Департамент образования города Москвы  
Государственное бюджетное общеобразовательное учреждение  
города Москвы  
«Школа № 1505 «Преображенская»»

**ДИПЛОМНОЕ ИССЛЕДОВАНИЕ**на тему:

**«Корпоративная защита от внутренних угроз информационной безопасности»**

Выполнила:

Дмитриева Екатерина Владимировна, 10 класс «А»

Руководитель

Коняхин Александр Валерьевич

Москва

2018/2019 уч.г.

Содержание

Введение ……………………………………………………………………………………………………………………………………………… 2

Глава 1 ………………………………………………………………………………………………………………………………..……………….. 3

Глава 2 …………………………………………………………………………………………………………………………………………………. 8

Заключение ……………………………………………………………………………………………………………………………………..… 15

Источники ………………………………………………………………………………………………………………………………………….. 16

Введение

Некоммерческая ассоциация WorldSkills была основана в 1953 году с целью привлечения молодых людей к рабочим профессиям и улучшения профессионального образования. Основная деятельность организации – проведение конкурсов профессионального мастерства для школьников и студентов по всему миру. На сегодняшний в движении участвуют 76 стран, в том числе и Россия. Участники соревнуются в двух возрастных категориях –14-16 лет в 72 компетенциях и 16-20 лет в 91 компетенции. Соревнования проводятся по 72 компетенциям для младших участников и по 91 компетенции для старших.

В своей работе я хочу рассмотреть задания компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

На сегодняшний день приоритетной задачей обеспечения корпоративной безопасности является предотвращение внутренних утечек информации. Угроза утечки данных может появится из-за халатности сотрудников, незнания правил безопасности компании и намеренной передачи информации.

Специалисты по обеспечению корпоративной безопасности используют технологии класса Data Leak Prevention (DLP). DLP-система анализирует трафик, циркулирующий внутри компании и выходящий за ее пределы. Это позволяет отследить и предотвратить передачу конфиденциальных данных.

Специалисты должны уметь устанавливать и настраивать DLP-систему, в том числе разрабатывать политики безопасности, анализировать полученные данные для выявления нарушений со стороны сотрудников.

Глава 1. Знакомство с программой

На олимпиаде участники работают с программами InfoWatch Traffic Monitor и InfoWatch Device Monitor. Работа в InfoWatch Traffic Monitor ведется в тематических разделах (рисунок 1). Разберем каждый из них.

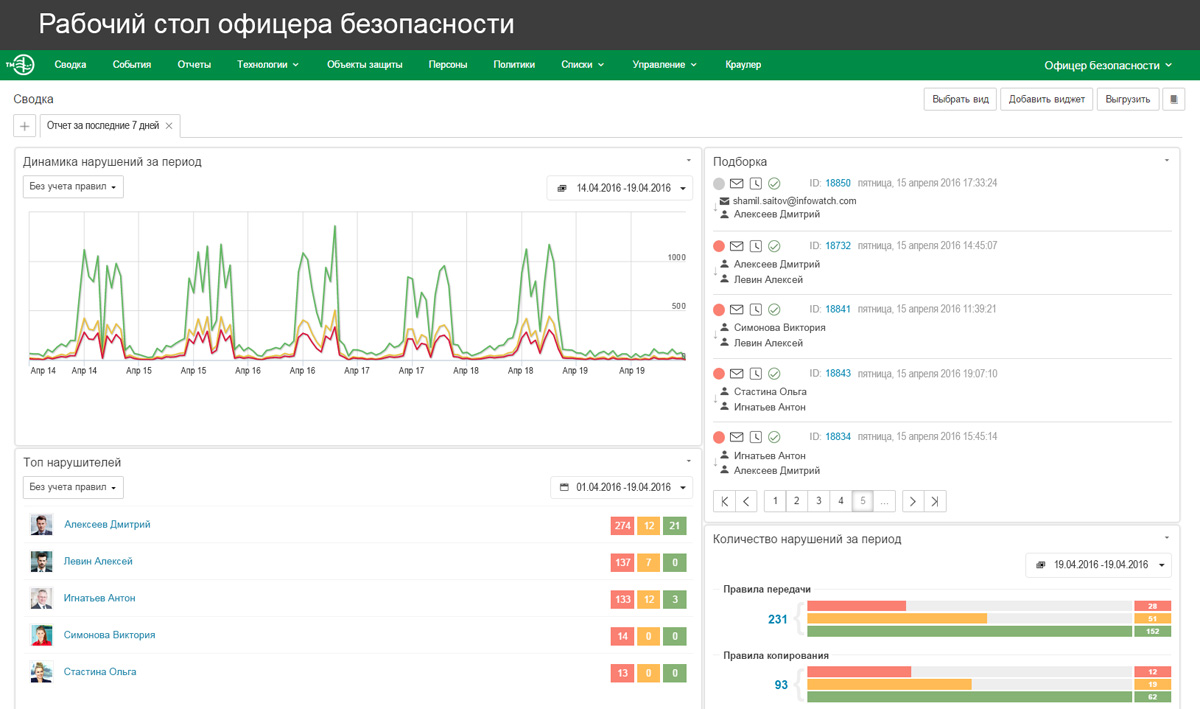


Рисунок 1.  
Консоль InfoWatch Traffic Monitor

1. Сводка

В разделе Сводка хранится статистическая информация о нарушениях и нарушителях в виджетах. Данные, отображаемые на виджите, зависят от его типа.

| Таблица 1. Виджеты сводок | |
| --- | --- |
| **Виджет** | **Описание** |
| Динамика нарушений за период | Показывает количественное изменение выбранных видов нарушений за указанный период времени |
| [Топ нарушителей](https://kb.infowatch.com/pages/viewpage.action?pageId=128588853) | Список персон с наибольшим количеством нарушений за выбранное период |
| [Количество нарушений за период](https://kb.infowatch.com/pages/viewpage.action?pageId=128588860) | Для каждого из типа нарушений отображается его количество высокого, среднего, низкого уровня за выбранный период времени |
| [Подборка](https://kb.infowatch.com/pages/viewpage.action?pageId=128588866) | События для выбранной подборки |
| [Динамика статусов за период](https://kb.infowatch.com/pages/viewpage.action?pageId=128588872) | Динамика статусов за выбранный период времени |
| [Статистика по политикам](https://kb.infowatch.com/pages/viewpage.action?pageId=128588878) | Количество нарушений по настроенным политикам хранения, копирования и передачи |
| [Статистика по объектам защиты](https://kb.infowatch.com/pages/viewpage.action?pageId=128588885) | Общее количество нарушений для каждого объекта защиты и количество нарушений высокого, среднего, низкого уровня за выбранный период времени |
| [Статистика по каталогам объектов защиты](https://kb.infowatch.com/pages/viewpage.action?pageId=128588893) | Общее количество нарушений по каталогам защиты и количество нарушений высокого, среднего, низкого уровня за выбранный период времени |

1. События

В разделе События хранятся данные о нарушениях политик безопасности за выбранный период времени.

1. Отчеты

Раздел содержит инструменты для создания отчетов и работы с ними. В отчетах отображена статистическая информация о перехваченных данных, которые могут быть представлены в виде графика, линейчатой и круговой диаграмме.

| Таблица 2. Виджеты отчетов | |
| --- | --- |
| **Тип статистики** | **Описание** |
| Веб-ресурсы | Веб-ресурсы, на которые сотрудники отправляли наибольшее число запросов |
| Диалоги | Маршруты передачи сообщений (без учёта направления), для которых Системой зафиксировано наибольшее количество событий |
| Динамика активности | Динамика количества событий, перехваченных Системой |
| Каталоги объектов защиты | Каталоги объектов защиты, наиболее часто встречающиеся в перехваченных Системой данных |
| Компьютеры | Компьютеры, для которых Системой зафиксировано наибольшее количество событий |
| Объекты защиты | Объекты защиты, наиболее часто встречающиеся в перехваченных Системой данных |
| Отправители | Отправители, для которых Системой зафиксировано наибольшее количество событий |
| Политики | Политики, наиболее часто применявшиеся к перехваченным данным |
| Получатели | Получатели, для которых Системой зафиксировано наибольшее количество событий |
| Решения пользователей | Статистика решений, принятых офицером безопасности по событиям, перехваченным Системой |
| Списки веб-ресурсов | Наиболее частые тематики веб-ресурсов, на которые сотрудники отправляли запросы |
| Типы событий | Распределение количества событий по типам |

1. Технологии  
   Технологии – ряд данных, используемых системой при анализе трафика. Раздел содержит следующие подразделы:

Категорий и термины – это набор данных, используемых для лингвистического анализа. Наличие определенных терминов помогает определить категорию текста и классифицировать возможные нарушения политик безопасности.

Текстовые объекты нужны для обнаружения передачи стандартизированных данных, например, номера банковской карты. Текстовые объекты задаются шаблоном вида [A-Za-z]{3}\d{2} , где «[A-Za-z]» – диапазон строчных и заглавных букв английского алфавита, «{3}» – количество букв, «\d» – диапазон цифр от 0 до 9, «{2}» – количество цифр.

В разделе «Эталонные документы» можно загрузить образец документа, поиск совпадений с которым ведется в анализируемом трафике. Для каждого документа можно настроить порог цитируемости – процент совпадающих данных, достаточных для отнесения текста к эталону.

В разделе «Бланки» содержаться эталоны текстовых документов с полями для заполнения, которые необходимо обнаружить при анализе.

В разделе «Печати» хранятся образцы печатей. Для добавления печати в Систему необходимо, чтобы изображение печати было не меньше 500х500 пикселей, она должна находиться на белом фоне и иметь сплошную рамку по периметру. Если печать треугольная, ее необходимо расположить основанием вниз.

Выгрузка из БД – часть базы данных, совпадение с которой будет искать Система в трафике. Пример выгрузки из базы данных – список контактов сотрудников.

Графический объект - изображение, присутствие которого в трафике будет детектироваться Системой.

1. Объекты защиты

Объект защиты – набор элементов технологий, используемых для поиска совпадений анализируемых данных с выбранными. Они используются при создании политик безопасности. Для добавления нового объекта защиты необходимо выбрать элементы технологий, на основе которых будет проводиться анализ.

1. Персоны

Раздел содержит справочник персон и компьютеров информационной системы организации (рисунок 2).

1. Политики

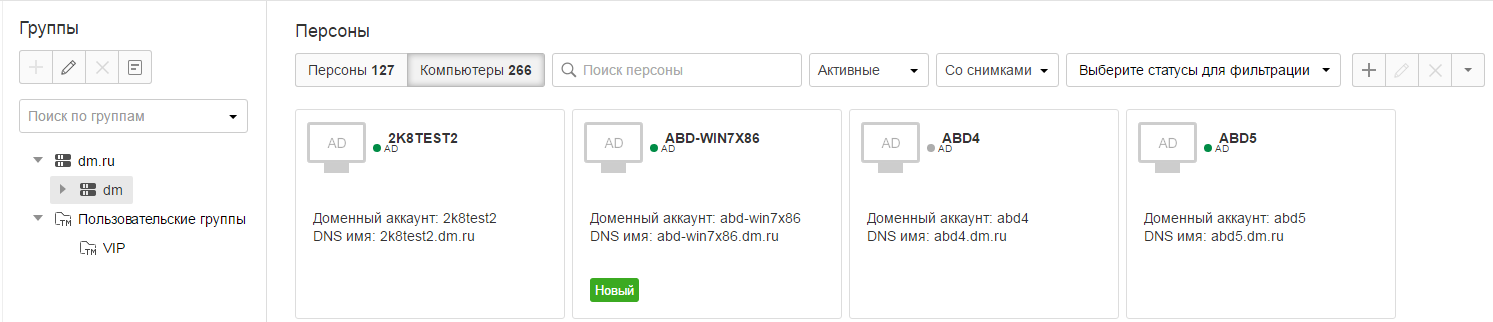


Рисунок 2.  
Раздел «Персоны»

Политики – список правил, в соответствии с которым идет анализ и обработка трафика (рисунок 3).

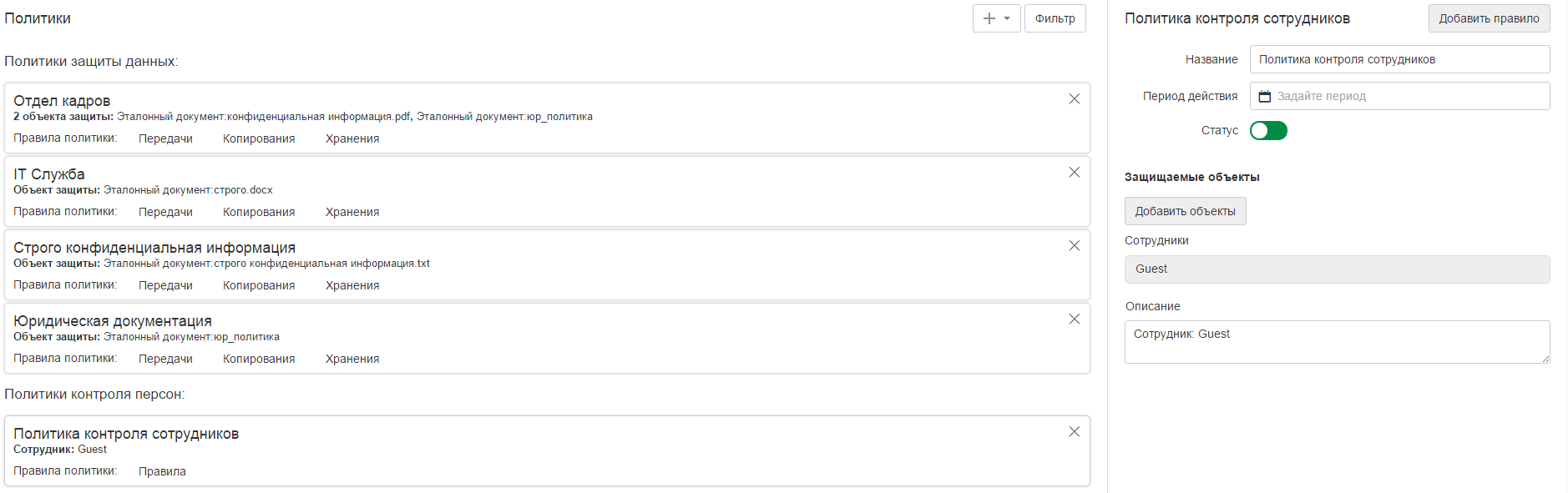


Рисунок 3.  
Раздел «Политики»

Политики разделены на три вида:

* политика защиты данных – действует на всю систему
* политика защиты данных на агентах – применяется непосредственно на агентах Device Monitor
* политика контроля персон – распространяется только на действия указанных персон.

Для создания новой политики нужно:

1. В верхней части рабочей области нажать «Добавить политику**»** и в раскрывающемся списке выбрать нужный тип правил.
2. Указать атрибуты политики:
   * Название
   * Описание
   * Статус
   * Период действия
3. Выбрать защищаемые данные из списка объектов защиты. По умолчанию политика распространяется на все данные.
4. Добавить правила.

|  |  |
| --- | --- |
| Таблица 3. Виды политик | |
| **Политика** | **Правило** |
| Защита данных | Передача |
| Копирование |
| Хранение |
| Буфер Обмена |
| Защита данных на агентах | Передача |
| Копирование |
| Контроль персон | Правила |

1. Списки

Раздел содержит следующие справочники:

* *Теги* используют при создании политик безопасности для сортировки нарушений.
* *Веб-ресурсы* – список сайтов, которые Система будет определять нецелевое использование рабочего времени.
* *Статусы* указываются для персон. Примеры статусов – под наблюдением; на испытательном сроке.
* *Периметры* нужны для разграничения организации на структурные единицы. Разграничение можно производить по доменам, группам персон и компьютеров.
* *Файловые типы* – набор типов файлов, которые будет детектировать Система.

1. Управление

Раздел Управление содержит следующие подразделы:

* LDAP-синхронизация   
  Синхронизация с LDAP-сервером. Сервер обычно используют для хранения учетных записей пользователей.
* Лицензии  
  В подразделе хранится информация о текущей и предыдущих лицензиях InfoWatch Traffic Monitor и инструменты для работы с ней. По истечении срока действия лицензии в этом разделе можно загрузить новую, а также узнать токен для синхронизации с программой InfoWatch Device Monitor.
* Управление доступом  
  Создание ролей для работы с системой InfoWatch Traffic Monitor с указанием прав для сотрудников.
* Состояние Системы  
  Состояние серверов, на которых развернута система Traffic Monitor.
* Аудит  
  Аудит позволяет отслеживать действия пользователей в консоли управления Traffic Monitor.
* Контроль целостности  
  Подраздел предназначен для отслеживания состояния системных файлов.
* Службы  
  Подраздел позволяет управлять службам Linux, не используя командную строку.
* Плагины  
  Плагины позволяют подключать дополнительные перехватчики.

1. Краулер

Краулер проверяет файлы на наличие нарушений политик безопасности. При выявлении нарушения подсистема информирует об инциденте.

Глава 2. Разбор заданий

* **Модуль 1. Установка и настройка системы**

*Необходимо установить InfoWatch Traffic Monitor версии Enterprise с базой данных PostgreSQL в среде VMWare ESXi, InfoWatch Device Monitor + Agent.*

Участнику дают ссылку на VMWare ESXi, на котором находятся 2 виртуальные машины. На первой необходимо установить операционную систему Linux RedHat версии Enterprise вместе с программой InfoWatch Traffic Monitor, на второй виртуальной машине, на которой установлен Windows Server 2012, находятся дистрибутивы PostgreSQL и InfoWatch Device Monitor.   
  
Начинаем установку Traffic Monitor, так как она занимает больше времени. Запускаем виртуальную машину и попадаем в начало установки (рисунок 4). Нам нужна версия Enterprise, выбираем соответствующий пункт в первом окне. Далее выбираем базу данных PostgreSQL, как и указано в задании. В третьем окне выбираем All-in-one – база данных и Traffic Monitor.

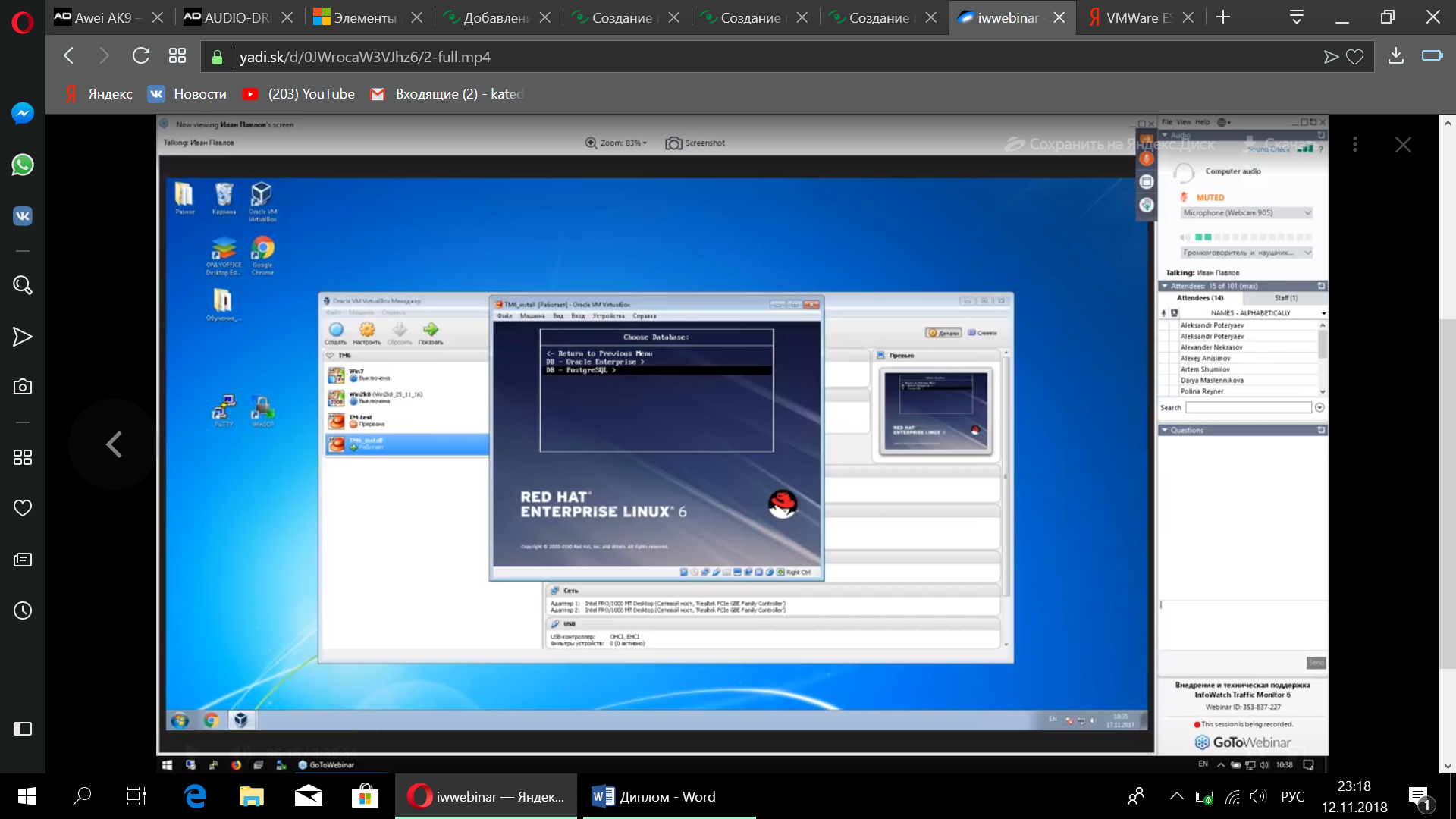
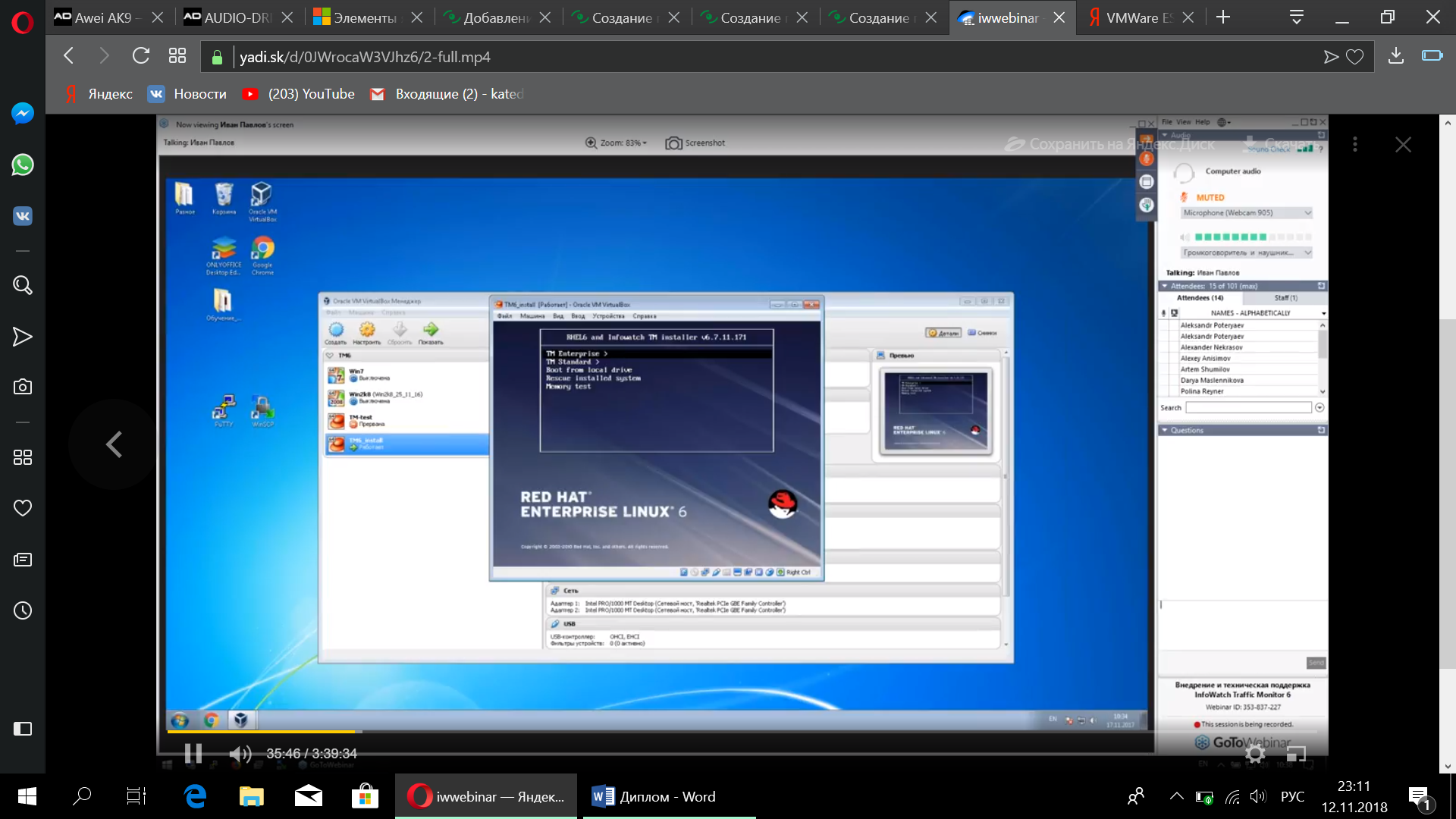
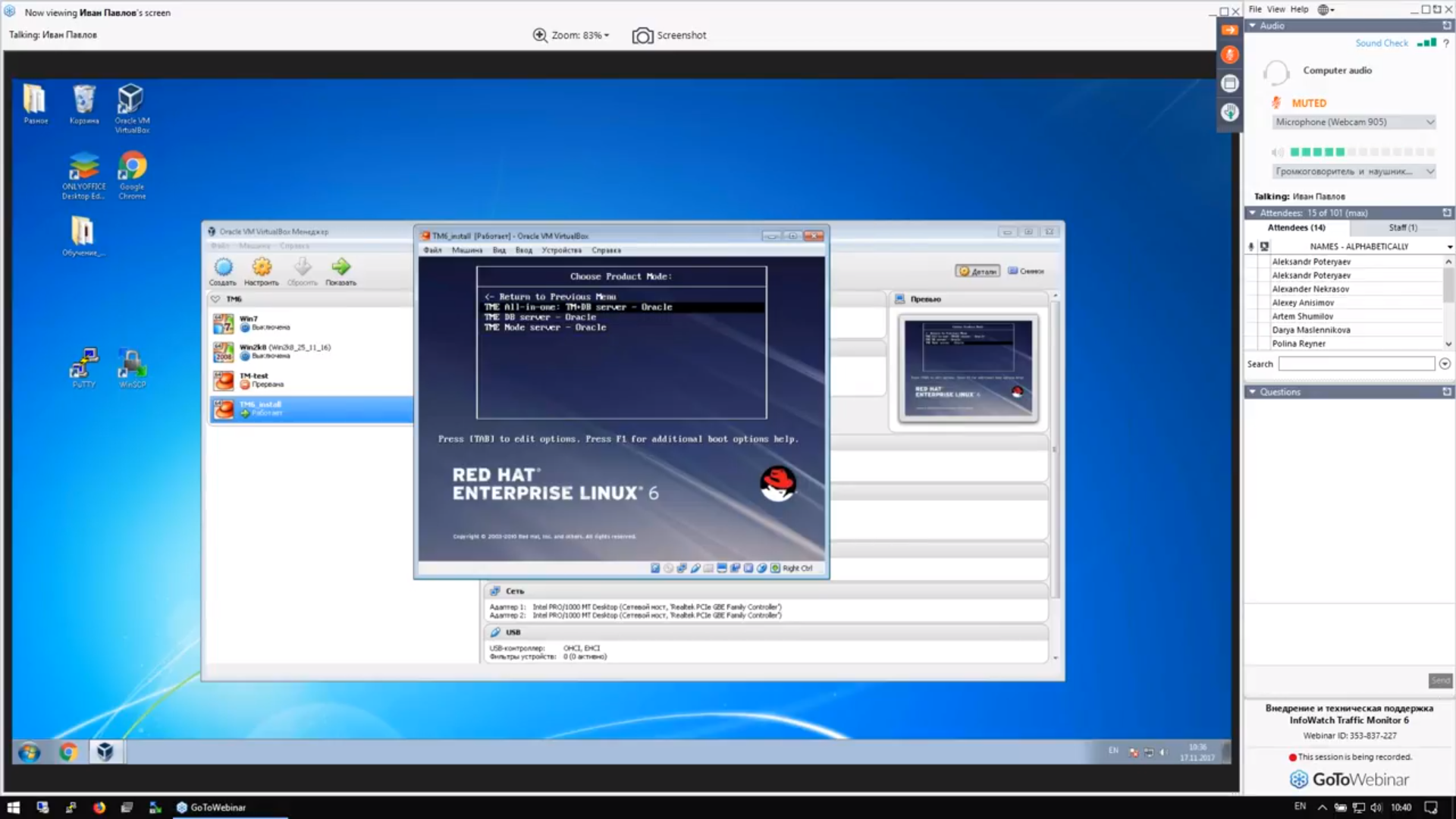


Рисунок 4.  
Установка InfoWatch Traffic Monitor

Следующий пункт – выбрать часовой пояс, а именно Московский. Затем нужно задать пароль для привилегированного пользователя в соответствии с заданием (если Вы ошиблись при заполнении пароля, создайте файл на рабочем столе с верным паролем, чтобы организаторы смогли проверить Вашу работу). Тип установки – Use all space. После этого последует ряд настроек, которые не нужно изменять, а затем начнется установка (установка занимает большое количество времени. Во время нее можно начать установку базы данных на второй виртуальной машине. Главное помните, что до полной установки нельзя ничего делать с системой, иначе Вам придется начать все заново).

Когда закончится установка, необходимо войти в привилегированного пользователя и узнать ip-адрес Traffic Monitor (команда ifconfig). Этот адрес вводим в браузере и попадаем на страницу Traffic Monitor, где нужно авторизоваться. Далее заходим в раздел Статусы, выбираем пункт Лицензии. Нажимаем добавить лицензию и загружаем ее с рабочего стола. В этом же разделе находится токен для связи Traffic Monitor и Device Monitor.

Переходим к установке PostgreSQL на второй виртуальной машине. При установке все настройки нужно оставить по умолчанию, и нужно будет только задать пароль для администратора базы данных в соответствии с заданием.

Начинаем установку программы Device Monitor (все настройки оставляем по умолчанию, кроме тех, которые описаны далее). В окне «Тип устанавливаемого сервера» выбираем пункт «Основной сервер» и «Установить новую базу данных», обязательно убрать выделение с пункта «Опубликовать сервер в Active Directory». В окне «Выбор базы данных» выбираем PostgreSQL, в следующем окне в пункте «Сервер БД» пишем «localhost», имя базы данных задаем любое, а в имени пользователя пишем «postgres» (логин администратора в PostgreSQL). В «Настройках защищенного канала» создаем новый ключ, сохраняем его в любом месте. Далее в «Настройках учетной записи сервера» выбираем «Local System», в следующем окне создаем учетную запись администратора в соответствии с заданием. В «Настройках соединения с Traffic Monitor» прописываем адрес сервера, на котором находится программу, вводим токен из раздела «Лицензии». Если установка Traffic Monitor еще не завершена, то выбираем пункт «Работать в автономном режиме», после окончания установки запускаем программу, во вкладке «Инструменты» заходим в пункт «Настройки», затем «Серверы», снимаем выбор с пункта «Работать в автономном режиме», и прописываем адрес сервера и токен лицензии.

Далее нужно создать пакет установки агента Device Monitor. Для этого заходим в программу Device Monitor, во вкладке «Инструменты» заходим в пункт «Создать пакет установки», выбрать в первом окне место, в которое установится пакет. Остальные настройки оставляем по умолчанию. Созданный пакет переносим на ноутбук и устанавливаем на нем агента.

* **Модуль 2, 3. Разработка политик безопасности, Поиск и предотвращение инцидентов**

*Задание № 1*

*Необходимо ввести под наблюдение руководителя отдела кадров.*

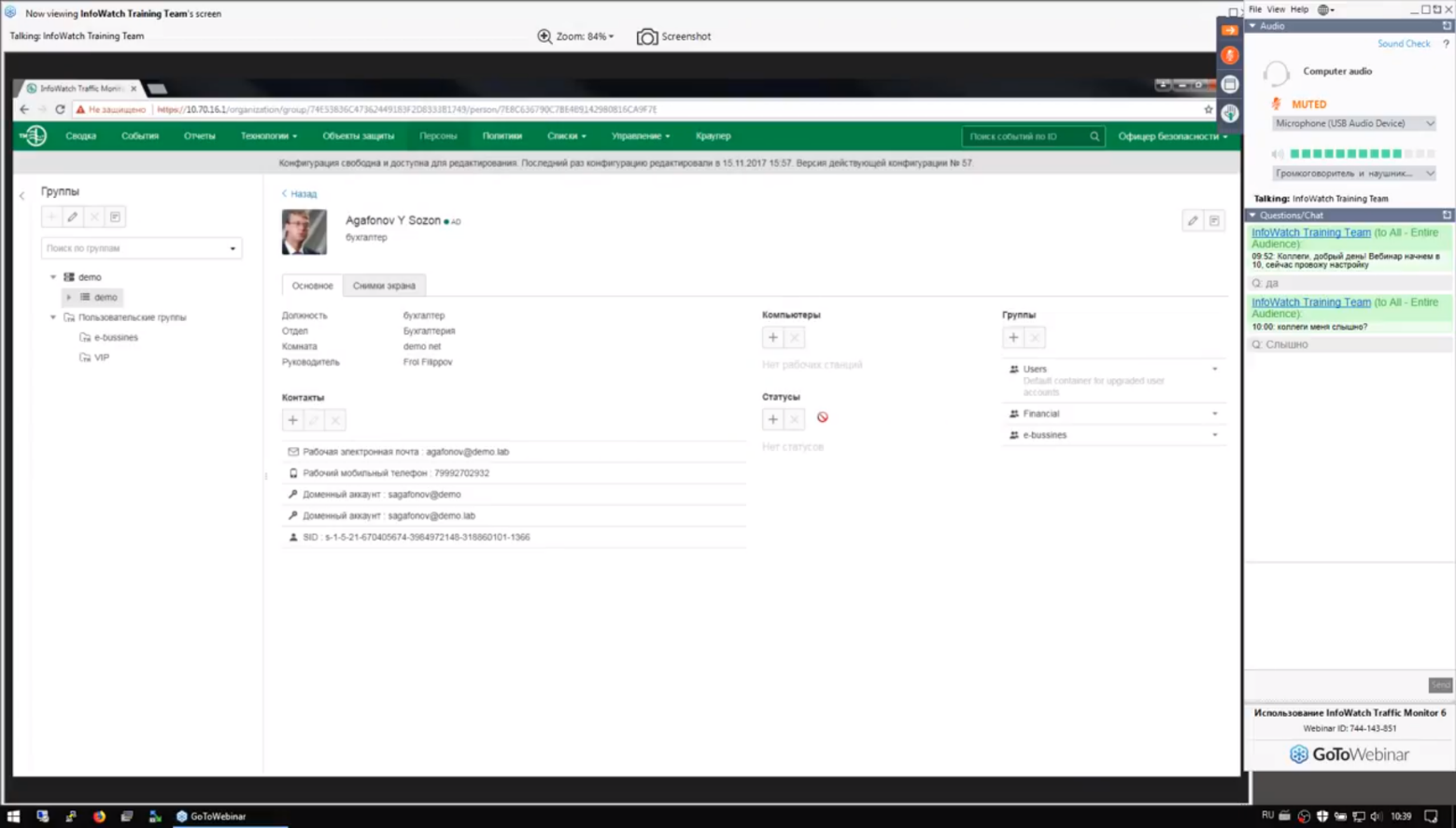
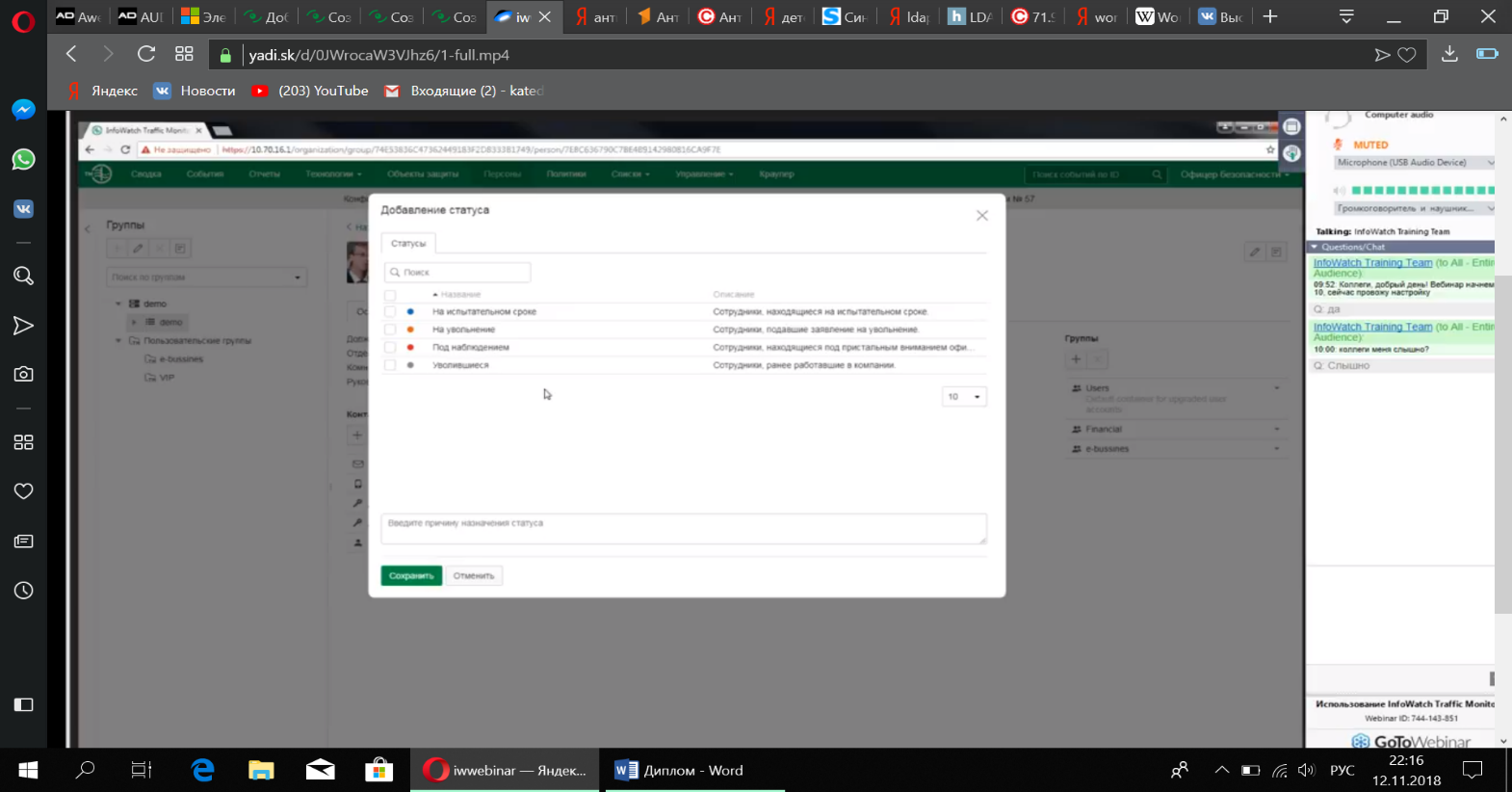


Рисунок 5.  
Редактирование профиля сотрудника

Заходим в раздел «Персоны» и ищем руководителя отдела кадров в списке сотрудников. Заходим в его профиль и в пункте «Статус» выбираем статус «Под наблюдением».

*Задание №2*

*Сотрудникам запрещено отправлять паспортные данные, в том числе сканы и фото паспортов РФ за пределы компании.*

Создаем новый объект защиты «Паспортные данные». Добавляем в него стандартный текстовый объект, содержащий шаблон паспортных данных, а также добавляем стандартный графический объект «Скан паспорта». Далее необходимо создать политику защиты данных на правило передачи. В настройке правила выбираем все возможные способы передачи, прикрепляем созданный ранее объект защиты, а также запрещаем передачу. Применяем политику и проверяем ее работоспособность.

*Задание № 3*

*Необходимо запретить передачу информации о мандаринах, лимонах, апельсинах и просто о цитрусовых к генеральному директору компании (у него на них аллергия). Стоит учесть морфологию и прочие варианты написания, а также единственное или множественное употребление данных слов.*

В разделе Технологии заходим в «Категории и термины», создаем новую категорию и называем ее «Цитрусовые». В нее добавляем термины, указанные в задании «Мандарин», «Лимон», «Апельсин», «Цитрусовые». Для каждого термина в настройках выбираем пункты характеристический (нужно для того, чтобы при обнаружении Системой указанного слова в тексте она относила его к данной категории), учитывать морфологию (для того, чтобы Система могла детектировать формы слова) и выбираем язык термина – русский.

Следующий шаг – создать объект защиты, в который нужно добавить каталог «Цитрусовые». Далее создаем политику защиты данных для правила передачи. В настройке правила выбираем все возможные способы передачи, а также прикрепляем созданный ранее объект защиты.  
 *Задание №4*

*Необходимо предотвратить передачу любых стандартизированных паролей в открытом виде любыми отправителями и получателями. Стандартизированные форматы паролей (кириллица):*

*6 букв – 2 цифры – 3 буквы – 2 знака ? или ! (например, ПаРолЬ67рКЕ!? )*

В разделе «Технологии» создаем новый текстовый объект. Для нового объекта указываем шаблон [А-Яа-я]{6}\d{2}[ А-Яа-я]{3}\W{2}. В разделе «Объекты защиты создаем» новый объект и прикрепляем к нему шаблон паролей. В разделе «Политики» создаем правило передачи для политики защиты данных. Выбираем все виды передачи данных, прикрепляем объект защиты и применяем политику.

*Задание № 5*

*Необходимо отслеживать финансовые документы на базе стандартных объектов защиты «Финансовая информация». Уровень угрозы низкий, не блокировать.*

Создаем политику защиты информации и добавляем правила передачи, копирования, хранение и буфера обмена для нее. Для каждого правила указываем низкий уровень угрозы, для действия системы выбираем не блокировать, а также прикрепляем стандартный объект защиты «Финансовая документация». Применяем политику и проверяем ее работу.

*Задание № 6*

*Необходимо настроить новую категорию веб-ресурсов и внести в нее следующие сайты: kb.infowatch.com, digitalskills.ru, vmware.com*

В разделе «Списки» выбираем подраздел «Веб-ресурсы». В нем создаем новую категорию и вносим в нее указанные в задании сайты. Проверяем наличие событий в Систем при использовании данных сайтов.

* **Модуль 4. Технологии агентского мониторинга**

*Раздел 1*

*Необходимо заблокировать использование блокнота на компьютерах пользователей.*

В программе Device Monitor заходим в раздел «Приложения», создаем новый список и добавляем в него программу Блокнот из стандартного списка приложений (если там нет программы, то нужно запустить ее на ноутбуке и она появится в списке). В разделе «Правила» создаем правило Application Monitor (рисунок 6). В пункте «Блокирование запуска приложений» в черный список добавляем созданный ранее список приложений с блокнотом. Применяем правило и проверяем его работу.

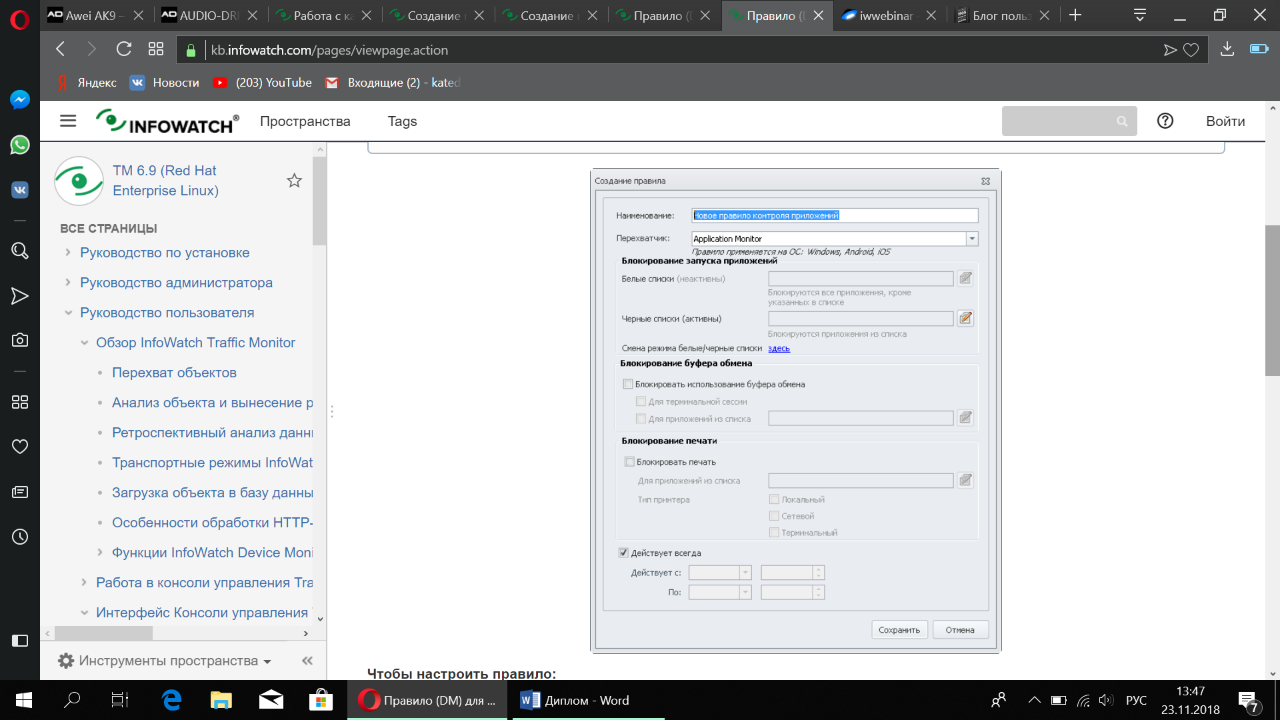


Рисунок 6.  
Правило Application Monitor

*Раздел 2*

*Необходимо запретить буфер обмена в WordPad.*

В программе Device Monitor заходим в раздел «Приложения», создаем новый список и добавляем в него программу WordPad. В разделе «Правила» добавляем правило Application Monitor. Выбираем пункт «Блокировать использование буфера обмена для приложений из списка» и добавляем созданный ранее список приложений с WordPad. Применяем правило и проверяем его работу.

*Раздел 3*

*Необходимо запретить запись на USB-flash носители.*

В программе Device Monitor создаем правило Device Monitor (рисунок 7)и выбираем тип устройства «Съемное устройство хранения», в области «Доступ» выбираем пункт «Только чтение». Сохраняем правило и проверяем его действие.

*Раздел 4*

*Необходимо заблокировать возможность снятия скриншотов в текстовых процессорах MS Word и Libre Office Writer.*

В программе Device Monitor заходим в раздел «Приложения», создаем новый список и добавляем в него программы MS Word и Libre Office Writer. Далее создаем правило **ScreenShot Control Monitor (рисунок 8), выбираем пункт «Если запущены приложения» и прикрепляем наш список.**

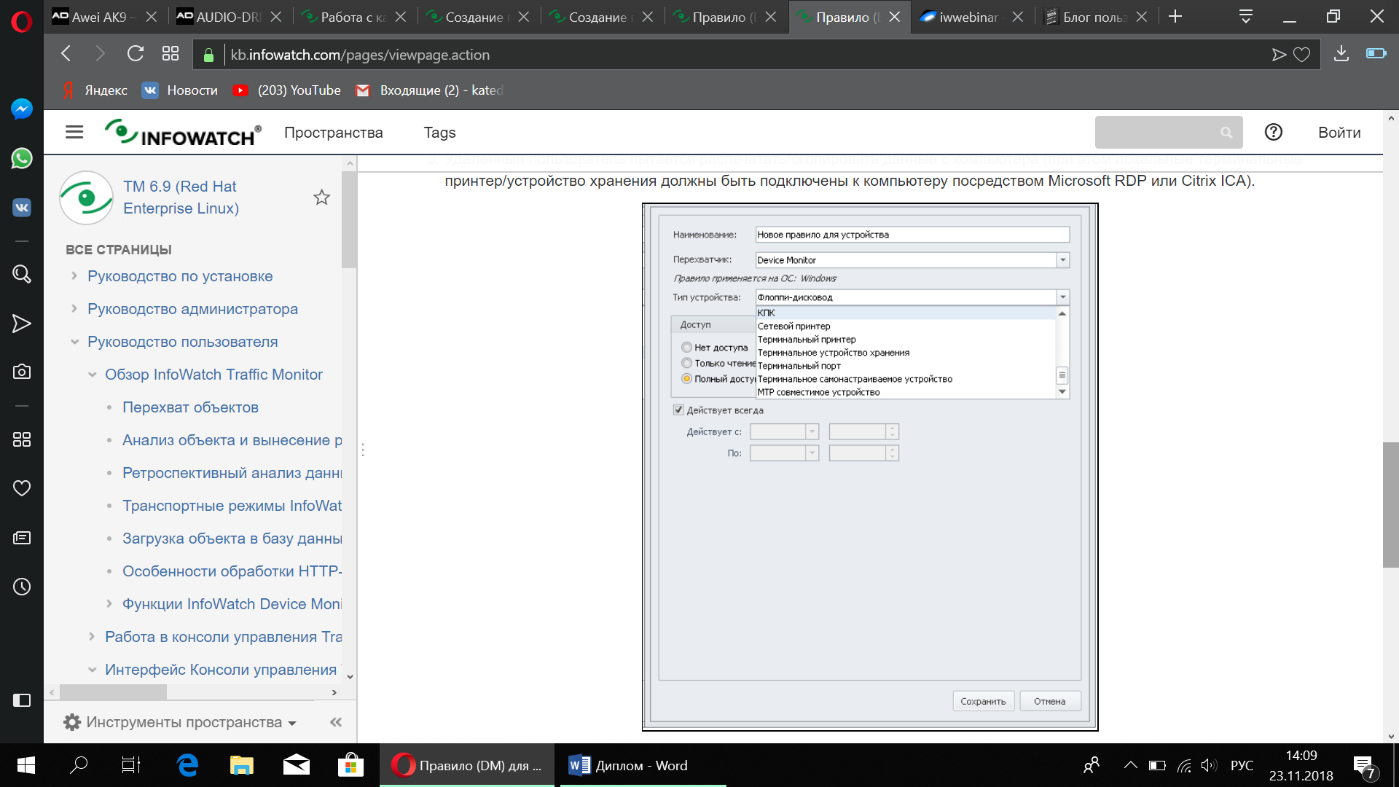


Рисунок 7.  
Правило Device Monitor

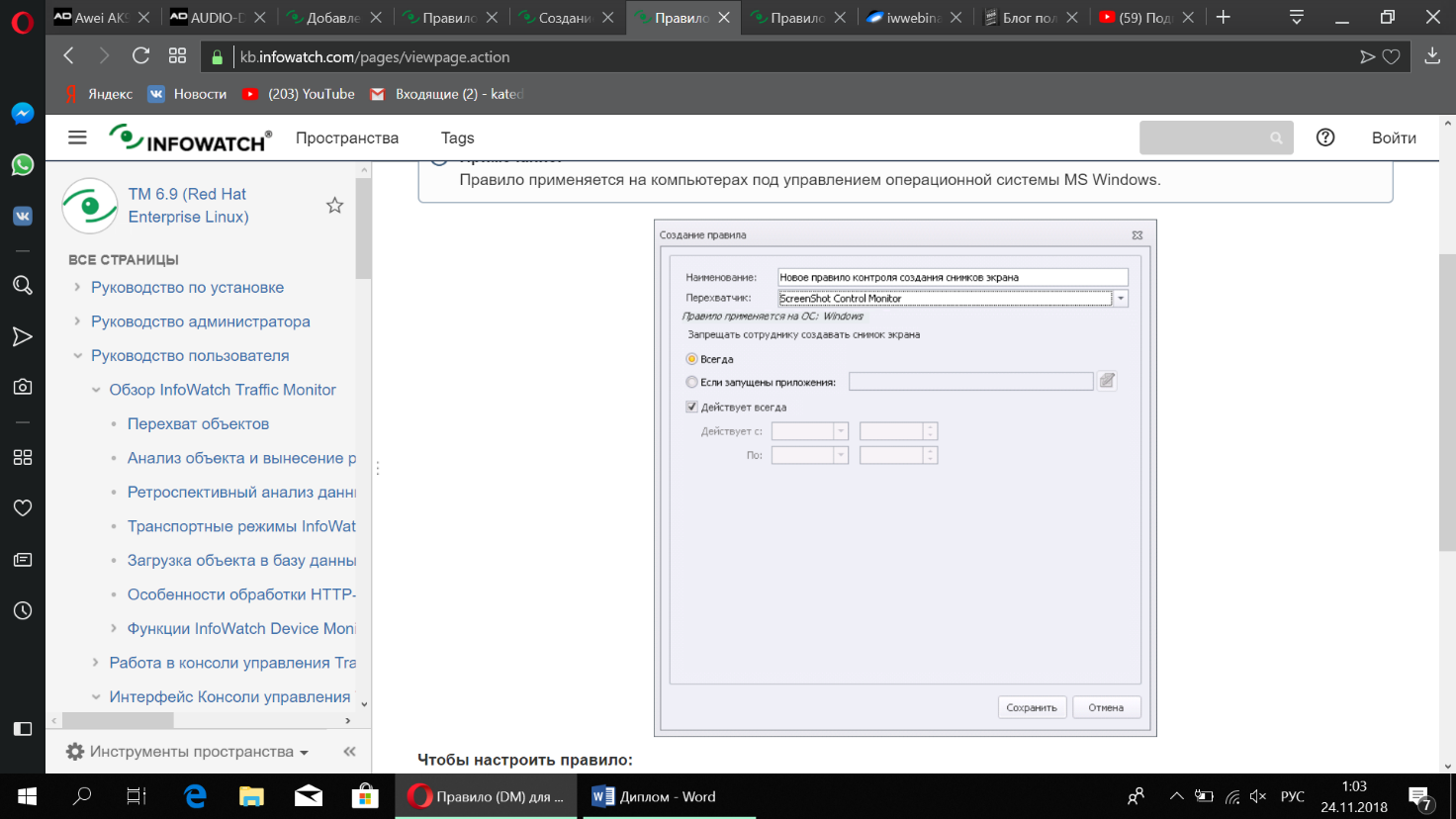


Рисунок 8.  
Правило **ScreenShot Control Monitor**

* **Модуль 5. Анализ выявленных инцидентов**

*Раздел 1*

*Необходимо создать новую панель сводок на главной странице в разделе «Сводка» и назвать ее «Сводка».*

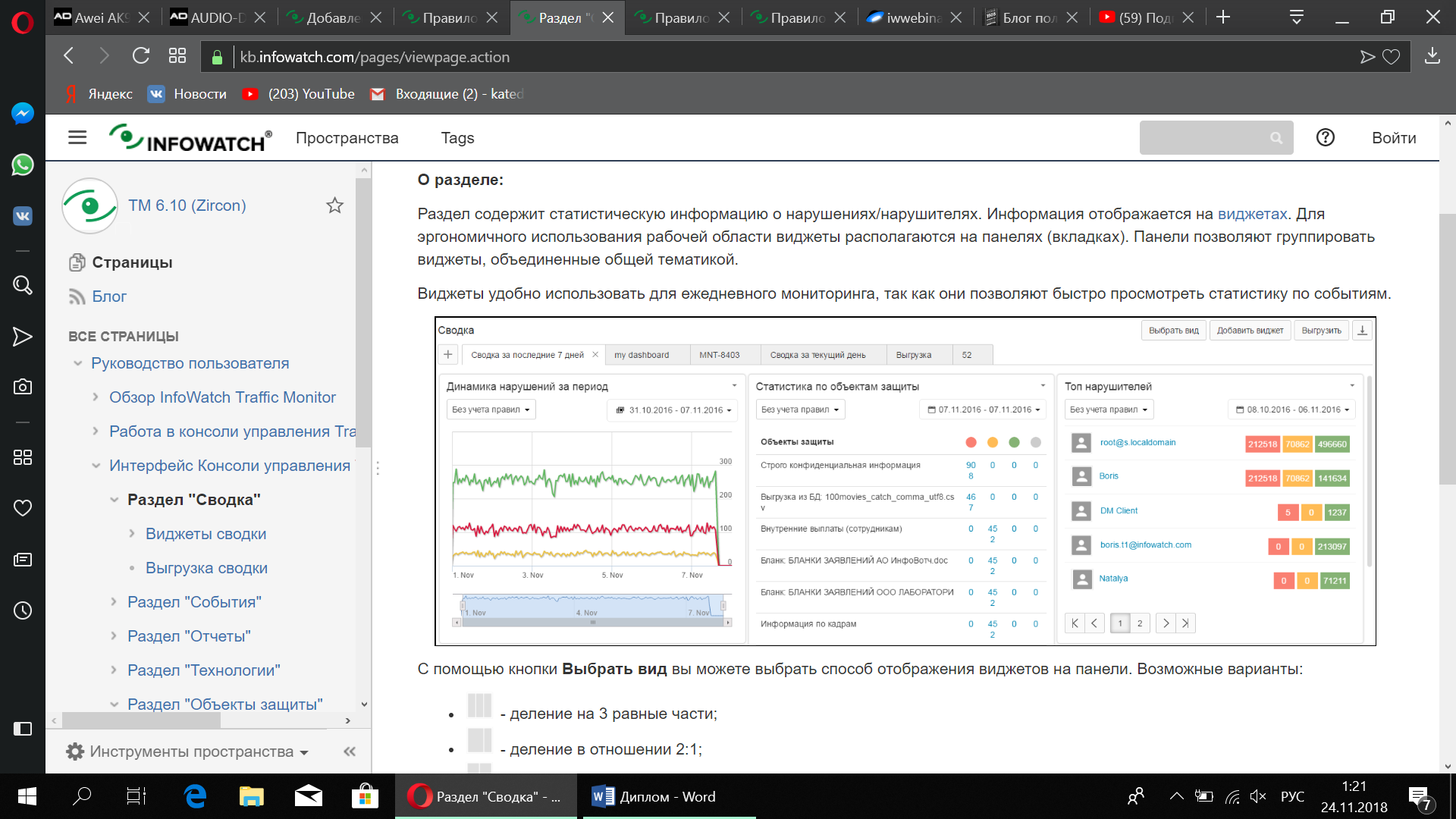


Рисунок 8.  
Раздел «Сводка»

Для создания новой сводки нажимаем на «+» (рисунок 9), указываем ее название и сохраняем.

*Раздел 2*

*Необходимо сформировать новые отчеты в ранее созданной сводке по следующим критериям:*

*1. Динамику нарушений за последние три дня*

*2. Статистику по политикам за последние три дня*

*3. Необработанные нарушения за последние три дня*

В разделе «Сводка» выбираем пункт «Добавить виджет» и указываем нужный тип виджета в соответствии с заданием. Для каждого из них в настройках указываем период за последние три дня.

* **Модуль 6. Исследование организации**

*Используя данные, полученные из каталога LDAP, отчетов в системе InfoWatch Traffic Monitor, а также на основе созданных ранее политик и выданной информации о компании, участнику необходимо создать отчет в заданном виде.*

В отчете нужно оформить титульный лист по заданным критериям, добавить информацию об указанных сотрудниках (данные можно взять из раздела «Персоны»), а также нужно будет написать развернутый ответ по указанной проблеме. К примеру, могут попросить рассказать каким образом InfoWatch Traffic Monitor помогает избежать утечки информации, тогда одним из вариантов ответов будет:InfoWatch Traffic Monitor анализирует циркулирующий в компании трафик и ищет совпадения с текстовыми и графическими объектами.

**Заключение**

В заключении хочу дать несколько советов на основе опыта участия в соревновании:

* Если у вас есть возможность, сходите на курсы подготовки к соревнованию. Вам более подробно расскажут о настройках политик и установке программ, и вы сможете самостоятельно поработать с ними и задать интересующие вопросы специалистам.
* При выполнении задания начните с тех пунктов, в которых вы уверены, затем те, которые вы частично знаете. На соревновании у вас будет доступ в Интернет, и вы сможете посмотреть что-нибудь на сайте kb.infowatch.com, однако вы можете потерять много времени и не успеть сделать другие задания. Баллы могут давать и за не полностью выполненный пункт.
* Внимательно читайте задания, чтобы не упустить детали, например, пароль, который нужно задать пользователю или как правильно называть политики.
* Если у вас возникла неполадка во время соревнований, обратитесь к техническому специалисту, так как в случае неполадки со стороны организатора вам остановят время и устранят неполадку или, если проблему нельзя решить, у вас не будут снимать баллы за то задание, которое вы не сможете сделать из-за неполадки.
* Обязательно проверяйте работу каждой настраиваемой политики.
* Если вы обнаружите среди стандартных политик правило похожее на то, которое требуется создать вам, удалите его. Если вы этого не сделаете, вам могут не поставить баллы.
* Если вы случайно задали не тот пароль или логин, который требуется по заданию, создайте текстовый документ, введите там указанный вами пароль и предупредите об этом своего эксперта, чтобы при проверке не возникло трудностей.

**Источники**

1. Движение WorldSkills. [Электронный ресурс], - Режим доступа:  
    <https://worldskills.ru/o-nas/dvizhenie-worldskills/czel-i-missiya.html>
2. Руководство пользователя InfoWatch. Виджеты сводки. [Электронный ресурс], - Режим доступа: <https://kb.infowatch.com/pages/viewpage.action?pageId=129565867>
3. Руководство пользователя InfoWatch. Виджеты отчетов. [Электронный ресурс],- Режим доступа: <https://kb.infowatch.com/pages/viewpage.action?pageId=129566069>
4. Задание компетенции «Корпоративная защита от внутренних угроз информационной безопасности». [Электронный ресурс],- Режим доступа: <https://ocm18.worldskills.moscow/kompetentsii/#comp_list>