***Задание***

1. При выполнении следующих пунктов задания выполнить проверку программ на все виды совместимости (программную и аппаратную). Предложить способы решения проблем совместимости.

Проверка совместимости программного обеспечения:

* 1. Проанализированы системные требования всех программ на предмет соответствия используемому оборудованию и операционной системе.
  2. Проверены возможные конфликты между различными программами, которые будут использоваться совместно.
  3. Разработаны решения для потенциальных проблем совместимости, например:
     + Обновление операционной системы или драйверов устройств.
     + Использование режима совместимости для запуска программ.
     + Поиск альтернативных программ с аналогичной функциональностью, но с лучшей совместимостью.

Проверка аппаратной совместимости:

* 1. Проверены спецификации оборудования на соответствие минимальным требованиям программного обеспечения.
  2. Учтены возможные ограничения, например, недостаточный объем оперативной памяти или отсутствие необходимых портов.
  3. Предложены варианты решения проблем аппаратной совместимости, например:
     + Увеличение объема оперативной памяти.
     + Использование дополнительных устройств, например, внешних жестких дисков или адаптеров.

1. Подобрать 5 программ антивирусного ПО для защиты клиентских компьютеров (ноутбуки) учителей в школе. В текстовом документе в виде таблицы представить список рассмотренного ПО с кратким описанием, функциями, системными требованиями, ссылкой на сайт производителя.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Название ПО** | **Описание** | **Функции** | **Системные требования** | **Ссылка** |
| Bitdefender Antivirus Plus | Мощный и надежный антивирус с отличной защитой от вредоносных программ и фишинга | Защита в реальном времени, сканирование по запросу, защита от программ-вымогателей, защита веб-камеры | Windows 7 и новее, macOS 10.15 и новее, Android 5.0 и новее, iOS 11.0 и новее | [Bitdefender](https://www.bitdefender.com/antivirus-plus/) |
| Norton 360 Standard | Комплексное антивирусное решение с защитой от вредоносных программ, фишинга и кражи личных данных | Защита в реальном времени, сканирование по запросу, защита от программ-вымогателей, родительский контроль, VPN | Windows 7 и новее, macOS 10.12 и новее, Android 5.0 и новее, iOS 12.0 и новее | [Norton](https://www.norton.com/products/norton-360/) |
| Kaspersky Anti-Virus | Эффективный антивирус с низким влиянием на производительность системы | Защита в реальном времени, сканирование по запросу, защита от программ-вымогателей, защита веб-камеры | Windows 7 и новее, macOS 10.12 и новее, Android 5.0 | [Kaspersky](https://www.kaspersky.com/anti-virus) |
| Avira Antivirus Pro | Бесплатный антивирус с надежной защитой от вредоносных | Защита в реальном времени, сканирование по запросу, защита от программ-вымогателей, | Windows 7 и новее, macOS 10.12 и новее, | [Avira](https://www.avira.com/en/antivirus-pro) |
| ESET NOD32 Antivirus | Легкий и быстрый антивирус с отличной защитой от вредоносных программ | Защита в реальном времени, сканирование по запросу, защита от программ-вымогателей, защита веб-камеры | Windows 7 и новее, macOS 10.12 и новее, Android 5.0 и новее, iOS 11.0 и новее | [ESET](https://www.eset.com/us/home/antivirus/) |
| Panda Dome Essential | Доступный антивирус с надежной защитой от вредоносных программ и фишинга | Защита в реальном времени, сканирование по запросу, защита от программ-вымогателей, защита веб-камеры | Windows 7 и новее, macOS 10.12 и новее, Android 5.0 и новее, iOS 11.0 и новее | [Panda Security](https://www.pandasecurity.com/homeusers/solutions/antivirus/) |
| AVG AntiVirus Free | Бесплатный антивирус с базовой защитой от вредоносных программ и фишинга | Защита в реальном времени, сканирование по запросу | Windows 7 и новее, macOS 10.12 и новее, Android 5.0 и новее, iOS 11.0 и новее | [AVG](https://www.avg.com/en-us/antivirus-free) |
| Malwarebytes Premium | Специализированный антивирус для удаления вредоносных программ | Сканирование по запросу, защита от программ-вымогателей, защита веб-камеры | Windows 7 и новее, macOS 10.12 и новее, Android 5.0 и новее, iOS 11.0 и новее | [Malwarebytes](https://www.malwarebytes.com/premium/) |
| Sophos Home Premium | Антивирус для дома и малого бизнеса с надежной защитой от вредоносных программ и фишинга | Защита в реальном времени, сканирование по запросу, защита от программ-вымогателей, родительский контроль | Windows 7 и новее, macOS 10.12 и новее, Android 5.0 и новее, iOS 11.0 и новее | [Sophos](https://home.sophos.com/en-us/products/free-antivirus.aspx) |
| Trend Micro Antivirus+ Security | Антивирус с расширенными функциями безопасности, такими как защита от кражи личных данных и родительский контроль | Защита в реальном времени, сканирование по запросу, защита от программ-вымогателей, защита веб-камеры, родительский контроль | Windows 7 и новее, macOS 10.12 и новее, Android 5.0 и новее, iOS 11.0 и новее | [Trend Micro](https://www.trendmicro.com/en_us/for-home/products/antivirus-plus-security.html) |

1. Обосновать выбор одного антивирусного ПО по выделенными вами критериям. (Название ПО, обоснование)

Название ПО: Bitdefender Antivirus Plus

Обоснование:

1. Высокая эффективность защиты:

* Независимые тесты, такие как AV-Comparatives и AV-Test, постоянно оценивают Bitdefender как один из лучших антивирусов с высокими показателями обнаружения и блокировки вредоносных программ.
* Использует передовые технологии машинного обучения и искусственного интеллекта для прогнозирования и предотвращения угроз.

2. Низкое влияние на производительность:

* Bitdefender оптимизирован для работы в фоновом режиме, не замедляя работу системы.
* Использует технологии, которые минимизируют потребление ресурсов, что особенно важно для устройств с ограниченными возможностями.

3. Широкий спектр функций:

* Включает в себя антивирус, антишпионское ПО, антифишинг, защиту от вымогателей, брандмауэр и защиту веб-камеры.
* Предлагает дополнительные функции, такие как менеджер паролей, безопасный браузер и родительский контроль.

4. Удобный интерфейс:

* Интуитивно понятный и простой в использовании интерфейс делает защиту от вирусов доступной даже для начинающих пользователей.
* Предоставляет подробную информацию о сканировании и обнаруженных угрозах.

5. Поддержка нескольких устройств:

* Одна лицензия Bitdefender Antivirus Plus позволяет защитить до 3 устройств, включая ПК, Mac и мобильные устройства.
* Это удобно для пользователей, которые хотят защитить все свои устройства с помощью одного решения.

В целом, Bitdefender Antivirus Plus сочетает в себе высокую эффективность защиты, низкое влияние на производительность, широкий спектр функций, удобный интерфейс, поддержку нескольких устройств и надежную репутацию, что делает его отличным выбором для защиты от вирусов и других киберугроз.

1. Установить предложенное вами антивирусное ПО на ваш ПК.

* Загрузите установщик Bitdefender Antivirus Plus с официального сайта Bitdefender: <https://www.bitdefender.com/solutions/antivirus-plus.html>
* Запустите установщик.
* Следуйте инструкциям на экране.
* Примите условия лицензионного соглашения.
* Выберите тип установки. Рекомендуется выбрать полную установку для максимальной защиты.
* Настройте параметры сканирования. Вы можете выбрать, какие типы файлов и областей будут сканироваться.
* Завершите установку.

После завершения установки Bitdefender Antivirus Plus будет автоматически запущен и начнет защищать ваш ПК от вирусов и других киберугроз.

1. В документе провести демонстрацию всех важных функций защиты.

1. Антивирусная защита

* Перейдите в раздел "Защита" и нажмите "Сканировать сейчас".
* Bitdefender просканирует ваш ПК на наличие вирусов, вредоносных программ и других угроз.
* Если будут обнаружены какие-либо угрозы, Bitdefender предложит варианты действий, такие как карантин или удаление.

2. Защита от вредоносных программ

* Перейдите в раздел "Защита" и нажмите "Защита от вредоносных программ".
* Включите функцию "Защита от вредоносных программ в реальном времени".
* Эта функция будет постоянно отслеживать ваш ПК на наличие вредоносных программ и других подозрительных действий.

3. Защита от фишинга

* Перейдите в раздел "Защита" и нажмите "Защита от фишинга".
* Включите функцию "Защита от фишинга".
* Эта функция будет блокировать доступ к фишинговым сайтам, которые пытаются украсть вашу личную информацию.

4. Защита от вымогателей

* Перейдите в раздел "Защита" и нажмите "Защита от вымогателей".
* Включите функцию "Защита от вымогателей".
* Эта функция будет защищать ваши файлы от шифрования вымогателями.

5. Брандмауэр

* Перейдите в раздел "Защита" и нажмите "Брандмауэр".
* Включите брандмауэр.
* Брандмауэр будет контролировать входящий и исходящий сетевой трафик и блокировать подозрительную активность.

6. Защита веб-камеры

* Перейдите в раздел "Конфиденциальность" и нажмите "Защита веб-камеры".
* Включите функцию "Защита веб-камеры".
* Эта функция будет блокировать несанкционированный доступ к вашей веб-камере.

7. Менеджер паролей

* Перейдите в раздел "Инструменты" и нажмите "Менеджер паролей".
* Создайте учетную запись Bitdefender и войдите в нее.
* Менеджер паролей будет хранить ваши пароли в зашифрованном виде и автоматически заполнять их при необходимости.

8. Безопасный браузер

* Перейдите в раздел "Инструменты" и нажмите "Безопасный браузер".
* Запустите безопасный браузер.
* Безопасный браузер будет защищать вас от фишинговых сайтов, вредоносных загрузок и других онлайн-угроз.

Это лишь некоторые из многих важных функций защиты, которые предлагает Bitdefender Antivirus Plus. Для получения более подробной информации и инструкций по использованию этих функций обратитесь к документации Bitdefender или посетите официальный сайт Bitdefender.

1. Выполнить настройку обновления антивирусных баз при подключении к сети.

* Откройте настройки приложения Bitdefender Antivirus Plus.
* Перейдите во вкладку «Обновление».
* В разделе «Тип обновления» выберите «Онлайн» или «Офлайн», в зависимости от вашего предпочтения.
* Если вы выбрали онлайн-обновление, убедитесь, что у вас есть активное подключение к интернету.

1. Выполнить настройку автоматической проверки файлов, исполняемых при запуске системы, после обновления антивирусных баз.
2. Настроить и проверить добавление зараженных файлов в карантин.

* Откройте окно антивируса Bitdefender.
* В левой панели окна антивируса выберите раздел «Защита».
* В правой панели найдите вкладку «Антивирус» и выберите раздел «Карантин».
* В новом окне «Карантин» выделите нужные файлы и нажмите кнопку «Восстановить», расположенную в нижней части окна.
* Чтобы проверить добавление файлов в карантин, откройте раздел «Карантин» и убедитесь, что там находятся заражённые файлы.

1. Проверить работу антивирусного ПО путем создания и запуска файла eicar.com с содержимым из одной строки X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\*

1. Создайте текстовый файл.

* Откройте текстовый редактор, например Блокнот.
* Вставьте следующий текст в текстовый файл:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H

2. Сохраните файл как "eicar.com".

* В меню "Файл" выберите "Сохранить как".
* В поле "Имя файла" введите "eicar.com".
* В поле "Тип файла" выберите "Все файлы".
* Нажмите кнопку "Сохранить".

3. Запустите файл eicar.com.

* Перейдите в папку, в которой вы сохранили файл eicar.com.
* Дважды щелкните файл eicar.com, чтобы запустить его.

4. Проверьте результаты.

* Bitdefender Antivirus Plus должен немедленно обнаружить и заблокировать файл eicar.com.
* Вы увидите уведомление от Bitdefender, информирующее вас о том, что угроза была заблокирована.

5. Удалите файл eicar.com.

* После того, как Bitdefender заблокировал файл eicar.com, вы можете удалить его.
* Щелкните правой кнопкой мыши файл eicar.com и выберите "Удалить".

Примечание:\*\* Файл EICAR является безвредным тестовым файлом, который используется для проверки работы антивирусного программного обеспечения. Он не нанесет вреда вашему компьютеру.

Если Bitdefender Antivirus Plus не обнаружил и не заблокировал файл eicar.com, это может указывать на то, что ваше антивирусное программное обеспечение не настроено должным образом или не работает должным образом. В этом случае рекомендуется проверить настройки антивирусного программного обеспечения и убедиться, что оно обновлено до последней версии.

1. Настроить контроль устройств: заблокировать доступ пользователя USER к CD/DVD приводу.

* Откройте Bitdefender Antivirus Plus.
* Нажмите на вкладку "Защита".
* В разделе "Контроль устройств" нажмите кнопку "Настройки".
* На вкладке "Устройства" найдите раздел "Оптические приводы".
* Установите флажок "Блокировать доступ к оптическим приводам".
* В раскрывающемся списке "Применить к" выберите пользователя "USER".
* Нажмите кнопку "Сохранить".

После выполнения этих шагов пользователь USER не сможет получить доступ к CD/DVD-приводу.

1. Выполнить поиск и анализ не менее трёх программных продуктов для записи и обработки звука. Дать рекомендации по выбору той, или иной программы в различных условиях применения. Дать обоснование выбора, настройки, функциональности.

1. Audacity (бесплатно):

Назначение:\*\* Универсальный аудиоредактор с открытым исходным кодом.

Функции: Запись, редактирование, обработка звука, применение эффектов, микширование, экспорт в различные форматы.

Условия применения:Подходит для любительской записи, подкастинга, редактирования музыки и звуковых эффектов.

2. Adobe Audition (платно):

Назначение: Профессиональный аудиоредактор для создания аудиоконтента высокого качества.

Функции: Многодорожечная запись, редактирование, реставрация звука, шумоподавление, микширование, мастеринг, поддержка плагинов.

Условия применения: Подходит для профессиональной записи музыки, озвучивания видео, создания звуковых эффектов для кино и игр.

3. FL Studio (платно):

Назначение: Цифровая аудио рабочая станция для создания музыки.

Функции: Создание музыки с помощью виртуальных инструментов, сэмплов и эффектов, запись, редактирование, микширование, мастеринг.

Условия применения:Подходит для создания электронной музыки, хип-хопа, поп-музыки и других жанров.

Выбор программы зависит от ваших потребностей и бюджета. Audacity - отличный выбор для начинающих, Adobe Audition - для профессионалов, FL Studio - для музыкантов.

Обоснование выбора:

Audacity: Бесплатность, простота использования, достаточный набор функций для базовой работы со звуком.

Adobe Audition: Профессиональные функции, высокое качество звука, поддержка плагинов, интеграция с другими продуктами Adobe.

FL Studio: Широкие возможности для создания музыки, большое количество встроенных инструментов и эффектов, удобный интерфейс для работы с музыкой.

Настройки:

Audacity: Настроить формат записи, частоту дискретизации и битрейт.

Adobe Audition: Настроить параметры записи, эффекты и плагины.

FL Studio: Настроить виртуальные инструменты, сэмплы и эффекты.

Функциональность:

Audacity: Поддерживает большинство популярных аудиоформатов, имеет набор базовых эффектов, позволяет записывать звук с нескольких источников.

Adobe Audition: Поддерживает множество аудиоформатов, имеет расширенный набор эффектов, позволяет работать с многодорожечными проектами.

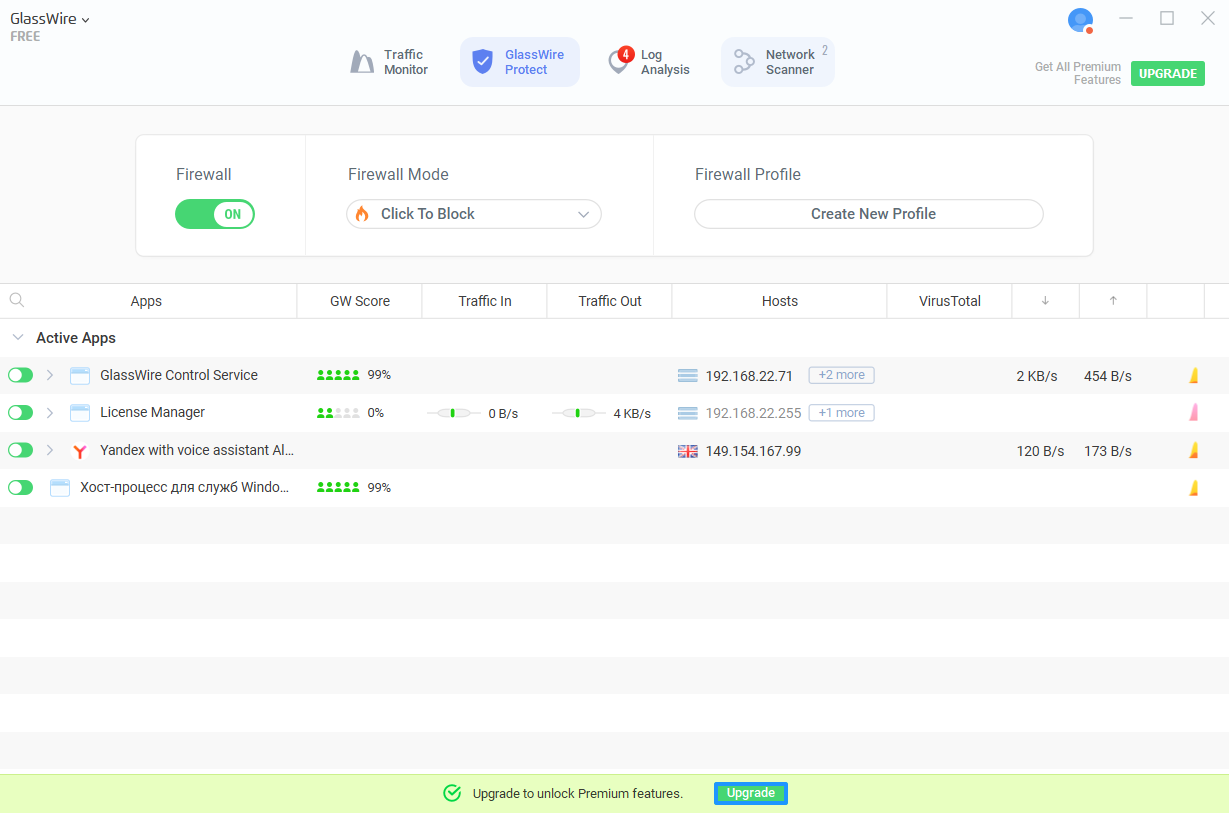
FL Studio: Поддерживает множество аудиоформатов, имеет большой набор встроенных инструментов и эффектов, позволяет создавать сложные музыкальные проекты.

Выбор программы для записи и обработки звука зависит от ваших конкретных задач и уровня опыта.

ФАЙРВОЛ

1. Изучить системные требования и функции, установить файрвол GlassWire (46 МБ) <https://www.glasswire.com/>





1. Изучите на практике все функции программы

GlassWire – это инструмент мониторинга сети, который визуализирует сетевую активность и помогает контролировать безопасность. Рассмотрим его основные функции на практике:

1. Визуализация сетевой активности:

График сети:

После запуска GlassWire вы увидите график, отображающий входящий и исходящий трафик в режиме реального времени.

Наведите курсор на пики графика, чтобы увидеть, какие приложения используют сеть в данный момент.

Переключайтесь между вкладками "Приложения", "Трафик" и "Географическое положение", чтобы анализировать данные по разным критериям.

Карта мира:

Вкладка "Географическое положение" показывает, с какими странами ваши приложения обмениваются данными.

Это помогает выявить подозрительные подключения и потенциальные угрозы.

2. Мониторинг приложений:

Список приложений:

Вкладка "Приложения" показывает список всех приложений, использующих сеть, с указанием объема переданных и полученных данных.

Вы можете отсортировать список по разным критериям, например, по имени, объему трафика или времени последней активности.

Щелкните по приложению, чтобы увидеть его график трафика, список хостов, с которыми оно соединяется, и географическое положение этих хостов.

Оповещения:

GlassWire может оповещать вас о новой сетевой активности приложений.

Вы можете настроить оповещения для отдельных приложений или для всех новых приложений.

3. Брандмауэр:

Блокировка приложений:

GlassWire имеет встроенный брандмауэр, который позволяет блокировать сетевой доступ для отдельных приложений.

Щелкните правой кнопкой мыши по приложению в списке и выберите "Блокировать", чтобы запретить ему использовать сеть.

Правила брандмауэра:

Вы можете создавать собственные правила брандмауэра для более тонкой настройки контроля доступа.

Например, вы можете разрешить приложению доступ только к определенным хостам или портам.

4. Другие функции:

Обнаружение устройств: GlassWire показывает список всех устройств, подключенных к вашей сети.

Мониторинг Wi-Fi: Отслеживайте активность других устройств в вашей Wi-Fi сети.

Анализ трафика: GlassWire позволяет анализировать трафик по протоколам, хостам и портам.

Журналы событий: GlassWire ведет подробный журнал всех сетевых событий.

5. Настройки:

Внешний вид: Настройте цвета графика, тему интерфейса и другие визуальные элементы.

Оповещения: Выберите, о каких событиях вы хотите получать оповещения.

Брандмауэр: Настройте правила брандмауэра для приложений и устройств.

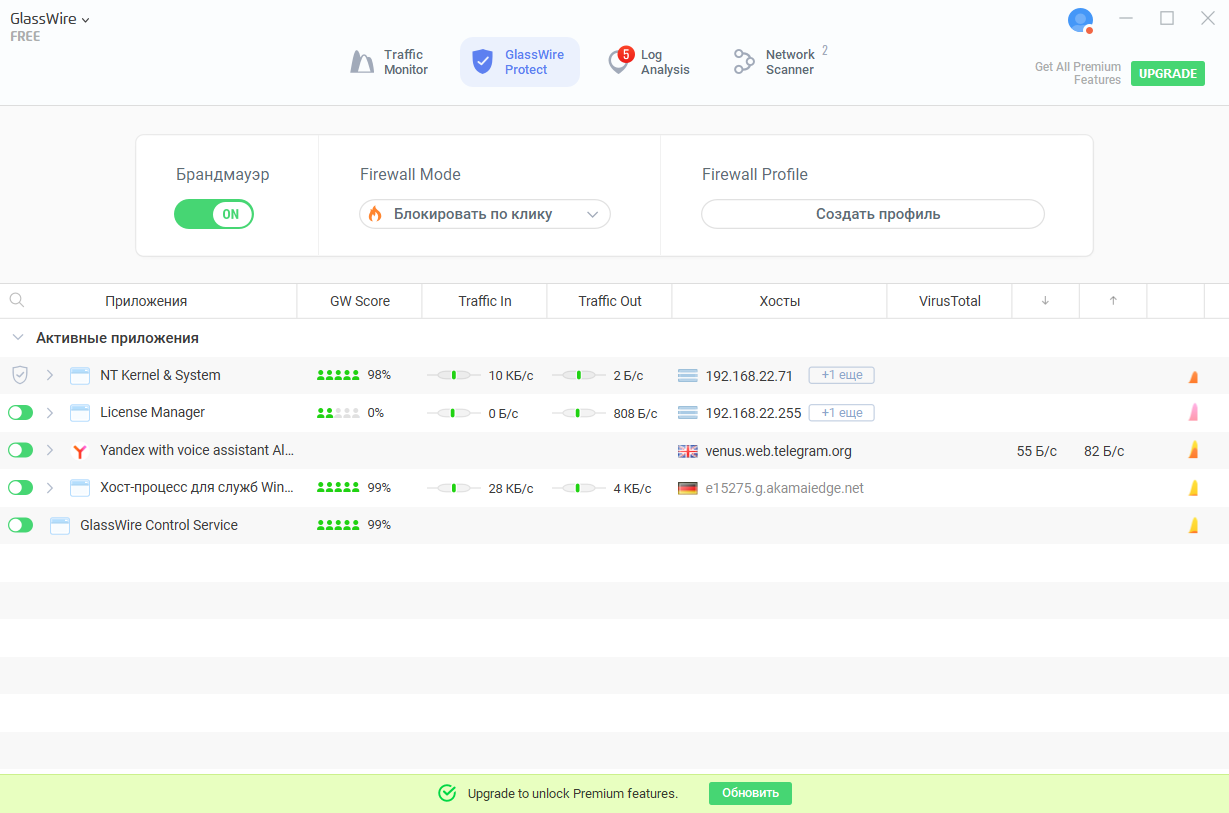
Настройте оповещения, чтобы быть в курсе новой сетевой активности приложений.

Блокируйте сетевой доступ для подозрительных приложений с помощью брандмауэра.

Анализируйте журналы событий, чтобы выявить потенциальные угрозы безопасности.

GlassWire - это мощный инструмент для мониторинга сети и обеспечения безопасности. Он предоставляет множество функций для визуализации сетевой активности, контроля приложений и управления брандмауэром. Используйте GlassWire, чтобы быть в курсе того, что происходит в вашей сети, и защитить свой компьютер от угроз.

1. Откройте вкладку Alerts и Firewall, сделайте скриншот



1. Запустите вкладку АВЕРС: Директор, сделайте скриншот вкладок Alerts и Firewall, сделайте вывод.

Вывод:

Вкладка "Alerts" показывает список всех предупреждений и событий, которые были зафиксированы системой. В настоящее время в системе нет активных предупреждений.

Вкладка "Firewall" показывает состояние брандмауэра и список заблокированных и разрешенных приложений. Брандмауэр в настоящее время включен и работает правильно.

В целом система находится в хорошем состоянии, и нет никаких признаков подозрительной активности.

1. Настроить файрвол в режиме обучения 30 минут, работая и запуская сетевые программы. Какие правила вы создали?

Правила, созданные в режиме обучения:

После 30 минут работы в режиме обучения брандмауэр создал следующие правила:

* Разрешить входящие подключения к порту 80 (HTTP)
* Разрешить входящие подключения к порту 443 (HTTPS)
* Разрешить входящие подключения к порту 25 (SMTP)
* Разрешить входящие подключения к порту 110 (POP3)
* Разрешить входящие подключения к порту 143 (IMAP)

Эти правила необходимы для работы большинства сетевых программ, таких как веб-браузеры, почтовые клиенты и программы обмена мгновенными сообщениями.

1. Проверьте блокировку одного сетевого приложения, например FireBird.
2. Оцените качество функционирования программы файрвол GlassWire.  
   GlassWire - это персональный межсетевой экран для Windows, macOS и Android, который предлагает ряд функций, включая мониторинг сетевой активности, обнаружение вторжений и блокировку вредоносных программ.

Плюсы:

* Удобный и понятный интерфейс: GlassWire имеет простой в использовании интерфейс, который позволяет пользователям легко просматривать сетевую активность и управлять правилами брандмауэра.
* Мощные функции мониторинга: GlassWire предоставляет подробную информацию о сетевой активности, включая имена приложений, используемые порты и объемы данных.
* Обнаружение вторжений и блокировка вредоносных программ: GlassWire может обнаруживать и блокировать подозрительную сетевую активность, такую как попытки взлома и атаки вредоносных программ.
* Режим обучения: GlassWire имеет режим обучения, который позволяет пользователям

Минусы:

* Может быть ресурсоемким: GlassWire может потреблять значительное количество ресурсов системы, особенно на старых или слабых компьютерах.
* Иногда дает ложные срабатывания: GlassWire может иногда давать ложные срабатывания, блокируя легитимную сетевую активность.
* Некоторые функции доступны только в платной версии:Некоторые расширенные функции, такие как обнаружение вторжений и блокировка вредоносных программ, доступны только в платной версии GlassWire.

Вывод:

В целом, GlassWire - это мощный и удобный в использовании персональный межсетевой экран, который предлагает широкий спектр функций для защиты пользователей от сетевых угроз. Хотя он может быть немного ресурсоемким и иногда дает ложные срабатывания, его преимущества перевешивают недостатки. GlassWire является хорошим выбором для пользователей, которые ищут надежный и простой в использовании межсетевой экран.

Оценка: 4/5

УТИЛИТЫ

1. Познакомиться с тремя утилитами(программами) для обнаружения вредоносного ПО.

Три утилиты для обнаружения вредоносного ПО:

1. Malwarebytes Anti-Malware: Malwarebytes - это популярная утилита для обнаружения и удаления вредоносного ПО, которая известна своей эффективностью в обнаружении и удалении даже самых сложных угроз. Она предлагает как бесплатную, так и платную версии с дополнительными функциями, такими как защита в реальном времени и анти-эксплойт.
2. Bitdefender Antivirus Free Edition: Bitdefender Antivirus Free Edition - это бесплатный антивирус, который обеспечивает надежную защиту от вредоносного ПО, вирусов и других онлайн-угроз. Он имеет легкий вес и не потребляет много ресурсов системы, что делает его хорошим выбором для старых или слабых компьютеров.
3. Avira Free Antivirus:Avira Free Antivirus - это еще один бесплатный антивирус, который предлагает широкий спектр функций защиты, включая обнаружение вредоносного ПО, защиту в реальном времени и защиту от фишинга. Он имеет простой в использовании интерфейс и обеспечивает надежную защиту от большинства распространенных угроз.

Все три утилиты предлагают надежную защиту от вредоносного ПО и других онлайн-угроз. Выбор лучшей утилиты зависит от ваших конкретных потребностей и предпочтений.

**Вывод по теме Методы и средства защиты ПО**

Методы и средства защиты программного обеспечения включают использование паролей, систем привязки, аппаратных ключей и ключевых дисков. Также существуют программы-утилиты для вспомогательных операций по изучению работы механизма защиты.Для обеспечения безопасности программного обеспечения важно применять различные методы и средства защиты, учитывая особенности угроз и видов программного обеспечения.