МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Тульский государственный университет»

Институт прикладной математики и компьютерных наук

Кафедра информационной безопасности

**Исследование программ Adguard, утилит CurrPorts и SmartSniff**

отчёт по лабораторной работе №5

по курсу «Системы обнаружения вторжений»

Выполнили: студенты гр. 230781 \_\_\_\_\_\_\_\_\_ Глейм С.М.

(подпись)

\_\_\_\_\_\_\_\_\_ Ивлев А.Р.

(подпись)

Проверил: асс. каф. ИБ \_\_\_\_\_\_\_\_\_ Чаговец С.Н.

(подпись)

Тула, 2022 г.

**Цель работы**

Изучение и исследование программы Adguard, CurrPorts и SmartSniff.

**Задание на работу**

1. Исследовать эффективность модуля «Антибаннер».
2. Исследовать эффективность модуля «Антифишинг».
3. Исследовать эффективность модуля «Родительский контроль».
4. Установить и исследовать утилиту CurrPorts: вывод данных (пути, версии, файла и времени запуска и соответствующего пользователя ПК) об открытии TCP-порта, закрытие нежелательных подключений, завершение работы процессов.
5. Установить и исследовать утилиту SmartSniff: вывод данных (пути, версии, тип протокола и др.), содержимое передаваемых данных в рамках исследуемого сетевого взаимодействия.

**Ход работы**

Для выполнения работы была установлена программа Adguard.

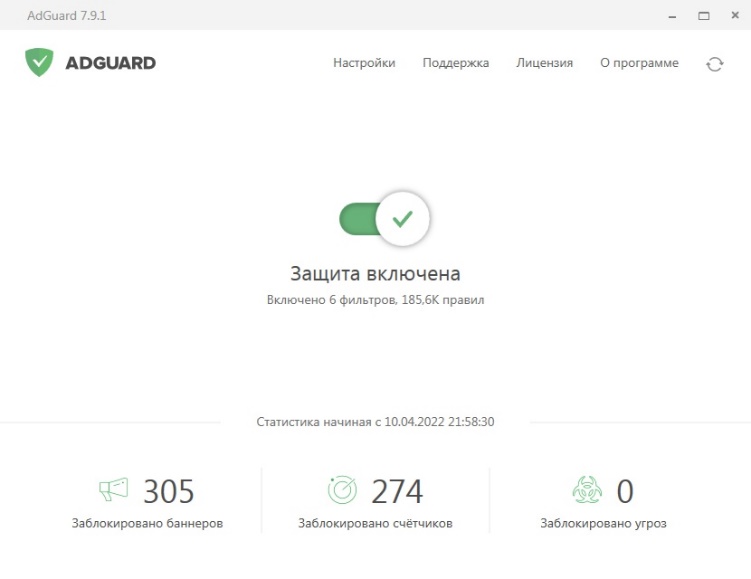


Рисунок 1 - Стартовое окно программы Adguard

После установки была проверена работа модуля «Антибаннер». На рисунках ниже представлена исходная страница и страница с активированной программой.

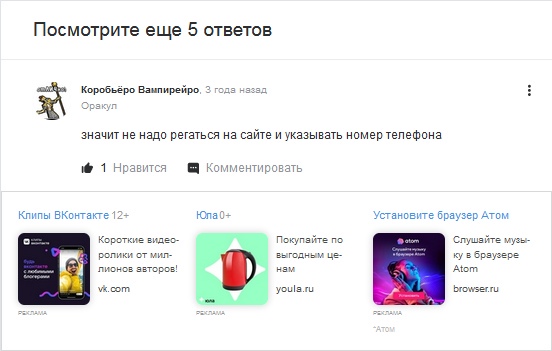


Рисунок 2 - Страница при не рабочей программе Adguard

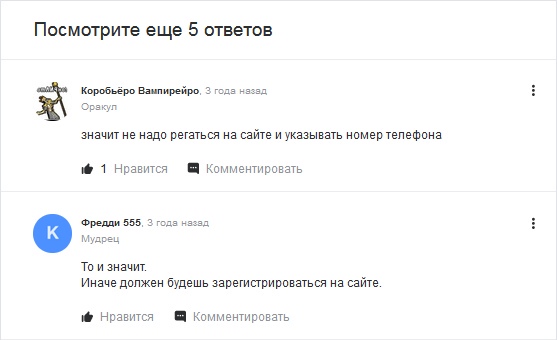


Рисунок 3 - Страница сайта при включенной программе Adguard

Данный пример демонстрирует работу модуля «Антибаннер».

При попытке зайти на фишинговую страницу модуль программы «Антифишинг» заблокирует страницу и покажет предупреждение.

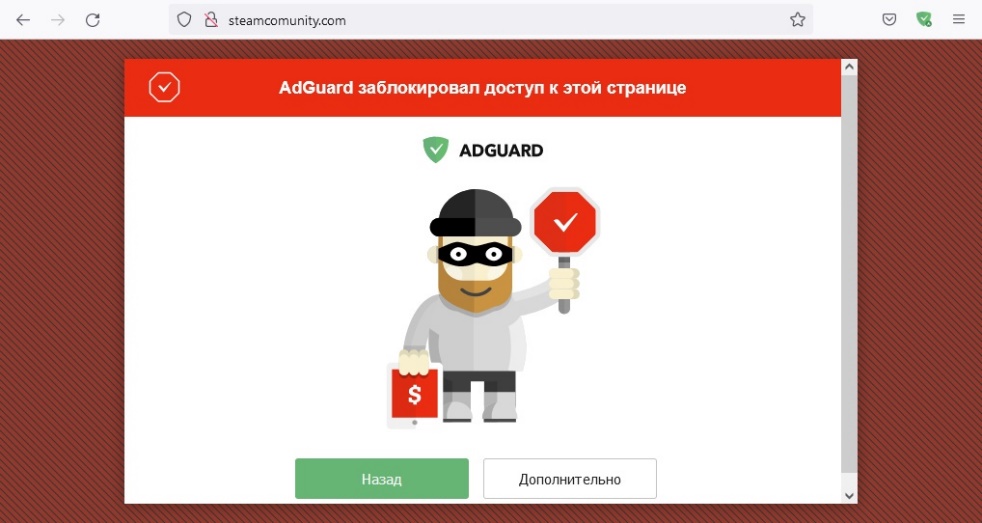


Рисунок 4 - Заблокированная фишинговая страница

Затем был проверен на эффективность модуль «Родительский контроль». С помощью этого модуля можно настроить черный и белый списки сайтов, которые запрещают и разрешают доступ соответственно. На рисунках ниже представлены примеры работы этого модуля.

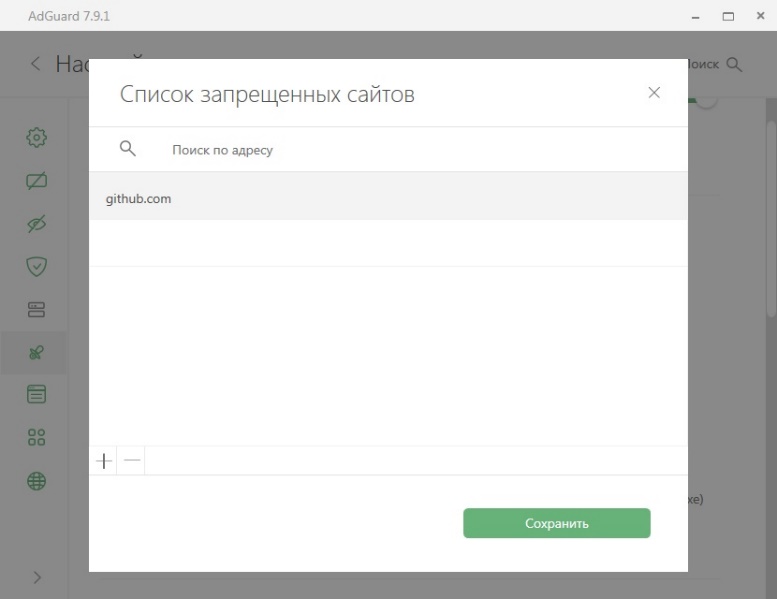


Рисунок 5 - Редактор черного списка сайтов

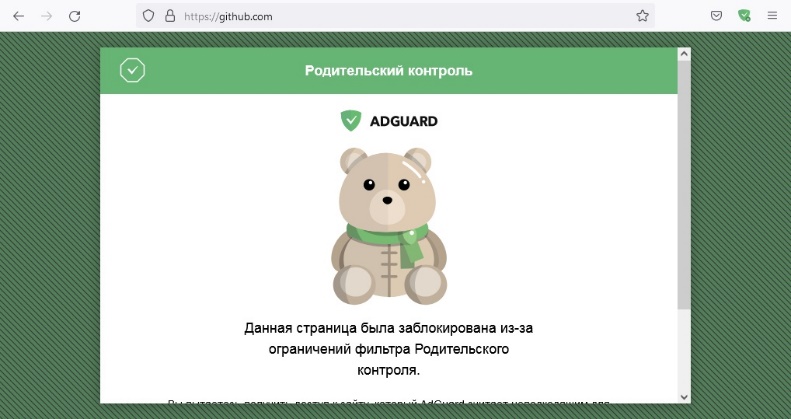


Рисунок 6 - Попытка перехода на сайт из черного списка

Также была установлена и опробована утилита CurrPorts. С её помощью была получена информация о портах, которые используются различными процессами.

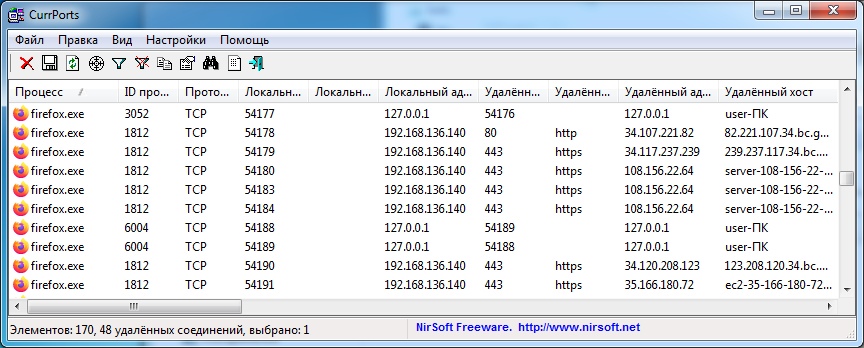


Рисунок 7 - Информация о привязанных к процессам портах в утилите CurrPorts

Утилита SmartSniff представляет собой сниффер пакетов без разделения на установленные адаптеры (т.е. все перехваченные пакеты просматриваются формате диалога клиент-сервер). На рисунке ниже представлены результаты работы программы.

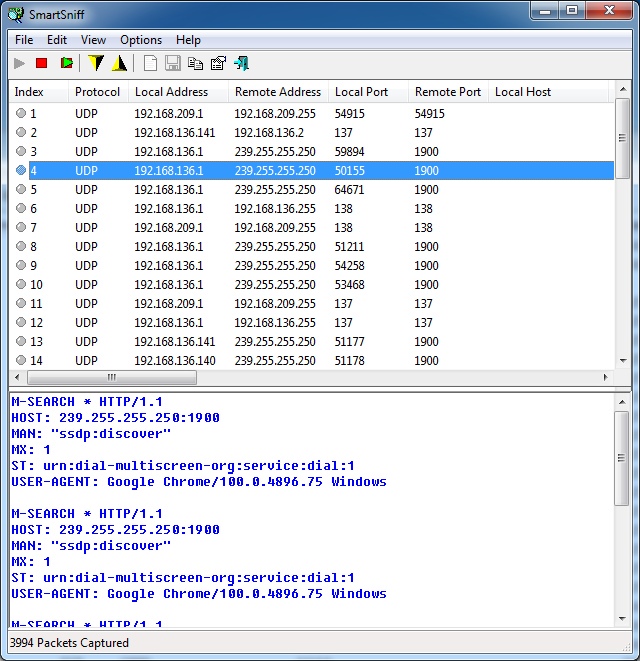


Рисунок 8 – Перехваченный траффик утилитой SmartSniff

Вывод: были изучены и исследованы программа Adguard и утилиты CurrPorts и SmartSniff. Данные программные средства обеспечивают безопасность при поиске в сети Интернет.