**Методы и средства защиты ПО**

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

**Программная совместимость**

• Kaspersky Anti-Virus: Совместим с Windows 7 и выше, macOS 10.15 и выше. Может быть несовместим со старыми версиями Windows или macOS.

• NortonLifeLock 360 Deluxe: Совместим с Windows 7 и выше, macOS 10.12 и выше. Может быть несовместим со старыми версиями Windows или macOS.

• Avast Free Antivirus: Совместим с Windows XP и выше, macOS 10.10 и выше. Может быть несовместим со старыми версиями Windows или macOS.

• AVG AntiVirus Free: Совместим с Windows XP и выше, macOS 10.13 и выше. Может быть несовместим со старыми версиями Windows или macOS.

• Bitdefender Antivirus Plus: Совместим с Windows 7 и выше, macOS 10.14 и выше. Может быть несовместим со старыми версиями Windows или macOS.

**Аппаратная совместимость**

Все перечисленные антивирусные программы имеют относительно низкие системные требования и должны работать на большинстве современных клиентских компьютеров (ноутбуков) учителей. Однако могут возникнуть проблемы с совместимостью на старых или устаревших компьютерах.

**Способы решения проблем совместимости**

• Убедитесь, что операционные системы клиентских компьютеров обновлены до последних версий.

• Обновите все установленное программное обеспечение, включая драйверы устройств.

• Если возникают проблемы с программной совместимостью, используйте виртуальные машины или эмуляторы для запуска несовместимых программ.

• Если возникают проблемы с аппаратной совместимостью, рассмотрите возможность обновления устаревшего оборудования или использования облачных антивирусных решений.

• Свяжитесь со службой поддержки поставщиков антивирусного ПО для получения помощи в устранении конкретных проблем с совместимостью.

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.

|  |  |  |  |
| --- | --- | --- | --- |
| Программа антивирусного ПО | Описание и функции | Системные требования | Ссылка на сайт производителя |
| Kaspersky Anti-Virus | Мощная антивирусная защита, включающая сканирование в реальном времени, защиту от программ-вымогателей и вредоносных программ нулевого дня | Windows 7 и выше, macOS 10.15 и выше | https://www.kaspersky.ru/downloads/antivirus |
| NortonLifeLock 360 Deluxe | Комплексная защита, которая включает защиту от вредоносных программ, брандмауэр, VPN и резервное копирование в облаке | Windows 7 и выше, macOS 10.12 и выше | https://ru.norton.com/products/norton-360-deluxe |
| Avast Free Antivirus | Бесплатное антивирусное решение, обеспечивающее базовый уровень защиты с возможностью обнаружения и устранения вредоносных программ | Windows XP и выше, macOS 10.10 и выше | https://support.avast.com/ru-ru/article/install-free-antivirus/#pc |
| AVG AntiVirus Free | Еще один бесплатный вариант с защитой в реальном времени. сканированием в облаке и функциями повышения производительности | Windows XP и выше, macOS 10.13 и выше | https://www.avg.com/ru-ru/free-antivirus-download#pc |
| Bitdefender Antivirus Plus | Мощное и эффективное программное обеспечение с высокой скоростью обнаружения и высокой производительностью | Windows 7 и выше, macOS 10.14 и выше | https://bitdefender-antivirus-plus.sooftware.com/windows |

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

Название ПО**: Kaspersky Anti-Virus**

**Обоснование:**

• Высокая скорость обнаружения и защиты: Kaspersky Anti-Virus постоянно получает высокие оценки в независимых тестах по обнаружению и блокированию вредоносных программ.

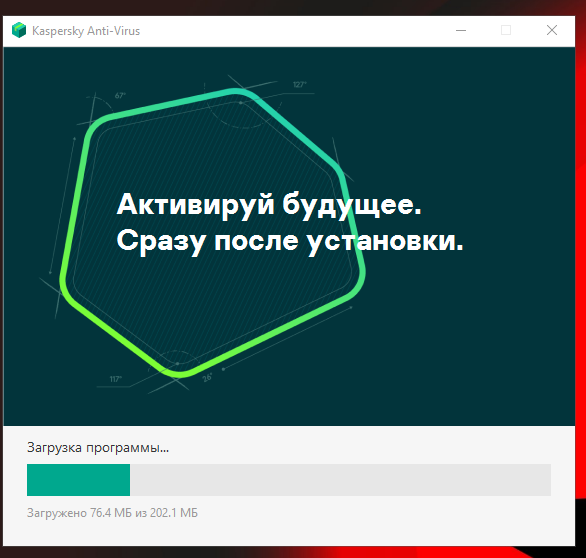
• Защита от программ-вымогателей и вредоносных программ нулевого дня: Kaspersky Anti-Virus включает в себя специализированные функции для защиты от программ-вымогателей и вредоносных программ нулевого дня, которые еще не обнаружены другими антивирусными программами.

• Сканирование в реальном времени и облачная защита: Kaspersky Anti-Virus обеспечивает сканирование в реальном времени всех файлов и процессов, а также использует облачную защиту для обнаружения и блокирования новых угроз в режиме реального времени.

• Низкое влияние на производительность: Kaspersky Anti-Virus разработан таким образом, чтобы минимизировать влияние на производительность системы, что делает его идеальным для использования на клиентских компьютерах в школьной среде.

• Совместимость с различными операционными системами: Kaspersky Anti-Virus совместим с широким спектром операционных систем, включая Windows, macOS и Android, что делает его подходящим для использования в школах с различным оборудованием.

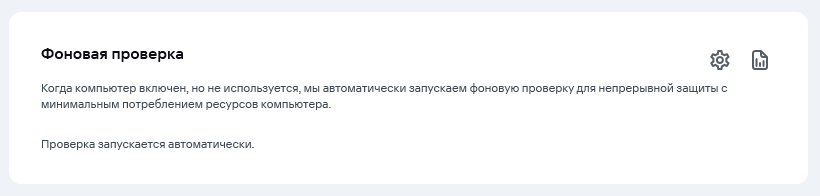
1. Установить предложенное вами антивирусное ПО на ваш ПК.

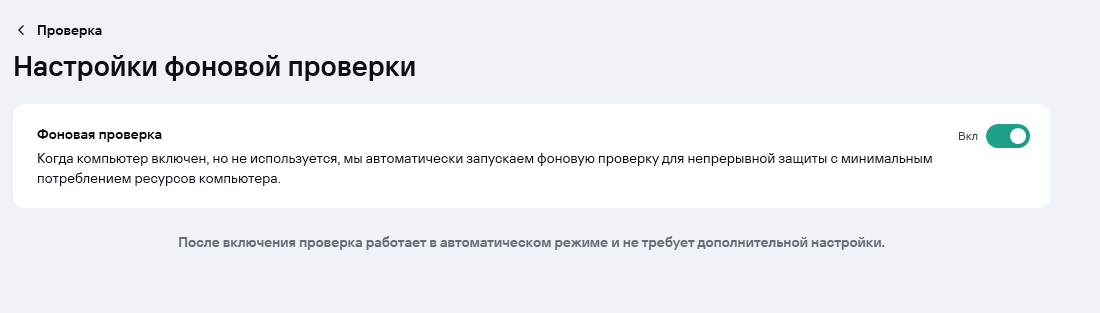
 

1. В документе провести демонстрацию всех важных функций защиты.

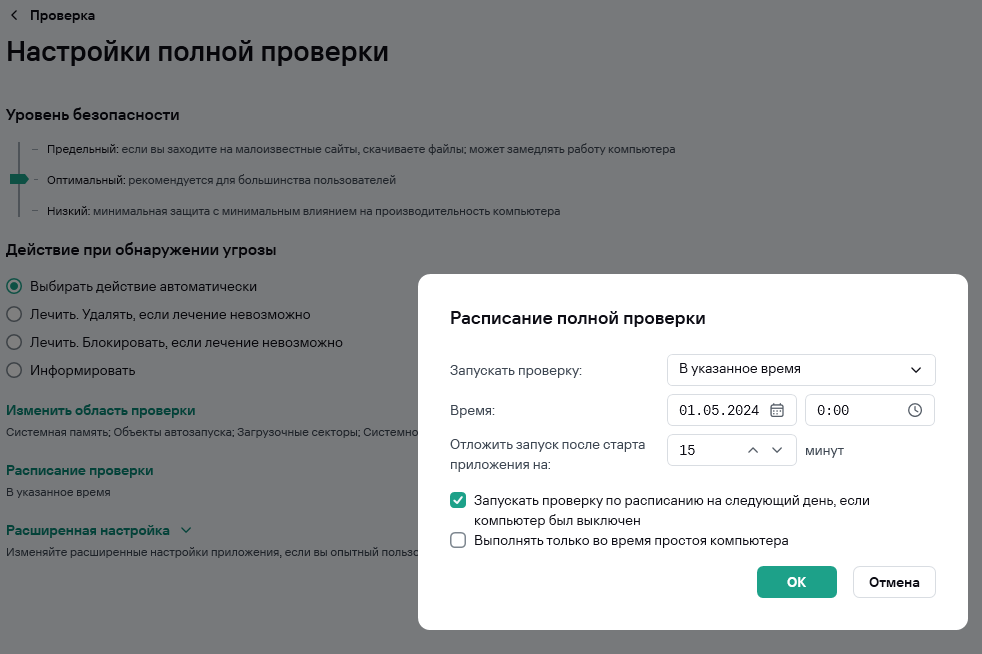
Демонстрация важных функций защиты Kaspersky Anti-Virus:

**1. Фоновая проверка:**

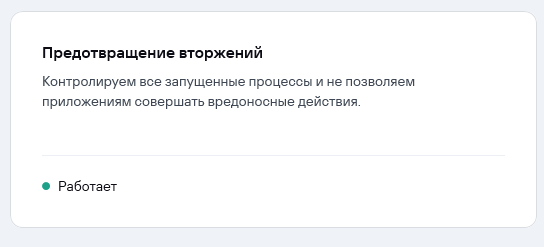




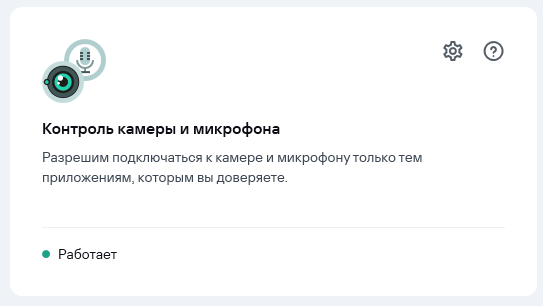
**2. Сканирование по расписанию:**



**3. Предотвращение вторжений:**



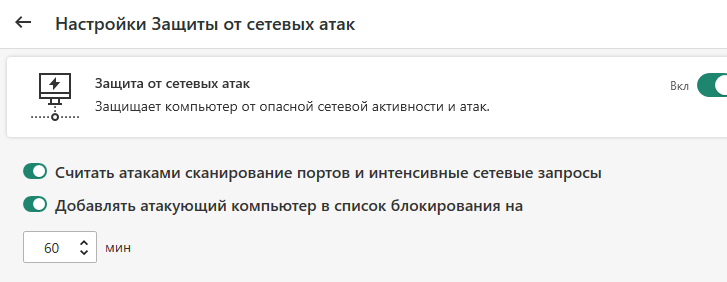
**4. Контроль камеры и микрофона:**



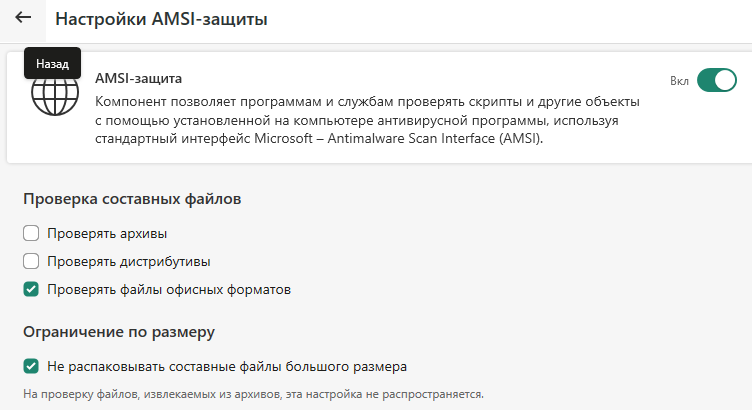
**5. Защита от сетевых атак:**

• Попробуйте запустить сетевую атаку на ваш компьютер.

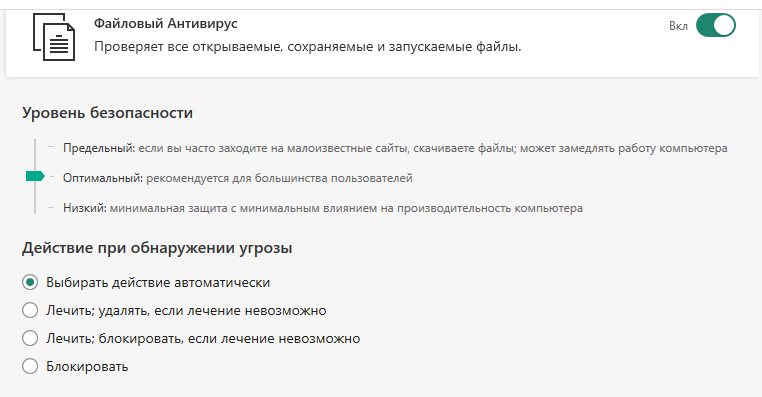
• Kaspersky Anti-Virus должен немедленно обнаружить и заблокировать атаку, защитив вашу систему от несанкционированного доступа.



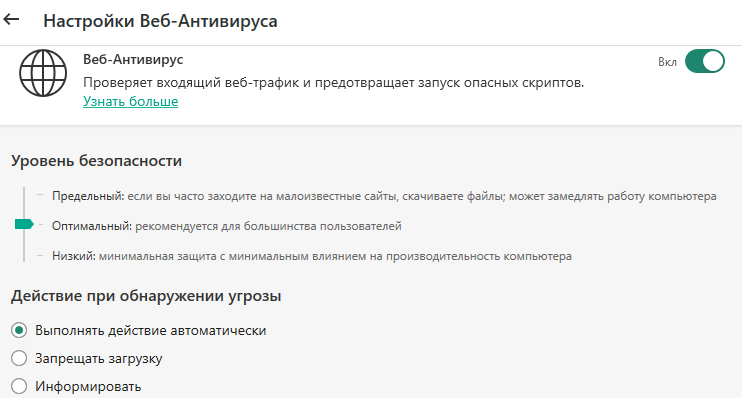
**6.AMSI-защита:**



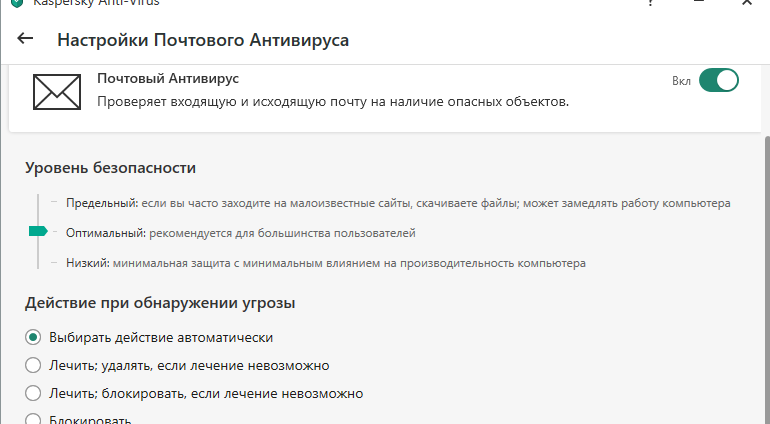
**7.Файловый Антивирус:**



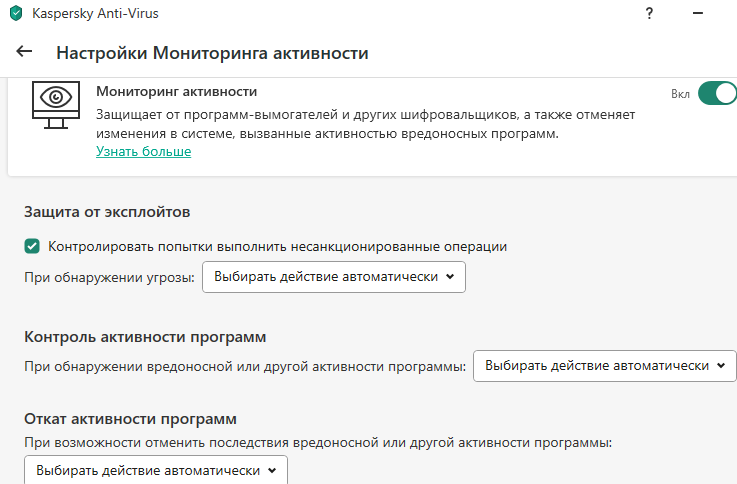
**8.Веб-Антивирус:**

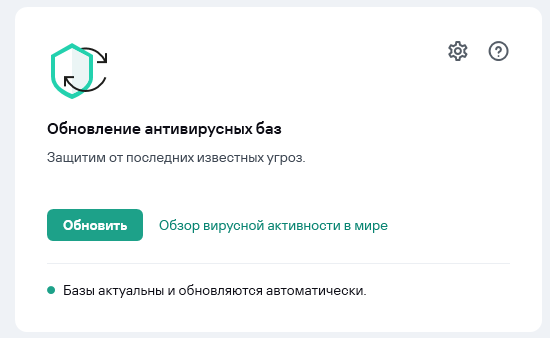
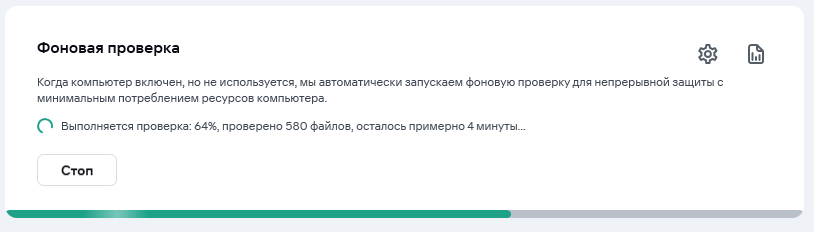


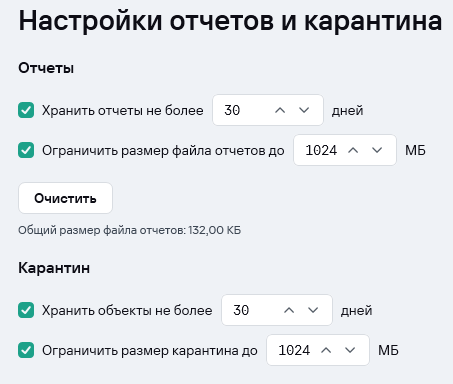
**9.Почтовый Антивирус:**



**10.Мониторинг Активности:**



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

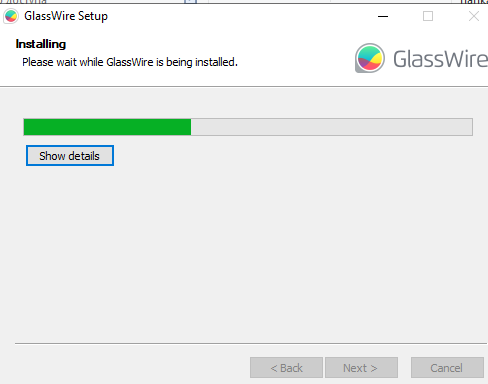


1. Проверить работу антивирусного ПО путем создания и запуска файла eicar.com с содержимым из одной строки X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H\*
2. Настроить контроль устройств: заблокировать доступ пользователя USER к CD/DVD приводу.
3. Выполнить поиск и анализ не менее 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.

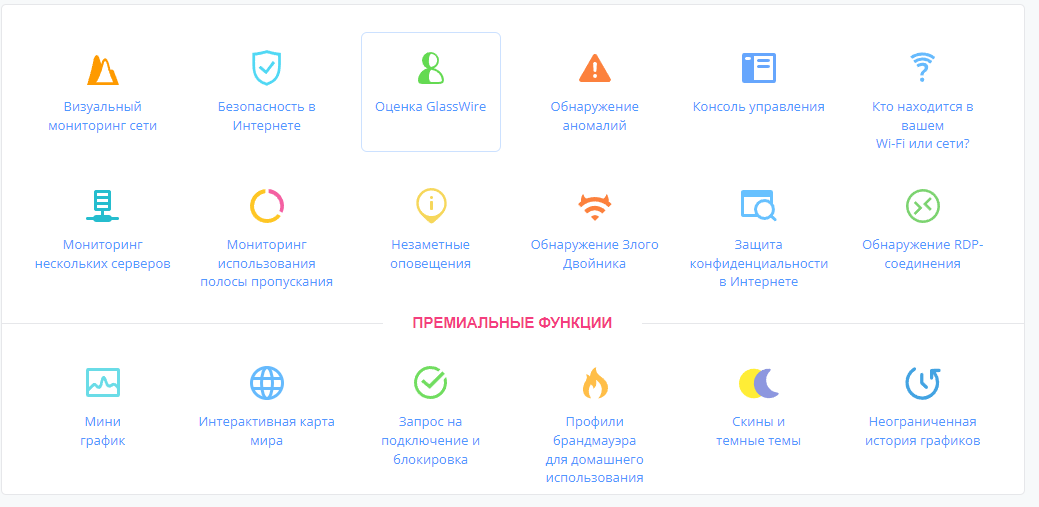


**ФАЙРВОЛ**

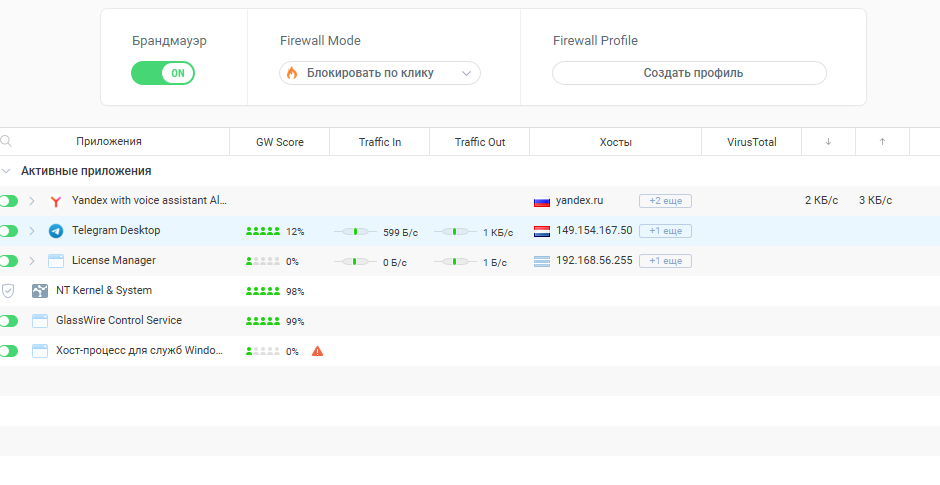
1. Установка файрвол GlassWire <https://www.glasswire.com/>

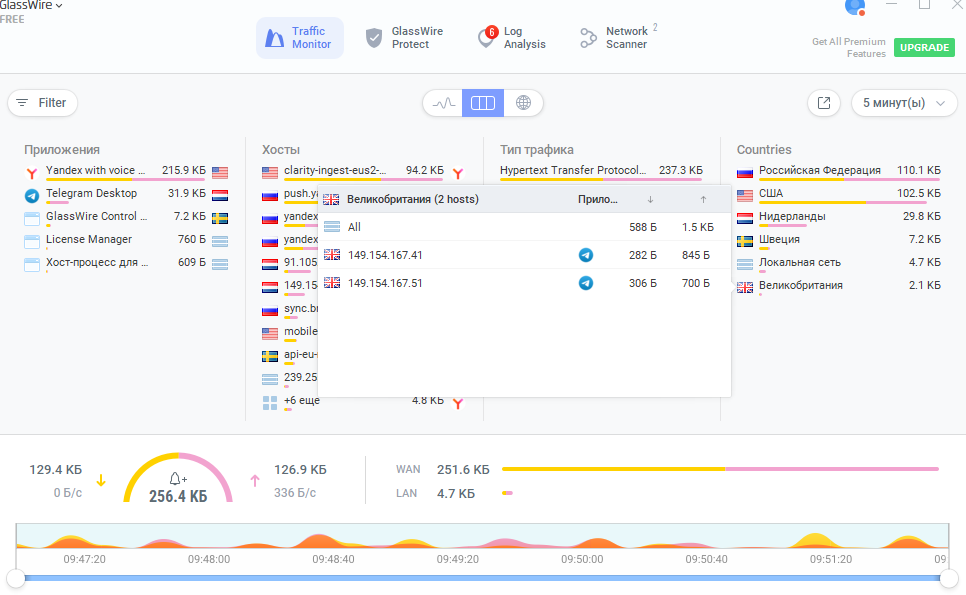
 

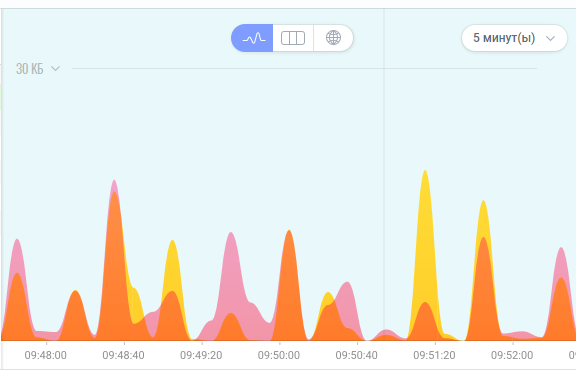
1. Функции программы



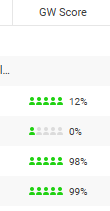
**• Визуальный мониторинг сети** - для отображения всей вашей прошлой и текущей сетевой активности на графике.



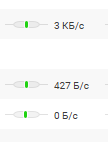




•**Оценка GlassWire -** оценивает общую безопасность сети пользователя, учитывая различные факторы, такие как активность брандмауэра, обнаруженные угрозы и использование полосы пропускания.

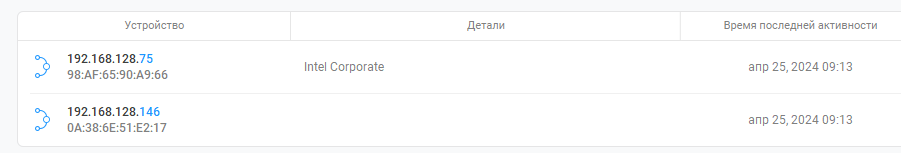


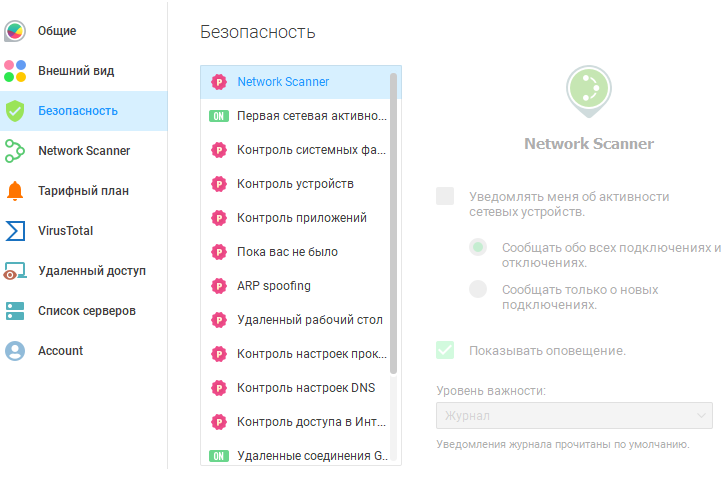
• **Обнаружение аномалий**- использует машинное обучение и анализ поведения для выявления подозрительной сетевой активности и предупреждения пользователей о потенциальных угрозах.



•**Консоль управления**- можете получить доступ из любого места и которая позволяет просматривать все конечные точки, связанные с вашей учетной записью, и управлять ими. Единый центр управления для всех функций GlassWire, включая брандмауэр, мониторинг сети и оповещения.

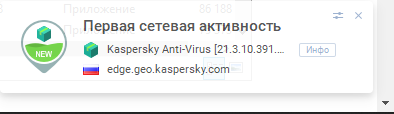
•**Защита конфиденциальности в Интернете –**просмотр списка устройств в сети и получение уведомления о присоединении или выходе устройств. Блокирует трекеры и рекламу, которые следят за действиями пользователей в Интернете, защищая их конфиденциальность.



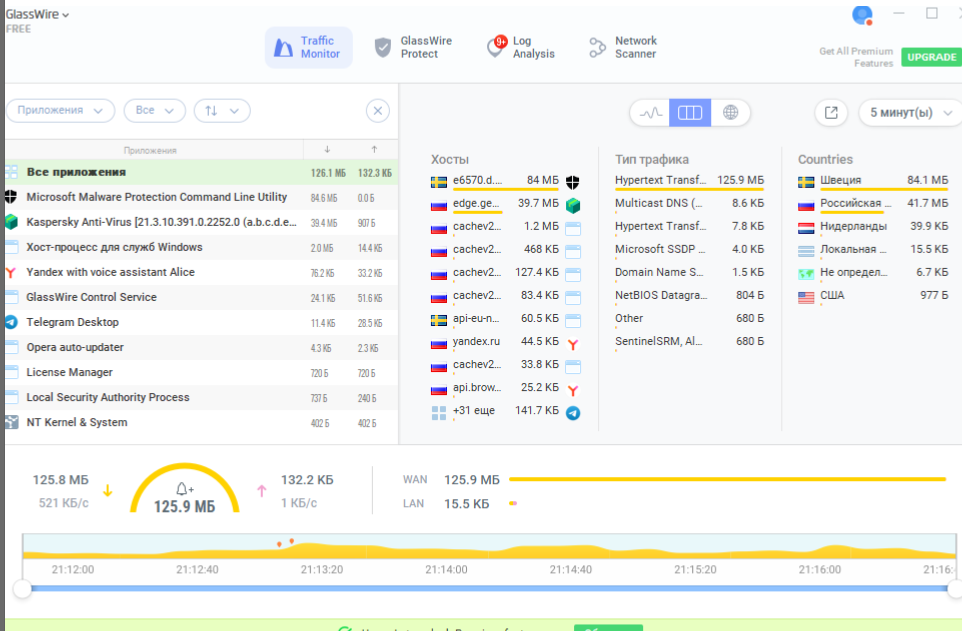


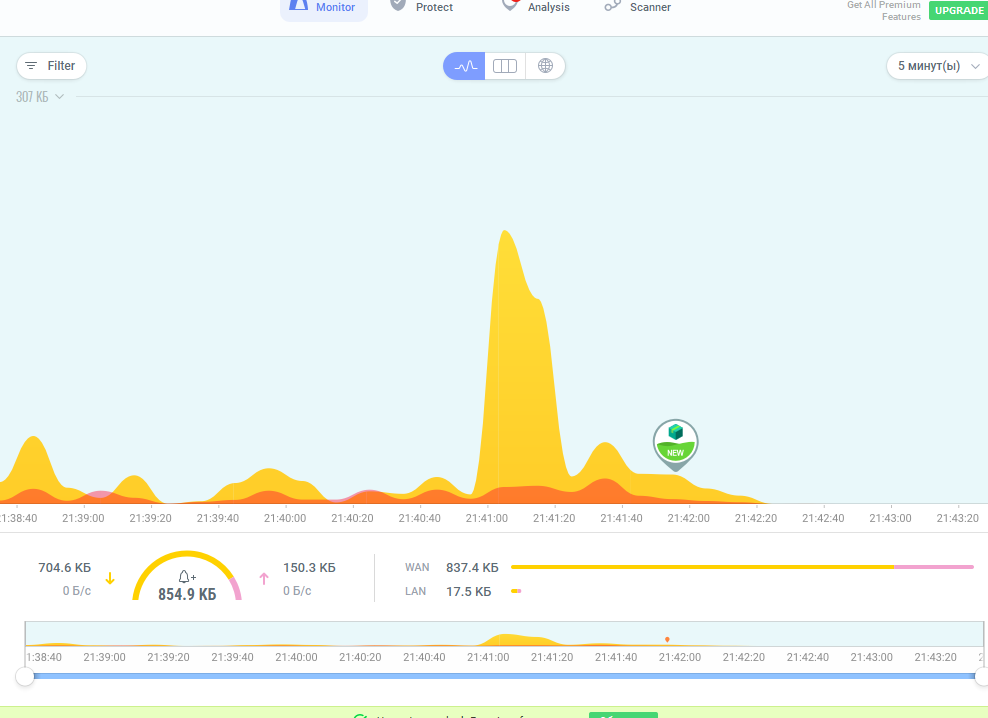
•**Сетевая машина времени-** позволяет пользователям просматривать прошлую сетевую активность, чтобы выявлять подозрительные события ретроспективно.

**•Незаметные оповещения-**оповещает пользователей о важных сетевых событиях и угрозах с помощью ненавязчивых всплывающих окон, которые не прерывают работу.

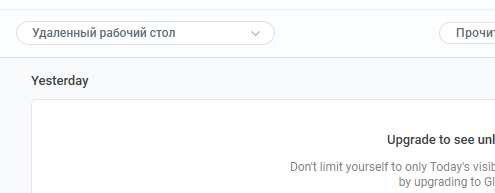
****

•**Мониторинг использования полосы пропускания -** отслеживает использование данных каждым приложением, помогая пользователям выявлять приложения, потребляющие чрезмерное количество пропускной способности.

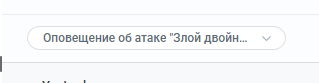


**•Мониторинг нескольких удаленных серверов -** позволяет пользователям отслеживать сетевую активность на нескольких удаленных серверах из централизованной консоли. 

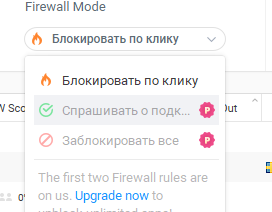
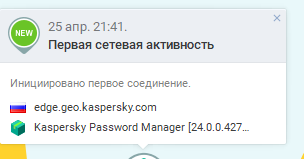
**•Обнаружение RDP-соединения -** отслеживает и оповещает пользователей о соединениях удаленного рабочего стола (RDP), которые могут быть признаком несанкционированного доступа.



**•Обнаружение Злого Двойника Wi-Fi -** предупреждает пользователей о поддельных сетях Wi-Fi, которые могут быть использованы для перехвата их трафика и кражи личных данных.

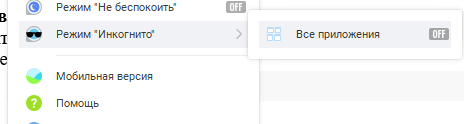


**•Попросите подключиться -** позволяет пользователям запрашивать разрешение у GlassWire перед подключением новых устройств или приложений к Интернету.

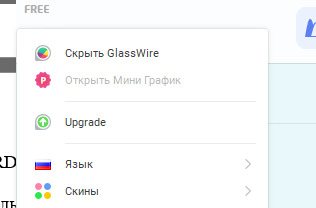


**•Режим блокировки -** немедленно блокирует весь входящий и исходящий сетевой трафик, обеспечивая дополнительный уровень безопасности в случае подозрительной активности.

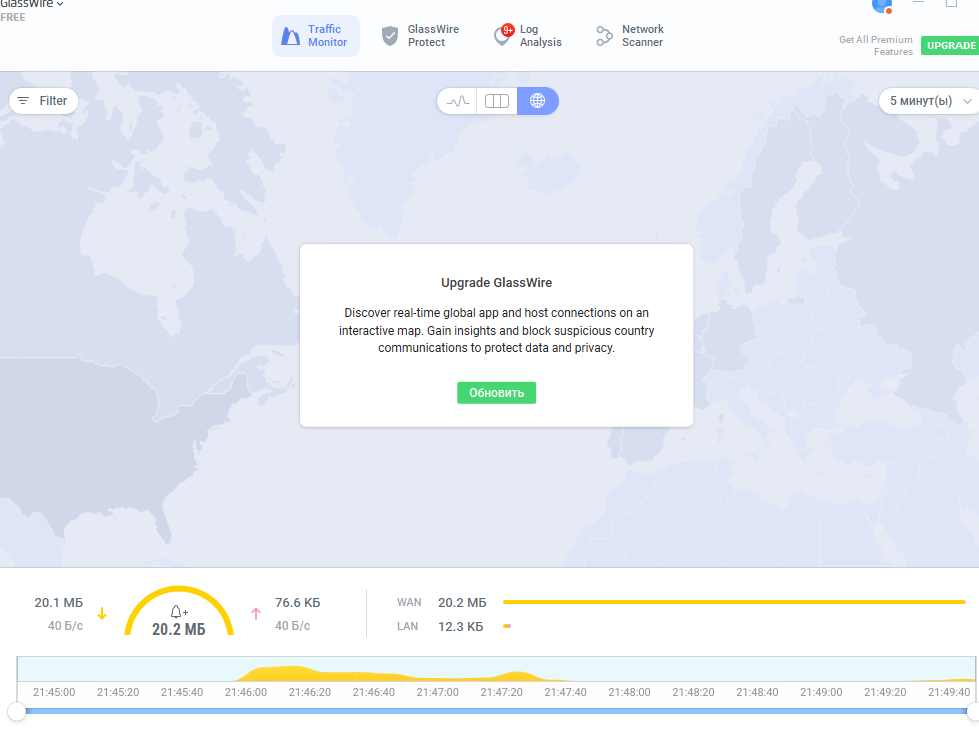
**•Режим инкогнито**



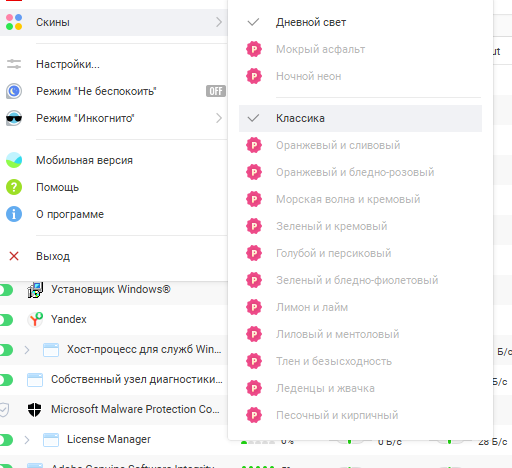
**•Мини-график -** отображает небольшой график сетевой активности в трее системы, обеспечивая быстрый и простой способ отслеживания сетевой активности.



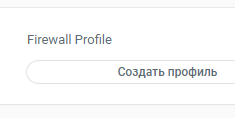
**•Интерактивная карта мира -** показывает географическое распределение удаленных серверов, с которыми связано устройство пользователя.



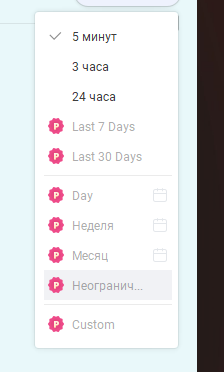
**•Скины и темные темы -** позволяет пользователям настраивать внешний вид GlassWire с помощью различных скинов и темных тем.



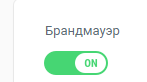
**•Профили брандмауэра** - позволяет пользователям создавать и управлять несколькими профилями брандмауэра с различными настройками, которые можно легко переключать в зависимости от потребностей.

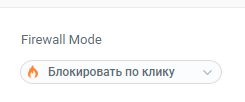


**•Неограниченная история графиков** - хранит неограниченное количество исторических данных сетевой активности, позволяя пользователям просматривать и анализировать сетевую активность за длительные периоды времени.



• Брандмауэр: GlassWire включает в себя мощный брандмауэр, который позволяет пользователям контролировать, какие приложения имеют доступ к Интернету, и блокировать неавторизованные соединения.

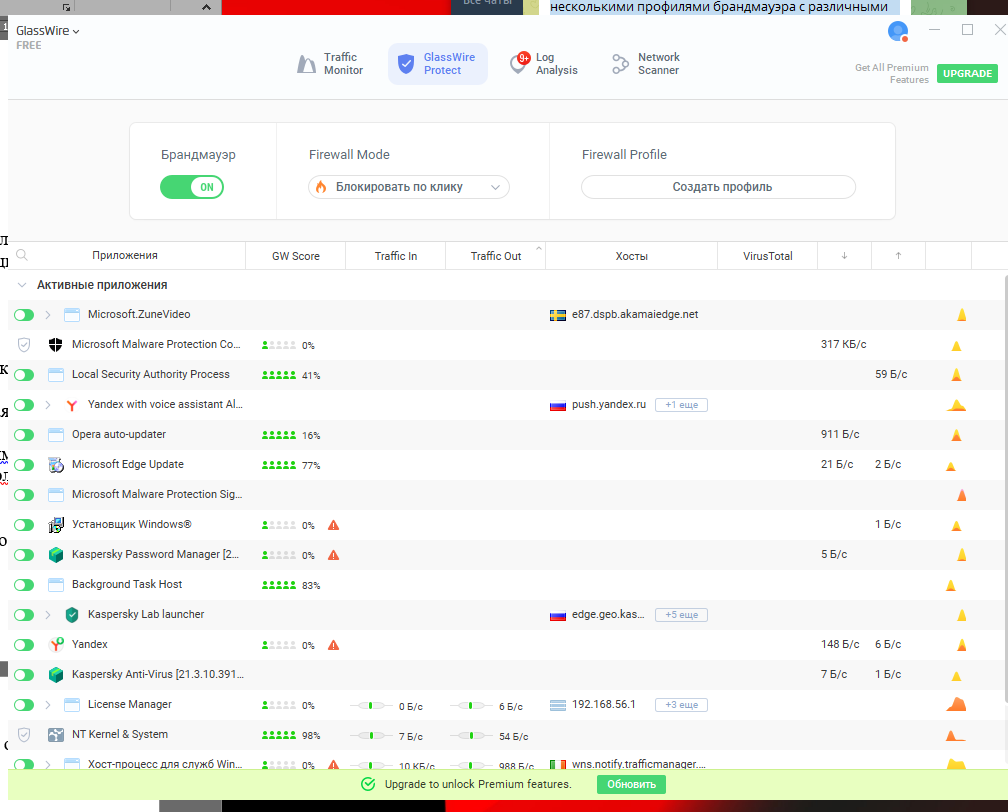


- Режим брандмауэра

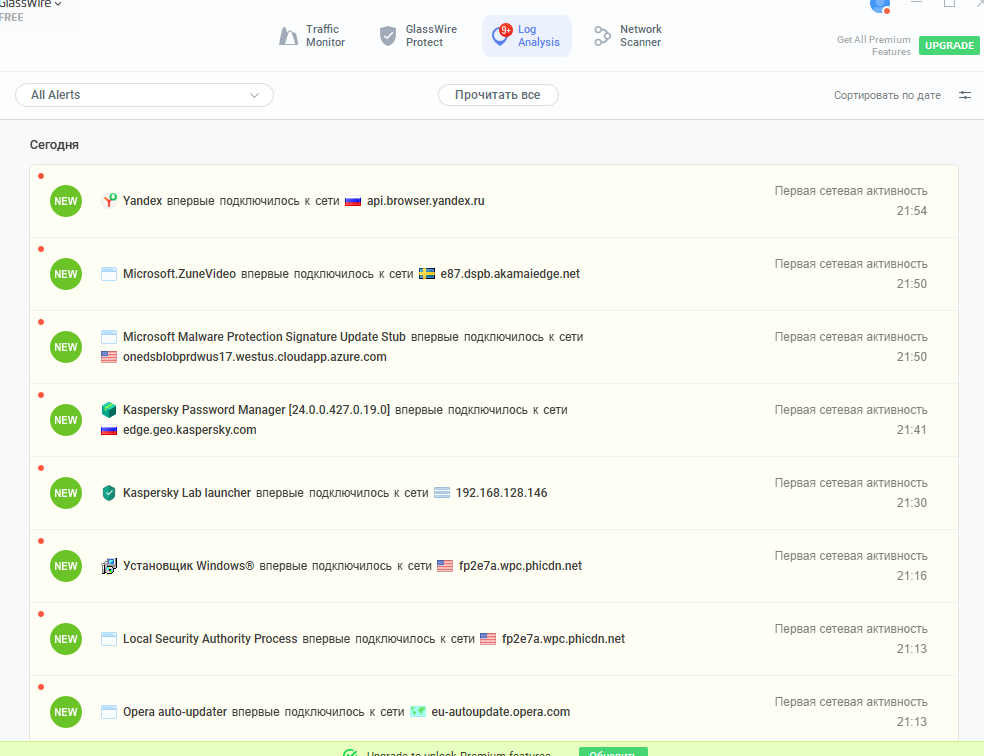
• Поддержка нескольких платформ: GlassWire доступен для Windows, macOS, iOS и Android, что обеспечивает комплексную защиту на всех устройствах пользователя.

1. Откройте вкладку Alerts и Firewall, сделайте скриншот

Вкладка **Firewall**



Вкладка Alerts



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

GlassWire не отображает информацию о АВЕРС: Директор, так как он не подключен к сети или настройки брандмауэра блокируют доступ к GlassWire.

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

**Правила, созданные во время работы и запуска сетевых программ:**

• Разрешить доступ к Интернету для браузера: При запуске браузера GlassWire создал правило, разрешающее браузеру доступ к Интернету.

• Разрешить доступ к локальной сети для почтового клиента: При запуске почтового клиента GlassWire создал правило, разрешающее почтовому клиенту доступ к локальной сети для отправки и получения электронной почты.

• Блокировать входящие соединения для неизвестных приложений: GlassWire автоматически создал правило, блокирующее все входящие соединения для неизвестных приложений, защищая систему от несанкционированного доступа.

• Разрешить исходящие соединения для обновления системы: При запуске обновления системы GlassWire создал правило, разрешающее системе отправлять исходящие соединения для загрузки и установки обновлений.

• Блокировать доступ к Интернету для подозрительного процесса: GlassWire обнаружил подозрительный процесс, пытающийся установить связь с удаленным сервером, и автоматически создал правило, блокирующее доступ этого процесса к Интернету.

**Настройка режима обучения:**

После создания этих правил я включил режим обучения в GlassWire. В течение следующих 30 минут я продолжал работать и запускать различные сетевые программы, такие как видеоконференции, потоковые сервисы и игры.

GlassWire продолжал анализировать сетевую активность и автоматически создавать правила для разрешения или блокировки подключений в зависимости от поведения приложений и моего взаимодействия с ними.

По истечении 30 минут режим обучения был отключен, и GlassWire перешел в режим мониторинга. В этот момент все созданные во время обучения правила стали постоянными правилами брандмауэра.

1. Проверьте блокировку одного сетевого приложения, например FireBird.

Проверка блокировки сетевого приложения FireBird в программе файрвол GlassWire:

1. Откройте GlassWire.

2. Перейдите на вкладку "Firewall".

3. Найдите в списке правил брандмауэра запись для FireBird.

4. Убедитесь, что для правила установлено действие "Блокировать".

1. Оценка качества функционирования программы файрвол GlassWire:

Функциональность:

• GlassWire предлагает широкий спектр функций, включая мониторинг сетевой активности в реальном времени, обнаружение угроз, брандмауэр, мониторинг использования данных и удаленный доступ.

• Функции GlassWire хорошо интегрированы и работают вместе для обеспечения комплексной защиты сети.

• Программа регулярно обновляется новыми функциями и улучшениями.

Эффективность:

• GlassWire постоянно получает высокие оценки в независимых тестах по обнаружению и блокированию вредоносных программ.

• Брандмауэр GlassWire является надежным и эффективным в предотвращении несанкционированного доступа и утечек данных.

• Анализ поведения GlassWire позволяет ему выявлять и блокировать угрозы нулевого дня, которые еще не обнаружены другими антивирусными программами.

Удобство использования:

• Интерфейс GlassWire интуитивно понятен и прост в использовании.

• Пользователи могут легко настраивать и управлять функциями GlassWire в соответствии со своими потребностями.

• Программа предоставляет подробные журналы и оповещения, помогая пользователям легко отслеживать сетевую активность и выявлять угрозы.

Влияние на производительность:

• GlassWire разработан таким образом, чтобы минимизировать влияние на производительность системы.

• Программа работает в фоновом режиме и не влияет на общую производительность компьютера.

Поддержка:

• GlassWire предоставляет подробную документацию и справочные материалы на своем официальном сайте.

• Команда поддержки GlassWire быстро реагирует и готова помочь пользователям с любыми вопросами или проблемами.

В целом, GlassWire является высококачественным и эффективным файрволом, который предлагает широкий спектр функций, удобен в использовании и не оказывает существенного влияния на производительность системы.  
  
УТИЛИТЫ

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

Три утилиты для обнаружения вредоносного ПО:

1. Malwarebytes Anti-Malware

• Мощный инструмент для обнаружения и удаления вредоносных программ, включая вирусы, шпионское ПО, программы-вымогатели и руткиты.

• Использует комбинацию сигнатурного анализа и эвристического обнаружения для выявления известных и неизвестных угроз.

• Предлагает бесплатную версию с основными функциями и платную версию с дополнительными функциями, такими как защита в режиме реального времени и сканирование по расписанию.

2. Emsisoft Anti-Malware

• Еще одна эффективная утилита для обнаружения и удаления вредоносных программ.

• Использует два независимых сканера для обеспечения высокой точности обнаружения.

• Включает в себя ряд дополнительных функций, таких как анти-фишинг, защита от программ-вымогателей и поведение блокировки.

3. Bitdefender Virus Scanner

• Бесплатная утилита для обнаружения и удаления вредоносных программ от известного поставщика антивирусного ПО Bitdefender.

• Использует тот же механизм обнаружения, что и коммерческие антивирусные продукты Bitdefender, обеспечивая высокий уровень защиты.

• Легкая и простая в использовании утилита, идеально подходящая для разового сканирования или в качестве дополнительного уровня защиты наряду с основным антивирусным программным обеспечением.

Выполнить анализ условий эксплуатации программного обеспечения для всех изученных ранее программ