Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра ИИТ

Лабораторная работа №2

По дисциплине: «Безопасность компьютерных систем и сетей»

Тема: «Настройка брандмауэра.»

Выполнил:

Студент 4 курса

Группы ПО-7

Комиссаров А.Е.

Проверил:

Самолюк О.Ю.

2023

**Цель:** обучение подбору программных средств защиты сетевого соединения компьютера в рабочем окружении операционной системы Windows и научиться пользоваться выбранным средством.

**Ход работы:**

1. Проведём анализ доступного ПО на рынке и выберем брандмауэр для своей системы. В процессе поиска доступных и совместимых средств защиты были выделены следующие:

**ZoneAlarm**

ZoneAlarm — это хорошо известный брандмауэр с простым в использовании интерфейсом. За дружественным интерфейсом есть множество функций, которые могут удовлетворить требования даже самых требовательных пользователей .

**TinyWall**

TinyWall — очень простое приложение, которое работает со встроенным межсетевым экраном . Он не имеет раздражающих всплывающих окон, а установочный пакет очень маленький (чуть более 1 МБ ).

**Outpost Firewall**

Этот брандмауэр повышает уровень безопасности вашей системы, не влияя на ее производительность . Интерфейс прост и интуитивно понятен. Вы можете установить ограничения для программ, которые вы устанавливаете на свой компьютер, и настроить уровень безопасности. Outpost Firewall имеет 4 уровня безопасности, которые полностью настраиваются. По умолчанию « Оптимальный » параметр отслеживает только самые опасные действия, такие как инъекции памяти, расширения оболочки, настройки Интернета и многое другое.

Вы можете настроить уровни, нажав на кнопку Настройки / Защита хоста / Настроить.

Этот брандмауэр предлагает очень интуитивную систему безопасности . Единственный недостаток бесплатной версии — большое количество рекламы, но это незначительно по сравнению с дополнительным уровнем безопасности, который она добавляет в вашу систему.

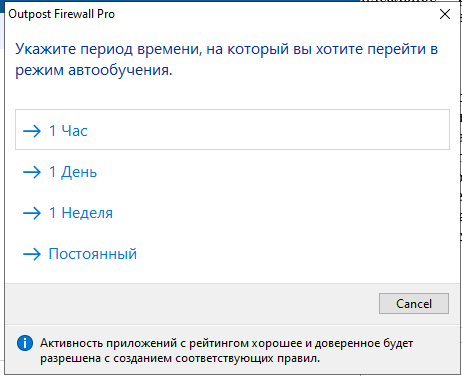
**Emsisoft Anti-Malware**

Этот брандмауэр имеет надежную систему сканирования с выдающимся уровнем HIPS. Его основная функция называется « Выполнить безопаснее », которая позволяет устанавливать различные ограничения для любого процесса , включая веб-браузеры , программы чтения электронной почты , мультимедийные программы, менеджеры загрузки и многое другое.

**Comodo Firewall**

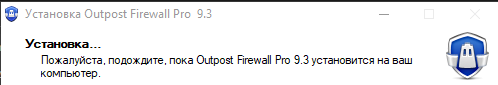
Comodo Firewall — это проактивный брандмауэр с надежной защитой HIPS , идеальное решение для пользователей, которым необходим надежный дополнительный уровень безопасности . Последняя версия этой программы подходит для всех пользователей , опытных и начинающих пользователей .

Выбор пал на Outpost Firewall в виду его удобной системы всплывающих окон, эта программа запоминает выбор пользователя при появлении нового соединения и называет это “самообучающаяся система”. После первых 24 часов программа разрешает соединение только тем программам, которые пользователь разрешил в процессе обучения, остальные блокирует. Процесс обучения можно начать заново на разные периоды времени:

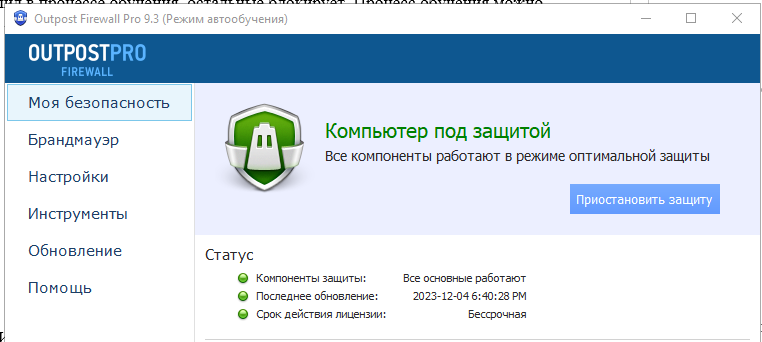


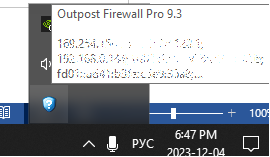
1. Изучить документацию на ПО и установить в систему

Ссылка на скачивание была получена на стороннем ресурсе ввиду присутствия там полной русской версии приложения. Размер ПО – 50мб. Начинаем процесс установки.



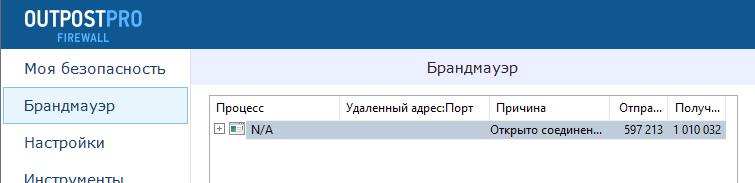
После краткого процесса установки брандмауэр запущен и работает.



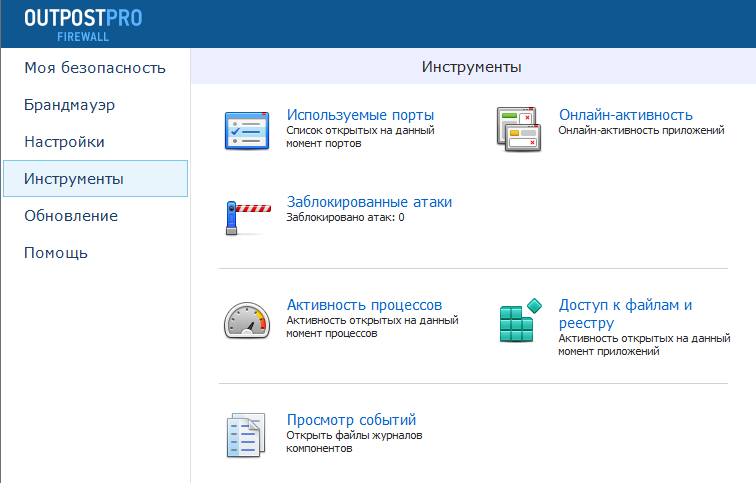


1. Разберем функциональность данного брандмауэра. Проведём настройку ПО для защиты системы.

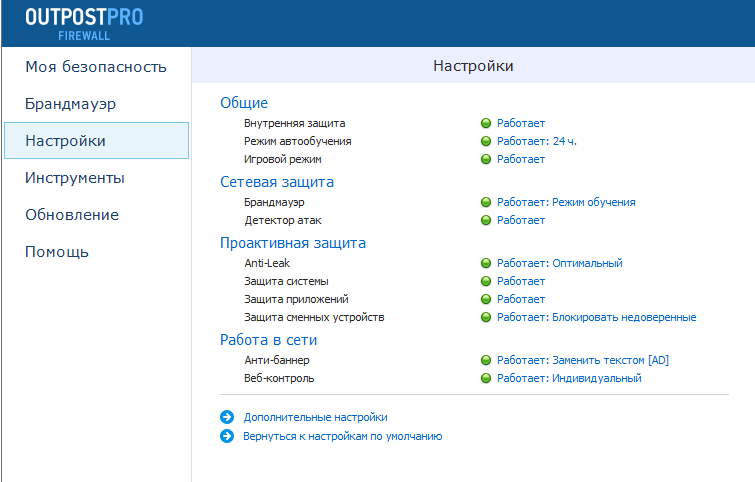
Во вкладке “брандмауэр” данного приложения можно задать, какие программы могут выходить в сеть, а какие – нет:



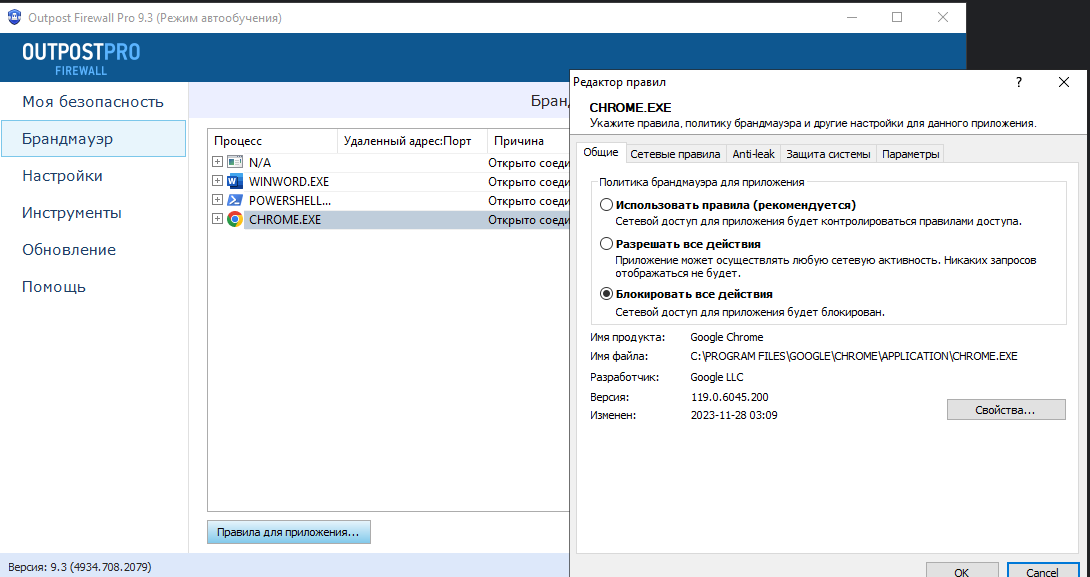
Также приложение позволяет получить доступ к различным инструментам, где можно мониторить порты, онлайн активность, историю отражённых атак и другие функции:



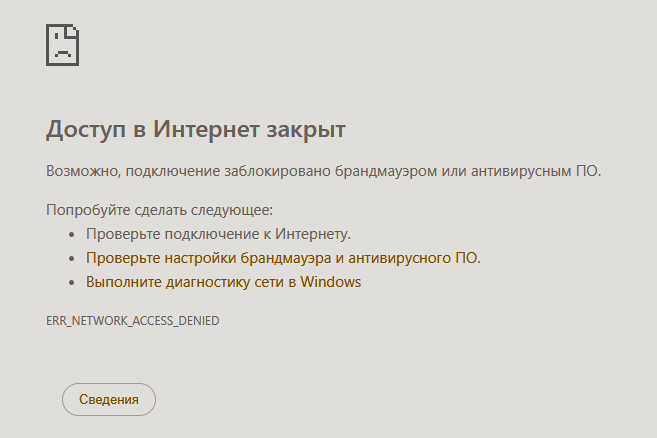
В настройках приложения можно включить или выключить отдельные части средства защиты:



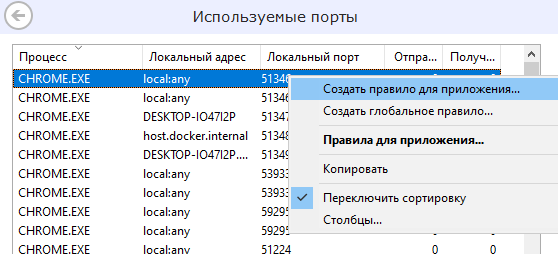
Протестируем работу приложения на практике. Откроем настройки брандмауэра и запретим интернет-браузеру доступ в интернет:



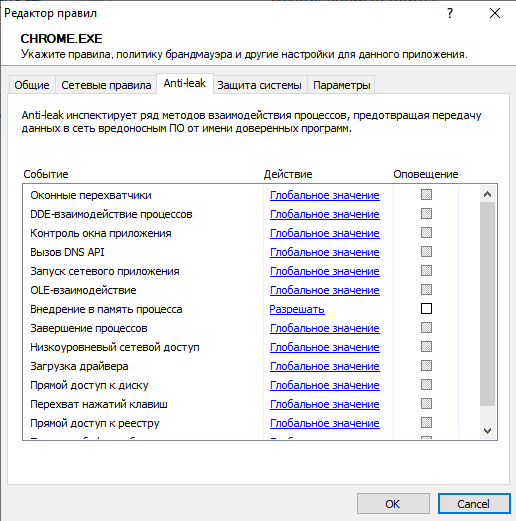
Открываем интернет-браузер, теперь доступ в интернет отсутствует.



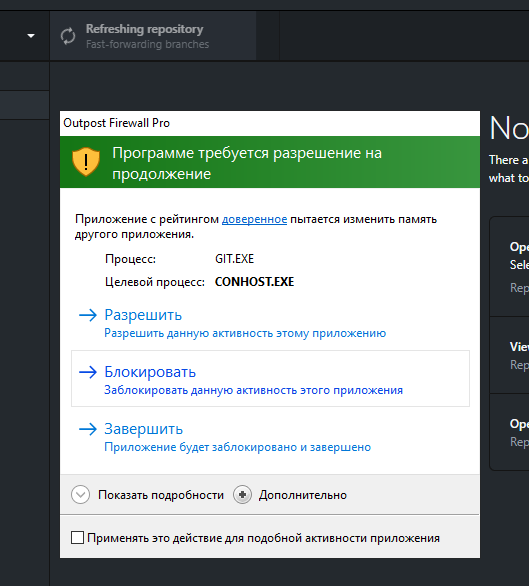
Откроем доступ заново, доступ сразу восстановлен и сетевые ресурсы загружаются. Воспользуемся средством мониторинга портов. Здесь можно просмотреть порт, используемый процессом и создать для порта глобальное правило либо, локальное правило (действует на всю систему или на отдельное приложение соответственно).



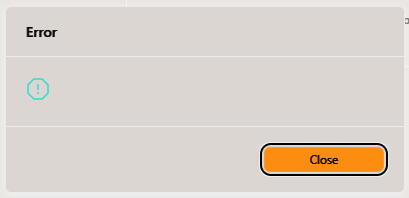
Также в приложении можно настраивать оповещения и правила при возникновении отдельных событий, связанных с программами (действия при загрузке драйвера, либо перехват нажатий клавиш, либо доступ к диску и тд)



Попробуем воспользоваться режимом повышенной защиты. В настройках приложения переключаемся с режима защиты “Оптимальный” на “Повышенный”. В таком режиме все соединения потребуют разрешения. Откроем GitHub Desktop и попробуем обновить репозиторий. По появлению всплывающего окна нажмём “Блокировать”.



Естественно, с заблокированным соединением обновить репозиторий не получилось и выскакивает окно ошибки.



**Вывод:** я обучился подбору программных средств защиты сетевого соединения компьютера в рабочем окружении операционной системы Windows и научился пользоваться выбранным средством.