**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ**

Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«ИЖЕВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ  
ИМЕНИ М.Т. КАЛАШНИКОВА»

Институт «Информатика и вычислительная техника»

Кафедра «Защита информации в компьютеризированных системах»

Отчёт

по лабораторной работе №1

по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем»

на тему «Формирование доверенной среды ПО антивирусными средствами защиты»

Выполнил: студент группы С17-361-1

Буров К.А.

Проверил: Кудашев П.А.

Ижевск 2021

**Цель работы:**

Для обеспечения безопасности информации при работе, связанной с использованием автоматизированных рабочих мест, настроить доверенную среду, посредством применения специализированного программного обеспечения в интерактивном режиме с помощью создания правил и запретов для исполняемых процессов.

**Задачи:**

1. Скачать и установить специализированное программное обеспечение.
2. Настроить интерактивный режим работы программы.
3. Для каждого возникающего события определить название процесса, путь до исполняемого файла и на основе его назначения выбрать соответствующее сетевое правило.
4. Настроить системные запреты по умолчанию и при необходимости для каждого конкретного процесса.

**Ход работы**

Для выполнения лабораторной работы была выбрана программа Dr.Web Security Space 12.0, так как она предоставляет все возможности, необходимые для создания доверенной среды, имеет удобный интерфейс и позволяет экспортировать заданные настройки для дальнейшего их переиспользования.

После включения интерактивного режима появляются события (рисунок 1). В уведомлении о событии отображается название самого процесса, путь до исполняемого файла, название удаленного процесса, дата создания, размер, цифровая подпись и предлагается выбор действия.

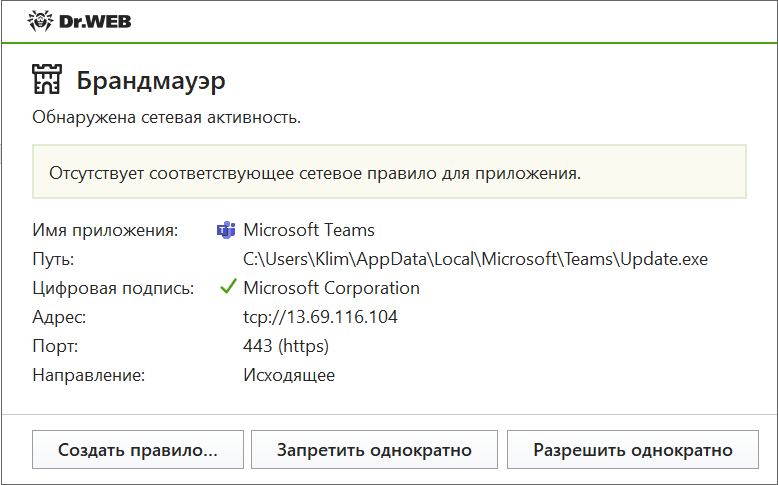


Рисунок . Пример события

Для приложений WinWord.exe. Outlook.exe и Excel.exe были созданы системные запреты (рисунок 2).

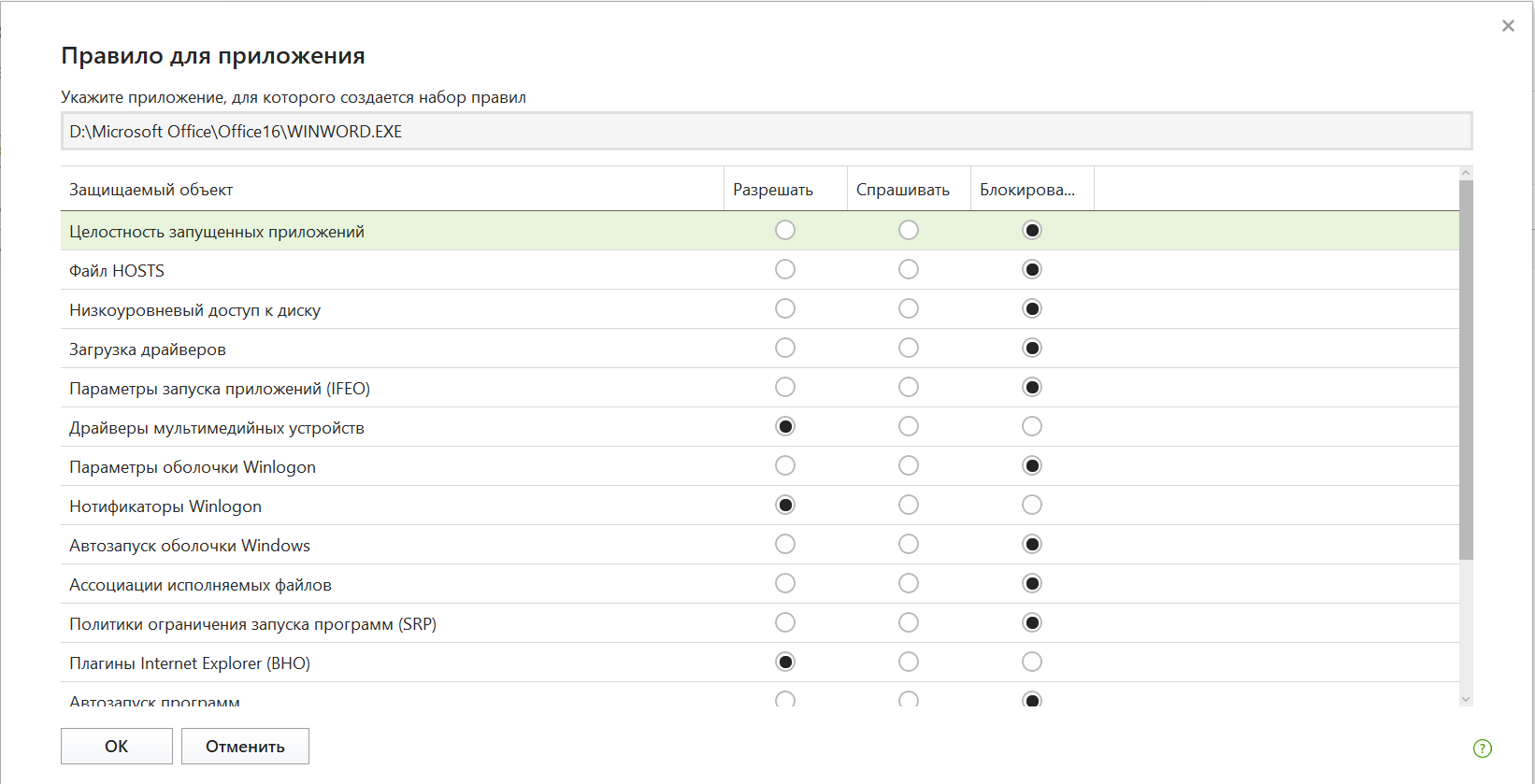


Рисунок . Создание системных запретов

Часть таблицы с описанием настроенных сетевых правил и системных запретов приведена в приложении А, полная таблица в отдельном файле.

**Вывод**

В процессе выполнения лабораторной работы была создана доверенная среда на АРМ, посредством задания сетевых правил и системных запретов для исполняемых процессов. Был получен опыт ручного создания доверенной среды с помощью программного обеспечения Dr.Web Security Space 12.0.

Приложение А



