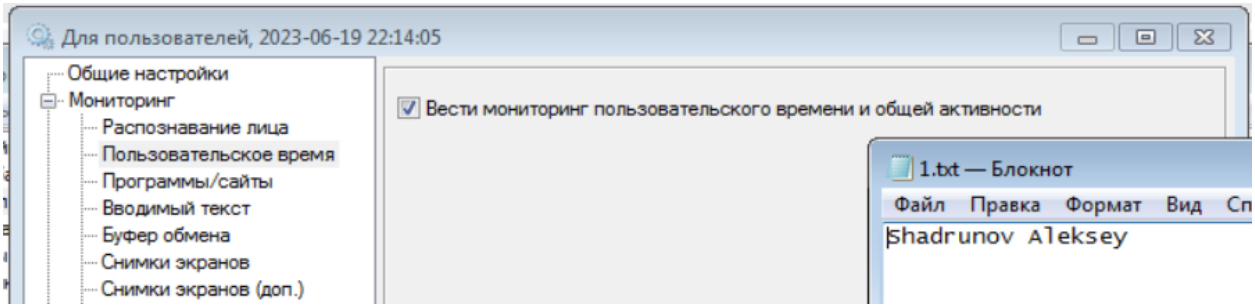


Рисунок 12 – Пользовательское время

### 2.2.7 Программы/сайты

Вкладка программы/сайты позволяет подключить детализацию по приложениям и сайтам (Рисунок 13).

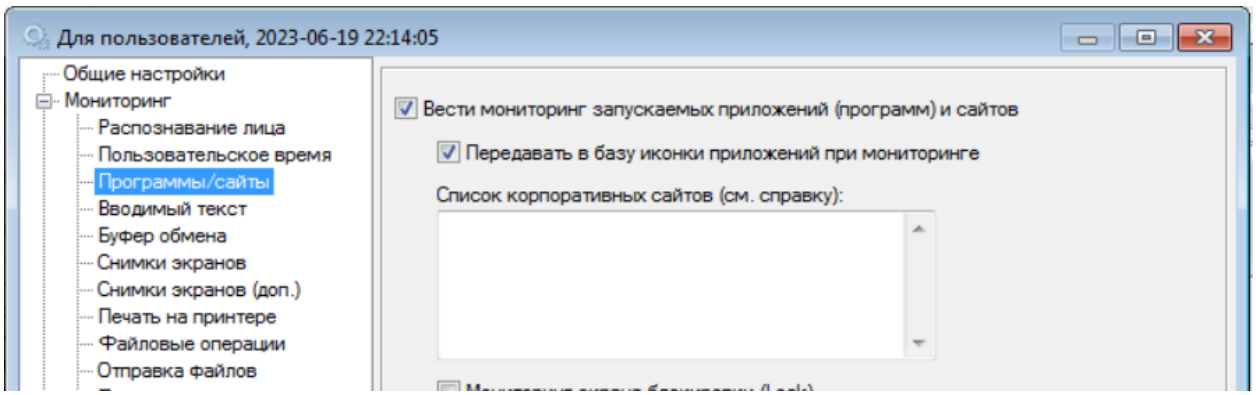


Рисунок 13 – Пользовательское время

### 2.2.8 Снимки с экранов

Вкладка Снимки с экранов настраивает параметры выгрузки скриншотов с рабочих станций (Рисунок 14).

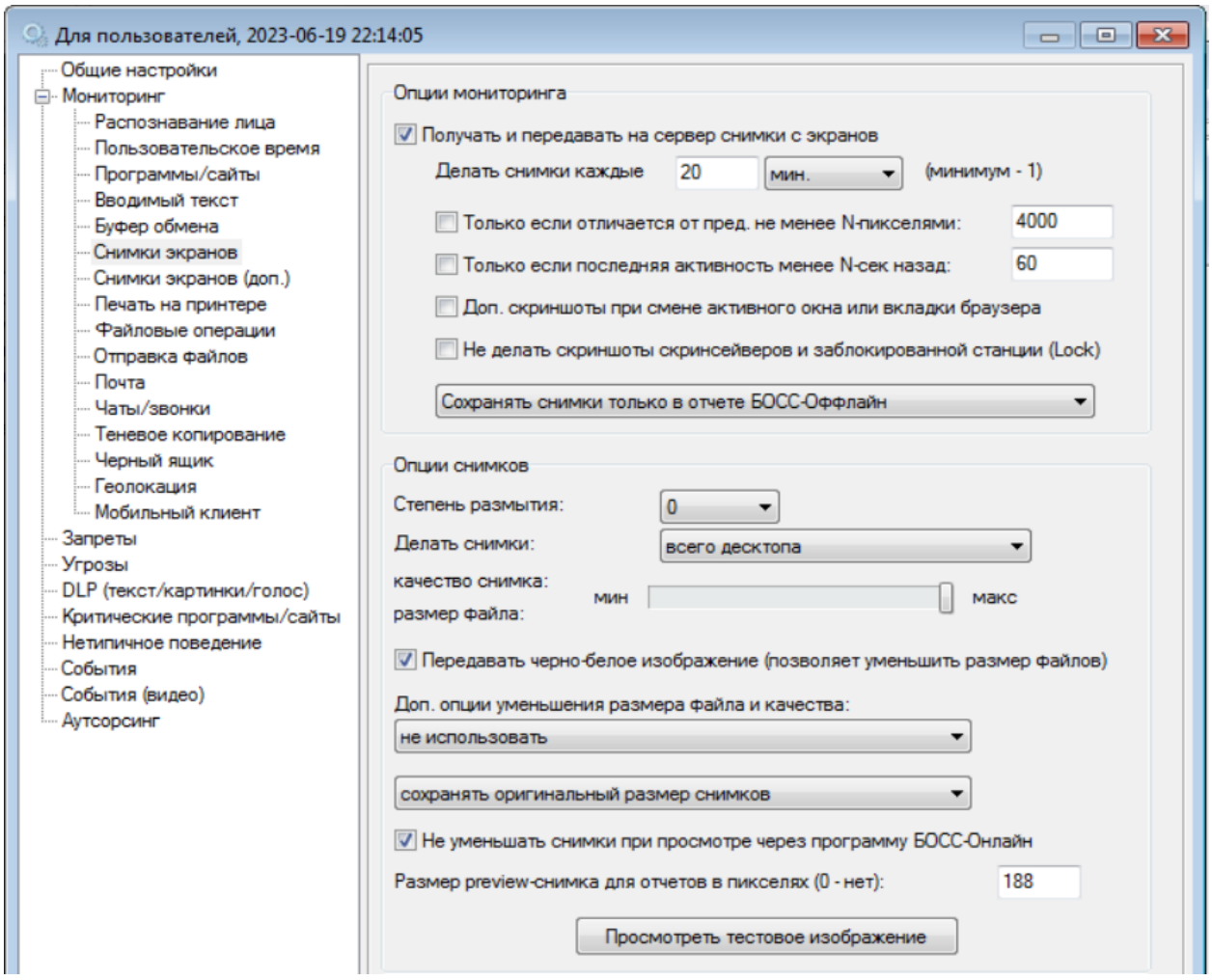


Рисунок 14 – Снимки с экранов

Наиболее важные опции на этой вкладке: получать и передавать на сервер снимки с экранов — нужно включить, чтобы получать скриншоты в системе босс. Делать снимки каждые 20 минут — частота снимков. Также можно изменить качество скришнотов, чтобы отрегулировать нагрузку на сеть и занимаемое место.

## 2.3 Тестирование возможностей

### 2.3.1 Запрет использования программ

Протестируем работу запрета. Попробуем запустить iexplorer.exe. Программа открывается, затем принудительно закрывается, а в трее появляется сообщение (Рисунок 15).

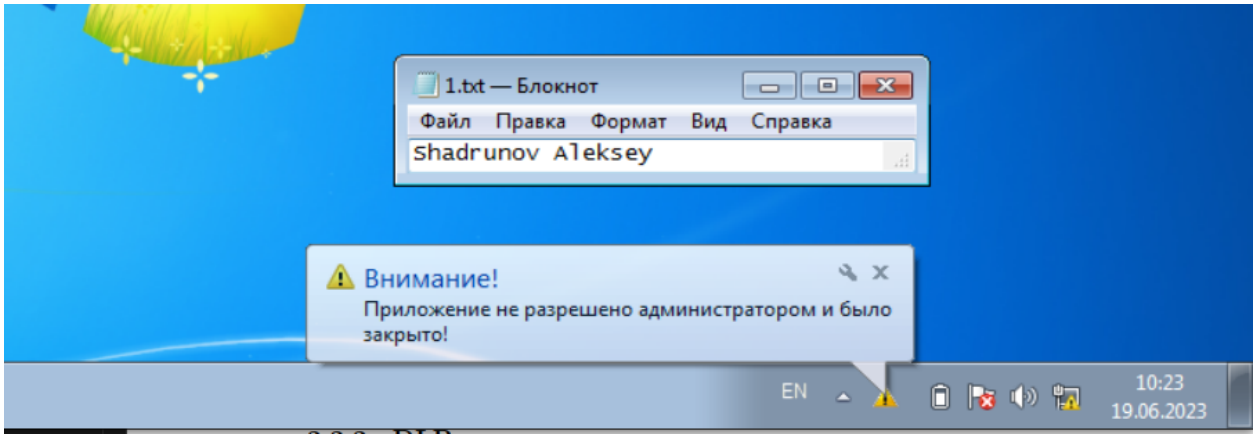


Рисунок 15 – Блокировка iexplorer.exe

### 2.3.2 DLP для печати документов

Протестируем работу DLP для печати документов. Для этого создадим текстовый документ, содержащий чувствительную фразу "Совершенно секретно" (Рисунок 16). Отправим документ на печать. В результате срабатывает уведомление в босс-онлайн (Рисунок 17).

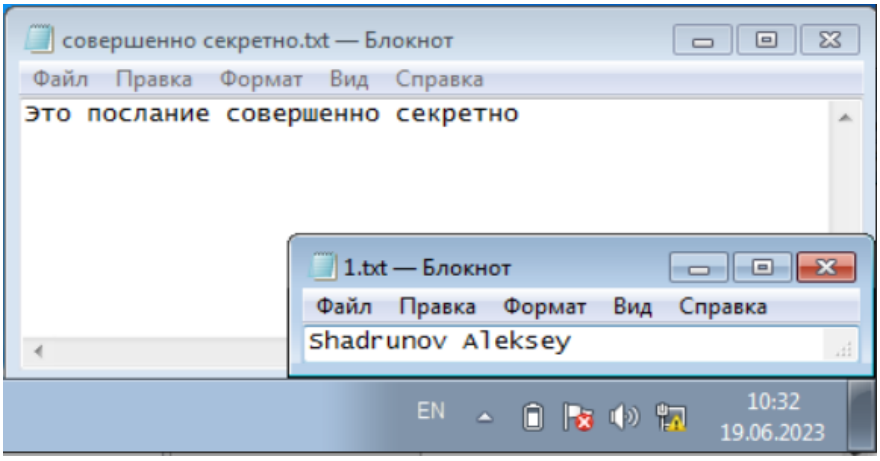


Рисунок 16 – Секретный документ

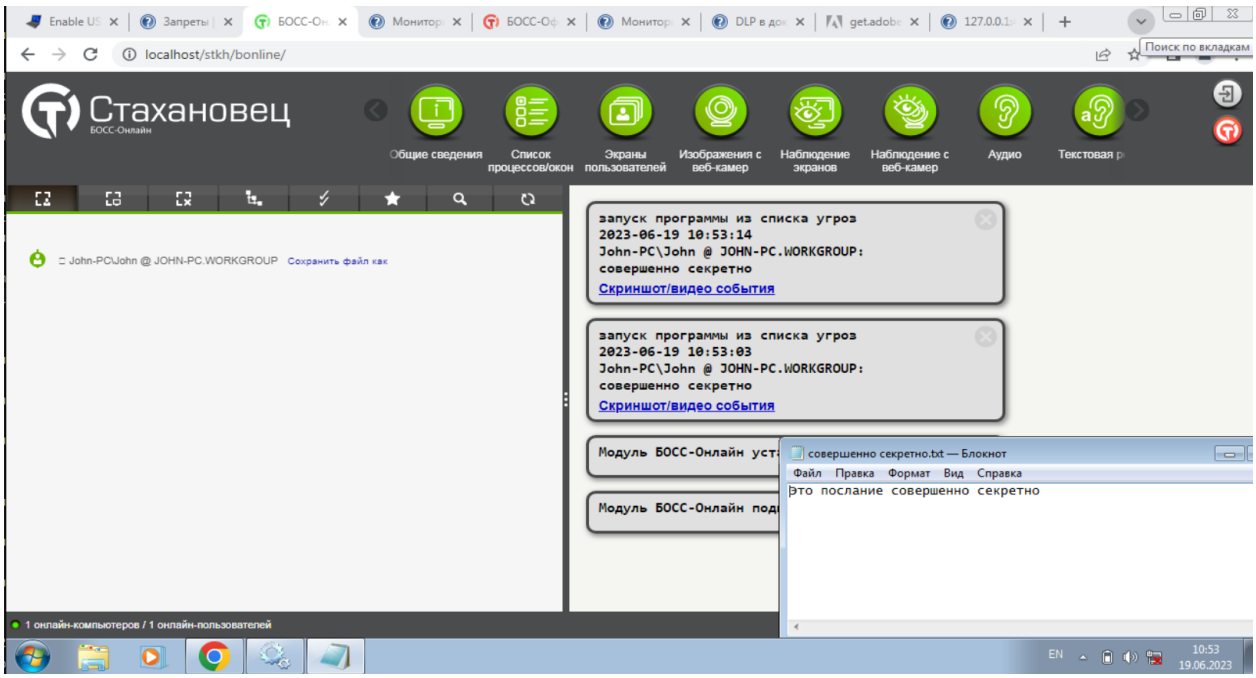


Рисунок 17 – Уведомление для босса

### 2.3.3 DLP для документов в буфере обмена

Протестируем работу DLP для документов в буфере обмена. Для этого найдём текстовый документ, содержащий чувствительную фразу "Совершенно секретно" (Рисунок 18). Скопируем документ. В результате срабатывает уведомление в босс-онлайн.

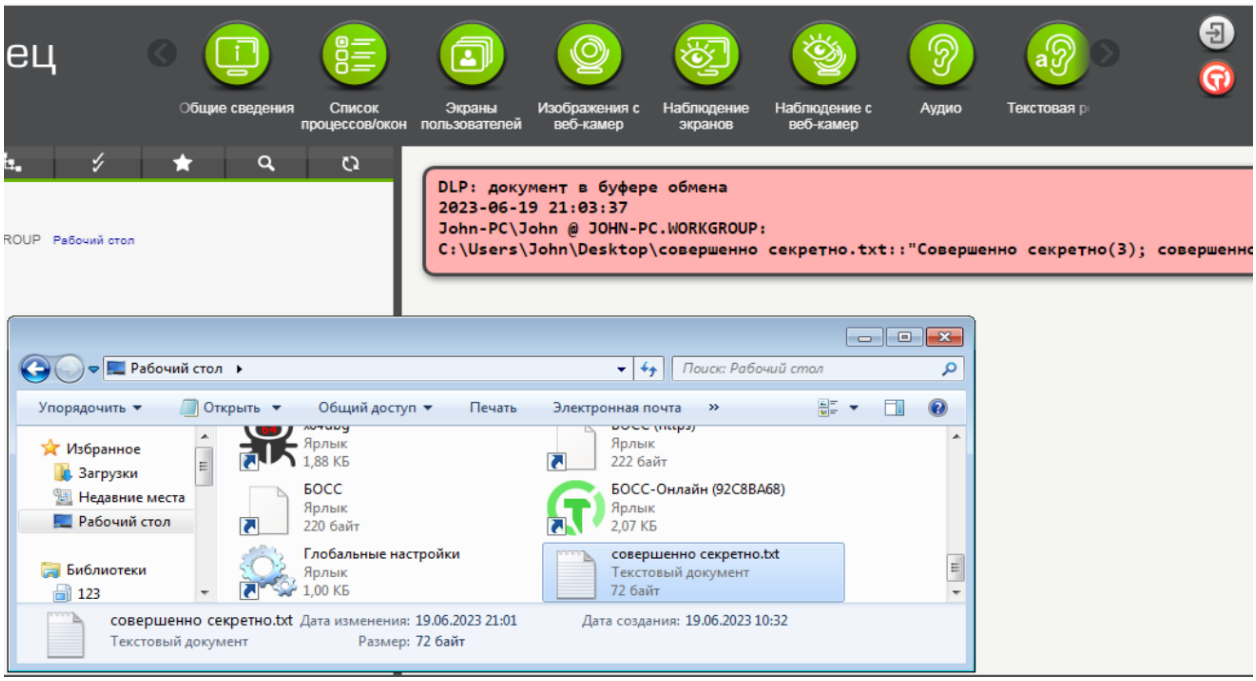


Рисунок 18 – Уведомление для босса

### 2.3.4 Ограничения в критичных программах

Протестируем работу ограничений в критичных программах. Для этого запустим критичный процесс (winword.exe) и попробуем сделать скриншот. Видим, что

защита сработала и скриншот сделать не удалось, а в боссе-онлайн появилось уведомление (Рисунок 19).

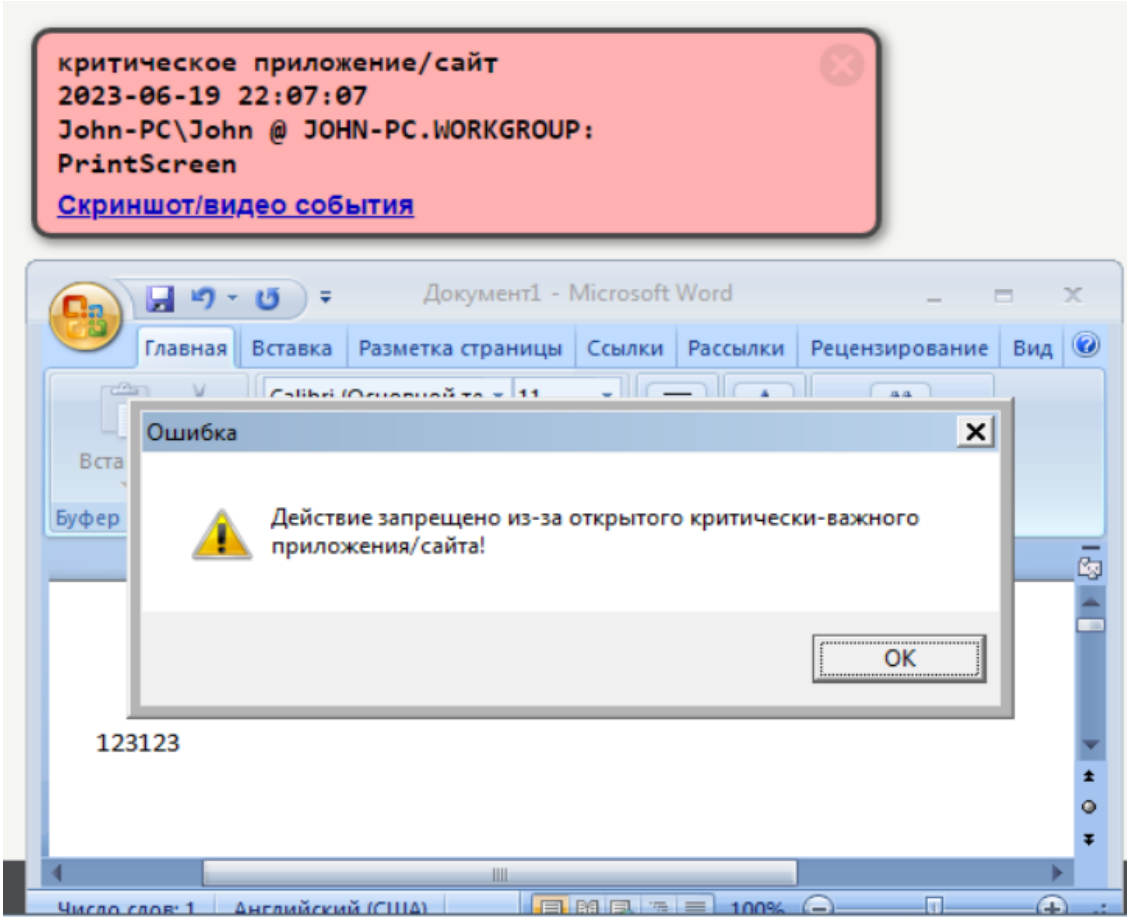


Рисунок 19 – Уведомление для босса

### 2.3.5 Нетипичное поведение

Протестируем работу нетипичного поведения. Удалим несколько файлов с рабочего стола. Видим, как в боссе срабатывает алерт (Рисунок 20).

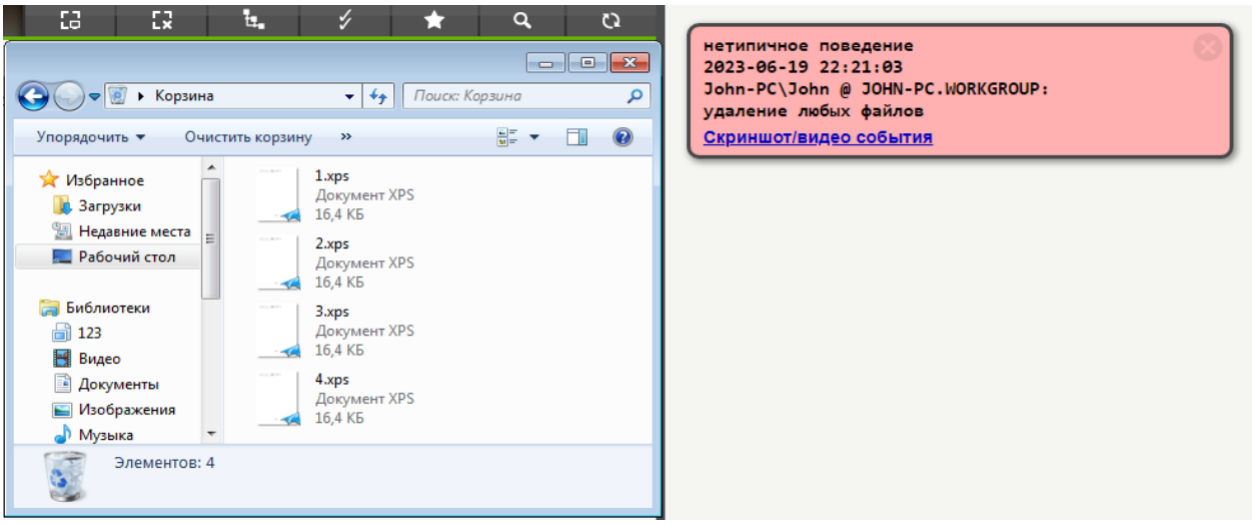


Рисунок 20 – Уведомление для босса

### 2.3.6 Пользовательское время

Протестируем работу пользовательского времени. Для этого в системе босс-офлайн построим отчёты по времени. Примеры на рисунках ниже.


Рисунок 21 – Пользовательское время

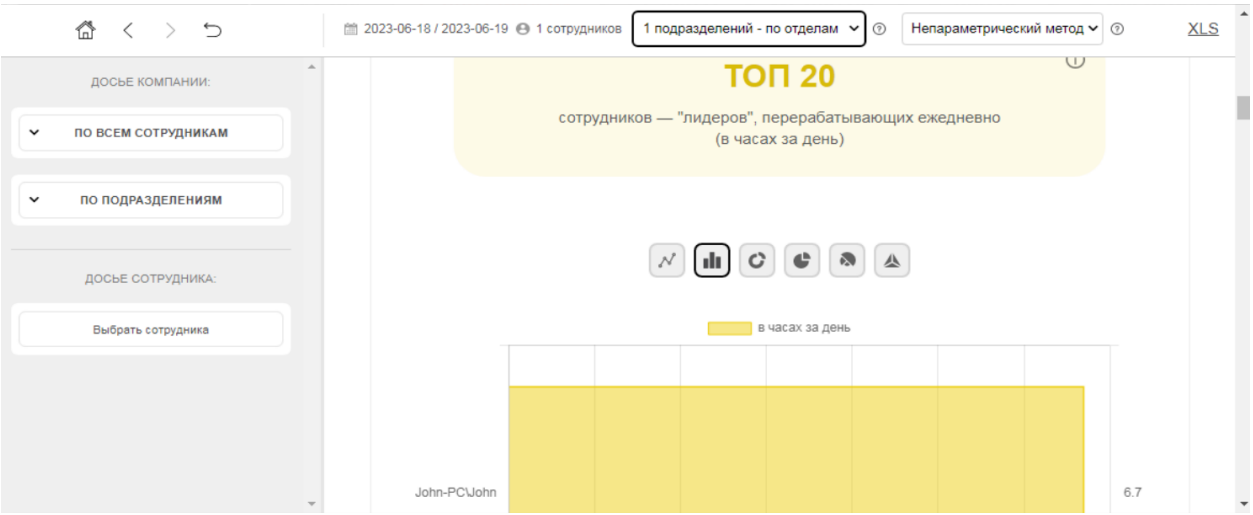


Рисунок 22 – Переработал, пока делал лабу

### 2.3.7 Программы/сайты

Протестируем работу функции Программы/сайты. Для этого в системе босс-офлайн построим отчёты по времени в приложениях. Примеры на рисунках ниже.

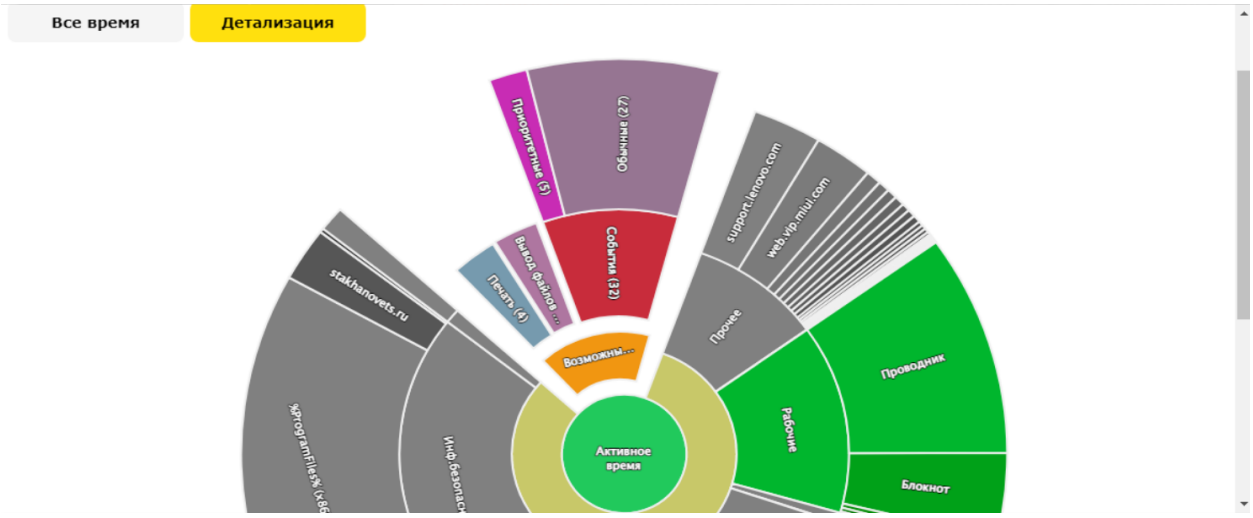


Рисунок 23 – Программы/сайты

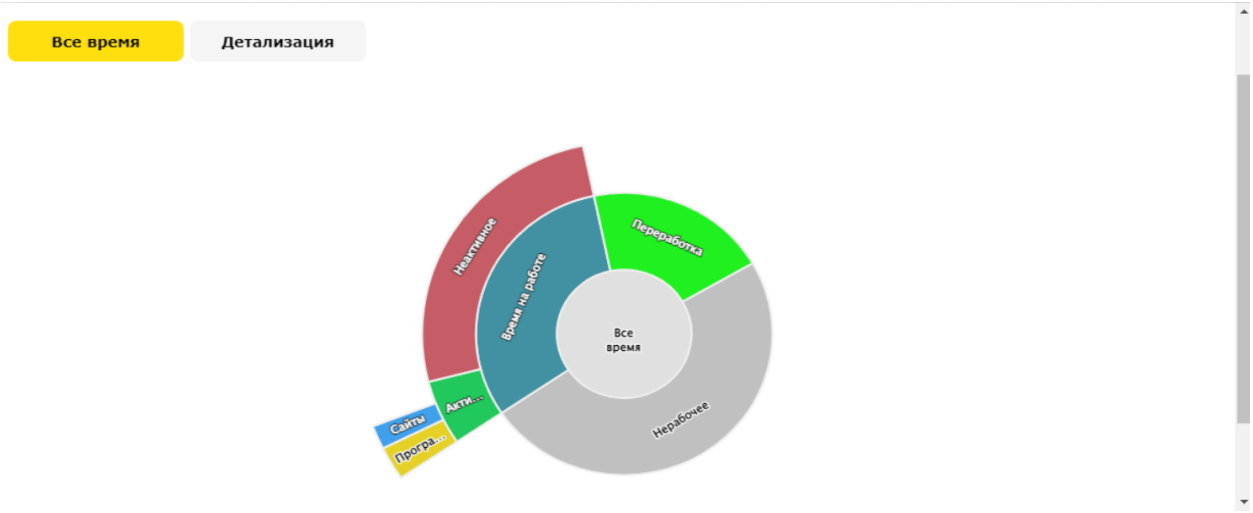


Рисунок 24 – Программы/сайты (упрощённый)

### 2.3.8 Снимки с экранов

Протестируем работу функции Снимки с экранов. По сути эта функция встроена во многие другие возможности, в том числе на срабатывание событий присылается скриншот. Пример текущего скриншота на рисунке 26.

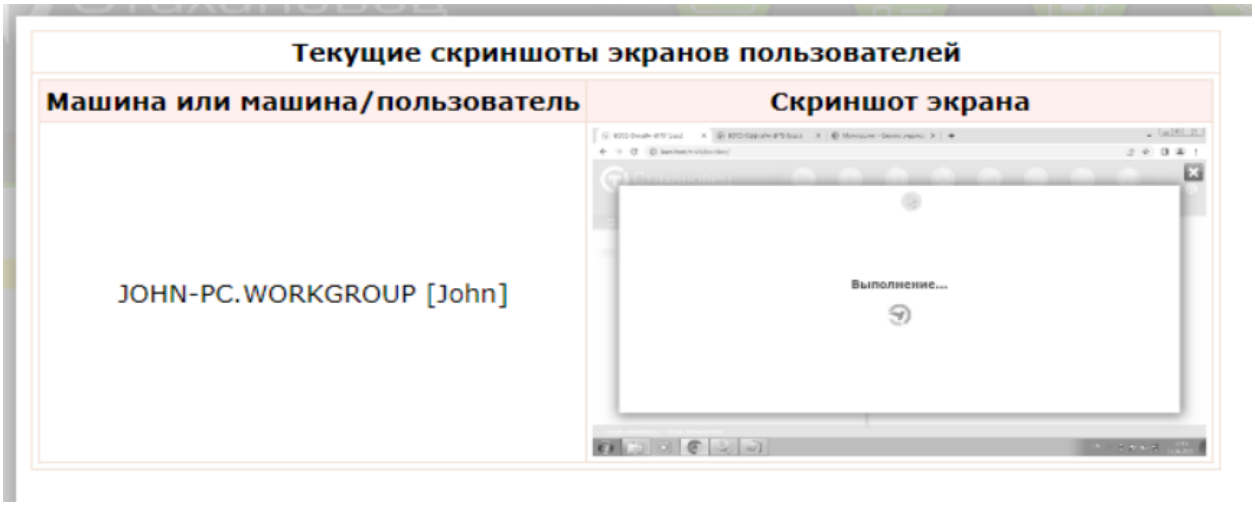


Рисунок 25 – Скриншот

## 3 Выводы о проделанной работе

Я изучил и приобрёл навыки работы с комплексом Стахановец, настроил мониторинг событий информационной безопасности и контроль за сотрудниками.